



Web 应用程序报告

该报告包含有关 **web** 应用程序的重要安全信息。

安全报告

该报告由 IBM Security AppScan Standard 创建 9.0.3.5, 规则: 8804
扫描开始时间: 2021/12/8 15:45:59

目录

介绍

- 常规信息
- 登陆设置

摘要

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- 查询中的密码参数 ①
- 链接注入（便于跨站请求伪造） ①
- SSL 请求中的查询参数 ⑨⑩
- 发现可高速缓存的 SSL 页面 ①
- 未实施加密 ①
- 检测到隐藏目录 ②
- 缺少 HTTP Strict-Transport-Security 头 ①
- 缺少“Content-Security-Policy”头 ①
- 缺少“X-Content-Type-Options”头 ①
- 缺少“X-XSS-Protection”头 ①
- 过度许可的 CORS 访问测试 ①

修订建议

- 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

- 查看危险字符注入的可能解决方案
- 修改“Access-Control-Allow-Origin”头以仅获取允许的站点
- 发送敏感信息时，强制使用 HTTPS
- 实施 HTTP Strict-Transport-Security 策略
- 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去
- 将您的服务器配置为使用“Content-Security-Policy”头
- 将您的服务器配置为使用“X-Content-Type-Options”头
- 将您的服务器配置为使用“X-XSS-Protection”头
- 通过在响应中添加“Cache-Control: no-store”和“Pragma: no-cache”标题，可以阻止高速缓存 SSL 页面。

咨询

- 查询中的密码参数
- 链接注入（便于跨站请求伪造）
- SSL 请求中的查询参数
- 发现可高速缓存的 SSL 页面
- 未实施加密
- 检测到隐藏目录
- 缺少 HTTP Strict-Transport-Security 头
- 缺少“Content-Security-Policy”头
- 缺少“X-Content-Type-Options”头
- 缺少“X-XSS-Protection”头
- 过度许可的 CORS 访问测试

应用程序数据

- cookie
- JavaScript
- 参数
- 注释
- 已访问的 URL
- 失败的请求
- 已过滤的 URL

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题: 1
中等严重性问题: 1
低严重性问题: 99
报告中包含的严重性问题总数: 101
扫描中发现的严重性问题总数: 101

常规信息

扫描文件名称: 未命名
扫描开始时间: 2021/12/8 15:45:59
测试策略: Default

主机 pare-twp-stg.pingan.com.cn
端口 0
操作系统: Win32
Web 服务器: IIS
应用程序服务器: 任何

登陆设置

登陆方法: 记录的登录
并发登陆: 已启用
JavaScript 执行文件: 已禁用
会话中检测: 已启用
会话中模式:
跟踪或会话标识 cookie:
跟踪或会话标识参数:
登陆序列: https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=Login&Attribute=<attributes><Net>1</Net><Account>1906-

```
twzxcsl9</Account>  
<LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd>  
<LoginType>tw</LoginType><VCode></VCode><ValidateCode>  
</ValidateCode><RequestId></RequestId><Mobile></Mobile>  
</attributes>&Class=PingAnSSO&Mac=ca253f041c5de3a808358ac27db460d3&A  
ttribute->attributes=&Attribute->attributes->Net=1&Attribute-  
>attributes->Account=1906-twzxcsl9&Attribute->attributes-...
```

摘要

问题类型 11

TOC

问题类型	问题的数量
高 查询中的密码参数	1
中 链接注入（便于跨站请求伪造）	1
低 SSL 请求中的查询参数	90
低 发现可高速缓存的 SSL 页面	1
低 未实施加密	1
低 检测到隐藏目录	2
低 缺少 HTTP Strict-Transport-Security 头	1
低 缺少“Content-Security-Policy”头	1
低 缺少“X-Content-Type-Options”头	1
低 缺少“X-XSS-Protection”头	1
低 过度许可的 CORS 访问测试	1

有漏洞的 URL 1

TOC

URL	问题的数量
高 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.aspx	1
0	0
1	1

修订建议 10

TOC

修复任务	问题的数量
高 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	91
中 查看危险字符注入的可能解决方案	1

低	修改“Access-Control-Allow-Origin”头以仅获取允许的站点	1	
低	发送敏感信息时，强制使用 HTTPS	1	
低	实施 HTTP Strict-Transport-Security 策略	1	
低	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去	2	
低	将您的服务器配置为使用“Content-Security-Policy”头	1	
低	将您的服务器配置为使用“X-Content-Type-Options”头	1	
低	将您的服务器配置为使用“X-XSS-Protection”头	1	
低	通过在响应中添加“Cache-Control: no-store”和“Pragma: no-cache”标题，可以阻止高速缓存 SSL 页面。	1	

安全风险 7

TOC

风险	问题的数量		
高	可能会窃取查询字符串中发送的敏感数据，例如用户名和密码	1	
中	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	6	
中	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	1	
中	可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件	1	
低	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据	91	
低	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	6	
低	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点	2	

原因 7

TOC

原因	问题的数量		
高	查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）	1	
中	未对用户输入正确执行危险字符清理	1	
低	查询参数通过 SSL 进行了传递，并且可能包含敏感信息	90	
低	浏览器可能已将敏感信息高速缓存	1	
低	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	1	
低	Web 服务器或应用程序服务器是以不安全的方式配置的	2	
低	Web 应用程序编程或配置不安全	5	

WASC 威胁分类

TOC

威胁	问题的数量
信息泄露	100
内容电子欺骗	1

按问题类型分类的问题

高

查询中的密码参数 ①

TOC

问题 1 / 1

TOC

查询中的密码参数

严重性:

高

CVSS 分数: 8.5

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->LoginPwd (Parameter)

风险:

可能会窃取查询字符串中发送的敏感数据, 例如用户名和密码

原因:

查询字符串中传递了敏感输入字段 (例如用户名、密码和信用卡号)

固定值:

发送敏感信息时, 始终使用 **SSL** 和 **POST** (主体) 参数。

差异:

推理: AppScan 识别出查询字符串中接收到的密码参数

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8
```

```
{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

问题 1 / 1

TOC

链接注入（便于跨站请求伪造）

严重性: 中

CVSS 分数: 6.4

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Command (Parameter)

风险: 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

原因: 未对用户输入正确执行危险字符清理

固定值: [查看危险字符注入的可能解决方案](#)差异: 参数 从以下位置进行控制: `FuzzySearchArrearageList` 至:`%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2728.html%22%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/TWI/TWInterface/Service/Service.ashx?Command=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF2728.html%22%3E&
Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 75
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 08:02:44 GMT
```

Content-Type: text/plain; charset=utf-8

```
{"Result": "false", "data": "未找到命令"><IMG SRC="/WF_XSRF2728.html">"}
```

问题 1 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Command (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET
/TWI/TWInterface/Service/Service.ashx?Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CORGanCode%3E010103%3C/ORGanCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data": [ { "Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, { "Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, { "Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{ "Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, { "Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"} ], "TotalCount": 0 }
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":[{"Name":"本月报事工单完成率","Value":"0.00","Unit":"%"}, {"Name":"本月设备巡检完成率","Value":"0.00","Unit":"%"}, {"Name":"本月设备维保完成率","Value":"0.00","Unit":"%"}, {"Name":"本月分户查验完成率","Value":"0.00","Unit":"%"}, {"Name":"本月设备故障发生率","Value":"0.00","Unit":"%"}], "TotalCount":0}

```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Mac (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->UserCode (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMessageList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CCorpID%3E1906%3C/CorpID%3E%3CState%3E1%3C/
State%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%3C/attributes%3E&Class=On
lineMessage&Mac=7e68cec1012655d7ce99927bb529d069 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3193
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:50:11 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"MessageCode": "8B6CCBE7-F3DB-4FB9-B4B0-
430AC1A900F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/8
0:00:13", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "1"},
{"MessageCode": "55F0F2AE-8B2F-47D0-93CA-
D2D357BDB0F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】租客名称发生了变更!", "SendTime": "2021/12/8
0:00:11", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "2"},
{"MessageCode": "93256352-0347-42AC-A31A-
53710EFACCD9", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/7
0:00:22", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "3"},
{"MessageCode": "5AC8AB5B-B44D-4FCA-911A-
45F518776008", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】租客名称发生了变更!", "SendTime": "2021/12/7
0:00:12", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "4"},
{"MessageCode": "928E9CB7-61A8-42A7-B6C2-
C3B2ACBE04B5", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/6
0:00:21", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "5"},
{"MessageCode": "8F591E18-07E9-4029-B766-
25F04768AD1E", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】租客名称发生了变更!", "SendTime": "2021/12/6
0:00:18", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "6"},
{"MessageCode": "2AB651FB-0546-4323-A3FF-
0A73FA165CB7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/6
0:00:14", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "7"},
{"MessageCode": "5B99302F-3149-4474-9079-
D574921EB89D", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
```



```
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/5
0:00:15", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "8"},
{"MessageCode": "0955A045-BC61-4324-909A-
5560938465BD", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/5
0:00:10", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "9"},
{"MessageCode": "19A45360-BBAC-43FB-B579-
0A3D92D4C898", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/5
0:00:06", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "10"}}}
```

问题 5 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->Net (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3
E1906-
twzxc519%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CORGanCode%3E010103%3C/ORGanCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->Account (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}

```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->LoginPwd (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Class (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3
E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->CommID (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrgancode%3E010103%3C/Organcode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->CorpID (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMessageList&Attribute=%3Cattributes%3E%3CNet%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CCorpID%3E1906%3C/CorpID%3E%3CState%3E1%3C/
State%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%3C/attributes%3E&Class=On
lineMessage&Mac=7e68cec1012655d7ce99927bb529d069 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3193
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:50:11 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"MessageCode": "8B6CCBE7-F3DB-4FB9-B4B0-
430AC1A900F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/8
0:00:13", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "1"},
{"MessageCode": "55F0F2AE-8B2F-47D0-93CA-
D2D357BDB0F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】租客名称发生了变更!", "SendTime": "2021/12/8
0:00:11", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "2"},
{"MessageCode": "93256352-0347-42AC-A31A-
53710EFACCD9", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/7
0:00:22", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "3"},
{"MessageCode": "5AC8AB5B-B44D-4FCA-911A-
45F518776008", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】租客名称发生了变更!", "SendTime": "2021/12/7
0:00:12", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "4"},
{"MessageCode": "928E9CB7-61A8-42A7-B6C2-
C3B2ACBE04B5", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/6
0:00:21", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "5"},
{"MessageCode": "8F591E18-07E9-4029-B766-
25F04768AD1E", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】租客名称发生了变更!", "SendTime": "2021/12/6
0:00:18", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "6"},
{"MessageCode": "2AB651FB-0546-4323-A3FF-
0A73FA165CB7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/6
0:00:14", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "7"},
{"MessageCode": "5B99302F-3149-4474-9079-
D574921EB89D", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
```

```
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/5
0:00:15", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "8"},
{"MessageCode": "0955A045-BC61-4324-909A-
5560938465BD", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/5
0:00:10", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "9"},
{"MessageCode": "19A45360-BBAC-43FB-B579-
0A3D92D4C898", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/5
0:00:06", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "10"}}}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->Page (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMaterialSearch&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CWareHouseName%3EL9%E4%BB%93%E5%BA%93%3C/Wa
reHouseName%3E%3CMaterialName%3E%3C/MaterialName%3E%3CNum%3E%3C/Num%3E%3CPage%3E1%3C/Page%3E%3C/a
ttributes%3E&Class=SearchManage&Mac=1c0619679d02301e68ebaecbca5c5e4 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1044
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:52:51 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗
品", "Num": "10005075", "Specification": "商业施工人员出入证(A
证)", "Spell": "HC", "UnitName": "张", "ColorName": null, "Brand": null, "Quantity": 1400.00},
{"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005076", "Specification": "商业施工
人员出入证(B证)", "Spell": "HC", "UnitName": "张", "ColorName": null, "Brand": null, "Quantity": 1400.00},
{"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005100", "Specification": "拐
杖", "Spell": "HC", "UnitName": "个", "ColorName": null, "Brand": null, "Quantity": 1.00},
{"WarehouseName": "L9仓库", "MaterialTypeName": "劳保清洁用
品", "Num": "40005065", "Specification": "Soffell驱蚊
```



```
水", "Spell": "HC", "UnitName": "瓶", "ColorName": null, "Brand": null, "Quantity": 0.00},
{"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005043", "Specification": "IPAD防盗
支架", "Spell": "HC", "UnitName": "个", "ColorName": null, "Brand": null, "Quantity": 1.00}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->PageSize (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMessageList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CCorpID%3E1906%3C/CorpID%3E%3CState%3E1%3C/
State%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%3C/attributes%3E&Class=On
lineMessage&Mac=7e68cec1012655d7ce99927bb529d069 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3193
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:50:11 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"MessageCode": "8B6CCBE7-F3DB-4FB9-B4B0-
430AC1A900F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/8
0:00:13", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "1"},
{"MessageCode": "55F0F2AE-8B2F-47D0-93CA-
D2D357BDB0F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/8
0:00:11", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "2"},
{"MessageCode": "93256352-0347-42AC-A31A-
53710EFACCD9", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/7
0:00:22", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "3"},
{"MessageCode": "5AC8AB5B-B44D-4FCA-911A-
45F518776008", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/7
0:00:12", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "4"},
```

```
{
  "MessageCode": "928E9CB7-61A8-42A7-B6C2-C3B2ACBE04B5",
  "CutID": null,
  "UserCode": "001349",
  "UserName": "天问的测试账号",
  "DepName": "人事部",
  "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!",
  "SendTime": "2021/12/6 0:00:21",
  "SendMan": null,
  "SendManName": null,
  "SendManDepName": null,
  "RN": "5"
},
{
  "MessageCode": "8F591E18-07E9-4029-B766-25F04768AD1E",
  "CutID": null,
  "UserCode": "001349",
  "UserName": "天问的测试账号",
  "DepName": "人事部",
  "MsgTitle": "【租赁租客】租客名称发生了变更!",
  "SendTime": "2021/12/6 0:00:18",
  "SendMan": null,
  "SendManName": null,
  "SendManDepName": null,
  "RN": "6"
},
{
  "MessageCode": "2AB651FB-0546-4323-A3FF-0A73FA165CB7",
  "CutID": null,
  "UserCode": "001349",
  "UserName": "天问的测试账号",
  "DepName": "人事部",
  "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!",
  "SendTime": "2021/12/6 0:00:14",
  "SendMan": null,
  "SendManName": null,
  "SendManDepName": null,
  "RN": "7"
},
{
  "MessageCode": "5B99302F-3149-4474-9079-D574921EB89D",
  "CutID": null,
  "UserCode": "001349",
  "UserName": "天问的测试账号",
  "DepName": "人事部",
  "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!",
  "SendTime": "2021/12/5 0:00:15",
  "SendMan": null,
  "SendManName": null,
  "SendManDepName": null,
  "RN": "8"
},
{
  "MessageCode": "0955A045-BC61-4324-909A-5560938465BD",
  "CutID": null,
  "UserCode": "001349",
  "UserName": "天问的测试账号",
  "DepName": "人事部",
  "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!",
  "SendTime": "2021/12/5 0:00:10",
  "SendMan": null,
  "SendManName": null,
  "SendManDepName": null,
  "RN": "9"
},
{
  "MessageCode": "19A45360-BBAC-43FB-B579-0A3D92D4C898",
  "CutID": null,
  "UserCode": "001349",
  "UserName": "天问的测试账号",
  "DepName": "人事部",
  "MsgTitle": "【租赁租客】租客名称发生了变更!",
  "SendTime": "2021/12/5 0:00:06",
  "SendMan": null,
  "SendManName": null,
  "SendManDepName": null,
  "RN": "10"
}
}]}
```

问题 14 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->OrganCode (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcs19%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
```

```

Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}

```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->PageIndex (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMessageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxc19%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CCorpID%3E1906%3C/CorpID%3E%3CState%3E1%3C/
State%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%3C/attributes%3E&Class=On
lineMessage&Mac=7e68cec1012655d7ce99927bb529d069 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3193
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:50:11 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"MessageCode": "8B6CCBE7-F3DB-4FB9-B4B0-
430AC1A900F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/8
0:00:13", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "1"}, {"MessageCode": "55F0F2AE-8B2F-47D0-93CA-
D2D357BDB0F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/8
0:00:11", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "2"}, {"MessageCode": "93256352-0347-42AC-A31A-
53710EFACCD9", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事

```

```

部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/7
0:00:22", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "3"},
{"MessageCode": "5AC8AB5B-B44D-4FCA-911A-
45F518776008", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/7
0:00:12", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "4"},
{"MessageCode": "928E9CB7-61A8-42A7-B6C2-
C3B2ACBE04B5", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/6
0:00:21", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "5"},
{"MessageCode": "8F591E18-07E9-4029-B766-
25F04768AD1E", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/6
0:00:18", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "6"},
{"MessageCode": "2AB651FB-0546-4323-A3FF-
0A73FA165CB7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/6
0:00:14", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "7"},
{"MessageCode": "5B99302F-3149-4474-9079-
D574921EB89D", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/5
0:00:15", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "8"},
{"MessageCode": "0955A045-BC61-4324-909A-
5560938465BD", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/5
0:00:10", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "9"},
{"MessageCode": "19A45360-BBAC-43FB-B579-
0A3D92D4C898", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/5
0:00:06", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "10"}]}

```

问题 16 / 90

TOC

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->Code (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3
E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E6C1714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CORGanCode%3E010103%3C/ORGanCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

```

```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:48:59 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}

```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->State (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMessageList&Attribute=%3Cattributes%3E%3CNet%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CCorpID%3E1906%3C/CorpID%3E%3CState%3E1%3C/
State%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%3C/attributes%3E&Class=On
lineMessage&Mac=7e68cec1012655d7ce99927bb529d069 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

```

```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3193
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:50:11 GMT
Content-Type: text/plain; charset=utf-8

```

```

{"Result": "true", "data": [{"MessageCode": "8B6CCBE7-F3DB-4FB9-B4B0-
430AC1A900F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事
部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/8
0:00:13", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "1"}],

```

```

{"MessageCode": "55F0F2AE-8B2F-47D0-93CA-D2D357BDB0F7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/8 0:00:11", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "2"},
{"MessageCode": "93256352-0347-42AC-A31A-53710EFACCD9", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/7 0:00:22", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "3"},
{"MessageCode": "5AC8AB5B-B44D-4FCA-911A-45F518776008", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/7 0:00:12", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "4"},
{"MessageCode": "928E9CB7-61A8-42A7-B6C2-C3B2ACBE04B5", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/6 0:00:21", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "5"},
{"MessageCode": "8F591E18-07E9-4029-B766-25F04768AD1E", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/6 0:00:18", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "6"},
{"MessageCode": "2AB651FB-0546-4323-A3FF-0A73FA165CB7", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/6 0:00:14", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "7"},
{"MessageCode": "5B99302F-3149-4474-9079-D574921EB89D", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁合同】合同起始日期、到期日期发生了变更!", "SendTime": "2021/12/5 0:00:15", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "8"},
{"MessageCode": "0955A045-BC61-4324-909A-5560938465BD", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁房屋】房屋单元状态、生效时间、失效时间发生了变更!", "SendTime": "2021/12/5 0:00:10", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "9"},
{"MessageCode": "19A45360-BBAC-43FB-B579-0A3D92D4C898", "CutID": null, "UserCode": "001349", "UserName": "天问的测试账号", "DepName": "人事部", "MsgTitle": "【租赁租客】租客名称发生了变更!", "SendTime": "2021/12/5 0:00:06", "SendMan": null, "SendManName": null, "SendManDepName": null, "RN": "10"}

```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->WhereStr (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=QueryWarehouse&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CWhereStr%3E%3C/WhereStr%3E%3C/attributes%3E&Class=IncidentAcceptManage&Mac=fc
bb27f29fbd0e7bfe3040b0decde989 HTTP/1.1

```

```
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2521
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:52:37 GMT
Content-Type: text/plain; charset=utf-8
```

```
{
  "Result": "true",
  "data": [
    {
      "Key": "037b3588-cbfb-41c9-87ff-bc39945b29ff",
      "Value": "SZPAFC"
    },
    {
      "Key": "0a8b6e9f-e9aa-47ae-9a3c-d4dc0e2d1ee6",
      "Value": "L9仓库"
    },
    {
      "Key": "0c6eaf8f-a186-412f-8c32-c97444a0b791",
      "Value": "工程部库房"
    },
    {
      "Key": "206a6c0e-b168-4f89-8c7d-a81e3b967aba",
      "Value": "12"
    },
    {
      "Key": "24a827f9-7d47-42a8-8894-c7736c7b63dc",
      "Value": "客服部库房"
    },
    {
      "Key": "2ab848e0-8148-431f-8dc7-del379464b22",
      "Value": "233"
    },
    {
      "Key": "35c78dd4-43e6-4056-9f98-dbb1ecd777ee",
      "Value": "B2-4仓库"
    },
    {
      "Key": "3abeaa6c-d382-45d0-9668-2bb4e63d7469",
      "Value": "工程部仓库"
    },
    {
      "Key": "3b8b67c6-5a80-4e8d-8423-8c95e08b9916",
      "Value": "B1秩序仓库"
    },
    {
      "Key": "3c0d3259-614c-48a3-be37-1000e1348520",
      "Value": "B2-1仓库"
    },
    {
      "Key": "3eeb3bf0-dd31-484c-99e7-a7d5dd1e1f57",
      "Value": "杭州平安金融中心仓库"
    },
    {
      "Key": "50d15e06-cbba-4081-9065-89fdd5b30492",
      "Value": "33"
    },
    {
      "Key": "677572eb-bb1e-4a90-8206-0734ce5033ef",
      "Value": "CDPFC"
    },
    {
      "Key": "67e03ba6-9ce9-443e-bb15-dbb8c945f9bc",
      "Value": "WHPAFC"
    },
    {
      "Key": "6ca363dc-333a-4b12-8ed3-4fec3aa21281",
      "Value": "123123"
    },
    {
      "Key": "6ef27323-54b0-45d1-a4ba-fdf608e0a536",
      "Value": "B1行政仓库"
    },
    {
      "Key": "70b73866-10c8-4aed-9091-c7fb2ab14e64",
      "Value": "测试项目"
    },
    {
      "Key": "801208ff-0cb0-4b3a-ba5d-109f5dfbc1f5",
      "Value": "B2工程仓库"
    },
    {
      "Key": "88d40c8d-f505-49b2-bef5-b4c662466733",
      "Value": "项目测试"
    },
    {
      "Key": "9b93e767-11e4-48fd-8ea6-2def75e4cc22",
      "Value": "B3-1仓库"
    },
    {
      "Key": "9cf4fdb6-9822-4493-8d83-7d517742a78b",
      "Value": "L10仓库"
    },
    {
      "Key": "a8ae10df-8461-421b-b62b-5fffe11f8f45",
      "Value": "测试"
    },
    {
      "Key": "ae0dfc44-b41c-4e14-986c-4f8fc6b3943b",
      "Value": "B1客服仓库"
    },
    {
      "Key": "aeb9665b-aeda-48fa-8523-d506f0ac5596",
      "Value": "B-B2仓库"
    },
    {
      "Key": "b17b051a-125a-4206-9823-c9712d77977a",
      "Value": "2"
    },
    {
      "Key": "b3be0854-b01f-434c-9c2a-c668c519d070",
      "Value": "2楼办公室"
    },
    {
      "Key": "bcl136ef7-3b48-4858-a0f3-ab2028f27a6c",
      "Value": "B2工具仓库"
    },
    {
      "Key": "bdd0fc6d-9aff-4e7e-8830-4c0690727823",
      "Value": "50F-1仓库"
    },
    {
      "Key": "be0ddc9b-2816-47ca-8ce3-edec987138d7",
      "Value": "21"
    },
    {
      "Key": "d851522c-ad88-48a7-9d32-7b60daf862ce",
      "Value": "物资总库"
    },
    {
      "Key": "dc027c2a-7755-421c-84f0-1aba7c3a6707",
      "Value": "B1-1仓库"
    },
    {
      "Key": "e4f5243d-56be-417f-8e32-d380615d76b9",
      "Value": "2"
    },
    {
      "Key": "e9168f65-ee83-495e-ab7b-927b96b47093",
      "Value": "1"
    },
    {
      "Key": "edd8ac5e-2ea9-4cdf-b659-0e426e3a1ffe",
      "Value": "B1行政仓库"
    },
    {
      "Key": "f0e1dfe0-ab5c-4e87-be22-414ffa2b0e7e",
      "Value": "B2-3仓库"
    },
    {
      "Key": "f1296eb5-32c8-4750-b283-3272097ee068",
      "Value": "1"
    },
    {
      "Key": "fb0d7797-3c02-461d-9b75-693261a06209",
      "Value": "B2-2仓库"
    }
  ]
}
```

问题 19 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->Num (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:


```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMaterialSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CUserCode%3E%3E001349%3C/UserCode%3E%3CWareHouseName%3E%3EL9%4%BB%93%93%3E%3C/Wa
reHouseName%3E%3CMaterialName%3E%3C/MaterialName%3E%3CNum%3E%3C/Num%3E%3CPage%3E%3E1%3C/Page%3E%3C/a
tttributes%3E&Class=SearchManage&Mac=1c0619679d02301e68ebaecbca5c5e4 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1044
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:52:51 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":[{"WareHouseName":"L9仓库","MaterialTypeName":"低值易耗品","Num":"10005075","Specification":"商业施工人员出入证(A证)","Spell":"HC","UnitName":"张","ColorName":null,"Brand":null,"Quantity":1400.00}, {"WareHouseName":"L9仓库","MaterialTypeName":"低值易耗品","Num":"10005076","Specification":"商业施工人员出入证(B证)","Spell":"HC","UnitName":"张","ColorName":null,"Brand":null,"Quantity":1400.00}, {"WareHouseName":"L9仓库","MaterialTypeName":"低值易耗品","Num":"10005100","Specification":"拐杖","Spell":"HC","UnitName":"个","ColorName":null,"Brand":null,"Quantity":1.00}, {"WareHouseName":"L9仓库","MaterialTypeName":"劳保清洁用品","Num":"40005065","Specification":"Soffell驱蚊水","Spell":"HC","UnitName":"瓶","ColorName":null,"Brand":null,"Quantity":0.00}, {"WareHouseName":"L9仓库","MaterialTypeName":"低值易耗品","Num":"10005043","Specification":"IPAD防盗支架","Spell":"HC","UnitName":"个","ColorName":null,"Brand":null,"Quantity":1.00}],{"TotalCount":0}

```

问题 20 / 90

TOC

SSL 请求中的查询参数	
严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->roomSign (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetTopRoomList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E%3E001349%3C/CommID%3E%3CRoomSign%3E%3C/roomSign%3E%3C/attributes%3
E&Class=IncidentAcceptManage&Mac=17d7023414bfa764bab3e1c90b0914bc HTTP/1.1

```



```
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3318
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:56:41 GMT
Content-Type: text/plain; charset=utf-8
```

```
{"Result": "true", "data":
[{"RoomID": "19060300000242", "CommID": "190603", "RoomSign": "10001", "UnitSNum": "1", "CustName": "平安不动
产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000242", "CommID": "190603", "RoomSign": "10001", "UnitSNum": "1", "CustName": "青岛律
翼管理咨询有限责任公司", "MobilePhone": null, "CustID": "190603000000079"},
{"RoomID": "19060300000269", "CommID": "190603", "RoomSign": "1001", "UnitSNum": "1", "CustName": "平安不动
产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000234", "CommID": "190603", "RoomSign": "101", "UnitSNum": "1", "CustName": "平安不动
产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000087", "CommID": "190603", "RoomSign": "101", "UnitSNum": "1", "CustName": "平安不动
产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000087", "CommID": "190603", "RoomSign": "101", "UnitSNum": "1", "CustName": "平安银行
股份有限公司深圳分行", "MobilePhone": null, "CustID": "19060300000143"},
{"RoomID": "19060300000171", "CommID": "190603", "RoomSign": "10101", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000171", "CommID": "190603", "RoomSign": "10101", "UnitSNum": "1", "CustName": "国盛金
融控股集团股份有限公司", "MobilePhone": null, "CustID": "19060300000014"},
{"RoomID": "19060300000265", "CommID": "190603", "RoomSign": "10102", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000265", "CommID": "190603", "RoomSign": "10102", "UnitSNum": "1", "CustName": "深圳前
海弘大嘉豪资本管理有限公司", "MobilePhone": null, "CustID": "19060300000065"},
{"RoomID": "19060300000118", "CommID": "190603", "RoomSign": "10103", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000118", "CommID": "190603", "RoomSign": "10103", "UnitSNum": "1", "CustName": "深圳国
盛前海投资有限公司", "MobilePhone": null, "CustID": "19060300000086"},
{"RoomID": "19060300000079", "CommID": "190603", "RoomSign": "10104", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000079", "CommID": "190603", "RoomSign": "10104", "UnitSNum": "1", "CustName": "深圳前
海国盛科技有限公司", "MobilePhone": null, "CustID": "19060300000061"},
{"RoomID": "19060300000200", "CommID": "190603", "RoomSign": "10201", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000243", "CommID": "190603", "RoomSign": "10301", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000243", "CommID": "190603", "RoomSign": "10301", "UnitSNum": "1", "CustName": "上海富
唐资产管理有限公司", "MobilePhone": null, "CustID": "19060300000027"},
{"RoomID": "19060300000220", "CommID": "190603", "RoomSign": "10302", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"},
{"RoomID": "19060300000220", "CommID": "190603", "RoomSign": "10302", "UnitSNum": "1", "CustName": "正谷
(上海) 农业发展有限公司深圳分公司", "MobilePhone": null, "CustID": "19060300000042"},
{"RoomID": "19060300000134", "CommID": "190603", "RoomSign": "10303", "UnitSNum": "1", "CustName": "平安不
动产", "MobilePhone": null, "CustID": "19060300000000"}]}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->MaterialName (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMaterialSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3CCommID%3E%3CLoginPwd%3E%3CLoginPwd%3E%3CLoginPwd%3E%3CCommID%3E%3CCommID%3E%3CUserCode%3E%3CUserCode%3E%3CWareHouseName%3E%3CWareHouseName%3E%3CWareHouseName%3E%3CMaterialName%3E%3CMaterialName%3E%3CNum%3E%3CNum%3E%3CPage%3E%3CPage%3E%3Cattributes%3E&Class=SearchManage&Mac=1c0619679d02301e68ebaecbca5c5e4 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1044
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:52:51 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005075", "Specification": "商业施工人员出入证 (A证)", "Spell": "HC", "UnitName": "张", "ColorName": null, "Brand": null, "Quantity": 1400.00}, {"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005076", "Specification": "商业施工人员出入证 (B证)", "Spell": "HC", "UnitName": "张", "ColorName": null, "Brand": null, "Quantity": 1400.00}, {"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005100", "Specification": "拐杖", "Spell": "HC", "UnitName": "个", "ColorName": null, "Brand": null, "Quantity": 1.00}, {"WarehouseName": "L9仓库", "MaterialTypeName": "劳保清洁用品", "Num": "40005065", "Specification": "Soffell驱蚊水", "Spell": "HC", "UnitName": "瓶", "ColorName": null, "Brand": null, "Quantity": 0.00}, {"WarehouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005043", "Specification": "IPAD防盗支架", "Spell": "HC", "UnitName": "个", "ColorName": null, "Brand": null, "Quantity": 1.00}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->WareHouseName (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetMaterialSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3CCommID%3E%3CLoginPwd%3E%3CLoginPwd%3E%3CLoginPwd%3E%3CLoginPwd%3E%3CCommID%3E%3CCommID%3E%3CUserCode%3E%3CUserCode%3E%3CWareHouseName%3E%3CWareHouseName%3E%3CMaterialName%3E%3CMaterialName%3E%3CNum%3E%3CNum%3E%3CPage%3E%3CPage%3E%3Cattributes&Class=SearchManage&Mac=1c0619679d02301e68ebaecbca5c5e4 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1044
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:52:51 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"WareHouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005075", "Specification": "商业施工人员出入证 (A证)", "Spell": "HC", "UnitName": "张", "ColorName": null, "Brand": null, "Quantity": 1400.00}, {"WareHouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005076", "Specification": "商业施工人员出入证 (B证)", "Spell": "HC", "UnitName": "张", "ColorName": null, "Brand": null, "Quantity": 1400.00}, {"WareHouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005100", "Specification": "拐杖", "Spell": "HC", "UnitName": "个", "ColorName": null, "Brand": null, "Quantity": 1.00}, {"WareHouseName": "L9仓库", "MaterialTypeName": "劳保清洁用品", "Num": "40005065", "Specification": "Soffell驱蚊水", "Spell": "HC", "UnitName": "瓶", "ColorName": null, "Brand": null, "Quantity": 0.00}, {"WareHouseName": "L9仓库", "MaterialTypeName": "低值易耗品", "Num": "10005043", "Specification": "IPAD防盗支架", "Spell": "HC", "UnitName": "个", "ColorName": null, "Brand": null, "Quantity": 1.00}], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->CustID (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3C61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CCommID%3E%3CCommID%3E%3C/CustID%3E%3CCommID%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%3E
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E%3E1900/01/01%3C/FromDate%3E%3CToDate%3E%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E%3E1%3C/PageIndex%3E%3CPageSize%3E
%3E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":
{"ArrearageRoomCount":4,"DebtsAmountCount":1138.50,"DebtsLateAmountCount":0.0,"Details":
[{"CustID":19060300000001,"CustName":"北京平安联想智慧医疗信息技术有限公司","MobilePhone":"","Rooms":
[{"RoomID":190603000000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":2,"ComplainCount":2,"
UrgeFeesCount":0,"SendLetterCount":0},{"CustID":19060300000000,"CustName":"平安不动
产","MobilePhone":"","Rooms":[{"RoomID":190603000000234,"RoomSign":"101","RoomName":"101"},
{"RoomID":190603000000002,"RoomSign":"26联通","RoomName":"26联通"},
{"RoomID":190603000000254,"RoomSign":"701","RoomName":"701"},
{"RoomID":190603000000192,"RoomSign":"B101","RoomName":"B101"},
{"RoomID":190603000000045,"RoomSign":"B102","RoomName":"B102"},
{"RoomID":190603000000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":6,"ArrearageNum":6,"Ma
xFeesAging":5,"DebtsTotalAmount":838.50,"PrecBalance":0.00,"IncidentCount":12,"ComplainCount":12,
"UrgeFeesCount":0,"SendLetterCount":0},{"CustID":190603000000117,"CustName":"平安数字信息科技(深圳)
有限公司","MobilePhone":"","Rooms":
[{"RoomID":190603000000192,"RoomSign":"B101","RoomName":"B101"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0},{"CustID":190603000000101,"CustName":"彤彤科技(深圳)有限公
司","MobilePhone":"","Rooms":
[{"RoomID":190603000000045,"RoomSign":"B102","RoomName":"B102"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}],"TotalCount":0,"PageCount":0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->Key (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchUserSimpleInfo&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906
-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CKey%3E%3C/Key%3E%3C/attributes%3E&Class=PMSUserManage&Mac=6191ba9d629523f956e
3c831388645de HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 3672
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:53:05 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"UserCode": "000099", "UserName": "测试
002", "MobileTel": "", "DepName": null, "Email": "", "EmployeeCode": "", "RoleName": "欢测试岗"},
{"UserCode": "000130", "UserName": "天问技术
员", "MobileTel": "13000001111", "DepName": null, "Email": "", "EmployeeCode": "", "RoleName": "弱电/消防领
班, 弱电/消防技工, 报事派单人, 报事处理人, 物业专员, 写字楼管理, 商业安防员, 环境管理员, 工程经理"},
{"UserCode": "000131", "UserName": "admins", "MobileTel": "", "DepName": "深圳地区--深圳平安金融中
心", "Email": "", "EmployeeCode": "", "RoleName": "系统管理"}, {"UserCode": "000134", "UserName": "盛
世", "MobileTel": "13632847485", "DepName": "深圳平安金融中心--工程
部", "Email": "", "EmployeeCode": "", "RoleName": "工程总监"}, {"UserCode": "000135", "UserName": "王自
立", "MobileTel": "18923428169", "DepName": "深圳平安金融中心--工程
部", "Email": "", "EmployeeCode": "", "RoleName": "工程副经理"}, {"UserCode": "000140", "UserName": "贺利
平", "MobileTel": "13590222054", "DepName": "工程部--二装", "Email": "", "EmployeeCode": "", "RoleName": "二
装工程师, 二装派单岗"}, {"UserCode": "000155", "UserName": "张乐", "MobileTel": "13925263254", "DepName": "工
程部--弱电", "Email": "", "EmployeeCode": "", "RoleName": "弱电/消防技工"},
{"UserCode": "000163", "UserName": "张长军", "MobileTel": "13713544637", "DepName": "工程部--空
调", "Email": "", "EmployeeCode": "", "RoleName": "空调/给排水技工, 仓库主管"},
{"UserCode": "000165", "UserName": "骆贵贵", "MobileTel": "13480191432", "DepName": "工程部--空
调", "Email": "", "EmployeeCode": "", "RoleName": "空调/给排水技工"}, {"UserCode": "000179", "UserName": "杨柏
声", "MobileTel": "13480774417", "DepName": "工程部--空调", "Email": "", "EmployeeCode": "", "RoleName": "空
调/给排水技工, 空调/给排水领班, 空调/给排水派单岗"}, {"UserCode": "000189", "UserName": "王旭
瑞", "MobileTel": "13430562427", "DepName": "工程部--电梯", "Email": "", "EmployeeCode": "", "RoleName": "电
梯技工, 电梯领班"}, {"UserCode": "000190", "UserName": "张述标", "MobileTel": "13715389404", "DepName": "工
程部--电梯", "Email": "", "EmployeeCode": "", "RoleName": "电梯派单岗, 电梯主管"},
{"UserCode": "000196", "UserName": "杨辅军", "MobileTel": "18576608649", "DepName": "工程部--电
```

```

梯", "Email": "", "EmployeeCode": "", "RoleName": "电梯技工, 电梯领班, 电梯派单岗"},
{"UserCode": "000201", "UserName": "何菊根", "MobileTel": "13724282072", "DepName": "工程部--二装", "Email": "", "EmployeeCode": "", "RoleName": "二装领班, 二装派单岗"},
{"UserCode": "000225", "UserName": "钟文聪", "MobileTel": "13760197870", "DepName": "工程部--空调", "Email": "", "EmployeeCode": "", "RoleName": "空调/给排水派单岗, 空调工程师"},
{"UserCode": "000228", "UserName": "罗国云", "MobileTel": "18902832178", "DepName": "工程部--弱电", "Email": "", "EmployeeCode": "", "RoleName": "弱电/消防派单岗, 弱电/消防工程主管"},
{"UserCode": "000255", "UserName": "肖文波", "MobileTel": "18682213236", "DepName": "工程部--空调", "Email": "", "EmployeeCode": "", "RoleName": "空调/给排水技工, 空调/给排水派单岗, 空调主管"},
{"UserCode": "000262", "UserName": "姚润子", "MobileTel": "13510148893", "DepName": "工程部--强电", "Email": "", "EmployeeCode": "", "RoleName": "强电派单岗, 强电工程师"},
{"UserCode": "000263", "UserName": "王亚政", "MobileTel": "18988755320", "DepName": "工程部--弱电", "Email": "", "EmployeeCode": "", "RoleName": "强电派单岗, 弱电/消防工程主管"},
{"UserCode": "000267", "UserName": "林礼锋", "MobileTel": "13554838985", "DepName": "工程部--强电", "Email": "", "EmployeeCode": "", "RoleName": "强电派单岗, 工程主管"}], "TotalCount": 0}

```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->RoomID (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E%3E1900/01/01%3C/FromDate%3E%3CToDate%3E%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

```

```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

```

```

{"Result": "true", "data":

```

```

{"ArrearageRoomCount":4,"DebtsAmountCount":1138.50,"DebtsLateAmountCount":0.0,"Details":
[{"CustID":19060300000001,"CustName":"北京平安联想智慧医疗信息技术有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":2,"ComplainCount":2,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000000,"CustName":"平安不动
产","MobilePhone":"","Rooms":[{"RoomID":19060300000234,"RoomSign":"101","RoomName":"101"},
{"RoomID":19060300000002,"RoomSign":"26联通","RoomName":"26联通"},
{"RoomID":19060300000254,"RoomSign":"701","RoomName":"701"},
{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"},
{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"},
{"RoomID":19060300000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":6,"ArrearageNum":6,"Ma
xFeesAging":5,"DebtsTotalAmount":838.50,"PrecBalance":0.00,"IncidentCount":12,"ComplainCount":12,
"UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000117,"CustName":"平安数字信息科技(深圳)
有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000101,"CustName":"彤彤科技(深圳)有限公
司","MobilePhone":"","Rooms":
[{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}]},"TotalCount":0,"PageCount":0}

```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->ParkName (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetParkSearch&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcs19%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CParkName%3Eggg%3C/ParkName%3E%3CCarSign%3E%3C/CarSign%3E%3CRoomSign%3E%3C/Roo
mSign%3E%3CCustID%3E%3C/CustID%3E%3CPhone%3E%3C/Phone%3E%3C/attributes%3E&Class=SearchManage&Mac=
84306465e35c4a2a65c8e9b780673d0f HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 67
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:56:41 GMT

```

```
Content-Type: text/plain; charset=utf-8
{"Result": "false", "data": "未查询到相关信息", "TotalCount": 0}
```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->CustName (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcs19%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
{"ArrearageRoomCount": 4, "DebtsAmountCount": 1138.50, "DebtsLateAmountCount": 0.0, "Details":
[{"CustID": 19060300000001, "CustName": "北京平安联想智慧医疗信息技术有限公司", "MobilePhone": "", "Rooms":
[{"RoomID": 190603000000158, "RoomSign": "B103", "RoomName": "B103"}], "RoomCount": 1, "ArrearageNum": 1, "M
axFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 2, "ComplainCount": 2, "
UrgeFeesCount": 0, "SendLetterCount": 0}, {"CustID": 19060300000000, "CustName": "平安不动
产", "MobilePhone": "", "Rooms": [{"RoomID": 190603000000234, "RoomSign": "101", "RoomName": "101"},
{"RoomID": 190603000000002, "RoomSign": "26联通", "RoomName": "26联通"},
{"RoomID": 190603000000254, "RoomSign": "701", "RoomName": "701"},
{"RoomID": 190603000000192, "RoomSign": "B101", "RoomName": "B101"},
{"RoomID": 190603000000045, "RoomSign": "B102", "RoomName": "B102"},
{"RoomID": 190603000000158, "RoomSign": "B103", "RoomName": "B103"}], "RoomCount": 6, "ArrearageNum": 6, "Ma
xFeesAging": 5, "DebtsTotalAmount": 838.50, "PrecBalance": 0.00, "IncidentCount": 12, "ComplainCount": 12,
```



```

"UrgeFeesCount":0,"SendLetterCount":0},{ "CustID":19060300000117,"CustName":"平安数字信息科技（深圳）有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"}],"RoomCount":1,"ArrearageNum":1,"MaxFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"UrgeFeesCount":0,"SendLetterCount":0},{ "CustID":19060300000101,"CustName":"彤彤科技（深圳）有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"}],"RoomCount":1,"ArrearageNum":1,"MaxFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"UrgeFeesCount":0,"SendLetterCount":0}]],"TotalCount":0,"PageCount":0}

```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->CarparkID (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递，并且可能包含敏感信息

固定值: 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcs19%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":
{"ArrearageRoomCount":4,"DebtsAmountCount":1138.50,"DebtsLateAmountCount":0.0,"Details":
[{"CustID":19060300000001,"CustName":"北京平安联想智慧医疗信息技术有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":2,"ComplainCount":2,"
UrgeFeesCount":0,"SendLetterCount":0},{ "CustID":19060300000000,"CustName":"平安不动
产","MobilePhone":"","Rooms":[{"RoomID":19060300000234,"RoomSign":"101","RoomName":"101"},

```

```

{"RoomID":19060300000002,"RoomSign":"26联通","RoomName":"26联通"},
{"RoomID":19060300000254,"RoomSign":"701","RoomName":"701"},
{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"},
{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"},
{"RoomID":19060300000158,"RoomSign":"B103","RoomName":"B103"}],{"RoomCount":6,"ArrearageNum":6,"MaxFeesAging":5,"DebtsTotalAmount":838.50,"PrecBalance":0.00,"IncidentCount":12,"ComplainCount":12,"UrgeFeesCount":0,"SendLetterCount":0},{ "CustID":19060300000117,"CustName":"平安数字信息科技(深圳)有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"}],{"RoomCount":1,"ArrearageNum":1,"MaxFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"UrgeFeesCount":0,"SendLetterCount":0},{ "CustID":19060300000101,"CustName":"彤彤科技(深圳)有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"}],{"RoomCount":1,"ArrearageNum":1,"MaxFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"UrgeFeesCount":0,"SendLetterCount":0}]],"TotalCount":0,"PageCount":0}

```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->RoomSign (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E%3E1900/01/01%3C/FromDate%3E%3CToDate%3E%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5fff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

```

```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

```

```

{"Result":"true","data":

```

```

{"ArrearageRoomCount":4,"DebtsAmountCount":1138.50,"DebtsLateAmountCount":0.0,"Details":
[{"CustID":19060300000001,"CustName":"北京平安联想智慧医疗信息技术有限公司","MobilePhone":"","Rooms":
[{"RoomID":190603000000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":2,"ComplainCount":2,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000000,"CustName":"平安不动
产","MobilePhone":"","Rooms":[{"RoomID":190603000000234,"RoomSign":"101","RoomName":"101"},
{"RoomID":190603000000002,"RoomSign":"26联通","RoomName":"26联通"},
{"RoomID":190603000000254,"RoomSign":"701","RoomName":"701"},
{"RoomID":190603000000192,"RoomSign":"B101","RoomName":"B101"},
{"RoomID":190603000000045,"RoomSign":"B102","RoomName":"B102"},
{"RoomID":190603000000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":6,"ArrearageNum":6,"Ma
xFeesAging":5,"DebtsTotalAmount":838.50,"PrecBalance":0.00,"IncidentCount":12,"ComplainCount":12,
"UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":190603000000117,"CustName":"平安数字信息科技(深圳)
有限公司","MobilePhone":"","Rooms":
[{"RoomID":190603000000192,"RoomSign":"B101","RoomName":"B101"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":190603000000101,"CustName":"彤彤科技(深圳)有限公
司","MobilePhone":"","Rooms":
[{"RoomID":190603000000045,"RoomSign":"B102","RoomName":"B102"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}]},"TotalCount":0,"PageCount":0}

```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->CarparkName (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcs19%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319

```

```
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data":
{ "ArrearageRoomCount": 4, "DebtsAmountCount": 1138.50, "DebtsLateAmountCount": 0.0, "Details":
[ { "CustID": 19060300000001, "CustName": "北京平安联想智慧医疗信息技术有限公司", "MobilePhone": "", "Rooms":
[ { "RoomID": 19060300000158, "RoomSign": "B103", "RoomName": "B103" }, { "RoomID": 19060300000234, "RoomSign": "101", "RoomName": "101" },
{ "RoomID": 19060300000002, "RoomSign": "26联通", "RoomName": "26联通" },
{ "RoomID": 19060300000254, "RoomSign": "701", "RoomName": "701" },
{ "RoomID": 19060300000192, "RoomSign": "B101", "RoomName": "B101" },
{ "RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102" },
{ "RoomID": 19060300000158, "RoomSign": "B103", "RoomName": "B103" } ], "RoomCount": 6, "ArrearageNum": 6, "MaxFeesAging": 5, "DebtsTotalAmount": 838.50, "PrecBalance": 0.00, "IncidentCount": 12, "ComplainCount": 12,
"UrgeFeesCount": 0, "SendLetterCount": 0 }, { "CustID": 19060300000117, "CustName": "平安数字信息科技（深圳）有限公司", "MobilePhone": "", "Rooms":
[ { "RoomID": 19060300000192, "RoomSign": "B101", "RoomName": "B101" }, { "RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102" } ], "RoomCount": 1, "ArrearageNum": 1, "MaxFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 0, "ComplainCount": 0,
"UrgeFeesCount": 0, "SendLetterCount": 0 }, { "CustID": 19060300000101, "CustName": "彤彤科技（深圳）有限公司", "MobilePhone": "", "Rooms":
[ { "RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102" } ], "RoomCount": 1, "ArrearageNum": 1, "MaxFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 0, "ComplainCount": 0,
"UrgeFeesCount": 0, "SendLetterCount": 0 } ], "TotalCount": 0, "PageCount": 0 }
```

问题 31 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->FromDate (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递，并且可能包含敏感信息

固定值: 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twwxcs19%3C/Account%3E%3CLoginPwd%3E%3C61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%3E
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E%3E1900/01/01%3C/FromDate%3E%3CToDate%3E%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E%3C/ExcludeLetter%3E%3CPageIndex%3E%3E1%3C/PageIndex%3E%3CPageSize%3E%3E3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":
{"ArrearageRoomCount":4,"DebtsAmountCount":1138.50,"DebtsLateAmountCount":0.0,"Details":
[{"CustID":19060300000001,"CustName":"北京平安联想智慧医疗信息技术有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000158,"RoomSign":"B103","RoomName":"B103"},"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":2,"ComplainCount":2,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000000,"CustName":"平安不动
产","MobilePhone":"","Rooms":[{"RoomID":19060300000234,"RoomSign":"101","RoomName":"101"},
{"RoomID":19060300000002,"RoomSign":"26联通","RoomName":"26联通"},
{"RoomID":19060300000254,"RoomSign":"701","RoomName":"701"},
{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"},
{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"},
{"RoomID":19060300000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":6,"ArrearageNum":6,"Ma
x FeesAging":5,"DebtsTotalAmount":838.50,"PrecBalance":0.00,"IncidentCount":12,"ComplainCount":12,
"UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000117,"CustName":"平安数字信息科技（深圳）
有限公司","MobilePhone":"","Rooms":
[{"RoomID":19060300000192,"RoomSign":"B101","RoomName":"B101"},"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000101,"CustName":"彤彤科技（深圳）有限公
司","MobilePhone":"","Rooms":
[{"RoomID":19060300000045,"RoomSign":"B102","RoomName":"B102"},"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}]},"TotalCount":0,"PageCount":0}

```

问题 32 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->CarSign (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetParkSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E%3E%3CLoginPwd%3E%3C61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E%3E%3CCommID%3E%3CParkName%3E%3C3Eggg%3C/ParkName%3E%3CCarSign%3E%3C/CarSign%3E%3CRoomSign%3E%3C/RoomSign%3E%3CCustID%3E%3C/CustID%3E%3CPhone%3E%3C/Phone%3E%3C/attributes%3E&Class=SearchManage&Mac=84306465e35c4a2a65c8e9b780673d0f HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive

```

```
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 67
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:56:41 GMT
Content-Type: text/plain; charset=utf-8
```

```
{"Result": "false", "data": "未查询到相关信息", "TotalCount": 0}
```

问题 33 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->ExcludeUrged (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8
```

```
{"Result": "true", "data":
```

```

{"ArrearageRoomCount":4,"DebtsAmountCount":1138.50,"DebtsLateAmountCount":0.0,"Details":
[{"CustID":19060300000001,"CustName":"北京平安联想智慧医疗信息技术有限公司","MobilePhone":"","Rooms":
[{"RoomID":190603000000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":2,"ComplainCount":2,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":19060300000000,"CustName":"平安不动
产","MobilePhone":"","Rooms":[{"RoomID":190603000000234,"RoomSign":"101","RoomName":"101"},
{"RoomID":190603000000002,"RoomSign":"26联通","RoomName":"26联通"},
{"RoomID":190603000000254,"RoomSign":"701","RoomName":"701"},
{"RoomID":190603000000192,"RoomSign":"B101","RoomName":"B101"},
{"RoomID":190603000000045,"RoomSign":"B102","RoomName":"B102"},
{"RoomID":190603000000158,"RoomSign":"B103","RoomName":"B103"}],"RoomCount":6,"ArrearageNum":6,"M
axFeesAging":5,"DebtsTotalAmount":838.50,"PrecBalance":0.00,"IncidentCount":12,"ComplainCount":12,
"UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":190603000000117,"CustName":"平安数字信息科技(深圳)
有限公司","MobilePhone":"","Rooms":
[{"RoomID":190603000000192,"RoomSign":"B101","RoomName":"B101"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}, {"CustID":190603000000101,"CustName":"彤彤科技(深圳)有限公
司","MobilePhone":"","Rooms":
[{"RoomID":190603000000045,"RoomSign":"B102","RoomName":"B102"}],"RoomCount":1,"ArrearageNum":1,"M
axFeesAging":1,"DebtsTotalAmount":100.00,"PrecBalance":0.00,"IncidentCount":0,"ComplainCount":0,"
UrgeFeesCount":0,"SendLetterCount":0}]},"TotalCount":0,"PageCount":0}

```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->IncidentPlace (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentBigType&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CDrClass%3E1%3C/DrClass%3E%3CIncidentPlace%
3E%3E6%88%B7%E5%86%85%3C/IncidentPlace%3E%3CDuty%3E%3E7%89%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3C/attri
butes%3E&Class=PMSIncidentAccept&Mac=a98c9f57ba5e43c8b6d1bae77c1b2226 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1824
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:02:21 GMT

```

Content-Type: text/plain; charset=utf-8

```
{ "Result": "true", "data":
[{"CorpTypeID": 100000011, "TypeID": 1906030000000084, "TypeCode": "0004", "TypeName": "环境卫生", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000012, "TypeID": 1906030000000094, "TypeCode": "0005", "TypeName": "装饰装修", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000013, "TypeID": 1906030000000073, "TypeCode": "0006", "TypeName": "电梯", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000014, "TypeID": 1906030000000098, "TypeCode": "0007", "TypeName": "弱电类", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 0.05, "DealLimit2": 0.05, "IsTousu": 0},
{"CorpTypeID": 100000015, "TypeID": 1906030000000104, "TypeCode": "0008", "TypeName": "强电类", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 0.50, "DealLimit2": 0.50, "IsTousu": 0},
{"CorpTypeID": 100000016, "TypeID": 1906030000000079, "TypeCode": "0009", "TypeName": "安防安保", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000100, "TypeID": 1906030000000089, "TypeCode": "0024", "TypeName": "消防类", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000101, "TypeID": 1906030000000109, "TypeCode": "0025", "TypeName": "停车场", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000102, "TypeID": 1906030000000113, "TypeCode": "0026", "TypeName": "空调给排水", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 24.00, "DealLimit2": 72.00, "IsTousu": 0},
{"CorpTypeID": 100000103, "TypeID": 1906030000000118, "TypeCode": "0027", "TypeName": "其他", "RatedWorkHour": 0.00, "KPIRatio": 0.00, "DealLimit": 0.03, "DealLimit2": 0.03, "IsTousu": 0}], "TotalCount": 0}
```

问题 35 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->ToDate (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5fff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
```



```

Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
{"ArrearageRoomCount": 4, "DebtsAmountCount": 1138.50, "DebtsLateAmountCount": 0.0, "Details":
[{"CustID": 19060300000001, "CustName": "北京平安联想智慧医疗信息技术有限公司", "MobilePhone": "", "Rooms":
[{"RoomID": 19060300000158, "RoomSign": "B103", "RoomName": "B103"}], "RoomCount": 1, "ArrearageNum": 1, "M
axFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 2, "ComplainCount": 2, "
UrgeFeesCount": 0, "SendLetterCount": 0}, {"CustID": 19060300000000, "CustName": "平安不动
产", "MobilePhone": "", "Rooms": [{"RoomID": 19060300000234, "RoomSign": "101", "RoomName": "101"},
{"RoomID": 19060300000002, "RoomSign": "26联通", "RoomName": "26联通"},
{"RoomID": 19060300000254, "RoomSign": "701", "RoomName": "701"},
{"RoomID": 19060300000192, "RoomSign": "B101", "RoomName": "B101"},
{"RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102"},
{"RoomID": 19060300000158, "RoomSign": "B103", "RoomName": "B103"}], "RoomCount": 6, "ArrearageNum": 6, "Ma
x FeesAging": 5, "DebtsTotalAmount": 838.50, "PrecBalance": 0.00, "IncidentCount": 12, "ComplainCount": 12,
"UrgeFeesCount": 0, "SendLetterCount": 0}, {"CustID": 19060300000117, "CustName": "平安数字信息科技（深圳）
有限公司", "MobilePhone": "", "Rooms":
[{"RoomID": 19060300000192, "RoomSign": "B101", "RoomName": "B101"}], "RoomCount": 1, "ArrearageNum": 1, "M
axFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 0, "ComplainCount": 0, "
UrgeFeesCount": 0, "SendLetterCount": 0}, {"CustID": 19060300000101, "CustName": "彤彤科技（深圳）有限公
司", "MobilePhone": "", "Rooms":
[{"RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102"}], "RoomCount": 1, "ArrearageNum": 1, "M
axFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 0, "ComplainCount": 0, "
UrgeFeesCount": 0, "SendLetterCount": 0}]]}, {"TotalCount": 0, "PageCount": 0}

```

问题 36 / 90

TOC

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->Phone (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetParkSearch&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E%3E%3CLoginPwd%3E%3C/Account%3E%3CLoginPwd%3E%3CCommID%3E%3E%3C/CommID%3E%3CParkName%3E%3C/ParkName%3E%3CCarSign%3E%3C/CarSign%3E%3CRoomSign%3E%3C/RoomSign%3E%3CCustID%3E%3C/CustID%3E%3CPhone%3E%3C/Phone%3E%3C/attributes%3E%3C&Class=SearchManage&Mac=84306465e35c4a2a65c8e9b780673d0f HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

```

```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 67
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:56:41 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"false","data":"未查询到相关信息","TotalCount":0}

```

问题 37 / 90

TOC

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->DrClass (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentBigType&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CDrClass%3E1%3C/DrClass%3E%3CIncidentPlace%
3E%3E688%3E%3E586%3E%3C/IncidentPlace%3E%3CDuty%3E%3E789%A9E4%B8%3E%3C/Duty%3E%3C/attri
butes%3E&Class=PMSIncidentAccept&Mac=a98c9f57ba5e43c8b6d1bae77c1b2226 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1824
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:02:21 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":
[{"CorpTypeID":100000011,"TypeID":1906030000000084,"TypeCode":"0004","TypeName":"环境卫
生","RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
{"CorpTypeID":100000012,"TypeID":1906030000000094,"TypeCode":"0005","TypeName":"装修装
饰","RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
{"CorpTypeID":100000013,"TypeID":1906030000000073,"TypeCode":"0006","TypeName":"电
梯","RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},

```

```
{
  "CorpTypeID":10000014,"TypeID":1906030000000098,"TypeCode":"0007","TypeName":"弱电类",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":0.05,"DealLimit2":0.05,"IsTousu":0},
  {"CorpTypeID":10000015,"TypeID":1906030000000104,"TypeCode":"0008","TypeName":"强电类",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":0.50,"DealLimit2":0.50,"IsTousu":0},
  {"CorpTypeID":10000016,"TypeID":1906030000000079,"TypeCode":"0009","TypeName":"安防安保",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
  {"CorpTypeID":10000100,"TypeID":1906030000000089,"TypeCode":"0024","TypeName":"消防类",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
  {"CorpTypeID":10000101,"TypeID":1906030000000109,"TypeCode":"0025","TypeName":"停车场",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
  {"CorpTypeID":10000102,"TypeID":1906030000000113,"TypeCode":"0026","TypeName":"空调给排水",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
  {"CorpTypeID":10000103,"TypeID":1906030000000118,"TypeCode":"0027","TypeName":"其他",
  "RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":0.03,"DealLimit2":0.03,"IsTousu":0}],
  "TotalCount":0}
}
```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->Duty (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentBigType&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CDrClass%3E1%3C/DrClass%3E%3CIncidentPlace%
3E%3E6%88%8B7%8E5%86%85%3C/IncidentPlace%3E%3CDuty%3E%3E7%89%A9%4%88%9A%7%8B%3C/Duty%3E%3C/attri
butes%3E&Class=PMSIncidentAccept&Mac=a98c9f57ba5e43c8b6d1bae77c1b2226 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1824
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:02:21 GMT
Content-Type: text/plain; charset=utf-8
```

```
{"Result":"true","data":
[{"CorpTypeID":10000011,"TypeID":1906030000000084,"TypeCode":"0004","TypeName":"环境卫
生","RatedWorkHour":0.00,"KPIRatio":0.00,"DealLimit":24.00,"DealLimit2":72.00,"IsTousu":0},
{"CorpTypeID":10000012,"TypeID":1906030000000094,"TypeCode":"0005","TypeName":"装修装
```

```

饰", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":24.00, "DealLimit2":72.00, "IsTousu":0},
{"CorpTypeID":10000013, "TypeID":1906030000000073, "TypeCode": "0006", "TypeName": "电
梯", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":24.00, "DealLimit2":72.00, "IsTousu":0},
{"CorpTypeID":10000014, "TypeID":1906030000000098, "TypeCode": "0007", "TypeName": "弱电
类", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":0.05, "DealLimit2":0.05, "IsTousu":0},
{"CorpTypeID":10000015, "TypeID":1906030000000104, "TypeCode": "0008", "TypeName": "强电
类", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":0.50, "DealLimit2":0.50, "IsTousu":0},
{"CorpTypeID":10000016, "TypeID":1906030000000079, "TypeCode": "0009", "TypeName": "安防安
保", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":24.00, "DealLimit2":72.00, "IsTousu":0},
{"CorpTypeID":10000100, "TypeID":1906030000000089, "TypeCode": "0024", "TypeName": "消防
类", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":24.00, "DealLimit2":72.00, "IsTousu":0},
{"CorpTypeID":10000101, "TypeID":1906030000000109, "TypeCode": "0025", "TypeName": "停车
场", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":24.00, "DealLimit2":72.00, "IsTousu":0},
{"CorpTypeID":10000102, "TypeID":1906030000000113, "TypeCode": "0026", "TypeName": "空调给排
水", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":24.00, "DealLimit2":72.00, "IsTousu":0},
{"CorpTypeID":10000103, "TypeID":1906030000000118, "TypeCode": "0027", "TypeName": "其
他", "RatedWorkHour":0.00, "KPIRatio":0.00, "DealLimit":0.03, "DealLimit2":0.03, "IsTousu":0}}, {"TotalC
ount":0}

```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->ExcludeLetter (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=FuzzySearchArrearageList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CCustID%3E%3C/CustID%3E%3CCustName%3E%3C/CustName%3E%3CRoomID%3E%3C/RoomID%3E%
3CRoomSign%3E%3C/RoomSign%3E%3CCarparkID%3E%3C/CarparkID%3E%3CCarparkName%3E%3C/CarparkName%3E%3C
FromDate%3E1900/01/01%3C/FromDate%3E%3CToDate%3E2021/12/30%3C/ToDate%3E%3CExcludeUrged%3E0%3C/Exc
ludeUrged%3E%3CExcludeLetter%3E0%3C/ExcludeLetter%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3
E10%3C/PageSize%3E%3C/attributes%3E&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17
b6d5e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1797
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 06:54:28 GMT

```

Content-Type: text/plain; charset=utf-8

```
{ "Result": "true", "data":
{ "ArrearageRoomCount": 4, "DebtsAmountCount": 1138.50, "DebtsLateAmountCount": 0.0, "Details":
[ { "CustID": 19060300000001, "CustName": "北京平安联想智慧医疗信息技术有限公司", "MobilePhone": "", "Rooms":
[ { "RoomID": 19060300000158, "RoomSign": "B103", "RoomName": "B103" }, { "RoomID": 19060300000234, "RoomSign": "101", "RoomName": "101" },
{ "RoomID": 19060300000002, "RoomSign": "26联通", "RoomName": "26联通" },
{ "RoomID": 19060300000254, "RoomSign": "701", "RoomName": "701" },
{ "RoomID": 19060300000192, "RoomSign": "B101", "RoomName": "B101" },
{ "RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102" },
{ "RoomID": 19060300000158, "RoomSign": "B103", "RoomName": "B103" } ], "RoomCount": 6, "ArrearageNum": 6, "MaxFeesAging": 5, "DebtsTotalAmount": 838.50, "PrecBalance": 0.00, "IncidentCount": 12, "ComplainCount": 12,
"UrgeFeesCount": 0, "SendLetterCount": 0 }, { "CustID": 19060300000117, "CustName": "平安数字信息科技(深圳)有限公司", "MobilePhone": "", "Rooms":
[ { "RoomID": 19060300000192, "RoomSign": "B101", "RoomName": "B101" }, { "RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102" } ], "RoomCount": 1, "ArrearageNum": 1, "MaxFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 0, "ComplainCount": 0,
"UrgeFeesCount": 0, "SendLetterCount": 0 }, { "CustID": 19060300000101, "CustName": "彤彤科技(深圳)有限公司", "MobilePhone": "", "Rooms":
[ { "RoomID": 19060300000045, "RoomSign": "B102", "RoomName": "B102" } ], "RoomCount": 1, "ArrearageNum": 1, "MaxFeesAging": 1, "DebtsTotalAmount": 100.00, "PrecBalance": 0.00, "IncidentCount": 0, "ComplainCount": 0,
"UrgeFeesCount": 0, "SendLetterCount": 0 } ], "TotalCount": 0, "PageCount": 0 }
```

问题 40 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->Size (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CPage%3E%3E1%3C/Page%3E%3CSize%3E%3E10%3C/Size%3E%3CIsOwe%3E%3C/IsOwe%3E%3CIsIncide
nt%3E%3C/IsIncident%3E%3CIsTousu%3E%3C/IsTousu%3E%3CIsDecorate%3E%3C/IsDecorate%3E%3CCustID%3E%3C
/CustID%3E%3CRoomID%3E%3C/RoomID%3E%3CMobile%3E%3C/Mobile%3E%3CCarparkID%3E%3C/CarparkID%3E%3C/at
tributes%3E&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 36830
```

X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:05:03 GMT
Content-Type: text/plain; charset=utf-8

```
{
  "Result": "true",
  "data": [
    {
      "CustID": "19060300000001",
      "CustName": "北京平安联想智慧医疗信息技术有限公司",
      "MobilePhone": null,
      "RoomList": [
        {
          "RoomID": 19060300000158,
          "RoomSign": "B103",
          "RoomName": "B103"
        }
      ],
      "OweCount": 1,
      "OweAmount": 100.00,
      "OweMonth": 0,
      "PrecAmount": 0.00,
      "IncidentCount": 66,
      "TousuCount": 0,
      "RenoStartDate": "2020/8/2 0:00:00",
      "RenoEndDate": "2020/8/6 0:00:00"
    },
    {
      "CustID": "19060300000000",
      "CustName": "平安不动产",
      "MobilePhone": null,
      "RoomList": [
        {
          "RoomID": 19060300000242,
          "RoomSign": "10001",
          "RoomName": "10001"
        },
        {
          "RoomID": 19060300000269,
          "RoomSign": "1001",
          "RoomName": "1001"
        },
        {
          "RoomID": 19060300000234,
          "RoomSign": "101",
          "RoomName": "101"
        },
        {
          "RoomID": 19060300000087,
          "RoomSign": "101",
          "RoomName": "101"
        },
        {
          "RoomID": 19060300000171,
          "RoomSign": "10101",
          "RoomName": "10101"
        },
        {
          "RoomID": 19060300000265,
          "RoomSign": "10102",
          "RoomName": "10102"
        },
        {
          "RoomID": 19060300000118,
          "RoomSign": "10103",
          "RoomName": "10103"
        },
        {
          "RoomID": 19060300000079,
          "RoomSign": "10104",
          "RoomName": "10104"
        },
        {
          "RoomID": 19060300000200,
          "RoomSign": "10201",
          "RoomName": "10201"
        }
      ]
    }
  ]
}
```

```
},
{
  "RoomID": 19060300000243,
  "RoomSign": "10301",
  "RoomName": "10301"
},
{
  "RoomID": 19060300000220,
  "RoomSign": "10302",
  "RoomName": "10302"
},
{
  "RoomID": 19060300000134,
  "RoomSign": "10303",
  "RoomName": "10303"
},
{
  "RoomID": 19060300000278,
  "RoomSign": "10304",
  "RoomName": "10304"
},
{
  "RoomID": 19060300000138,
  "RoomSign": "10305",
  "RoomName": "10305"
},
{
  "RoomID": 19060300000013,
  "RoomSign": "10306",
  "RoomName": "10306"
},
{
  "RoomID": 19060300000170,
  "RoomSign": "10307",
  "RoomName": "10307"
},
{
  "RoomID": 19060300000173,
  "RoomSign": "10308",
  "RoomName": "10308"
},
{
  "RoomID": 19060300000062,
  "RoomSign": "10309",
  "RoomName": "10309"
},
{
  "RoomID": 19060300000235,
  "RoomSign": "10310",
  "RoomName": "10310"
},
{
  "RoomID": 19060300000193,
  "RoomSign": "10311",
  "RoomName": "10311"
},
{
  "RoomID": 19060300000139,
  "RoomSign": "10312",
  "RoomName": "10312"
},
{
  "RoomID": 19060300000221,
  "RoomSign": "1040104",
  "RoomName": "1040104"
},
{
  "RoomID": 19060300000106,
  "RoomSign": "104F0203",
  "RoomName": "104F0203"
},
{
  "RoomID": 19060300000203,
  "RoomSign": "10501",
  "RoomName": "10501"
},
{
  "RoomID": 19060300000286,
```

```

    "RoomSign": "10502",
    "RoomName": "10502"
  },
  {
    "RoomID": 19060300000006,
    "RoomSign": "10503",
    "RoomName": "10503"
  },
  {
    "RoomID": 19060300000086,
    "RoomSign": "10601",
    "RoomName": "10601"
  },
  {
    "RoomID": 190603000001
  }
  ...
  ...
  ...

```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->IncidentID (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentSimpleDetail&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E19060300000026993%3C/IncidentID%3E%3C/attributes%3E&Class=PMSIn
cidentAccept&Mac=7ebe4d7175ae461a40865e227b712ac5 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 886
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:06:10 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":
{"IncidentID":19060300000026993,"IncidentNum":"20211208000303","CommID":190603,"CommName":"深圳平

```



```

安全金融中心", "CustName": "平安不动产", "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "EqID": null, "
EquipmentName": null, "EquipmentNO": null, "SpaceID": null, "SpaceName": null, "SpaceNo": null, "IncidentPl
ace": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentMode": "项目受
理", "IncidentContent": "ghgg", "DrClass": 1, "IsTouSu": 0, "EmergencyDegree": null, "ReserveDate": "2021-
12-08
15:27:10", "ReserveLimit": null, "DispLimit": 0.50, "BigCorpTypeID": 100000011, "BigCorpTypeCode": "0004"
, "BigTypeName": "环境卫生", "Phone": "1355665555", "IsFee": 0, "TypeName": "环境卫生", "Duty": "物业
类", "IncidentImgs": "", "TotalCount": 0}

```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->IsOwe (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CPage%3E%3E1%3C/Page%3E%3CSize%3E%3E10%3C/Size%3E%3CIsOwe%3E%3E1%3C/IsOwe%3E%3CIsIncid
e%3E%3C/IsIncident%3E%3CIsTousu%3E%3C/IsTousu%3E%3CIsDecorate%3E%3C/IsDecorate%3E%3CCustID%3E%3C
/CustID%3E%3CRoomID%3E%3C/RoomID%3E%3CMobile%3E%3C/Mobile%3E%3CCarparkID%3E%3C/CarparkID%3E%3C/at
tributes%3E&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 36830
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:05:03 GMT
Content-Type: text/plain; charset=utf-8

{
  "Result": "true",
  "data": [
    {
      "CustID": "19060300000001",
      "CustName": "北京平安联想智慧医疗信息技术有限公司",
      "MobilePhone": null,
      "RoomList": [

```

```

    {
      "RoomID": 19060300000158,
      "RoomSign": "B103",
      "RoomName": "B103"
    }
  ],
  "OweCount": 1,
  "OweAmount": 100.00,
  "OweMonth": 0,
  "PrecAmount": 0.00,
  "IncidentCount": 66,
  "TousuCount": 0,
  "RenoStartDate": "2020/8/2 0:00:00",
  "RenoEndDate": "2020/8/6 0:00:00"
},
{
  "CustID": "19060300000000",
  "CustName": "平安不动产",
  "MobilePhone": null,
  "RoomList": [
    {
      "RoomID": 19060300000242,
      "RoomSign": "10001",
      "RoomName": "10001"
    },
    {
      "RoomID": 19060300000269,
      "RoomSign": "1001",
      "RoomName": "1001"
    },
    {
      "RoomID": 19060300000234,
      "RoomSign": "101",
      "RoomName": "101"
    },
    {
      "RoomID": 19060300000087,
      "RoomSign": "101",
      "RoomName": "101"
    },
    {
      "RoomID": 19060300000171,
      "RoomSign": "10101",
      "RoomName": "10101"
    },
    {
      "RoomID": 19060300000265,
      "RoomSign": "10102",
      "RoomName": "10102"
    },
    {
      "RoomID": 19060300000118,
      "RoomSign": "10103",
      "RoomName": "10103"
    },
    {
      "RoomID": 19060300000079,
      "RoomSign": "10104",
      "RoomName": "10104"
    },
    {
      "RoomID": 19060300000200,
      "RoomSign": "10201",
      "RoomName": "10201"
    },
    {
      "RoomID": 19060300000243,
      "RoomSign": "10301",
      "RoomName": "10301"
    },
    {
      "RoomID": 19060300000220,
      "RoomSign": "10302",
      "RoomName": "10302"
    },
    {
      "RoomID": 19060300000134,
      "RoomSign": "10303",

```

```
"RoomName": "10303"
},
{
  "RoomID": 19060300000278,
  "RoomSign": "10304",
  "RoomName": "10304"
},
{
  "RoomID": 19060300000138,
  "RoomSign": "10305",
  "RoomName": "10305"
},
{
  "RoomID": 19060300000013,
  "RoomSign": "10306",
  "RoomName": "10306"
},
{
  "RoomID": 19060300000170,
  "RoomSign": "10307",
  "RoomName": "10307"
},
{
  "RoomID": 19060300000173,
  "RoomSign": "10308",
  "RoomName": "10308"
},
{
  "RoomID": 19060300000062,
  "RoomSign": "10309",
  "RoomName": "10309"
},
{
  "RoomID": 19060300000235,
  "RoomSign": "10310",
  "RoomName": "10310"
},
{
  "RoomID": 19060300000193,
  "RoomSign": "10311",
  "RoomName": "10311"
},
{
  "RoomID": 19060300000139,
  "RoomSign": "10312",
  "RoomName": "10312"
},
{
  "RoomID": 19060300000221,
  "RoomSign": "1040104",
  "RoomName": "1040104"
},
{
  "RoomID": 19060300000106,
  "RoomSign": "104F0203",
  "RoomName": "104F0203"
},
{
  "RoomID": 19060300000203,
  "RoomSign": "10501",
  "RoomName": "10501"
},
{
  "RoomID": 19060300000286,
  "RoomSign": "10502",
  "RoomName": "10502"
},
{
  "RoomID": 19060300000006,
  "RoomSign": "10503",
  "RoomName": "10503"
},
{
  "RoomID": 19060300000086,
  "RoomSign": "10601",
  "RoomName": "10601"
},
{

```

```
"RoomID": 190603000001
...
...
...
```

SSL 请求中的查询参数	
严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->IsTousu (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CPage%3E1%3C/Page%3E%3CSize%3E10%3C/Size%3E%3CIsOwe%3E1%3C/IsOwe%3E%3CIsIncide
nt%3E%3C/IsIncident%3E%3CIsTousu%3E%3C/IsTousu%3E%3CIsDecorate%3E%3C/IsDecorate%3E%3CCustID%3E%3C
/CustID%3E%3CRoomID%3E%3C/RoomID%3E%3CMobile%3E%3C/Mobile%3E%3CCarparkID%3E%3C/CarparkID%3E%3C/at
tributes%3E&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 36830
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:05:03 GMT
Content-Type: text/plain; charset=utf-8

{
  "Result": "true",
  "data": [
    {
      "CustID": "19060300000001",
      "CustName": "北京平安联想智慧医疗信息技术有限公司",
      "MobilePhone": null,
      "RoomList": [
        {
          "RoomID": 19060300000158,
          "RoomSign": "B103",
          "RoomName": "B103"
        }
      ]
    }
  ],
}
```

```
"OweCount": 1,
"OweAmount": 100.00,
"OweMonth": 0,
"PrecAmount": 0.00,
"IncidentCount": 66,
"TousuCount": 0,
"RenoStartDate": "2020/8/2 0:00:00",
"RenoEndDate": "2020/8/6 0:00:00"
},
{
  "CustID": "19060300000000",
  "CustName": "平安不动产",
  "MobilePhone": null,
  "RoomList": [
    {
      "RoomID": 19060300000242,
      "RoomSign": "10001",
      "RoomName": "10001"
    },
    {
      "RoomID": 19060300000269,
      "RoomSign": "1001",
      "RoomName": "1001"
    },
    {
      "RoomID": 19060300000234,
      "RoomSign": "101",
      "RoomName": "101"
    },
    {
      "RoomID": 19060300000087,
      "RoomSign": "101",
      "RoomName": "101"
    },
    {
      "RoomID": 19060300000171,
      "RoomSign": "10101",
      "RoomName": "10101"
    },
    {
      "RoomID": 19060300000265,
      "RoomSign": "10102",
      "RoomName": "10102"
    },
    {
      "RoomID": 19060300000118,
      "RoomSign": "10103",
      "RoomName": "10103"
    },
    {
      "RoomID": 19060300000079,
      "RoomSign": "10104",
      "RoomName": "10104"
    },
    {
      "RoomID": 19060300000200,
      "RoomSign": "10201",
      "RoomName": "10201"
    },
    {
      "RoomID": 19060300000243,
      "RoomSign": "10301",
      "RoomName": "10301"
    },
    {
      "RoomID": 19060300000220,
      "RoomSign": "10302",
      "RoomName": "10302"
    },
    {
      "RoomID": 19060300000134,
      "RoomSign": "10303",
      "RoomName": "10303"
    },
    {
      "RoomID": 19060300000278,
      "RoomSign": "10304",
      "RoomName": "10304"
    }
  ]
}
```

```
},
{
  "RoomID": 19060300000138,
  "RoomSign": "10305",
  "RoomName": "10305"
},
{
  "RoomID": 19060300000013,
  "RoomSign": "10306",
  "RoomName": "10306"
},
{
  "RoomID": 19060300000170,
  "RoomSign": "10307",
  "RoomName": "10307"
},
{
  "RoomID": 19060300000173,
  "RoomSign": "10308",
  "RoomName": "10308"
},
{
  "RoomID": 19060300000062,
  "RoomSign": "10309",
  "RoomName": "10309"
},
{
  "RoomID": 19060300000235,
  "RoomSign": "10310",
  "RoomName": "10310"
},
{
  "RoomID": 19060300000193,
  "RoomSign": "10311",
  "RoomName": "10311"
},
{
  "RoomID": 19060300000139,
  "RoomSign": "10312",
  "RoomName": "10312"
},
{
  "RoomID": 19060300000221,
  "RoomSign": "1040104",
  "RoomName": "1040104"
},
{
  "RoomID": 19060300000106,
  "RoomSign": "104F0203",
  "RoomName": "104F0203"
},
{
  "RoomID": 19060300000203,
  "RoomSign": "10501",
  "RoomName": "10501"
},
{
  "RoomID": 19060300000286,
  "RoomSign": "10502",
  "RoomName": "10502"
},
{
  "RoomID": 19060300000006,
  "RoomSign": "10503",
  "RoomName": "10503"
},
{
  "RoomID": 19060300000086,
  "RoomSign": "10601",
  "RoomName": "10601"
},
{
  "RoomID": 1906030000001
```

```
...
...
...
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->IsIncident (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CPage%3E1%3C/Page%3E%3CSize%3E10%3C/Size%3E%3CIsOwe%3E1%3C/IsOwe%3E%3CIsIncide
nt%3E%3C/IsIncident%3E%3CIsTousu%3E%3C/IsTousu%3E%3CIsDecorate%3E%3C/IsDecorate%3E%3CCustID%3E%3C
/CustID%3E%3CRoomID%3E%3C/RoomID%3E%3CMobile%3E%3C/Mobile%3E%3CCarparkID%3E%3C/CarparkID%3E%3C/at
tributes%3E&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 36830
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:05:03 GMT
Content-Type: text/plain; charset=utf-8

{
  "Result": "true",
  "data": [
    {
      "CustID": "19060300000001",
      "CustName": "北京平安联想智慧医疗信息技术有限公司",
      "MobilePhone": null,
      "RoomList": [
        {
          "RoomID": 19060300000158,
          "RoomSign": "B103",
          "RoomName": "B103"
        }
      ],
      "OweCount": 1,
      "OweAmount": 100.00,
      "OweMonth": 0,
      "PrecAmount": 0.00,
      "IncidentCount": 66,
      "TousuCount": 0,
    }
  ]
}

```

```
"RenoStartDate": "2020/8/2 0:00:00",
"RenoEndDate": "2020/8/6 0:00:00"
},
{
  "CustID": "19060300000000",
  "CustName": "平安不动产",
  "MobilePhone": null,
  "RoomList": [
    {
      "RoomID": 19060300000242,
      "RoomSign": "10001",
      "RoomName": "10001"
    },
    {
      "RoomID": 19060300000269,
      "RoomSign": "1001",
      "RoomName": "1001"
    },
    {
      "RoomID": 19060300000234,
      "RoomSign": "101",
      "RoomName": "101"
    },
    {
      "RoomID": 19060300000087,
      "RoomSign": "101",
      "RoomName": "101"
    },
    {
      "RoomID": 19060300000171,
      "RoomSign": "10101",
      "RoomName": "10101"
    },
    {
      "RoomID": 19060300000265,
      "RoomSign": "10102",
      "RoomName": "10102"
    },
    {
      "RoomID": 19060300000118,
      "RoomSign": "10103",
      "RoomName": "10103"
    },
    {
      "RoomID": 19060300000079,
      "RoomSign": "10104",
      "RoomName": "10104"
    },
    {
      "RoomID": 19060300000200,
      "RoomSign": "10201",
      "RoomName": "10201"
    },
    {
      "RoomID": 19060300000243,
      "RoomSign": "10301",
      "RoomName": "10301"
    },
    {
      "RoomID": 19060300000220,
      "RoomSign": "10302",
      "RoomName": "10302"
    },
    {
      "RoomID": 19060300000134,
      "RoomSign": "10303",
      "RoomName": "10303"
    },
    {
      "RoomID": 19060300000278,
      "RoomSign": "10304",
      "RoomName": "10304"
    },
    {
      "RoomID": 19060300000138,
      "RoomSign": "10305",
      "RoomName": "10305"
    }
  ],
}
```



```
{
  "RoomID": 19060300000013,
  "RoomSign": "10306",
  "RoomName": "10306"
},
{
  "RoomID": 19060300000170,
  "RoomSign": "10307",
  "RoomName": "10307"
},
{
  "RoomID": 19060300000173,
  "RoomSign": "10308",
  "RoomName": "10308"
},
{
  "RoomID": 19060300000062,
  "RoomSign": "10309",
  "RoomName": "10309"
},
{
  "RoomID": 19060300000235,
  "RoomSign": "10310",
  "RoomName": "10310"
},
{
  "RoomID": 19060300000193,
  "RoomSign": "10311",
  "RoomName": "10311"
},
{
  "RoomID": 19060300000139,
  "RoomSign": "10312",
  "RoomName": "10312"
},
{
  "RoomID": 19060300000221,
  "RoomSign": "1040104",
  "RoomName": "1040104"
},
{
  "RoomID": 19060300000106,
  "RoomSign": "104F0203",
  "RoomName": "104F0203"
},
{
  "RoomID": 19060300000203,
  "RoomSign": "10501",
  "RoomName": "10501"
},
{
  "RoomID": 19060300000286,
  "RoomSign": "10502",
  "RoomName": "10502"
},
{
  "RoomID": 19060300000006,
  "RoomSign": "10503",
  "RoomName": "10503"
},
{
  "RoomID": 19060300000086,
  "RoomSign": "10601",
  "RoomName": "10601"
},
{
  "RoomID": 1906030000001
```

```
...
...
...
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->Mobile (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CPage%3E1%3C/Page%3E%3CSize%3E10%3C/Size%3E%3CIsOwe%3E1%3C/IsOwe%3E%3CIsIncide
nt%3E%3C/IsIncident%3E%3CIsTousu%3E%3C/IsTousu%3E%3CIsDecorate%3E%3C/IsDecorate%3E%3CCustID%3E%3C
/CustID%3E%3CRoomID%3E%3C/RoomID%3E%3CMobile%3E%3C/Mobile%3E%3CCarparkID%3E%3C/CarparkID%3E%3C/at
tributes%3E&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 36830
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:05:03 GMT
Content-Type: text/plain; charset=utf-8

{
  "Result": "true",
  "data": [
    {
      "CustID": "19060300000001",
      "CustName": "北京平安联想智慧医疗信息技术有限公司",
      "MobilePhone": null,
      "RoomList": [
        {
          "RoomID": 19060300000158,
          "RoomSign": "B103",
          "RoomName": "B103"
        }
      ],
      "OweCount": 1,
      "OweAmount": 100.00,
      "OweMonth": 0,
      "PrecAmount": 0.00,
      "IncidentCount": 66,
      "TousuCount": 0,
      "RenoStartDate": "2020/8/2 0:00:00",
      "RenoEndDate": "2020/8/6 0:00:00"
    },
    {
      "CustID": "19060300000000",

```

```
"CustName": "平安不动产",
"MobilePhone": null,
"RoomList": [
  {
    "RoomID": 19060300000242,
    "RoomSign": "10001",
    "RoomName": "10001"
  },
  {
    "RoomID": 19060300000269,
    "RoomSign": "1001",
    "RoomName": "1001"
  },
  {
    "RoomID": 19060300000234,
    "RoomSign": "101",
    "RoomName": "101"
  },
  {
    "RoomID": 19060300000087,
    "RoomSign": "101",
    "RoomName": "101"
  },
  {
    "RoomID": 19060300000171,
    "RoomSign": "10101",
    "RoomName": "10101"
  },
  {
    "RoomID": 19060300000265,
    "RoomSign": "10102",
    "RoomName": "10102"
  },
  {
    "RoomID": 19060300000118,
    "RoomSign": "10103",
    "RoomName": "10103"
  },
  {
    "RoomID": 19060300000079,
    "RoomSign": "10104",
    "RoomName": "10104"
  },
  {
    "RoomID": 19060300000200,
    "RoomSign": "10201",
    "RoomName": "10201"
  },
  {
    "RoomID": 19060300000243,
    "RoomSign": "10301",
    "RoomName": "10301"
  },
  {
    "RoomID": 19060300000220,
    "RoomSign": "10302",
    "RoomName": "10302"
  },
  {
    "RoomID": 19060300000134,
    "RoomSign": "10303",
    "RoomName": "10303"
  },
  {
    "RoomID": 19060300000278,
    "RoomSign": "10304",
    "RoomName": "10304"
  },
  {
    "RoomID": 19060300000138,
    "RoomSign": "10305",
    "RoomName": "10305"
  },
  {
    "RoomID": 19060300000013,
    "RoomSign": "10306",
    "RoomName": "10306"
  },
],
```

```
{
  "RoomID": 19060300000170,
  "RoomSign": "10307",
  "RoomName": "10307"
},
{
  "RoomID": 19060300000173,
  "RoomSign": "10308",
  "RoomName": "10308"
},
{
  "RoomID": 19060300000062,
  "RoomSign": "10309",
  "RoomName": "10309"
},
{
  "RoomID": 19060300000235,
  "RoomSign": "10310",
  "RoomName": "10310"
},
{
  "RoomID": 19060300000193,
  "RoomSign": "10311",
  "RoomName": "10311"
},
{
  "RoomID": 19060300000139,
  "RoomSign": "10312",
  "RoomName": "10312"
},
{
  "RoomID": 19060300000221,
  "RoomSign": "1040104",
  "RoomName": "1040104"
},
{
  "RoomID": 19060300000106,
  "RoomSign": "104F0203",
  "RoomName": "104F0203"
},
{
  "RoomID": 19060300000203,
  "RoomSign": "10501",
  "RoomName": "10501"
},
{
  "RoomID": 19060300000286,
  "RoomSign": "10502",
  "RoomName": "10502"
},
{
  "RoomID": 19060300000006,
  "RoomSign": "10503",
  "RoomName": "10503"
},
{
  "RoomID": 19060300000086,
  "RoomSign": "10601",
  "RoomName": "10601"
},
{
  "RoomID": 1906030000001
  ...
  ...
  ...
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->IsDecorate (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CPage%3E1%3C/Page%3E%3CSize%3E10%3C/Size%3E%3CIsove%3E1%3C/IsOve%3E%3CIIncide
nt%3E%3C/IsIncident%3E%3CIstousu%3E%3C/IsTousu%3E%3CIsDecorate%3E%3C/IsDecorate%3E%3CCustID%3E%3C
/CustID%3E%3CRoomID%3E%3C/RoomID%3E%3CMobile%3E%3C/Mobile%3E%3CCarparkID%3E%3C/CarparkID%3E%3C/at
tributes%3E&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 36830
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:05:03 GMT
Content-Type: text/plain; charset=utf-8
```

```
{
  "Result": "true",
  "data": [
    {
      "CustID": "19060300000001",
      "CustName": "北京平安联想智慧医疗信息技术有限公司",
      "MobilePhone": null,
      "RoomList": [
        {
          "RoomID": 19060300000158,
          "RoomSign": "B103",
          "RoomName": "B103"
        }
      ],
      "OweCount": 1,
      "OweAmount": 100.00,
      "OweMonth": 0,
      "PrecAmount": 0.00,
      "IncidentCount": 66,
      "TousuCount": 0,
      "RenoStartDate": "2020/8/2 0:00:00",
      "RenoEndDate": "2020/8/6 0:00:00"
    },
    {
      "CustID": "19060300000000",
      "CustName": "平安不动产",
      "MobilePhone": null,
      "RoomList": [
        {

```

```
"RoomID": 19060300000242,
"RoomSign": "10001",
"RoomName": "10001"
},
{
  "RoomID": 19060300000269,
  "RoomSign": "1001",
  "RoomName": "1001"
},
{
  "RoomID": 19060300000234,
  "RoomSign": "101",
  "RoomName": "101"
},
{
  "RoomID": 19060300000087,
  "RoomSign": "101",
  "RoomName": "101"
},
{
  "RoomID": 19060300000171,
  "RoomSign": "10101",
  "RoomName": "10101"
},
{
  "RoomID": 19060300000265,
  "RoomSign": "10102",
  "RoomName": "10102"
},
{
  "RoomID": 19060300000118,
  "RoomSign": "10103",
  "RoomName": "10103"
},
{
  "RoomID": 19060300000079,
  "RoomSign": "10104",
  "RoomName": "10104"
},
{
  "RoomID": 19060300000200,
  "RoomSign": "10201",
  "RoomName": "10201"
},
{
  "RoomID": 19060300000243,
  "RoomSign": "10301",
  "RoomName": "10301"
},
{
  "RoomID": 19060300000220,
  "RoomSign": "10302",
  "RoomName": "10302"
},
{
  "RoomID": 19060300000134,
  "RoomSign": "10303",
  "RoomName": "10303"
},
{
  "RoomID": 19060300000278,
  "RoomSign": "10304",
  "RoomName": "10304"
},
{
  "RoomID": 19060300000138,
  "RoomSign": "10305",
  "RoomName": "10305"
},
{
  "RoomID": 19060300000013,
  "RoomSign": "10306",
  "RoomName": "10306"
},
{
  "RoomID": 19060300000170,
  "RoomSign": "10307",
  "RoomName": "10307"
}
```

```
},
{
  "RoomID": 19060300000173,
  "RoomSign": "10308",
  "RoomName": "10308"
},
{
  "RoomID": 19060300000062,
  "RoomSign": "10309",
  "RoomName": "10309"
},
{
  "RoomID": 19060300000235,
  "RoomSign": "10310",
  "RoomName": "10310"
},
{
  "RoomID": 19060300000193,
  "RoomSign": "10311",
  "RoomName": "10311"
},
{
  "RoomID": 19060300000139,
  "RoomSign": "10312",
  "RoomName": "10312"
},
{
  "RoomID": 19060300000221,
  "RoomSign": "1040104",
  "RoomName": "1040104"
},
{
  "RoomID": 19060300000106,
  "RoomSign": "104F0203",
  "RoomName": "104F0203"
},
{
  "RoomID": 19060300000203,
  "RoomSign": "10501",
  "RoomName": "10501"
},
{
  "RoomID": 19060300000286,
  "RoomSign": "10502",
  "RoomName": "10502"
},
{
  "RoomID": 19060300000006,
  "RoomSign": "10503",
  "RoomName": "10503"
},
{
  "RoomID": 19060300000086,
  "RoomSign": "10601",
  "RoomName": "10601"
},
{
  "RoomID": 190603000001
```

...
...
...

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->Type (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentCanDiscard&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CType%3E1%3C/Type%3E%3C/attributes%3E&Class=IncidentAcceptManage_b1&Mac=bae00b
e940aeb4d37b668c2bcb2d67db HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 41
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:06:10 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": 1, "TotalCount": 0}
```

问题 48 / 90

TOC

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->CloseSituation (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentDelete&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CUserCode%3E
001349%3C/UserCode%3E%3CCommID%3E190603%3C/CommID%3E%3CIncidentID%3E19060300000026993%3C/Inciden
tID%3E%3CCloseSituation%3Euhh%3C/CloseSituation%3E%3CType%3Enull%3C/Type%3E%3C/attributes%3E&Clas
s=IncidentAcceptManage_jh&Mac=ccbc884fa4d7c5095af13fce4029874e HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:06:31 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "废弃成功", "TotalCount": 0}
```

问题 49 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->CorpTypeID (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetCanDealIncidentUserListWhenTransmit&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CA
ccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E19060300000026994%3C/IncidentID%3E%3CCorpTypeID%3E10000011%3C/
CorpTypeID%3E%3C/attributes%3E&Class=IncidentAcceptManage_bl&Mac=a6220a85ce7d9742bca8e3df980120d4
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 14127
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:11:32 GMT
Content-Type: text/plain; charset=utf-8

```
{
  "Result": "true",
  "data": [
    {
      "UserCode": "001345",
      "RoleName": "系统管理",
      "CommID": 190603,
      "UserName": "天问推送测试账号",
      "Tip": "#处理岗位#",
      "IncidentCount": "1",
      {
        "UserCode": "001284",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "尹华政",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001282",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "测试004",
        "Tip": "#处理岗位#",
        "IncidentCount": "4",
      },
      {
        "UserCode": "001285",
        "RoleName": "系统管理,通用环境管理员",
        "CommID": 190603,
        "UserName": "黄桂凤",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001296",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问测试员",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001344",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "test007",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001293",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "城市",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001348",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问推送的账号",
        "Tip": "#处理岗位#",
        "IncidentCount": "18",
      },
      {
        "UserCode": "001266",
        "RoleName": "系统管理,通用秩序员",
        "CommID": 190603,
        "UserName": "吴昊",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001351",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "查涛",
        "Tip": "#处理岗位#",
        "IncidentCount": "3",
      },
      {
        "UserCode": "001265",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "张亮",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001268",
        "RoleName": "系统管理,通用环境管理员",
        "CommID": 190603,
        "UserName": "天问测试账号",
        "Tip": "#处理岗位#",
        "IncidentCount": "4",
      },
      {
        "UserCode": "001271",
        "RoleName": "强电班通用岗位,系统管理",
        "CommID": 190603,
        "UserName": "王勇",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001269",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "测试003",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001350",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "张一明",
        "Tip": "#处理岗位#",
        "IncidentCount": "6",
      },
      {
        "UserCode": "001329",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "测试",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001303",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问测试账户10",
        "Tip": "#处理岗位#",
        "IncidentCount": "8",
      },
      {
        "UserCode": "001302",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问最新测试账号",
        "Tip": "#处理岗位#",
        "IncidentCount": "1",
      },
      {
        "UserCode": "001306",
        "RoleName": "系统管理,通用环境管理员",
        "CommID": 190603,
        "UserName": "天问测试12",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001317",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "tw508",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001326",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "twbn",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001307",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问测试13",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001331",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "ttww",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001298",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "测试验证员",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001343",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "邓聪二号",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001297",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问测试人员",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001299",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问最新测试员",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001301",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问测试账号3",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001300",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "天问测试账号2",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001342",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "邓聪",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001148",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "admin1",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001355",
        "RoleName": "空调通用岗位,系统管理",
        "CommID": 190603,
        "UserName": "范欢欢",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "000843",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "WANGHONGLIANG529",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001354",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "查涛UM",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001171",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "蔡基敏",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "000567",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "zhangkai021",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "001358",
        "RoleName": "空调通用岗位,系统管理",
        "CommID": 190603,
        "UserName": "getan",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      },
      {
        "UserCode": "000841",
        "RoleName": "系统管理",
        "CommID": 190603,
        "UserName": "test007",
        "Tip": "#处理岗位#",
        "IncidentCount": "0"
      }
    ]
  }
}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->DealMan (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentTransmit&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E19060300000026994%3C/IncidentID%3E%3CBigCorpTypeID%3E100000011%
3C/BigCorpTypeID%3E%3CDuty%3E%789%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CDealMan%3E%5%A4%A9%E9%97%A
E%E6%8E%A8%E9%80%81%E6%B5%8B%E8%AF%95%E8%B4%A6%E5%8F%B7%3C/DealMan%3E%3CDealManUserCode%3E001345%
3C/DealManUserCode%3E%3CTransmitReason%3Eghh%3C/TransmitReason%3E%3CConfirmTransmit%3E0%3C/Confir
mTransmit%3E%3C/attributes%3E&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcha
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:11:54 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"转发成功"}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->BigCorpTypeID (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentTransmit&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026994%3C/IncidentID%3E%3CBigCorpTypeID%3E100000011%
3C/BigCorpTypeID%3E%3CDuty%3E%3E7%89%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CDealMan%3E%3E5%A4%A9%E9%97%A
E%E6%8E%A8%E9%80%81%E6%B5%8B%E8%AF%95%E8%B4%A6%E5%8F%B7%3C/DealMan%3E%3CDealManUserCode%3E001345%
3C/DealManUserCode%3E%3CTransmitReason%3Eghh%3C/TransmitReason%3E%3CConfirmTransmit%3E0%3C/Confir
mTransmit%3E%3C/attributes%3E&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcb
a
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:11:54 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "转发成功"}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->DealManUserCode (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentTransmit&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026994%3C/IncidentID%3E%3CBigCorpTypeID%3E100000011%
3C/BigCorpTypeID%3E%3CDuty%3E%7%89%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CDealMan%3E%5%A4%A9%E9%97%A
E%E6%8E%A8%E9%80%81%E6%B5%8B%E8%AF%95%E8%B4%A6%E5%8F%B7%3C/DealMan%3E%3CDealManUserCode%3E001345%
3C/DealManUserCode%3E%3CTransmitReason%3Eghh%3C/TransmitReason%3E%3CConfirmTransmit%3E0%3C/Confir
mTransmit%3E%3C/attributes%3E&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcb
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:11:54 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "转发成功"}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->ConfirmTransmit (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentTransmit&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026994%3C/IncidentID%3E%3CBigCorpTypeID%3E100000011%
3C/BigCorpTypeID%3E%3CDuty%3E%7%89%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CDealMan%3E%5%A4%A9%E9%97%A
E%E6%8E%A8%E9%80%81%E6%B5%8B%E8%AF%95%E8%B4%A6%E5%8F%B7%3C/DealMan%3E%3CDealManUserCode%3E001345%
3C/DealManUserCode%3E%3CTransmitReason%3Eghh%3C/TransmitReason%3E%3CConfirmTransmit%3E0%3C/Confir
mTransmit%3E%3C/attributes%3E&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcb
a
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:11:54 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "转发成功"}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->TransmitReason (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentTransmit&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026994%3C/IncidentID%3E%3CBigCorpTypeID%3E100000011%
3C/BigCorpTypeID%3E%3CDuty%3E%7%89%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CDealMan%3E%5%A4%A9%E9%97%A
E%E6%8E%A8%E9%80%81%E6%B5%8B%E8%AF%95%E8%B4%A6%E5%8F%B7%3C/DealMan%3E%3CDealManUserCode%3E001345%
3C/DealManUserCode%3E%3CTransmitReason%3Eghh%3C/TransmitReason%3E%3CConfirmTransmit%3E0%3C/Confir
mTransmit%3E%3C/attributes%3E&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcb
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:11:54 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "转发成功"}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->OpType (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentCloseList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
06033C/CommID%3E%3COpType%3E1%3C/OpType%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/Pa
geSize%3E%3C/attributes%3E&Class=IncidentAcceptManage_bl&Mac=fd51e08a61fe1c2663062f56829afd36
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 6787
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:14:49 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": "190603000000026984", "IncidentNum": "20210820000294", "IncidentPlace": "户
内", "IncidentSource": "客户报事", "IncidentContent": "客梯", "IncidentDate": "2021/8/20
13:59:00", "ReserveDate": "2021/8/20 13:59:00", "Phone": "18482129036", "DealMan": "天问推送的账
号", "DealManCode": "001348", "IsTouSu": 0, "IsTouSuName": "否", "BigCorpTypeID": "100000015", "BigCorpTyp
eCode": "0008", "BigTypeName": "强电
类", "FineCorpTypeID": "100000132", "FineCorpTypeCode": "00080004", "FineTypeName": "其
他", "RegionalPlace": null, "DrClass": 1, "Duty": "物业
类", "CustID": "190603000000000", "RoomID": "19060300000231", "RoomSign": "8603", "RoomName": "8603", "CanC
lose": 1, "CanFollow": 1, "RN": "1"},
{"IncidentID": "190603000000026983", "IncidentNum": "20210802000293", "IncidentPlace": "公
区", "IncidentSource": "客户报事", "IncidentContent": "123456", "IncidentDate": "2021/8/2
22:24:11", "ReserveDate": "2021/8/2 22:53:00", "Phone": "18384245885", "DealMan": "天问测试账户
10", "DealManCode": "001303", "IsTouSu": 0, "IsTouSuName": "否", "BigCorpTypeID": "100000011", "BigCorpTyp
eCode": "0004", "BigTypeName": "环境卫
生", "FineCorpTypeID": "100000114", "FineCorpTypeCode": "00040002", "FineTypeName": "开
关", "RegionalPlace": "100F", "DrClass": 1, "Duty": "物业
类", "CustID": "190603000000000", "RoomID": "19060300000265", "RoomSign": "10102", "RoomName": "10102", "Ca
nClose": 1, "CanFollow": 1, "RN": "2"},
{"IncidentID": "190603000000026977", "IncidentNum": "20210730000287", "IncidentPlace": "户
内", "IncidentSource": "客户报事", "IncidentContent": "1001212", "IncidentDate": "2021/7/30
16:10:03", "ReserveDate": "2021/7/30 16:39:45", "Phone": "13823456789", "DealMan": "刘
涛", "DealManCode": "001352", "IsTouSu": 0, "IsTouSuName": "否", "BigCorpTypeID": "100000014", "BigCorpTyp
eCode": "0007", "BigTypeName": "弱电
类", "FineCorpTypeID": "100000126", "FineCorpTypeCode": "00070003", "FineTypeName": "停水及水
小", "RegionalPlace": null, "DrClass": 1, "Duty": "物业
类", "CustID": "190603000000000", "RoomID": "19060300000172", "RoomSign": "7102", "RoomName": "7102", "CanC
lose": 1, "CanFollow": 1, "RN": "3"},
{"IncidentID": "190603000000026976", "IncidentNum": "20210730000286", "IncidentPlace": "户
内", "IncidentSource": "客户报
```



```

%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeeper%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState%3E%3E5%85%A8%E9%83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E10%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":
[{"IncidentID":190603000000026994,"IncidentNum":"20211208000304","CommName":"深圳平安金融中心","CustName":null,"RoomID":0,"RoomSign":null,"RoomName":null,"RegionalID":1906030000000005,"RegionalPlace":"100F","LocalePosition":"西","LocaleFunction":"VIP卫生间","IncidentPlace":"公区","IncidentSource":"自查报事","IncidentMan":"天问的测试账号","IncidentDate":"2021-12-08 15:04:14","IncidentContent":"hjj","TaskType":null,"BigTypeName":"环境卫生","Duty":"物业类","ReserveDate":"2021-12-08 15:04:14","DealMan":"天问推送测试账号","Phone":"17790506691","NoNormalCloseReasons":null,"CloseType":null,"IncidentDealStateName":"已分派","RN":1},{IncidentID":190603000000026993,"IncidentNum":"20211208000303","CommName":"深圳平安金融中心","CustName":"平安不动产","RoomID":190603000000096,"RoomSign":"B3联通","RoomName":"B3联通","RegionalID":0,"RegionalPlace":null,"LocalePosition":null,"LocaleFunction":null,"IncidentPlace":"户内","IncidentSource":"客户报事","IncidentMan":"平安不动产","IncidentDate":"2021-12-08 15:02:33","IncidentContent":"ghgg","TaskType":null,"BigTypeName":"环境卫生","Duty":"物业类","ReserveDate":"2021-12-08 15:27:10","DealMan":null,"Phone":"1355665555","NoNormalCloseReasons":null,"CloseType":null,"IncidentDealStateName":"已废弃","RN":2},{IncidentID":190603000000026992,"IncidentNum":"20211207000302","CommName":"深圳平安金融中心","CustName":"深圳前海弘大嘉豪资本管理有限公司","RoomID":1906030000000265,"RoomSign":"10102","RoomName":"10102","RegionalID":1906030000000067,"RegionalPlace":"46F","LocalePosition":null,"LocaleFunction":null,"IncidentPlace":"公区","IncidentSource":"客户报事","IncidentMan":"深圳前海弘大嘉豪资本管理有限公司","IncidentDate":"2021-12-07 09:23:46","IncidentContent":"客梯","TaskType":null,"BigTypeName":"电梯","Duty":"物业类","ReserveDate":"2021-12-07 09:23:46","DealMan":"admins","Phone":"13618162586","NoNormalCloseReasons":null,"CloseType":null,"IncidentDealStateName":"已分派","RN":3}],{"TotalCount":0,"PageCount":0,"Count":3}

```

问题 57 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Attribute->attributes->CancleReasons (Parameter)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值:

发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentCancleFinish&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026984%3C/IncidentID%3E%3CCancleReasons%3Eyhghg%3C/Ca
ncleReasons%3E%3C/attributes%3E&Class=IncidentAcceptManage_jh&Mac=0752786ccd8849ecccl11206f0bd2543
6 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:15:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "退回成功", "TotalCount": 0}
```

问题 58 / 90

TOC

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->IsClose (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentClose&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026983%3C/IncidentID%3E%3CCloseSituation%3Ehhh%3C/Cl
oseSituation%3E%3CCloseType%3E0%3C/CloseType%3E%3CIsClose%3E1%3C/IsClose%3E%3CCloseReasons%3E%3C/
CloseReasons%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
```

```

Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:16:03 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "关闭成功", "TotalCount": 0}

```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->DealEndTime (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E5%85%A8%E9%83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": "190603000000026994", "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": "1906030000000005", "Reg

```

```
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": 1, {"IncidentID": 19060300000026993, "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": 19060300000096, "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "Incid
entDealStateName": "已废弃", "RN": 2},
{"IncidentID": 19060300000026992, "IncidentNum": "20211207000302", "CommName": "深圳平安金融中
心", "CustName": "深圳前海弘大嘉豪资本管理有限公
司", "RoomID": 190603000000265, "RoomSign": "10102", "RoomName": "10102", "RegionalID": 1906030000000067, "
RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公
区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-
12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业
类", "ReserveDate": "2021-12-07
09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "
IncidentDealStateName": "已分派", "RN": 3}], "TotalCount": 0, "PageCount": 0, "Count": 3}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->CloseType (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentClose&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906-
twzxcS19%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E19060300000026983%3C/IncidentID%3E%3CCloseSituation%3Ehh%3C/Cl
oseSituation%3E%3CCloseType%3E0%3C/CloseType%3E%3CIsClose%3E1%3C/IsClose%3E%3CCloseReasons%3E%3C/
CloseReasons%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
```

```
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:16:03 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "关闭成功", "TotalCount": 0}
```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->CloseReasons (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentClose&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E19060300000026983%3C/IncidentID%3E%3CCloseSituation%3Ehhh%3C/Cl
oseSituation%3E%3CCloseType%3E0%3C/CloseType%3E%3CIsClose%3E%3C/IsClose%3E%3CCloseReasons%3E%3C/
CloseReasons%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:16:03 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "关闭成功", "TotalCount": 0}
```


SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->DealStartTime (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E585A8E983%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pagSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data":
[ { "IncidentID": "190603000000026994", "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": "0", "RoomSign": null, "RoomName": null, "RegionalID": "1906030000000005", "Reg
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": "1", { "IncidentID": "190603000000026993", "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": "1906030000000096", "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": "0", "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
```



```

15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已废弃", "RN": 2},
{"IncidentID": 19060300000026992, "IncidentNum": "20211207000302", "CommName": "深圳平安金融中心", "CustName": "深圳前海弘大嘉豪资本管理有限公司", "RoomID": 19060300000265, "RoomSign": "10102", "RoomName": "10102", "RegionalID": 1906030000000067, "RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业类", "ReserveDate": "2021-12-07 09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已分派", "RN": 3}}, {"TotalCount": 0, "PageCount": 0, "Count": 3}

```

问题 64 / 90

TOC

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->AdmiMan (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906-
twzxc%3CAccount%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E%85%A8%E9%83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": 19060300000026994, "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": 1906030000000005, "Reg

```

```
ionalPlace":"100F","LocalePosition":"西","LocaleFunction":"VIP卫生间","IncidentPlace":"公
区","IncidentSource":"自查报事","IncidentMan":"天问的测试账号","IncidentDate":"2021-12-08
15:04:14","IncidentContent":"hjj","TaskType":null,"BigTypeName":"环境卫生","Duty":"物业
类","ReserveDate":"2021-12-08 15:04:14","DealMan":"天问推送测试账
号","Phone":"17790506691","NoNormalCloseReasons":null,"CloseType":null,"IncidentDealStateName":"
已分派","RN":1},{ "IncidentID":19060300000026993,"IncidentNum":"20211208000303","CommName":"深圳平
安金融中心","CustName":"平安不动产","RoomID":19060300000096,"RoomSign":"B3联通","RoomName":"B3联
通","RegionalID":0,"RegionalPlace":null,"LocalePosition":null,"LocaleFunction":null,"IncidentPlac
e":"户内","IncidentSource":"客户报事","IncidentMan":"平安不动产","IncidentDate":"2021-12-08
15:02:33","IncidentContent":"ghgg","TaskType":null,"BigTypeName":"环境卫生","Duty":"物业
类","ReserveDate":"2021-12-08
15:27:10","DealMan":null,"Phone":"1355665555","NoNormalCloseReasons":null,"CloseType":null,"Incid
entDealStateName":"已废弃","RN":2},
{ "IncidentID":19060300000026992,"IncidentNum":"20211207000302","CommName":"深圳平安金融中
心","CustName":"深圳前海弘大嘉豪资本管理有限公
司","RoomID":190603000000265,"RoomSign":"10102","RoomName":"10102","RegionalID":1906030000000067,"
RegionalPlace":"46F","LocalePosition":null,"LocaleFunction":null,"IncidentPlace":"公
区","IncidentSource":"客户报事","IncidentMan":"深圳前海弘大嘉豪资本管理有限公司","IncidentDate":"2021-
12-07 09:23:46","IncidentContent":"客梯","TaskType":null,"BigTypeName":"电梯","Duty":"物业
类","ReserveDate":"2021-12-07
09:23:46","DealMan":"admins","Phone":"13618162586","NoNormalCloseReasons":null,"CloseType":null,"
IncidentDealStateName":"已分派","RN":3}], "TotalCount":0, "PageCount":0, "Count":3}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->pageSize (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcxs19%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E5%85%A8%3E%3E83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
```

```

Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": 19060300000026994, "IncidentNum": "20211208000304", "CommName": "深圳平安金融中心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": 1906030000000005, "RegionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08 15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已分派", "RN": 1}, {"IncidentID": 19060300000026993, "IncidentNum": "20211208000303", "CommName": "深圳平安金融中心", "CustName": "平安不动产", "RoomID": 190603000000096, "RoomSign": "B3联通", "RoomName": "B3联通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08 15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业类", "ReserveDate": "2021-12-08 15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已废弃", "RN": 2}, {"IncidentID": 19060300000026992, "IncidentNum": "20211207000302", "CommName": "深圳平安金融中心", "CustName": "深圳前海弘大嘉豪资本管理有限公司", "RoomID": 190603000000265, "RoomSign": "10102", "RoomName": "10102", "RegionalID": 1906030000000067, "RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业类", "ReserveDate": "2021-12-07 09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已分派", "RN": 3}], "TotalCount": 0, "PageCount": 0, "Count": 3}

```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->StartTime (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E%3E1906-
twzxc%3E%3CLoginPwd%3E%3CE61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CStartTime%3E%3E2021-12-01%3E%3E00:00:00%3C/StartTime%3E%3CEndTime%3E%3E2021-12-
31%3E%3E59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E%3C/DrClass%3E%3CIsTousu%3E%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState

```

```

%3E%E5%85%A8%E9%83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSi ze%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": "19060300000026994", "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": "1906030000000005", "Reg
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": 1}, {"IncidentID": "19060300000026993", "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": "190603000000096", "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "Incid
entDealStateName": "已废弃", "RN": 2},
{"IncidentID": "190603000000026992", "IncidentNum": "20211207000302", "CommName": "深圳平安金融中
心", "CustName": "深圳前海弘大嘉豪资本管理有限公
司", "RoomID": "190603000000265", "RoomSign": "10102", "RoomName": "10102", "RegionalID": "1906030000000067", "
RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公
区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-
12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业
类", "ReserveDate": "2021-12-07
09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "
IncidentDealStateName": "已分派", "RN": 3}], "TotalCount": 0, "PageCount": 0, "Count": 3}

```

SSL 请求中的查询参数	
严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->HouseKeeper (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%58%5A8%983%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": 190603000000026994, "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": 1906030000000005, "Reg
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": 1}, {"IncidentID": 190603000000026993, "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": 190603000000096, "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "Incid
entDealStateName": "已废弃", "RN": 2}, {"IncidentID": 190603000000026992, "IncidentNum": "20211207000302", "CommName": "深圳平安金融中
心", "CustName": "深圳前海弘大嘉豪资本管理有限公
司", "RoomID": 190603000000265, "RoomSign": "10102", "RoomName": "10102", "RegionalID": 1906030000000067, "
RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公
区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-
12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业
类", "ReserveDate": "2021-12-07
09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "
IncidentDealStateName": "已分派", "RN": 3}], "TotalCount": 0, "PageCount": 0, "Count": 3}
```

SSL 请求中的查询参数

严重性: **低**

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->TaskCategory (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxc519%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E85%A8%E9%83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": "190603000000026994", "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": "0", "RoomSign": null, "RoomName": null, "RegionalID": "1906030000000005", "Reg
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": "1"}, {"IncidentID": "190603000000026993", "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": "190603000000096", "RoomSign": "E3联通", "RoomName": "E3联
通", "RegionalID": "0", "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "Incid
entDealStateName": "已废弃", "RN": "2"}, {"IncidentID": "190603000000026992", "IncidentNum": "20211207000302", "CommName": "深圳平安金融中
心", "CustName": "深圳前海弘大嘉豪资本管理有限公
司", "RoomID": "1906030000000265", "RoomSign": "10102", "RoomName": "10102", "RegionalID": "1906030000000067", "
RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公
区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-
12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业
类", "ReserveDate": "2021-12-07
09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "
IncidentDealStateName": "已分派", "RN": "3"}], "TotalCount": "0", "PageCount": "0", "Count": "3"}
```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->IncidentState (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%2000:00:00%3C/StartTime%3E%3CEndTime%3E2021-12-
31%2023:59:59%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E585A8E983A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pagSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data":
[ { "IncidentID": "190603000000026994", "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": "0", "RoomSign": null, "RoomName": null, "RegionalID": "1906030000000005", "Reg
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": "1", { "IncidentID": "190603000000026993", "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": "1906030000000096", "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": "0", "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
```



```

15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已废弃", "RN": 2},
{"IncidentID": 190603000000026992, "IncidentNum": "20211207000302", "CommName": "深圳平安金融中心", "CustName": "深圳前海弘大嘉豪资本管理有限公司", "RoomID": 19060300000265, "RoomSign": "10102", "RoomName": "10102", "RegionalID": 1906030000000067, "RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业", "ReserveDate": "2021-12-07 09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已分派", "RN": 3}}, {"TotalCount": 0, "PageCount": 0, "Count": 3}

```

问题 70 / 90

TOC

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->RegionalID (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E%3E1906-
twzxc%3E%3CLoginPwd%3E%3C61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E%3E19
0603%3C/CommID%3E%3CStartTime%3E%3C2021-12-01%3C/StartTime%3E%3CEndTime%3E%3C2021-12-
31%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim
e%3E%3CDrClass%3E%3C/DrClass%3E%3CIsTousu%3E%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E
%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeep
er%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState
%3E%3E5%85%A8%983%A8%3C/IncidentState%3E%3CpageIndex%20%3E%3C/pageIndex%20%3E%3CpageSize%20%3E1
0%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 2125
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": 190603000000026994, "IncidentNum": "20211208000304", "CommName": "深圳平安金融中
心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": 1906030000000005, "Reg

```



```
ionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公
区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08
15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账
号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "
已分派", "RN": 1}, {"IncidentID": 19060300000026993, "IncidentNum": "20211208000303", "CommName": "深圳平
安金融中心", "CustName": "平安不动产", "RoomID": 19060300000096, "RoomSign": "B3联通", "RoomName": "B3联
通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlac
e": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08
15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业
类", "ReserveDate": "2021-12-08
15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "Incid
entDealStateName": "已废弃", "RN": 2},
{"IncidentID": 19060300000026992, "IncidentNum": "20211207000302", "CommName": "深圳平安金融中
心", "CustName": "深圳前海弘大嘉豪资本管理有限公
司", "RoomID": 190603000000265, "RoomSign": "10102", "RoomName": "10102", "RegionalID": 1906030000000067, "
RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公
区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-
12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业
类", "ReserveDate": "2021-12-07
09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "
IncidentDealStateName": "已分派", "RN": 3}], "TotalCount": 0, "PageCount": 0, "Count": 3}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->EquipmentID (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=SearchEquipment&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CEquipmentID%3Ehhhh%3C/EquipmentID%3E%3CEqu
ipmentName%3E%3C/EquipmentName%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%
3C/attributes%3E&Class=EquipmentManage_bl&Mac=e34cf53132ec0d4723a610051e99165c HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 56
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
```

```
Date: Wed, 08 Dec 2021 07:22:20 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "pageCount": "1", "counts": "0", "data": []}
```

SSL 请求中的查询参数

严重性: **低**

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->Step (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentWarningList&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStep%3E1%3C/Step%3E%3CPageSize%3E10%3C/PageSize%3E%3CPageIndex%3E1%3C/PageInd
ex%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=4eeb7891784e345c8d834fb81ccb5efd HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 6117
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:19:21 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data":
[{"IncidentID": "19064400000000027", "IncidentNum": "20211129000027", "IncidentSource": "微信小程序报
事", "CommID": "190644", "CommName": "上海平安大
厦", "RoomID": null, "RoomName": null, "RoomSign": null, "RegionalID": "1906440000000003", "RegionalPlace":
"南部走廊", "DealSituation": null, "DispLimit": "0.03", "DealLimit": "0", "ReplyLimit": null, "Duty": "物业
类", "IsTousu": "0", "IncidentMan": "查涛", "IncidentMode": "业主APP/微信", "IncidentDate": "2021/11/29
10:36:04", "IncidentPlace": "公
区", "IncidentContent": "1", "Phone": "15021758341", "DispDate": null, "ReserveDate": "2021/11/29
10:36:04", "ReceivingDate": null, "ArriveDate": null, "FinishDate": null, "CloseTime": null, "BigCorpTypeI
D": "100000103", "BigTypeName": "其他", "TypeName": "其
他", "DispMan": null, "DispManMobile": null, "DealMan": null, "DealManMobile": null, "FinishUser": null, "Fi
nishManMobile": null, "CloseUser": null, "CloseManMobile": null, "ReplyMan": null, "ReplyManMobile": null,
"ReplyContent": null, "ReplyDate": null, "IncidentDealStateName": "未分派", "RN": "1"},
{"IncidentID": "190603000000026990", "IncidentNum": "20211126000300", "IncidentSource": "客户报
事", "CommID": "190603", "CommName": "深圳平安金融中
心", "RoomID": "19060300000269", "RoomName": "1001", "RoomSign": "1001", "RegionalID": "0", "RegionalPlace
```

```

":null,"DealSituation":null,"DispLimit":0.10,"DealLimit":0,"ReplyLimit":null,"Duty":"物业
类","IsTousu":0,"IncidentMan":"平安不动产","IncidentMode":"项目受理","IncidentDate":"2021/11/26
16:59:49","IncidentPlace":"户
内","IncidentContent":"ces","Phone":"13567890987","DispDate":null,"ReserveDate":"2021/11/26
16:59:49","ReceivingDate":null,"ArriveData":null,"FinishDate":null,"CloseTime":null,"BigCorpTypeI
D":"100000015","BigTypeName":"强电类","TypeName":"强电
类","DispMan":null,"DispManMobile":null,"DealMan":null,"DealManMobile":null,"FinishUser":null,"Fi
nishManMobile":null,"CloseUser":null,"CloseManMobile":null,"ReplyMan":null,"ReplyManMobile":null,
"ReplyContent":null,"ReplyDate":null,"IncidentDealStateName":"未分派","RN":"2"},
{"IncidentID":"19060300000026989","IncidentNum":"20211126000299","IncidentSource":"客户报
事","CommID":190603,"CommName":"深圳平安金融中
心","RoomID":"19060300000242","RoomName":"10001","RoomSign":"10001","RegionalID":0,"RegionalPla
ce":null,"DealSituation":null,"DispLimit":0.05,"DealLimit":0,"ReplyLimit":null,"Duty":"物业
类","IsTousu":0,"IncidentMan":"青岛律翼管理咨询有限责任公司","IncidentMode":"项目受
理","IncidentDate":"2021/11/26 16:58:08","IncidentPlace":"户内","IncidentContent":"ces
","Phone":"13567890987","DispDate":null,"ReserveDate":"2021/11/26
16:58:08","ReceivingDate":null,"ArriveData":null,"FinishDate":null,"CloseTime":null,"BigCorpTypeI
D":"100000014","BigTypeName":"弱电类","TypeName":"弱电
类","DispMan":null,"DispManMobile":null,"DealMan":null,"DealManMobile":null,"FinishUser":null,"Fi
nishManMobile":null,"CloseUser":null,"CloseManMobile":null,"ReplyMan":null,"ReplyManMobile":null,
"ReplyContent":null,"ReplyDate":null,"IncidentDealStateName":"未分派","RN":"3"},
{"IncidentID":"19064400000000024","IncidentNum":"20211125000024","IncidentSource":"微信小程序报
事","CommID":190644,"CommName":"上海平安大
厦","RoomID":null,"RoomName":null,"RoomSign":null,"RegionalID":"1906440000000001","RegionalPlace
":"东部大厅","DealSituation":null,"DispLimit":0.03,"DealLimit":0,"ReplyLimit":null,"Duty":"物业
类","IsTousu":0,"IncidentMan":"查涛","IncidentMode":"业主APP/微信","IncidentDate":"2021/11/25
15:23:46","IncidentPlace":"公
区","IncidentContent":"1","Phone":"15021758341","DispDate":null,"ReserveDate":"2021/11/25
15:23:46","ReceivingDate":null,"ArriveData":null,"FinishDate":null,"CloseTime":null,"BigCorpTypeI
D":"100000103","BigTypeName":"其他","TypeName":"其
他","DispMan":null,"DispManMobile":null,"DealMan":null,"DealManMobile":null,"FinishUser":null,"Fi
nishManMobile":null,"CloseUser":null,"CloseManMobile":null,"ReplyMan":null,"ReplyManMobile":null,
"ReplyContent":null,"ReplyDate":null,"IncidentDealStateName":"未分派","RN":"4"},
{"IncidentID":"19064400000000023","IncidentNum":"20211125000023","IncidentSource":"微信小程序报
事","CommID":190644,"CommName":"上海平安大
厦","RoomID":null,"RoomName":null,"RoomSign":null,"RegionalID":"1906440000000001","RegionalPlace
":"东部大厅","DealSituation":null,"DispLimit":0.03,"DealLimit":0,"ReplyLimit":null,"Duty":"物业
类","IsTousu":0,"IncidentMan":"查涛","IncidentMode":"业主APP/微信","IncidentDate":"2021/11/25
11:20:04","IncidentPlace":"公区","IncidentContent":"1","Phone":
...
...
...

```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->BuildSNum (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetFloorRoomList&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3C CorpID%3E19
06%3C/CorpID%3E%3CBuildSNum%3E1%3C/BuildSNum%3E%3CUnitSNum%3E1%3C/UnitSNum%3E%3CFloorNum%3E-
3%3C/FloorNum%3E%3CCommID%3E190603%3C/CommID%3E%3C/attributes%3E&Class=RoomManage&Mac=411f404a421
68ecc955c5979d4e0db58 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1165
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:22:49 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"RoomID": "19060300000096", "RoomSign": "B3联通", "RoomName": "B3联
通", "CustID": "19060300000000", "CustName": "平安不动
产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000096", "RoomSign": "B3联
通", "RoomName": "B3联通", "CustID": "19060300000097", "CustName": "中国联合网络通信有限公司深圳市分公
司", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000154", "RoomSign": "B3移
动", "RoomName": "B3移动", "CustID": "19060300000000", "CustName": "平安不动
产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000089", "RoomSign": "B3铁
塔", "RoomName": "B3铁塔", "CustID": "19060300000000", "CustName": "平安不动
产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}]}

```

问题 74 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->pageIndex (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=%3Cattributes%3E%3CNet%3E%3CNet%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CStartTime%3E2021-12-01%3C/StartTime%3E%3CEndTime%3E2021-12-
31%3C/EndTime%3E%3CDealStartTime%3E%3C/DealStartTime%3E%3CDealEndTime%3E%3C/DealEndTim

```

```
e%3E%3CDrClass%3E0%3C/DrClass%3E%3CIsTousu%3E0%3C/IsTousu%3E%3CTaskCategory%3E%3C/TaskCategory%3E%3CDealState%3E%3C/DealState%3E%3CAdmiMan%3E%3C/AdmiMan%3E%3CDealMan%3E%3C/DealMan%3E%3CHouseKeeper%3E%3C/HouseKeeper%3E%3CRoomID%3E%3C/RoomID%3E%3CRegionalID%3E%3C/RegionalID%3E%3CIncidentState%3E%3E5%85%A8%E9%83%A8%3C/IncidentState%3E%3CpageIndex%20%3E1%3C/pageIndex%20%3E%3CpageSize%20%3E10%3C/pageSize%20%3E%3C/attributes%3E&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c HTTP/1.1
```

```
User-Agent: okhttp/3.6.0  
Connection: Keep-Alive  
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK  
Connection: keep-alive  
Server: Microsoft-IIS/10.0  
Access-Control-Allow-Origin: *  
Content-Length: 2125  
X-AspNet-Version: 4.0.30319  
Cache-Control: private  
X-Powered-By: ASP.NET  
Date: Wed, 08 Dec 2021 07:19:06 GMT  
Content-Type: text/plain; charset=utf-8
```

```
{"Result": "true", "data":  
[{"IncidentID": "190603000000026994", "IncidentNum": "20211208000304", "CommName": "深圳平安金融中心", "CustName": null, "RoomID": 0, "RoomSign": null, "RoomName": null, "RegionalID": "1906030000000005", "RegionalPlace": "100F", "LocalePosition": "西", "LocaleFunction": "VIP卫生间", "IncidentPlace": "公区", "IncidentSource": "自查报事", "IncidentMan": "天问的测试账号", "IncidentDate": "2021-12-08 15:04:14", "IncidentContent": "hjj", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业类", "ReserveDate": "2021-12-08 15:04:14", "DealMan": "天问推送测试账号", "Phone": "17790506691", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已分派", "RN": 1}, {"IncidentID": "190603000000026993", "IncidentNum": "20211208000303", "CommName": "深圳平安金融中心", "CustName": "平安不动产", "RoomID": "190603000000096", "RoomSign": "B3联通", "RoomName": "B3联通", "RegionalID": 0, "RegionalPlace": null, "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "户内", "IncidentSource": "客户报事", "IncidentMan": "平安不动产", "IncidentDate": "2021-12-08 15:02:33", "IncidentContent": "ghgg", "TaskType": null, "BigTypeName": "环境卫生", "Duty": "物业类", "ReserveDate": "2021-12-08 15:27:10", "DealMan": null, "Phone": "1355665555", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已废弃", "RN": 2}, {"IncidentID": "190603000000026992", "IncidentNum": "20211207000302", "CommName": "深圳平安金融中心", "CustName": "深圳前海弘大嘉豪资本管理有限公司", "RoomID": "190603000000265", "RoomSign": "10102", "RoomName": "10102", "RegionalID": "1906030000000067", "RegionalPlace": "46F", "LocalePosition": null, "LocaleFunction": null, "IncidentPlace": "公区", "IncidentSource": "客户报事", "IncidentMan": "深圳前海弘大嘉豪资本管理有限公司", "IncidentDate": "2021-12-07 09:23:46", "IncidentContent": "客梯", "TaskType": null, "BigTypeName": "电梯", "Duty": "物业类", "ReserveDate": "2021-12-07 09:23:46", "DealMan": "admins", "Phone": "13618162586", "NoNormalCloseReasons": null, "CloseType": null, "IncidentDealStateName": "已分派", "RN": 3}], "TotalCount": 0, "PageCount": 0, "Count": 3}
```

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->TaskType (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=DownloadTask_v2&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CTaskType%3E1%3C/TaskType%3E%3C/attributes%3E&Class=EquipmentManage_bl&Mac=439
6f75b39d302c2d066eed03ea15385 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 42
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:10:16 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [], "TotalCount": 0}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->EquipmentName (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=SearchEquipment&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CEquipmentID%3Ehhhh%3C/EquipmentID%3E%3CEqu
ipmentName%3E%3C/EquipmentName%3E%3CPageIndex%3E1%3C/PageIndex%3E%3CPageSize%3E10%3C/PageSize%3E%
3C/attributes%3E&Class=EquipmentManage_bl&Mac=e34cf53132ec0d4723a610051e99165c HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
```

```

Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 56
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:22:20 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "pageCount": "1", "counts": "0", "data": []}

```

问题 77 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->UnitSNum (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=GetFloorRoomList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3C CorpID%3E19
06%3C/CorpID%3E%3CBuildSNum%3E%3C/BuildSNum%3E%3CUnitSNum%3E%3C/UnitSNum%3E%3CFloorNum%3E-
3%3C/FloorNum%3E%3CCommID%3E190603%3C/CommID%3E%3C/attributes%3E&Class=RoomManage&Mac=411f404a421
68ecc955c5979d4e0db58 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1165
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:22:49 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"RoomID": "19060300000096", "RoomSign": "B3联通", "RoomName": "B3联
通", "CustID": "19060300000000", "CustName": "平安不动
产", "MobilePhone": null, "PaperCode": null, "Sex": "1", "BuildSNum": "1", "UnitSNum": "1", "FloorSNum": "-
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000096", "RoomSign": "B3联
通", "RoomName": "B3联通", "CustID": "19060300000097", "CustName": "中国联合网络通信有限公司深圳市分公
司", "MobilePhone": null, "PaperCode": null, "Sex": "1", "BuildSNum": "1", "UnitSNum": "1", "FloorSNum": "-
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000154", "RoomSign": "B3移
动", "RoomName": "B3移动", "CustID": "19060300000000", "CustName": "平安不动
产", "MobilePhone": null, "PaperCode": null, "Sex": "1", "BuildSNum": "1", "UnitSNum": "1", "FloorSNum": "-

```

```
3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000089", "RoomSign": "B3铁塔", "RoomName": "B3铁塔", "CustID": "19060300000000", "CustName": "平安不动产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-3", "BuildName": "平安金融中心北塔", "ContSubDate": null}}}]}
```

问题 78 / 90

TOC

SSL 请求中的查询参数

严重性: 低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->FloorNum (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetFloorRoomList&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E%3C/Account%3E%3CLoginPwd%3E%3C/LoginPwd%3E%3CCorpID%3E%3C/CorpID%3E%3CBuildSNum%3E%3C/BuildSNum%3E%3CUnitSNum%3E%3C/UnitSNum%3E%3CFloorNum%3E%3C/FloorNum%3E%3CCommID%3E%3C/CommID%3E%3C/attributes%3E&Class=RoomManage&Mac=411f404a42168ecc955c5979d4e0db58 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 1165
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:22:49 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data": [{"RoomID": "19060300000096", "RoomSign": "B3联通", "RoomName": "B3联通", "CustID": "19060300000000", "CustName": "平安不动产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000096", "RoomSign": "B3联通", "RoomName": "B3联通", "CustID": "19060300000097", "CustName": "中国联合网络通信有限公司深圳市分公司", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000154", "RoomSign": "B3移动", "RoomName": "B3移动", "CustID": "19060300000000", "CustName": "平安不动产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-3", "BuildName": "平安金融中心北塔", "ContSubDate": null}, {"RoomID": "19060300000089", "RoomSign": "B3铁塔", "RoomName": "B3铁塔", "CustID": "19060300000000", "CustName": "平安不动产", "MobilePhone": null, "PaperCode": null, "Sex": 1, "BuildSNum": 1, "UnitSNum": "1", "FloorSNum": "-3", "BuildName": "平安金融中心北塔", "ContSubDate": null}]}]}
```


SSL 请求中的查询参数	
严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->ListDate (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递，并且可能包含敏感信息
固定值:	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```

GET /TWI/TWInterface/Service/Service.ashx?
Command=PublicMeterInsUpdate&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3CSta
rtDegree%3E1000.00%3C/StartDegree%3E%3CEndDegree%3E2000%3C/EndDegree%3E%3CNewStartDegree%3E%3C/Ne
wStartDegree%3E%3CNewEndDegree%3E%3C/NewEndDegree%3E%3CExtraDosage%3E0.00%3C/ExtraDosage%3E%3CLis
tDate%3E2021-12-
08%3C/ListDate%3E%3C/attributes%3E&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "操作成功"}
    
```

SSL 请求中的查询参数

严重性: **低**

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->MeterID (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetPublicMeterHistory&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CCommID%3E190603%3C/CommID%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3C/attrib
utes%3E&Class=MeterManage&Mac=f040a29fb07a834cb4d45702032d2943 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 447
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:06 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"MeterID": "19060300000004", "MeterSign": "200002", "MeterName": "测试
123", "MeterType": 2, "Ratio": 1.00, "MeterSource": "ERP单户抄表", "MeterPerson": "天问测试账
号", "Location": "A栋楼道", "RestID": "10046", "ListDate": "2021/1/5
0:00:00", "StartDegree": 0.00, "EndDegree": 1000.00, "Dosage": 1000.00, "OldDosage": 0.00, "ExtraDosage": 0
.00, "Price": 1.150000, "Amount": 1150.00, "MeterHint": "无上次抄表", "IsAudit": 0, "IsReverse": 0}]}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->NewEndDegree (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=PublicMeterInsUpdate&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3CSta
rtDegree%3E1000.00%3C/StartDegree%3E%3CEndDegree%3E2000%3C/EndDegree%3E%3CNewStartDegree%3E%3C/Ne
wStartDegree%3E%3CNewEndDegree%3E%3C/NewEndDegree%3E%3CExtraDosage%3E0.00%3C/ExtraDosage%3E%3CLis
tDate%3E2021-12-
08%3C/ListDate%3E%3C/attributes%3E&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdaf1c1b0
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"操作成功"}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->ExtraDosage (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=PublicMeterInsUpdate&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3CSta
rtDegree%3E1000.00%3C/StartDegree%3E%3CEndDegree%3E2000%3C/EndDegree%3E%3CNewStartDegree%3E%3C/Ne
wStartDegree%3E%3CNewEndDegree%3E%3C/NewEndDegree%3E%3CExtraDosage%3E0.00%3C/ExtraDosage%3E%3CLis
tDate%3E2021-12-
08%3C/ListDate%3E%3C/attributes%3E&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdaf1c1b0
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "操作成功"}
```

SSL 请求中的查询参数

严重性: **低**

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->IncidentContent (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSnatchOrAssign&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E190603%3C/CommID%3E%3CIncidentID%3E190603000000026992%3C/IncidentID%3E%3CIncidentContent%3E%5AE%A
2%E6%A2%AF%3C/IncidentContent%3E%3CDuty%3E%E7%89%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CBigCorpTypeID%
3E10000013%3C/BigCorpTypeID%3E%3CDealMan%3Eadmins%3C/DealMan%3E%3CDealManUserCode%3E000131%3C/De
alManUserCode%3E%3CIsSnatch%3E0%3C/IsSnatch%3E%3CAssistant%3E%3C/Assistant%3E%3CRegionalID%3E1906
03000000067%3C/RegionalID%3E%3CDispRemarks%3E%3C/DispRemarks%3E%3C/attributes%3E&Class=IncidentA
cceptManage_bl&Mac=d503c6f0b116af4a2acdbf152eb2be3 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:07:58 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"派单成功","TotalCount":0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->StartDegree (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=PublicMeterInsUpdate&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3CSta
rtDegree%3E1000.00%3C/StartDegree%3E%3CEndDegree%3E2000%3C/EndDegree%3E%3CNewStartDegree%3E%3C/Ne
wStartDegree%3E%3CNewEndDegree%3E%3C/NewEndDegree%3E%3CExtraDosage%3E0.00%3C/ExtraDosage%3E%3CLis
tDate%3E2021-12-
08%3C/ListDate%3E%3C/attributes%3E&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdaf1c1b0
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": "操作成功"}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->EndDegree (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=PublicMeterInsUpdate&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3CSta
rtDegree%3E1000.00%3C/StartDegree%3E%3CEndDegree%3E2000%3C/EndDegree%3E%3CNewStartDegree%3E%3C/Ne
wStartDegree%3E%3CNewEndDegree%3E%3C/NewEndDegree%3E%3CExtraDosage%3E0.00%3C/ExtraDosage%3E%3CLis
tDate%3E2021-12-
08%3C/ListDate%3E%3C/attributes%3E&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdaf1c1b0
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"操作成功"}
```

SSL 请求中的查询参数

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Attribute->attributes->NewStartDegree (Parameter)

风险: 可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因: 查询参数通过 SSL 进行了传递, 并且可能包含敏感信息

固定值: 发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=PublicMeterInsUpdate&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCorpID%3E19
06%3C/CorpID%3E%3CUserCode%3E001349%3C/UserCode%3E%3CMeterID%3E19060300000004%3C/MeterID%3E%3CSta
rtDegree%3E1000.00%3C/StartDegree%3E%3CEndDegree%3E2000%3C/EndDegree%3E%3CNewStartDegree%3E%3C/Ne
wStartDegree%3E%3CNewEndDegree%3E%3C/NewEndDegree%3E%3CExtraDosage%3E0.00%3C/ExtraDosage%3E%3CLis
tDate%3E2021-12-
08%3C/ListDate%3E%3C/attributes%3E&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdaf1c1b0
HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 39
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:24:19 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"操作成功"}
```


SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->DispRemarks (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSnatchOrAssign&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026992%3C/IncidentID%3E%3CIncidentContent%3E%5AE%A
2%E6%A2%AF%3C/IncidentContent%3E%3CDuty%3E%789%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CBigCorpTypeID%
3E10000013%3C/BigCorpTypeID%3E%3CDealMan%3Eadmins%3C/DealMan%3E%3CDealManUserCode%3E000131%3C/De
alManUserCode%3E%3CIsSnatch%3E0%3C/IsSnatch%3E%3CAssistant%3E%3C/Assistant%3E%3CRegionalID%3E1906
03000000067%3C/RegionalID%3E%3CDispRemarks%3E%3C/DispRemarks%3E%3C/attributes%3E&Class=IncidentA
cceptManage_bl&Mac=d503c6f0b116af4a2acdbf152eb2be3 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:07:58 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"派单成功","TotalCount":0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->Assistant (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSnatchOrAssign&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CIncidentID%3E190603000000026992%3C/IncidentID%3E%3CIncidentContent%3E%5AE%A
2%E6%A2%AF%3C/IncidentContent%3E%3CDuty%3E%789%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CBigCorpTypeID%
3E10000013%3C/BigCorpTypeID%3E%3CDealMan%3Eadmins%3C/DealMan%3E%3CDealManUserCode%3E000131%3C/De
alManUserCode%3E%3CIsSnatch%3E0%3C/IsSnatch%3E%3CAssistant%3E%3C/Assistant%3E%3CRegionalID%3E1906
03000000067%3C/RegionalID%3E%3CDispRemarks%3E%3C/DispRemarks%3E%3C/attributes%3E&Class=IncidentA
cceptManage_bl&Mac=d503c6f0b116af4a2acdbf152eb2be3 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:07:58 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"派单成功","TotalCount":0}
```

SSL 请求中的查询参数

严重性:	低
CVSS 分数:	5.0
URL:	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx
实体:	Attribute->attributes->IsSnatch (Parameter)
风险:	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
原因:	查询参数通过 SSL 进行了传递, 并且可能包含敏感信息
固定值:	发送敏感信息时, 始终使用 SSL 和 POST (主体) 参数。

差异:

推理: AppScan 在通过 SSL 发送的 HTTP 请求的查询部分中找到参数。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=IncidentSnatchOrAssign&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E190603%3C/CommID%3E%3CIncidentID%3E190603000000026992%3C/IncidentID%3E%3CIncidentContent%3E%5AE%A
2%E6%A2%AF%3C/IncidentContent%3E%3CDuty%3E%789%A9%E4%B8%9A%E7%B1%BB%3C/Duty%3E%3CBigCorpTypeID%
3E10000013%3C/BigCorpTypeID%3E%3CDealMan%3Eadmins%3C/DealMan%3E%3CDealManUserCode%3E000131%3C/De
alManUserCode%3E%3CIsSnatch%3E0%3C/IsSnatch%3E%3CAssistant%3E%3C/Assistant%3E%3CRegionalID%3E1906
03000000067%3C/RegionalID%3E%3CDispRemarks%3E%3C/DispRemarks%3E%3C/attributes%3E&Class=IncidentA
cceptManage_bl&Mac=d503c6f0b116af4a2acdbf152eb2be3 HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 54
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:07:58 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":"派单成功","TotalCount":0}
```



```

14:26:22", "Phone": "13691787761", "CommName": "深圳平安金融中
心", "RoomID": "19060300000200", "RoomSign": "10201", "RoomName": "10201", "RegionalID": null, "RegionalPl
ace": null, "BigTypeName": "弱电类", "SmallTypeName": null, "ReserveDate": "2021/7/30
14:55:00", "ReserveLimit": null, "DispDate": "2021/7/30
14:28:07", "CoordinateNum": "P20210730000121", "DealLimit": 0, "DealManCode": "000635", "Duty": "物业
类", "ReceivingDate": null, "ArriveData": null, "IsTouSu": 0, "BigCorpTypeID": "100000014", "CanDeal": 0, "R
N": "4"},
{"CommID": "190603", "IncidentID": "190603000000026963", "IncidentNum": "202107300000273", "IncidentConten
t": "3. 处理超时", "IncidentPlace": "户内", "IncidentDate": "2021/7/30
14:02:30", "Phone": "17891602182", "CommName": "深圳平安金融中
心", "RoomID": "19060300000074", "RoomSign": "9201", "RoomName": "9201", "RegionalID": "0", "RegionalPlace
": null, "BigTypeName": "消防类", "SmallTypeName": null, "ReserveDate": "2021/7/30
14:02:30", "ReserveLimit": 0, "DispDate": "2021/7/30
14:02:42", "CoordinateNum": "P20210730000117", "DealLimit": 24, "DealManCode": "000635", "Duty": "物业
类", "ReceivingDate": "2021/7/30
14:03:19", "ArriveData": null, "IsTouSu": 0, "BigCorpTypeID": "100000100", "CanDeal": 0, "RN": "5"},
{"CommID": "190603", "IncidentID": "190603000000026962", "IncidentNum": "202107300000272", "IncidentConten
t": "2. 接单超时", "IncidentPlace": "户内", "IncidentDate": "2021/7/30
14:01:05", "Phone": "17891602182", "CommName": "深圳平安金融中
心", "RoomID": "19060300000074", "RoomSign": "9201", "RoomName": "9201", "RegionalID": "0", "RegionalPlace
": null, "BigTypeName": "强电类", "SmallTypeName": null, "ReserveDate": "2021/7/30
14:01:05", "ReserveLimit": 0, "DispDate": "2021/7/30
14:01:21", "CoordinateNum": "P20210730000116", "DealLimit": 0, "DealManCode": "000635", "Duty": "物业
类", "ReceivingDate": null, "ArriveData": null, "IsTouSu": 0, "BigCorpTypeID": "100000015", "CanDeal": 0, "R
N": "6"},
{"CommID": "190603", "IncidentID": "190603000000026959", "IncidentNum": "202107300000269", "IncidentConten
t": "测试", "IncidentPlace": "户内", "IncidentDate": "2021/7/30
13:49:56", "Phone": "17891602182", "CommName": "深圳平安金融中
心", "RoomID": "19060300000046", "RoomSign": "6005", "RoomName": "6005", "RegionalID": "0", "RegionalPlace
": null, "BigTypeName": "弱电类", "SmallTypeName": null, "Rese
...
...
...

```

低

发现可高速缓存的 SSL 页面 ①

TOC

问题 1 / 1

TOC

发现可高速缓存的 SSL 页面

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Service.ashx (Page)

风险:

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因:

浏览器可能已将敏感信息高速缓存

固定值:

通过在响应中添加“Cache-Control: no-store”和“Pragma: no-cache”标题，可以阻止高速缓存 SSL 页面。

差异:

推理: 应用程序已进行响应，指示该页面应进行高速缓存，但不是所有高速缓存控制标题都进行了设置（“Cache-Control: no-store”和“Pragma: no-cache”或“Cache-Control: no-cache”）。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3
E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:58:08 GMT
Content-Type: text/plain; charset=utf-8

{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
{"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

低

未实施加密 ①

TOC

问题 1 / 1

TOC

未实施加密

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Service.ashx (Page)

风险:

可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据

原因:

诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值:

发送敏感信息时, 强制使用 HTTPS

差异:

从以下位置进行控制: <https> 至: <http>

从以下位置进行控制: <443> 至: <80>

标题 从以下位置进行控制: <pare-twp-stg.pingan.com.cn> 至: <pare-twp-stg.pingan.com.cn:80>

推理:

测试响应与原始响应非常相似。这表示已使用 HTTP 而不是 HTTPS 成功访问资源。

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3
E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn:80
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Set-Cookie: BIGipServerPOOL_PACLOUD_STGR2019091809829=1569213470.20480.0000; path=/; Httponly
Date: Wed, 08 Dec 2021 08:26:47 GMT
Content-Type: text/plain; charset=utf-8

{"Result":"true","data":[{"Name":"本月报事工单完成率","Value":"0.00","Unit":"%"}, {"Name":"本月设备巡检
完成率","Value":"0.00","Unit":"%"}, {"Name":"本月设备维保完成率","Value":"0.00","Unit":"%"},
{"Name":"本月分户查验完成率","Value":"0.00","Unit":"%"}, {"Name":"本月设备故障发生
率","Value":"0.00","Unit":"%"}], "TotalCount":0}
```

低

检测到隐藏目录 2

TOC

问题 1 / 2

TOC

检测到隐藏目录

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

app/ (Page)

风险:

可能会检索有关站点文件系统结构的信息, 这可能会帮助攻击者映射此 Web 站点

原因:

Web 服务器或应用程序服务器是以不安全的方式配置的

固定值:

对禁止的资源发布“404 - Not Found”响应状态代码, 或者将其完全除去

差异: 路径 从以下位置进行控制: `/TWI/TWInterface/Service/Service.ashx` 至: `/app/`

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录, 即使不允许对其进行访问。

测试请求和响应:

```

GET /app/?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: Microsoft-IIS/10.0
Content-Length: 1157
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 08:34:19 GMT
Content-Type: text/html; charset=UTF-8

```

问题 2 / 2

TOC

检测到隐藏目录

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: static/ (Page)

风险: 可能会检索有关站点文件系统结构的信息, 这可能会帮助攻击者映射此 Web 站点

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

固定值: 对禁止的资源发布“404 - Not Found”响应状态代码, 或者将其完全除去

差异: 路径 从以下位置进行控制: </TWI/TWInterface/Service/Service.ashx> 至: </TWI/static/>

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录, 即使不允许对其进行访问。

测试请求和响应:

```

GET /TWI/static/?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: Microsoft-IIS/10.0

```



```
Content-Length: 1157
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 08:34:19 GMT
Content-Type: text/html; charset=UTF-8
```

低 缺少 HTTP Strict-Transport-Security 头 ①

TOC

问题 1 / 1

TOC

缺少 HTTP Strict-Transport-Security 头

严重性: **低**

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Service.ashx (Page)

风险: 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 实施 HTTP Strict-Transport-Security 策略

差异:

推理: AppScan 检测到缺少 HTTP Strict-Transport-Security 响应头

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E190603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:58:08 GMT
Content-Type: text/plain; charset=utf-8
```

```
{"Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检
```

```
完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

低

缺少“Content-Security-Policy”头 ①

TOC

问题 1 / 1

TOC

缺少“Content-Security-Policy”头

严重性: **低**

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Service.ashx (Page)

风险: 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失，这可能会更大程度得暴露于各种跨站点注入攻击下之

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxc19%3C/Account%3E%3CLoginPwd%3E61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3CORGanCode%3E010103%3C/ORGanCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:58:08 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"},
```

```
{ "Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

低

缺少“X-Content-Type-Options”头 ①

TOC

问题 1 / 1

TOC

缺少“X-Content-Type-Options”头

严重性:

低

CVSS 分数: 5.0

URL:

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体:

Service.ashx (Page)

风险:

可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

原因:

Web 应用程序编程或配置不安全

固定值:

将您的服务器配置为使用“X-Content-Type-Options”头

差异:

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:58:08 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data": [{"Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备巡检完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%"}, {"Name": "本月设备故障发生率", "Value": "0.00", "Unit": "%"}]}
```

```
率", "Value": "0.00", "Unit": "%"}], "TotalCount": 0}
```

低

缺少“X-XSS-Protection”头 ①

TOC

问题 1 / 1

TOC

缺少“X-XSS-Protection”头

严重性:

低

CVSS 分数: 5.0

URL: <https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx>

实体: Service.ashx (Page)

风险: 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失, 这可能会造成跨站点脚本编制攻击

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3
E1906-
twzxcsl9%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3
E&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:58:08 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data": [ { "Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%", { "Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%", { "Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%",
{ "Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%", { "Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%", "TotalCount": 0 }
```

问题 1 / 1

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx

实体: Service.ashx (Page)

风险: 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置

原因: Web 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=%3Cattributes%3E%3CNet%3E1%3C/Net%3E%3CAccount%3E1906-
twxcs19%3C/Account%3E%3CLoginPwd%3EC61714AC0395696D6B4A8F0F6B4E7038%3C/LoginPwd%3E%3CCommID%3E19
0603%3C/CommID%3E%3COrganCode%3E010103%3C/OrganCode%3E%3CCode%3E999904%3C/Code%3E%3C/attributes%3E
&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba HTTP/1.1
User-Agent: okhttp/3.6.0
Connection: Keep-Alive
Host: pare-twp-stg.pingan.com.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Content-Length: 366
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Wed, 08 Dec 2021 07:58:08 GMT
Content-Type: text/plain; charset=utf-8
```

```
{ "Result": "true", "data": [ { "Name": "本月报事工单完成率", "Value": "0.00", "Unit": "%", { "Name": "本月设备巡检
完成率", "Value": "0.00", "Unit": "%", { "Name": "本月设备维保完成率", "Value": "0.00", "Unit": "%",
{ "Name": "本月分户查验完成率", "Value": "0.00", "Unit": "%", { "Name": "本月设备故障发生
率", "Value": "0.00", "Unit": "%", "TotalCount": 0 }
```

修订建议

高

发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

TOC

该任务修复的问题类型

- 查询中的密码参数
- SSL 请求中的查询参数

常规

查询中的密码参数

1. 确保所有登录请求都在主体中（并加密）发送到服务器。
2. 请确保敏感信息，例如：
 - 用户名
 - 密码
 - 社会保险号码
 - 信用卡号码
 - 驾照号码
 - 电子邮件地址
 - 电话号码
 - 邮政编码

始终放在请求主体中（并加密）来发送到服务器。

SSL 请求中的查询参数

请确保敏感信息，例如：

- 用户名
- 密码
- 社会保险号码
- 信用卡号码
- 驾照号码
- 电子邮件地址
- 电话号码
- 邮政编码

一律在 HTTP POST 请求的主体部分发送。

该任务修复的问题类型

- 链接注入（便于跨站请求伪造）

常规

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

可用于更轻松生成正确编码的输出的库和框架示例包括 Microsoft 的 Anti-XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。

[2] 了解将在其中使用数据的上下文，以及预期的编码。在不同组件之间传输数据时，或在生成可同时包含多个编码的输出（如 Web 页面或多部分邮件消息）时，这尤为重要。研究所有预期的通信协议和数据表示法以确定所需的编码策略。对于将输出到另一个 Web 页面的任何数据（尤其是从外部输入接收到的任何数据），请对所有非字母数字字符使用恰当的编码。

相同输出文档的某些部分可能需要不同的编码，具体取决于输出是在以下哪一项中：

[-] HTML 主体

[-] 元素属性（如 `src="XYZ"`）

[-] URI

[-] JavaScript 段

[-] 级联样式表和样式属性

请注意，“HTML 实体编码”仅适用于 HTML 主体。

请咨询 XSS Prevention Cheat Sheet

[http://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

以获取有关所需编码和转义类型的更多详细信息。

[3] 策略：识别和减少攻击出现的机会

了解您的软件中可能出现不可信输入的所有潜在区域：参数或自变量、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组成部分、电子邮件、文件、文件名、数据库以及向应用程序提供数据的任何外部系统。请记住，此类输入可通过 API 调用间接获取。

[4] 策略：输出编码

对于生成的每个 Web 页面，请使用并指定 ISO-8859-1 或 UTF-8 之类的字符编码。如果未指定编码，Web 浏览器可能通过猜测 Web 页面编码来选择不同的编码。这可能导致 Web 浏览器将特定序列视为特殊序列，从而使客户机暴露在不易察觉的 XSS 攻击之下。请参阅 CWE-116 以获取与编码/转义相关的更多减轻威胁的方法。

[5] 策略：识别和减少攻击出现的机会

要帮助减轻针对用户会话 cookie 的 XSS 攻击带来的威胁，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如 Internet Explorer 和 Firefox 的较新版本）中，此属性可防止使用 document.cookie 的恶意客户端脚本访问用户的会话 cookie。这不是完整的解决方案，因为 HttpOnly 并不受所有浏览器支持。更重要的是，XMLHttpRequest 和其他功能强大的浏览器技术提供了对 HTTP 头的读访问权，包括在其中设置 HttpOnly 标志的 Set-Cookie 头。

[6] 策略：输入验证

假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝没有严格遵守规范的输入，或者将其转换为严格遵守规范的内容。不要完全依赖于除去有潜在危险的字符的过滤机制。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入由于格式严重错误而应直接拒绝。以业务规则逻辑为例，“boat”可能在语法上有效，因为它仅包含字母数字字符，但如果预期为颜色（如“red”或“blue”），那么它无效。作为业务规则逻辑的示例，“boat”可能在语法上有效（因为它仅包含字母数字字符），但如果预期为颜色（如“red”或“blue”），那么它就无效。动态构造 Web 页面时，请使用严格的白名单以根据请求中参数的预期值来限制字符集。所有输入都应进行验证和清理：不仅限于用户应指定的参数，而是涉及请求中的所有数据，包括隐藏字段、cookie、头、URL 本身，等等。导致 XSS 脆弱性持续存在的一个常见错误是仅验证预期会由站点重新显示的字段。常见的情况是，在请求中出现由应用程序服务器或应用程序反射的数据，而开发团队却未能预料到此情况。另外，将来的开发者可能会使用当前未反映的字段。因此，建议验证 HTTP 请求的所有部分。请注意，适当的输出编码、转义和引用是防止 XSS 的最有效解决方案，虽然输入验证可能会提供一定的深度防御。这是因为它会有效限制将在输出中出现的内容。输入验证并不总是能够防止

XSS，尤其是在您需要支持可包含任意字符的自由格式文本字段的情况下。例如，在聊天应用程序中，心型表情图标（“<3”）可能会通过验证步骤，因为它的使用频率很高。但是，不能将其直接插入到 Web 页面中，因为它包含“<”字符，该字符需要转义或以其他方式进行处理。在此情况下，消除“<”可能会降低 XSS 的风险，但是这会产生不正确的行为，因为这样就不会记录表情图标。

这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。即使在验证中出错（例如，在 100 个输入字段中忘记一个字段），相应的编码仍有可能针对基于注入的攻击为您提供防护。只要输入验证不是孤立完成的，便仍是有用的技巧，因为它可以大大减少攻击出现的机会，使您能够检测某些攻击，并提供正确编码所无法解决的其他安全性优势。请确保在应用程序内定义良好的界面中执行输入验证。即使某个组件进行了复用或移动到其他位置，这也将有助于保护应用程序。

低

修改“Access-Control-Allow-Origin”头以仅获取允许的站点

TOC

该任务修复的问题类型

- 过度许可的 CORS 访问测试

常规

准备可信站点的列表，并将它们设置为“Access-Control-Allow-Origin”头的值。如果外部访问权不需要该值，请完全地除去该头。

低

发送敏感信息时，强制使用 HTTPS

TOC

该任务修复的问题类型

- 未实施加密

常规

请确保敏感信息，例如：

- 用户名
- 密码
- 社会保险号码
- 信用卡号码
- 驾照号码
- 电子邮件地址
- 电话号码
- 邮政编码

一律以加密方式传给服务器。

该任务修复的问题类型

- 缺少 HTTP Strict-Transport-Security 头

常规

通过向 web 应用程序响应添加“Strict-Transport-Security”响应头来实施 HTTP 严格传输安全策略。
有关更多信息，请参阅

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

该任务修复的问题类型

- 检测到隐藏目录

常规

如果不需要禁止的资源，请将其从站点中除去。

可能的话，请发出改用“404 - 找不到”响应状态代码，而不是“403 - 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

该任务修复的问题类型

- 缺少“Content-Security-Policy”头

常规

将您的服务器配置为发送“Content-Security-Policy”头。对于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
对于 IIS，请参阅：
<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>
对于 nginx，请参阅：
http://nginx.org/en/docs/http/nginx_http_headers_module.html

低

将您的服务器配置为使用“X-Content-Type-Options”头

TOC

该任务修复的问题类型

- 缺少“X-Content-Type-Options”头

常规

将您的服务器配置为在所有传出请求上发送值为“nosniff”的“X-Content-Type-Options”头。对于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
对于 IIS，请参阅：
<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>
对于 nginx，请参阅：
http://nginx.org/en/docs/http/nginx_http_headers_module.html

低

将您的服务器配置为使用“X-XSS-Protection”头

TOC

该任务修复的问题类型

- 缺少“X-XSS-Protection”头

常规

将您的服务器配置为在所有传出请求上发送值为“1”（例如已启用）的“X-XSS-Protection”头。对于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
对于 IIS，请参阅：
<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>
对于 nginx，请参阅：
http://nginx.org/en/docs/http/nginx_http_headers_module.html

该任务修复的问题类型

- 发现可高速缓存的 SSL 页面

常规

在所有 SSL 页面及含有敏感数据的所有页面上，禁用高速缓存。

通过使用您 SSL 页面标题中的“Cache-Control: no-store”和“Pragma: no-cache”或“Cache-Control: no-cache”响应伪指令来实现此操作。

Cache-Control: private - 此伪指令可向代理指示某个页面中包含私有信息，因此不能由共享高速缓存进行高速缓存。但是，它不会指示浏览器阻止高速缓存此页面。

Cache-Control: no-cache - 此伪指令也可向代理指示某个页面中包含私有信息，因此不能高速缓存。它还会指示浏览器重新验证服务器以检查是否有新的版本可用。这意味着浏览器可能会存储敏感页面或要在重新验证中使用的信息。某些浏览器不一定会跟踪 RFC，因此可能会将 **no-cache** 视为 **no-store**。

Cache-Control: no-store - 这是最安全的伪指令。它同时指示代理和浏览器不要高速缓存此页面或将其存储为它们的高速缓存文件夹。

Pragma: no-cache - 对于不支持高速缓存控制标题的较旧浏览器，该伪指令是必需的。

咨询

查询中的密码参数

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

安全性风险:

可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

受影响产品:

CWE:

523

引用:

金融隐私权: 格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 SB1386

技术描述:

在应用程序测试过程中，检测到查询字符串中接收到密码参数。由于登录过程所用的部分输入字段（例如：用户名、密码、电子邮件地址、社会保险号码，等等）是个人敏感信息，建议将其放在请求的主体部分或加密连接（如 **SSL**）中来发送到服务器。任何通过查询字符串传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。此外，若干隐私法规指出，用户凭证之类的敏感信息一律以加密方式传给网站。

链接注入（便于跨站请求伪造）

TOC

测试类型:

应用程序级别测试

威胁分类:

内容电子欺骗

原因:

未对用户输入正确执行危险字符清理

安全性风险:

- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
- 可能会窃取或操纵客户会话和 **cookie**，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
- 可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

受影响产品:

CWE:

74

X-Force:

6784

引用:

[OWASP 文章](#)

[跨站点请求伪造常见问题 \(FAQ\)](#)

[跨站点请求伪造培训模块](#)

技术描述:

该软件使用受外部影响的输入来构造命令、数据结构或记录的全部或一部分，但未能对可能修改其解析或解释方式的元素进行无害化处理。

“链接注入”是通过在某个站点中嵌入外部站点的 **URL**，或者在易受攻击的站点中嵌入脚本的 **URL**，从而修改该站点的内容。在易受攻击的站点中嵌入 **URL** 后，攻击者能够将其作为发起针对其他站点（以及针对这个易受攻击的站点本身）的攻击的平台。

其中一些可能的攻击需要用户在攻击期间登录站点。通过从易受攻击的站点本身发起这些攻击，攻击者成功的可能性更高，因为用户更倾向于登录。

“链接注入”脆弱性是未对用户输入进行充分清理所导致的结果，该输入以后会在站点响应中返回给用户。这样一来，攻击者能够将危险字符注入响应中，从而有可能嵌入 **URL**，以及做出其他可能的内容修改。

以下是“链接注入”的示例（我们假设站点“www.vulnerable.com”有一个名为“name”的参数，用于问候用户）。

下列请求：[HTTP://www.vulnerable.com/greet.asp?name=John Smith](http://www.vulnerable.com/greet.asp?name=John%20Smith)

会生成下列响应:

```
<HTML>
<BODY>
  Hello, John Smith.
</BODY>
</HTML>
```

然而，恶意的用户可以发送下列请求：

HTTP://www.vulnerable.com/greet.asp?name=

这会返回下列响应：

```
<HTML>
<BODY>
Hello, <IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">.
</BODY>
</HTML>
```

如以上示例所示，攻击者有可能导致用户浏览器向攻击者企图攻击的几乎任何站点发出自动请求。因此，“链接注入”脆弱性可用于发起几种类型的攻击：

- [] 跨站点请求伪造
- [] 跨站点脚本编制
- [] 网络钓鱼

SSL 请求中的查询参数

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

查询参数通过 **SSL** 进行了传递，并且可能包含敏感信息

安全性风险：

受影响产品：

CWE：

598

X-Force：

52845

引用：

金融隐私权：格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 **SB1386**

技术描述:

在应用程序测试期间，检测到通过 SSL 发送的请求包含在 HTTP 请求的 Query 部分中传输的参数。发送请求时，可以使用浏览器的历史记录来显现 URL，其中包含查询参数名称和值。

由于加密请求的敏感性，建议您尽可能使用 HTTP POST（不带 URL 字符串中的参数），以便避免向其他人泄露 URL 和参数值。

发现可高速缓存的 SSL 页面

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

浏览器可能已将敏感信息高速缓存

安全性风险:

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品:

CWE:

525

X-Force:

52512

技术描述:

缺省情况下，大部分 Web 浏览器都配置成会在使用期间高速缓存用户的页面。这表示也会高速缓存 SSL 页面。不建议让 Web 浏览器保存任何 SSL 信息，因为当有漏洞存在时，可能会危及这个信息。

未实施加密

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

安全性风险:

受影响产品:

CWE:

311

X-Force:

52586

引用:

金融隐私权: 格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 SB1386

技术描述:

在应用程序测试期间, 检测到网站利用加密的连接来保护敏感信息。

不过, 仍有可能利用 HTTP 接收这些资源, 这表示敏感信息可能是以未加密的方式传给服务器或返回给用户。任何以明文传给服务器的信息都可能被窃, 稍后可用来电子欺骗身份或伪装用户。此外, 若干隐私法规指出, 用户凭证之类的敏感信息一律以加密方式传给 Web 站点。

建议您强制采用加密连接 (如 SSL), 禁止利用未加密的 HTTP 来访问敏感信息。

检测到隐藏目录

TOC

测试类型:

基础结构测试

威胁分类:

信息泄露

原因:

Web 服务器或应用程序服务器是以不安全的方式配置的

安全性风险:

可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点

受影响产品:

CWE:

200

X-Force:

52599

技术描述:

Web 应用程序显现了站点中的目录。虽然目录并没有列出其内容，但此信息可以帮助攻击者发展对站点进一步的攻击。例如，知道目录名称之后，攻击者便可以猜测它的内容类型，也许还能猜出其中的文件名或子目录，并尝试访问它们。

内容的敏感度越高，此问题也可能越严重。

缺少 HTTP Strict-Transport-Security 头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品:

CWE:

200

引用:

OWASP“HTTP Strict Transport Security”
HSTS 规范

技术描述:

HTTP 严格传输安全 (HSTS) 是保护安全 (HTTPS) Web 站点不被降级到不安全 HTTP 的机制。该机制使 Web 服务器能指示器客户端 (Web 浏览器或其他用户代理程序) 在与服务器交互时始终使用安全 HTTPS 连接, 而绝不使用不安全的 HTTP 协议。HTTP 严格传输安全策略由服务器用于通过名为“Strict-Transport-Security”的响应头与其客户机通信。该头的值为客户机应仅使用 HTTPS 访问服务器的时间段。其他头属性包括“includeSubDomains”和“preload”。

缺少“Content-Security-Policy”头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息, 如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品:

CWE:

200

引用:

有用 HTTP 头的列表
内容安全策略的简介

技术描述:

“Content-Security-Policy”头设计用于修改浏览器渲染页面的方式, 并因此排除各种跨站点注入, 包括跨站点脚本编制。以不会阻止 web 站点的正确操作的方式正确地设置头值就非常的重要。例如, 如果头设置为阻止内联 JavaScript 的执行, 那么 web 站点不得在其页面中使用内联 JavaScript。

缺少“X-Content-Type-Options”头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品:

CWE:

200

引用:

有用 HTTP 头的列表
减小 MIME 类型安全性风险

技术描述:

“X-Content-Type-Options”头（具有“nosniff”值）可防止 IE 和 Chrome 忽略响应的内容类型。该操作可能防止在用户浏览器中执行不受信任的内容（例如用户上传的内容）（例如在恶意命名之后）。

缺少“X-XSS-Protection”头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品:

CWE:

200

引用:

有用 HTTP 头的列表
[IE XSS 过滤器](#)

技术描述:

“X-XSS-Protection”头强制将跨站点脚本编制过滤器加入“启用”方式，即使用户已禁用时也是如此。该过滤器被构建到最新的 web 浏览器中（IE 8+，Chrome 4+），通常在缺省情况下已启用。虽然它并非设计为第一个选择而且仅能防御跨站点脚本编制，但它充当额外的保护层。

过度许可的 CORS 访问测试

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品:

CWE:

200

引用:

启用跨源资源共享
[HTML5: 过度许可的 CORS 策略](#)

技术描述:

跨源资源共享 (CORS) 是允许 web 站点从外部站点请求资源的机制，从而避免复制资源。向外部站点授予访问权时，它们可对授予权限的站点执行各种操作，以及在这些站点上面执行脚本。因此，除了可信站点之外，不向任何其他站点授予访问权则非常重要。

应用程序数据

已访问的 URL 65

TOC

URL

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=RefreshAppDesktopStatistic&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999902</Code></attributes>&Class=PMS10AppDesktop&Mac=acf901505da4206d3c7c4918a07baafa>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetMessageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><CorpID>1906</CorpID><State>1</State><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=OnlineMessage&Mac=7e68cec1012655d7ce99927bb529d069>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=QueryWareHouse&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><WhereStr></WhereStr></attributes>&Class=IncidentAcceptManage&Mac=fccb27f29fbd0e7bfe3040b0decde989>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetMaterialSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</UserCode><WareHouseName>L9仓库</WareHouseName><MaterialName></MaterialName><Num></Num><Page>1</Page></attributes>&Class=SearchManage&Mac=1c0619679d02301e68ebaecbca5c5e4>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchUserSimpleInfo&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Key></Key></attributes>&Class=PMSUserManage&Mac=6191ba9d629523f956e3c831388645de>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetTopRoomList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><roomSign></roomSign></attributes>&Class=IncidentAcceptManage&Mac=17d7023414bfa764bab3e1c90b0914bc>

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetParkSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><WhereStr></WhereStr></attributes>&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba>

38</LoginPwd><CommID>190603</CommID><ParkName>ggg</ParkName><CarSign></CarSign><RoomSign></RoomSign><CustID></CustID><Phone></Phone></attributes>&Class=SearchManage&Mac=84306465e35c4a2a65c8e9b780673d0f

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetParkNameList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Key>gg</Key></attributes>&Class=SearchManage&Mac=b694ff626374dd9aad5530c8e222d1df

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetBuildingList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CorpID>1906</CorpID><CommID>190603</CommID></attributes>&Class=RoomManage&Mac=22f5c94bb1f1754a0437ed3d2e8c9fa2

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentBigType&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><DrClass>1</DrClass><IncidentPlace>户内</IncidentPlace><Duty>物业类</Duty></attributes>&Class=PMSIncidentAccept&Mac=a98c9f57ba5e43c8b6d1bae77c1b2226

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentPublicConfig&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID></attributes>&Class=PMSIncidentAccept&Mac=d6853aa7187d225d5583b4adc9c6bdb8

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentRegionals&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID></attributes>&Class=IncidentAcceptManage_bl&Mac=c5a5e7fb4713f6f7f6f30864589d9470

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentPublicPosition&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID></attributes>&Class=PMSIncidentAccept&Mac=d6853aa7187d225d5583b4adc9c6bdb8

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTousu><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><Mobile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchCustName&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustName></CustName></attributes>&Class=SearchCustomerManage_v2&Mac=a39aaf3407476a0d5aa0c1465e0eb10c

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentPoolList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=PMSIncidentAccept&Mac=5d3bf8f4279b025ff061943e30720f42

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentSimpleDetail&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026993</IncidentID></attributes>&Class=PMSIncidentAccept&Mac=7ebe4d7175ae461a40865e227b712ac5

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentCanDiscard&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Type>1</Type></attributes>&Class=IncidentAcceptManage_bl&Mac=bae00be940aeb4d37b668c2bcb2d67db

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentDelete&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026993</IncidentID><CloseSituation>uhh</CloseSituation><Type>null</Type></attributes>&Class=IncidentAcceptManage

_jh&Mac=ccbc884fa4d7c5095af13fce4029874e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCanDealIncidentUserList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CorpTypeID>10000011</CorpTypeID></attributes>&Class=IncidentAcceptManage_jh&Mac=54631ce974fb313d98eff97467ee995d

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><IncidentContent>hjj</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>10000011</BigCorpTypeID><DealMan></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsSnatch><Assistant></Assistant><RegionalID>190603000000005</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=40522da4e3c1764b598ee82e193400fe

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentDealList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><DrClass>2</DrClass><IsAll>0</IsAll><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=PMSIncidentAccept&Mac=eb89b1adcd210afda1e771b848731451

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentDetail&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID></attributes>&Class=PMSIncidentAccept&Mac=31b08ffd796f1fcffdc575169e242c3

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentCanDiscard&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Type>3</Type></attributes>&Class=IncidentAcceptManage_bl&Mac=7072228d587f667630c8b8e30465a245

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentFollowHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=d1d2f4ece1a4b4253e5d4849fa763184

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentTransmitHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=c00e6da2a233c7aa194bc1f92ed7290a

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCanDealIncidentUserListWhenTransmit&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><CorpTypeID>10000011</CorpTypeID></attributes>&Class=IncidentAcceptManage_bl&Mac=a6220a85ce7d9742bca8e3df980120d4

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentTransmit&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><BigCorpTypeID>10000011</BigCorpTypeID><Duty>物业类</Duty><DealMan>天问推送测试账号</DealMan><DealManUserCode>001345</DealManUserCode><TransmitReason>ghh</TransmitReason><ConfirmTransmit>0</ConfirmTransmit></attributes>&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcba

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentFollowHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=0271d9b746e6a99f58390665e9c881a3

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentServiceList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID></attributes>&Class=IncidentAcceptManage&Mac=0714e55094be8b218846e3ccd7da1dc0

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCloseBackList&Attribute

=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026991</IncidentID></attributes>&Class=IncidentAcceptManage_jh&Mac=ad25a5b6a931ffcafa019fcae381822

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentDetail&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026991</IncidentID></attributes>&Class=PMSIncidentAccept&Mac=8ebe6959661540c0b19a53d94556a6b7

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentTransmitHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026991</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=2784d90b7d3bc6a93fc0e0efd07af8bc

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentDelete&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026991</IncidentID><CloseSituation>ujh</CloseSituation><Type>null</Type></attributes>&Class=IncidentAcceptManage_jh&Mac=1854a3be6ef630a355f2cfa01dd6215

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentCloseList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OpType>1</OpType><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_bl&Mac=fd51e08a61fe1c2663062f56829afd36

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentCancleFinish&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026984</IncidentID><CancleReasons>yhhg</CancleReasons></attributes>&Class=IncidentAcceptManage_jh&Mac=0752786ccd8849ecc11206f0bd25436

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentClose&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026983</IncidentID><CloseSituation>hhh</CloseSituation><CloseType>0</CloseType><IsClose>1</IsClose><CloseReasons></CloseReasons></attributes>&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentWarningList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Step>1</Step><PageSize>10</PageSize><PageIndex>1</PageIndex></attributes>&Class=PMSIncidentAccept&Mac=4eeb7891784e345c8d834fb81ccb5efd

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentWarningCount&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID></attributes>&Class=IncidentAcceptManage_bl&Mac=c5a5e7fb4713f6f7f6f30864589d9470

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=DownloadTask_v2&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><TaskType>1</TaskType></attributes>&Class=EquipmentManage_bl&Mac=4396f75b39d302c2d066eed03ea15385

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=SearchEquipment&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</UserCode><EquipmentID>hhhh</EquipmentID><EquipmentName></EquipmentName><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=EquipmentManage_bl&Mac=e34cf53132ec0d4723a610051e99165c

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetFloorRoomList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><BuildSNum>1</BuildSNum><UnitSNum>1</UnitSNum><FloorNum>-3</FloorNum><CommID>190603</CommID></attributes>&Class=RoomManage&Mac=411f404a42168ecc955c5979d4e0db58

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCustMeterHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><RoomID>19060300000096</RoomID></attributes>&Class=MeterManage&Mac=90c2793414596981c8e8ffd4273f36c9

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetNotOutRenovationInfo&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size>10</Size></attributes>&Class=DecorateManage&Mac=d38afbed10148369ad57ba79f261860d

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCloseBackList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026977</IncidentID></attributes>&Class=IncidentAcceptManage_jh&Mac=16e60ffa632db0054eb1026229f13e46

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=PublicMeterList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><CommID>190603</CommID></attributes>&Class=MeterManage&Mac=90320448370f118fbee3cfba2b1bb06

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetPublicMeterHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><CommID>190603</CommID><MeterID>19060300000004</MeterID></attributes>&Class=MeterManage&Mac=f040a29fb07a834cb4d45702032d2943

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</UserCode><MeterID>19060300000004</MeterID><StartDegree>1000.00</StartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStartDegree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraDosage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetParkNameList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Key>ggg</Key></attributes>&Class=SearchManage&Mac=c7e7297c38e0888a14fb6f19eccc34d3

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentSimpleDetail&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026992</IncidentID></attributes>&Class=PMSIncidentAccept&Mac=7ee8c51082b4f9d6806bfa8701e60767

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026992</IncidentID><IncidentContent>客梯</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>10000013</BigCorpTypeID><DealMan>admins</DealMan><DealManUserCode>000131</DealManUserCode><IsSnatch>0</IsSnatch><Assistant></Assistant><RegionalID>1906030000000067</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=d503c6f0b1116af4a2acdbf152eb2be3

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentSimpleDetail&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026991</IncidentID></attributes>&Class=PMSIncidentAccept&Mac=8ebe6959661540c0b19a53d94556a6b7

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCanDealIncidentUserList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CorpTypeID>10000016</CorpTypeID></attributes>&Class=IncidentAcceptManage_jh&Mac=445d757ea91024fc76aaa4b1bd5c7938

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentDealList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><DrClass>1</DrClass><IsAll>

1</IsAll><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=PMSIncidentAccept&Mac=12d8a43c9984e9d3c31ec126661abc92

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentFollowHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026984</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=1406a57cae0da83b1f4b2bfddf2a177f

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentFollowHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026977</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=984ae8677a5260ed57eb099d21502c3a

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentTransmitHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026977</IncidentID><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_jh&Mac=e9c3cf8b0077087de74e4e114fa2d018

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCustMeterHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><RoomID>19060300000069</RoomID></attributes>&Class=MeterManage&Mac=537d25b6e22e2a65908ec383e33ab3ac

参数 94

TOC

名称	值	URL	类型
Attribute		https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</UserCode><MeterID>19060300000004</MeterID><StartDegree>1000.00</StartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStartDegree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraDosage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0	XML
Attribute		https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTousu><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><M	XML

at
tri
b
ut
es
->
ls
D
ec
or
at
e

obile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCust
omerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b

At hjj
tri 客梯

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?
Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><A
ccount>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8
F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190
603000000026994</IncidentID><IncidentContent>hjj</IncidentContent><Du
ty>物业类</Duty><BigCorpTypeID>100000011</BigCorpTypeID><DealMan
></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsS
natch><Assistant></Assistant><RegionalID>1906030000000005</Regional
ID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptMa
nage_bl&Mac=40522da4e3c1764b598ee82e193400fe

XML

->
In
ci
d
e
nt
C
o
nt
e
nt

C GetAppDesktopStatisticsD
o etails
m RefreshAppDesktopStatisti
m cs
a GetMessageList
n QueryWarehouse
d GetMaterialSearch
...

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?
Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</
Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D
6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCo
de>010103</OrganCode><Code>999904</Code></attributes>&Class=PMS
S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba

简单
链接

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
H
o
us
e
K
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1
906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E
7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 0
0:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStart
Time></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrCl
ass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState><
</DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper
></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><Incid
entState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10
</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2fe
ae48e680068529a5249c

XML

e
p
er

Cl as s ... At tri b ut e- > at tri b ut es -> T o D at e	PMS10AppDesktop OnlineMessage IncidentAcceptManage SearchManage PMSUserManage ... 2021/12/30	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</ Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D 6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCo de>010103</OrganCode><Code>999904</Code></attributes>&Class=PM S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba	简单 链接
At tri b ut e- > at tri b ut es -> T o D at e	0	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net> <Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4 A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></Cu stID><CustName></CustName><RoomID></RoomID><RoomSign></Room Sign><CarparkID></CarparkID><CarparkName></CarparkName><FromDa te>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged >0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</Pag eIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearag eManage&Mac=89827636aae053cb751abb5ff17b6d5e	XML
At tri b ut e- > at tri b ut es -> C o nfi r m Tr a ns mi t	0	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=IncidentTransmit&Attribute=<attributes><Net>1</Net><Account >1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B 4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000 000026994</IncidentID><BigCorpTypeID>100000011</BigCorpTypeID><D uty>物业类</Duty><DealMan>天问推送测试账号</DealMan><DealManUser Code>001345</DealManUserCode><TransmitReason>ghh</TransmitReas on><ConfirmTransmit>0</ConfirmTransmit></attributes>&Class=IncidentAc ceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcb	XML
At tri b ut e- > at tri b ut es ->	10	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1 906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E 7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 0 0:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStart Time></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrCl ass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState>< /DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper ></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><Incid entState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10 </pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2fe ae48e680068529a5249c	XML

p
a
g
e
S
i
z
e

At 001345
tri 000131
b
ut
e-
>
at
tri
b
ut
es
->
D
e
a
l
M
a
n
U
s
e
r
C
o
d
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000026994</IncidentID><IncidentContent>hjj</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>10000011</BigCorpTypeID><DealMan></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsSnatch><Assistant></Assistant><RegionalID>1906030000000005</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=40522da4e3c1764b598ee82e193400fe XML

At 1
tri
b
ut
e-
>
at
tri
b
ut
es
->
St
e
p

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentWarningList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Step>1</Step><PageSize>10</PageSize><PageIndex>1</PageIndex></attributes>&Class=PMSIncidentAccept&Mac=4eeb7891784e345c8d834fb81ccb5efd> XML

At 1906
tri
b
ut
e-
>
at
tri
b
ut
es
->
C
o
r
p
l

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetMessageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><CorpID>1906</CorpID><State>1</State><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=OnlineMessage&Mac=7e68cec1012655d7ce99927bb529d069> XML

D

At 0
tri
b
ut
e-
>
at
tri
b
ut
es
->
E
xc
lu
d
e
L
et
te
r

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e

XML

At hhhh
tri
b
ut
e-
>
at
tri
b
ut
es
->
E
q
ui
p
m
e
nt
ID

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=SearchEquipment&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</UserCode><EquipmentID>hhhh</EquipmentID><EquipmentName></EquipmentName><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=EquipmentManage_bl&Mac=e34cf53132ec0d4723a610051e99165c

XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
ro
om
Si
gn

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetTopRoomList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><roomSign></roomSign></attributes>&Class=IncidentAcceptManage&Mac=17d7023414bfa764bab3e1c90b0914bc

XML

M ac	IBM AppScan binary content placeholder	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx	主体
At tri b ut e- > at tri b ut es -> St ar tD e gr e e	1000.00	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</UserCode><MeterID>19060300000004</MeterID><StartDegree>1000.00</StartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStartDegree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraDosage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0	XML
At tri b ut e- > at tri b ut es -> A d mi n		https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2fae48e680068529a5249c	XML
At tri b ut e- > at tri b ut es -> T as k T yp e	1	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=DownloadTask_v2&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><TaskType>1</TaskType></attributes>&Class=EquipmentManage_bl&Mac=4396f75b39d302c2d066eed03ea15385	XML
At tri b	1	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetMessageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><TaskType>1</TaskType></attributes>&Class=EquipmentManage_bl&Mac=4396f75b39d302c2d066eed03ea15385	XML

ut
e-
>
at
tri
b
ut
es
->
St
at
e

E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><CorpID>1906</CorpID><State>1</State><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=OnlineMessage&Mac=7e68cec1012655d7ce99927bb529d069

At 1
tri
b
ut
e-
>
at
tri
b
ut
es
->
Is
O
w
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTousu><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><Mobile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b XML

At 999904
tri 999902
b
ut
e-
>
at
tri
b
ut
es
->
C
o
d
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PM S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
M
o
bil
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTousu><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><Mobile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCustomerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b XML

At 1906030000000005
tri 19060300000000067
b
ut
e-
>
at
tri
b
ut
es
->
R
e
gi
o
n
all
D

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000026994</IncidentID><IncidentContent>hjj</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>100000011</BigCorpTypeID><DealMan></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsSnatch><Assistant></Assistant><RegionalID>1906030000000005</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=40522da4e3c1764b598ee82e193400fe XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
Di
sp
R
e
m
ar
ks

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000026994</IncidentID><IncidentContent>hjj</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>100000011</BigCorpTypeID><DealMan></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsSnatch><Assistant></Assistant><RegionalID>1906030000000005</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=40522da4e3c1764b598ee82e193400fe XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
R
o
o
m
Si
gn

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e> XML

At 2000
tri
b

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F> XML

ut
e-
>
at
tri
b
ut
es
->
E
n
d
D
e
gr
e
e

0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</U
serCode><MeterID>19060300000004</MeterID><StartDegree>1000.00</S
tartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStart
Degree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraD
osage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManag
e&Mac=5c81444e8c50aa4aa4b8cc8cdaf1c1b0

At 1
tri
b
ut
e-
>
at
tri
b
ut
es
->
N
et

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</
Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D
6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCo
de>010103</OrganCode><Code>999904</Code></attributes>&Class=PM
S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba

At IBM AppScan binary conte
tri nt place holder
b
ut
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx 主体

At 10
tri
b
ut
e-
>
at
tri
b
ut
es
->
Si
ze

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account
>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B
4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size
>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTous
u><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><M
obile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCust
omerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b

At 100000011
tri 100000013
b
ut
e-
>
at
tri
b
ut

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><A
ccount>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8
F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190
603000000026994</IncidentID><IncidentContent>hjj</IncidentContent><Du
ty>物业类</Duty><BigCorpTypeID>100000011</BigCorpTypeID><DealMan
></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsS
natch><Assistant></Assistant><RegionalID>1906030000000005</Regional
ID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptMa
nage_bl&Mac=40522da4e3c1764b598ee82e193400fe

es
->
Bi
g
C
or
p
T
yp
el
D

At -3
tri
b
ut
e-
>
at
tri
b
ut
es
->
Fl
o
or
N
u
m

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetFloorRoomList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><BuildSNum>1</BuildSNum><UnitSNum>1</UnitSNum><FloorNum>-3</FloorNum><CommID>190603</CommID></attributes>&Class=RoomManage&Mac=411f404a42168ecc955c5979d4e0db58> XML

At gg
tri ggg
b
ut
e-
>
at
tri
b
ut
es
->
K
ey

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchUserSimpleInfo&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><Key></Key></attributes>&Class=PMSUserManage&Mac=6191ba9d629523f956e3c831388645de> XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
E
q
ui
p
m

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=SearchEquipment&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</UserCode><EquipmentID>hhhh</EquipmentID><EquipmentName></EquipmentName><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=EquipmentManage_bl&Mac=e34cf53132ec0d4723a610051e99165c XML

e
nt
N
a
m
e

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
D
e
al
E
n
d
Ti
m
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c

At 0
tri
b
ut
e-
>
at
tri
b
ut
es
->
E
xc
lu
d
e
Ur
g
e
d

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e

At 001349
tri
b
ut
e-
>
at
tri
b
ut
es
->

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetMessageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><CorpID>1906</CorpID><State>1</State><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=OnlineMessage&Mac=7e68cec1012655d7ce99927bb529d069

U
se
rC
o
d
e

全部
At
tri
b
ut
e-
>
at
tri
b
ut
es
->
In
ci
d
e
nt
St
at
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c

IBM AppScan binary content placeholder
Cl
as
s

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx

主体

户内
At
tri
b
ut
e-
>
at
tri
b
ut
es
->
In
ci
d
e
nt
Pl
ac
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetIncidentBigType&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><DrClass>1</DrClass><IncidentPlace>户内</IncidentPlace><Duty>物业类</Duty></attributes>&Class=PMSIncidentAccept&Mac=a98c9f57ba5e43c8b6d1bae77c1b2226

1
At
tri
b
ut
e-
>
at
tri
b
ut
es

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetMessageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><CorpID>1906</CorpID><State>1</State><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=OnlineMessage&Mac=7e68cec1012655d7ce99927bb529d069

->
P
a
g
e
I
n
d
e
x

At 1 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1
b 906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E
ut 7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 0
e- 0:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStart
> Time></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrCl
at ass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState><
tri /DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper><
b ></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><Incid
ut entState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10
es </pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2fe
> ae48e680068529a5249c

p
a
g
e
I
n
d
e
x

At 19060300000096 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri 19060300000069 Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net>
b <Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4
ut A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></Cu
e- stID><CustName></CustName><RoomID></RoomID><RoomSign></Room
> Sign><CarparkID></CarparkID><CarparkName></CarparkName><FromDa
at te>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged
tri >0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</Pag
b eIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearag
ut eManage&Mac=89827636aae053cb751abb5ff17b6d5e
es >

R
o
o
m
I
D

At yhhg https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=IncidentCancleFinish&Attribute=<attributes><Net>1</Net><Acc
b ount>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0
ut F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060
e- 3000000026984</IncidentID><CancleReasons>yhhg</CancleReasons></at
> tributes>&Class=IncidentAcceptManage_jh&Mac=0752786ccd8849eccc112
at 06f0bd25436
tri
b
ut
es
>

C
a
n
c
l
e

R
e
a
s
o
n
s

A
t
t
r
i
b
u
t
e
-
>
a
t
t
r
i
b
u
t
e
s
->
N
u
m

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetMaterialSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
s19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</UserCode><WarehouseName>L9仓库</WarehouseName><MaterialName></MaterialName><Num></Num><Page>1</Page></attributes>&Class=SearchManage&Mac=1c0619679d02301e68ebaecbca5c5e4

A
t
t
r
i
b
u
t
e
-
>
a
t
t
r
i
b
u
t
e
s
->
A
s
s
i
s
t
a
n
t

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
s19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000026994</IncidentID><IncidentContent>hjj</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>100000011</BigCorpTypeID><DealMan></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsSnatch><Assistant></Assistant><RegionalID>1906030000000005</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=40522da4e3c1764b598ee82e193400fe

A
t
t
r
i
b
u
t
e
-
>
a
t
t
r
i
b
u
t
e
s
->
N
e
w
E
n
d
D
e
g
r
e
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
s19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</UserCode><MeterID>190603000000004</MeterID><StartDegree>1000.00</StartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStartDegree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraDosage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0

At 10
tribut
es ->
Page
Size

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetMessageList&Attribute=<attributes><Net>1</Net><Account>
1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4
E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</C
ommiD><CorpID>1906</CorpID><State>1</State><PageIndex>1</PageIn
dex><PageSize>10</PageSize></attributes>&Class=OnlineMessage&Mac
=7e68cec1012655d7ce99927bb529d069

At 1
tribut
es ->
Page

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetMaterialSearch&Attribute=<attributes><Net>1</Net><Accou
nt>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6
B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</
UserCode><WareHouseName>L9仓库</WareHouseName><MaterialName
></MaterialName><Num></Num><Page>1</Page></attributes>&Class=Se
archManage&Mac=1c0619679d02301e68ebaeecbca5c5e4

At
tribut
es ->
Material
Name

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetMaterialSearch&Attribute=<attributes><Net>1</Net><Accou
nt>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6
B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</
UserCode><WareHouseName>L9仓库</WareHouseName><MaterialName
></MaterialName><Num></Num><Page>1</Page></attributes>&Class=Se
archManage&Mac=1c0619679d02301e68ebaeecbca5c5e4

At 0
tribut
es ->

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account
>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B
4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size
>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTous
u><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><M

at
tri
b
ut
es
->
Is
T
o
us
u

obile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCust
omerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b

At 物业类

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?
Command=GetIncidentBigType&Attribute=<attributes><Net>1</Net><Acco
unt>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F
6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>19060
3</CommID><DrClass>1</DrClass><IncidentPlace>户内</IncidentPlace><
Duty>物业类</Duty></attributes>&Class=PMSIncidentAccept&Mac=a98c9f
57ba5e43c8b6d1bae77c1b2226

XML

at
tri
b
ut
es
->
D
ut
y

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
Is
nc
id
e
nt

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?
Command=GetCustomerList&Attribute=<attributes><Net>1</Net><Account
>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B
4E7038</LoginPwd><CommID>190603</CommID><Page>1</Page><Size
>10</Size><IsOwe>1</IsOwe><IsIncident></IsIncident><IsTousu></IsTous
u><IsDecorate></IsDecorate><CustID></CustID><RoomID></RoomID><M
obile></Mobile><CarparkID></CarparkID></attributes>&Class=SearchCust
omerManage_v2&Mac=2074c16b1b652a170b35f1ae3f39694b

XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
D
e
al
St
ar

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?
Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1
906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E
7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 0
0:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStart
Time></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrCl
ass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState><
/DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper
></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><Incid
entState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10
</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2fe
ae48e680068529a5249c

XML

tT
im
e

At 天问推送测试账号
tribe admins
b
ut
e-
>
at
tribe
but
es
->
D
e
al
M
a
n

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSnatchOrAssign&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026994</IncidentID><IncidentContent>hjj</IncidentContent><Duty>物业类</Duty><BigCorpTypeID>10000011</BigCorpTypeID><DealMan></DealMan><DealManUserCode></DealManUserCode><IsSnatch>1</IsSnatch><Assistant></Assistant><RegionalID>1906030000000005</RegionalID><DispRemarks></DispRemarks></attributes>&Class=IncidentAcceptManage_bl&Mac=40522da4e3c1764b598ee82e193400fe XML

At
tribe
but
e-
>
at
tribe
but
es
->
D
e
al
St
at
e

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c> XML

At 1
tribe 2
b 0
ut
e-
>
at
tribe
but
es
->
Dr
Cl
as
s

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetIncidentBigType&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><DrClass>1</DrClass><IncidentPlace>户内</IncidentPlace><Duty>物业类</Duty></attributes>&Class=PMSIncidentAccept&Mac=a98c9f57ba5e43c8b6d1bae77c1b2226> XML

At uhh
tribe ujh
b hhh
ut
e-

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentDelete&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>190603</CommID><IncidentID>19060300000026993</IncidentID><CloseSituation>uhh> XML

>
at
tri
b
ut
es
->
Cl
os
e
Si
tu
ati
o
n

h</CloseSituation><Type>null</Type></attributes>&Class=IncidentAcceptM
anage_jh&Mac=ccbc884fa4d7c5095af13fce4029874e

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
C
ar
Si
g
n

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetParkSearch&Attribute=<attributes><Net>1</Net><Account>
1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4
E7038</LoginPwd><CommID>190603</CommID><ParkName>ggg</ParkN
ame><CarSign></CarSign><RoomSign></RoomSign><CustID></CustID><
Phone></Phone></attributes>&Class=SearchManage&Mac=84306465e35c
4a2a65c8e9b780673d0f

At 1
tri
b
ut
e-
>
at
tri
b
ut
es
->
U
nit
S
N
u
m

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetFloorRoomList&Attribute=<attributes><Net>1</Net><Accoun
t>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B
4E7038</LoginPwd><CorpID>1906</CorpID><BuildSNum>1</BuildSNum>
<UnitSNum>1</UnitSNum><FloorNum>-3</FloorNum><CommID>190603<
/CommID></attributes>&Class=RoomManage&Mac=411f404a42168ecc955
c5979d4e0db58

At L9仓库
tri
b
ut
e-
>
at
tri
b
ut

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetMaterialSearch&Attribute=<attributes><Net>1</Net><Accou
nt>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6
B4E7038</LoginPwd><CommID>190603</CommID><UserCode>001349</
UserCode><WareHouseName>L9仓库</WareHouseName><MaterialName
></MaterialName><Num></Num><Page>1</Page></attributes>&Class=Se
archManage&Mac=1c0619679d02301e68ebaecbca5c5e4

es
->
W
a
r
e
H
o
u
s
e
N
a
m
e

M 0510235c508553e3e554e7 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? 简单
ac 451b91daba Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
18a07baafa 19</Account><LoginPwd>C61714AC0395696D 6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PM
7e68cec1012655d7ce9992 de>010103</OrganCode><Code>999904</Code></attributes>&Class=PM
7bb529d069 S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba
fcb27f29bd0e7bfe3040b0
decde989
1c0619679d02301e68ebae
ecbca5c5e4
...

At https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net>
b <Account>1906-twzxc</Account><LoginPwd>C61714AC0395696D6B4
ut A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e
e-
>
at
tri
b
ut
es
->
C
u
s
t
i
D

At C61714AC0395696D6B4A https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri 8F0F6B4E7038 Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
b 19</Account><LoginPwd>C61714AC0395696D 6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PM
ut de>010103</OrganCode><Code>999904</Code></attributes>&Class=PM
e- S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba
>
at
tri
b
ut
es
->

L
o
g
i
n
P
w
d

At https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML

tribut-e->attribut-es
Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba

Attribut-es->TaskCategory
<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c> XML

Attribut-es->ExtraDose
<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</UserCode><MeterID>19060300000004</MeterID><StartDegree>1000.00</StartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStartDegree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraDosage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManage&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0> XML

Attribut-e->attribut-es
<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PMS10AppDesktop&Mac=0510235c508553e3e554e7451b91daba> XML

ut
es
->
A
cc
o
u
nt

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
C
ar
p
ar
kl
D

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e> XML

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
C
us
tN
a
m
e

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e> XML

At
tri
b
ut
e

<https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx?Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PM S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba> 简单
链接

<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes><attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</Or

```

ganCode><Code>999902<
/Code></attributes>
<attributes><Net>1</Net><
Account>1906-twzxc19</
Account><LoginPwd>C617
14AC0395696D6B4A8F0F
6B4E7038</LoginPwd><Us
erCode>001349</UserCod
e><CommID>190603</Co
mmID><CorpID>1906</Cor
pID><State>1</State><Pa
geIndex>1</PageIndex><P
ageSize>10</PageSize></
attributes>
<attributes><Net>1</Net><
Account>1906-twzxc19</
Account><LoginPwd>C617
14AC0395696D6B4A8F0F
6B4E7038</LoginPwd><C
ommID>190603</CommID
><WhereStr></WhereStr><
/attributes>
<attributes><Net>1</Net><
Account>1906-twzxc19</
Account><LoginPwd>C617
14AC0395696D6B4A8F0F
6B4E7038</LoginPwd><C
ommID>190603</CommID
><UserCode>001349</Use
rCode><WareHouseName
>L9仓库</WareHouseNam
e><MaterialName></Materi
alName><Num></Num><P
age>1</Page></attributes>

```

...

At tri b ut e- > at tri b ut es -> M et er ID	19060300000004	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetPublicMeterHistory&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><CommID>190603</CommID><MeterID>19060300000004</MeterID></attributes>&Class=MeterManage&Mac=f040a29fb07a834cb4d45702032d2943	XML
At tri b ut e- > at tri b ut	190603	https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCode>010103</OrganCode><Code>999904</Code></attributes>&Class=PM S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba	XML

es
->
C
o
m
m
i
D

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
E
n
d
Ti
m
e

2021-12-31 23:59:59 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1
906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E
7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 0
0:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStart
Time></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrCl
ass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState><
/DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper
></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><Incid
entState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10
</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2fe
ae48e680068529a5249c

At 1 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri null Command=IncidentCanDiscard&Attribute=<attributes><Net>1</Net><Acco
b 3 unt>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F
ut 6B4E7038</LoginPwd><CommID>190603</CommID><Type>1</Type></at
e- tributes>&Class=IncidentAcceptManage_bl&Mac=bae00be940aeb4d37b66
> 8c2bcb2d67db

At 0 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri 1 Command=GetIncidentDealList&Attribute=<attributes><Net>1</Net><Acco
b unt>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F
ut 6B4E7038</LoginPwd><UserCode>001349</UserCode><CommID>19060
e- 3</CommID><DrClass>2</DrClass><IsAll>0</IsAll><PageIndex>1</PageIn
> dex><PageSize>10</PageSize></attributes>&Class=PMSIncidentAccept&
at Mac=eb89b1adcd210afda1e771b848731451

At https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=IncidentClose&Attribute=<attributes><Net>1</Net><Account>19
b 06-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7
ut 038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000
e- 026983</IncidentID><CloseSituation>hhh</CloseSituation><CloseType>0<

>
at
tri
b
ut
es
->
Cl
os
e
R
e
as
o
ns

/CloseType><IsClose>1</IsClose><CloseReasons></CloseReasons></attributes>&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
C
ar
p
ar
k
N
a
m
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e XML

At 1900/01/01
tri
b
ut
e-
>
at
tri
b
ut
es
->
Fr
o
m
D
at
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=FuzzySearchArrearageList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CustID></CustID><CustName></CustName><RoomID></RoomID><RoomSign></RoomSign><CarparkID></CarparkID><CarparkName></CarparkName><FromDate>1900/01/01</FromDate><ToDate>2021/12/30</ToDate><ExcludeUrged>0</ExcludeUrged><ExcludeLetter>0</ExcludeLetter><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=CustomerArrearageManage&Mac=89827636aae053cb751abb5ff17b6d5e XML

At 190603000000026993
tri 190603000000026994
b 190603000000026991
ut 190603000000026984
e- 190603000000026983
> ...

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=GetIncidentSimpleDetail&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000026993</IncidentID></attributes>&Class=PMSIncidentAccept&Mac=7ebe4d7175ae461a40865e227b712ac5 XML

at
tri
b
ut
es
->
In
ci
d
e
nt
ID

At 1
tri
b
ut
e-
>
at
tri
b
ut
es
->
B
uil
d
S
N
u
m

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetFloorRoomList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><BuildSNum>1</BuildSNum><UnitSNum>1</UnitSNum><FloorNum>-3</FloorNum><CommID>190603</CommID></attributes>&Class=RoomManage&Mac=411f404a42168ecc955c5979d4e0db58

At 1
tri
b
ut
e-
>
at
tri
b
ut
es
->
O
p
T
yp
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=GetIncidentCloseList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OpType>1</OpType><PageIndex>1</PageIndex><PageSize>10</PageSize></attributes>&Class=IncidentAcceptManage_bl&Mac=fd51e08a61fe1c2663062f56829afd36

At ghh
tri
b
ut
e-
>
at
tri
b
ut
es
->

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
Command=IncidentTransmit&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000026994</IncidentID><BigCorpTypeID>10000011</BigCorpTypeID><Duty>物业类</Duty><DealMan>天问推送测试账号</DealMan><DealManUserCode>001345</DealManUserCode><TransmitReason>ghh</TransmitReason><ConfirmTransmit>0</ConfirmTransmit></attributes>&Class=IncidentAcceptManage_jh&Mac=9802faf74a9d147b2a23dd803129fcb

Tr
a
n
s
m
i
t
R
e
a
s
o
n

At 100000011 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri 100000016 Command=GetCanDealIncidentUserList&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
s19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><CorpTypeID>100000011</CorpTypeID></attributes>&Class=IncidentAcceptManage_j
h&Mac=54631ce974fb313d98eff97467ee995d

>
a
t
t
r
i
b
u
t
e
s
->
C
o
r
p
T
y
p
e
I
D

At https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=GetParkSearch&Attribute=<attributes><Net>1</Net><Account>
1906-twzxc
s19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><ParkName>ggg</ParkName><CarSign></CarSign><RoomSign></RoomSign><CustID></CustID><Phone></Phone></attributes>&Class=SearchManage&Mac=84306465e35c4a2a65c8e9b780673d0f

>
a
t
t
r
i
b
u
t
e
s
->
P
h
o
n
e

At 1 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=IncidentClose&Attribute=<attributes><Net>1</Net><Account>1906-twzxc
s19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>19060300000026983</IncidentID><CloseSituation>hhh</CloseSituation><CloseType>0</CloseType><IsClose>1</IsClose><CloseReasons></CloseReasons></attributes>&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb

>
a
t
t
r
i
b
u
t
e
s
->
I
s
C
l
o
s

e

At
tri
b
ut
e-
>
at
tri
b
ut
es
->
W
h
er
e
St
r

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=QueryWareHouse&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><WhereStr></WhereStr></attributes>&Class=IncidentAcceptManage&Mac=fccb27f29fbd0e7bfe3040b0decde989 XML

At 2021-12-01 00:00:00
tri
b
ut
e-
>
at
tri
b
ut
es
->
St
ar
tT
im
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=IncidentSearch&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><StartTime>2021-12-01 00:00:00</StartTime><EndTime>2021-12-31 23:59:59</EndTime><DealStartTime></DealStartTime><DealEndTime></DealEndTime><DrClass>0</DrClass><IsTousu>0</IsTousu><TaskCategory></TaskCategory><DealState></DealState><AdmiMan></AdmiMan><DealMan></DealMan><HouseKeeper></HouseKeeper><RoomID></RoomID><RegionalID></RegionalID><IncidentState>全部</IncidentState><pageIndex >1</pageIndex ><pageSize >10</pageSize ></attributes>&Class=PMSIncidentAccept&Mac=9a0742cdc2feae48e680068529a5249c XML

At 0
tri
b
ut
e-
>
at
tri
b
ut
es
->
Cl
os
e
T
yp
e

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=IncidentClose&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><IncidentID>190603000000026983</IncidentID><CloseSituation>hhh</CloseSituation><CloseType>0</CloseType><IsClose>1</IsClose><CloseReasons></CloseReasons></attributes>&Class=PMSIncidentAccept&Mac=c255c2e0ef4adff945a8de60e4a4adfb XML

At 2021-12-08
tri
b
ut
e-
>

https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? Command=PublicMeterInsUpdate&Attribute=<attributes><Net>1</Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4E7038</LoginPwd><CorpID>1906</CorpID><UserCode>001349</UserCode><MeterID>19060300000004</MeterID><StartDegree>1000.00</StartDegree><EndDegree>2000</EndDegree><NewStartDegree></NewStart XML

at Degree><NewEndDegree></NewEndDegree><ExtraDosage>0.00</ExtraD
tri osage><ListDate>2021-12-08</ListDate></attributes>&Class=MeterManag
b e&Mac=5c81444e8c50aa4aa4b8cc8cdf1c1b0
ut
es
->
Li
st
D
at
e

C IBM AppScan binary conte https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx 主体
o nt place holder
m
m
a
n
d

At ggg https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=GetParkSearch&Attribute=<attributes><Net>1</Net><Account>
b 1906-twzxc19</Account><LoginPwd>C61714AC0395696D6B4A8F0F6B4
ut E7038</LoginPwd><CommID>190603</CommID><ParkName>ggg</ParkN
e- ame><CarSign></CarSign><RoomSign></RoomSign><CustID></CustID><
> Phone></Phone></attributes>&Class=SearchManage&Mac=84306465e35c
at 4a2a65c8e9b780673d0f
tri
b
ut
es
->
P
ar
k
N
a
m
e

At 1 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri 0
b
ut
e-
>
at
tri
b
ut
es
->
ls
S
n
at
ch

At 010103 https://pare-twp-stg.pingan.com.cn/TWI/TWInterface/Service/Service.ashx? XML
tri Command=GetAppDesktopStatisticsDetails&Attribute=<attributes><Net>1</
b Net><Account>1906-twzxc19</Account><LoginPwd>C61714AC0395696D
ut 6B4A8F0F6B4E7038</LoginPwd><CommID>190603</CommID><OrganCo
e- de>010103</OrganCode><Code>999904</Code></attributes>&Class=PM
> S10AppDesktop&Mac=0510235c508553e3e554e7451b91daba

失败的请求 0

TOC

URL	原因
-----	----

已过滤的 URL 1

TOC

URL	原因
http://www.baidu.com/	未测试的 Web Server

注释 0

TOC

URL	注释
-----	----

JavaScript 0

TOC

URL / 代码

cookie 0

TOC

名称	首先设置	域	安全
值	请求的 URL		到期