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 HCL AppScan Standard 创建 10.0.0, 规则： 0
扫描开始时间： 2025/1/23 15:21:32

目录

介绍

该报告包含由 HCL 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：	8
低严重性问题：	23
参考严重性问题：	3
报告中包含的严重性问题总数：	35
扫描中发现的严重性问题总数：	35

常规信息

扫描文件名称：	user
扫描开始时间：	2025/1/23 15:21:32
测试策略：	Default

主机	192.168.1.1
端口	80
操作系统：	未知
Web 服务器：	未知
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
会话中检测：	已启用
会话中模式：	`user_index":"1`
跟踪或会话 ID cookie：	`Token`
跟踪或会话 ID 参数：	`web_login_password`
登陆序列：	`http://192.168.1.1/` `http://192.168.1.1/boaform/web_login_exe.cgi`

```
http://192.168.1.1/welcome.html
http://192.168.1.1/boaform/login_user_index_show.cgi
```

摘要

问题类型 10

TOC

	问题类型	问题的数量
高	存储的跨站点脚本编制	1
中	跨站点请求伪造	8
低	“Content-Security-Policy”头缺失或不安全	5
低	“X-Content-Type-Options”头缺失或不安全	5
低	“X-XSS-Protection”头缺失或不安全	5
低	Microsoft IIS 缺少 Host 头信息泄露	1
低	查询中接受的主体参数	2
低	跨帧脚本编制防御缺失或不安全	5
参	发现可能的服务器路径泄露模式	1
参	发现内部 IP 泄露模式	2

有漏洞的 URL 15

TOC

	URL	问题的数量
高	http://192.168.1.1/aoaform/url_filter_show.cgi	3
中	http://192.168.1.1/aoaform/device_basic_show.cgi	2
中	http://192.168.1.1/aoaform/url_filter_set.cgi	2
中	http://192.168.1.1/aoaform/wan_connect_show.cgi	1
中	http://192.168.1.1/boaform/login_user_index_show.cgi	2
中	http://192.168.1.1/boaform/web_loid_auth_ext.cgi	3
中	http://192.168.1.1/boaform/web_loid_auth_show.cgi	2
中	http://192.168.1.1/js/common.js	1
低	http://192.168.1.1/	4
低	http://192.168.1.1/boaform/web_login_exe.cgi	4
低	http://192.168.1.1/js/aes_1.js	3
低	http://192.168.1.1/js/main.js	3

低	http://192.168.1.1/welcome.html	3	
参	http://192.168.1.1/js/jquery.js	1	
参	http://192.168.1.1/aoaform/admin/url_filter_show.cgi	1	

修订建议 10

TOC

	修复任务	问题的数量
高	查看危险字符注入的可能解决方案	1
中	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	8
低	除去 Web 站点中的内部 IP 地址	2
低	根据 Q218180 应用配置更改	1
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	5
低	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头	5
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	5
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	5
低	请勿接受在查询字符串中发送的主体参数	2
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	1

安全风险 4

TOC

	风险	问题的数量
高	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	9
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	25
低	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	22
参	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	1

原因 5

TOC

	原因	问题的数量
高	未对用户输入正确执行危险字符清理	1

中	应用程序使用的认证方法不充分	8
低	Web 应用程序编程或配置不安全	24
低	Web 服务器或应用程序服务器是以不安全的方式配置的	1
参	未安装第三方产品的最新补丁或最新修补程序	1

WASC 威胁分类

TOC

威胁	问题的数量
跨站点脚本编制	1
跨站点请求伪造	8
信息泄露	26

按问题类型分类的问题

高 存储的跨站点脚本编制 1 TOC

问题 1 / 1 TOC

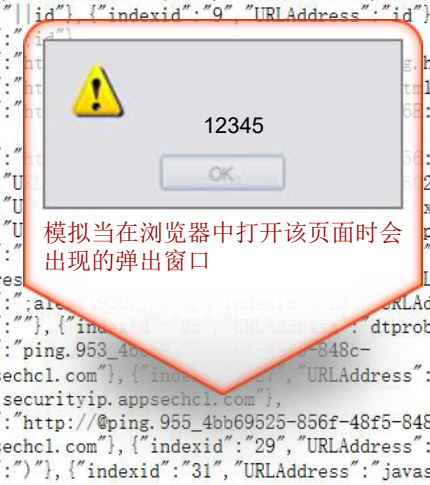
存储的跨站点脚本编制

严重性:	高
CVSS 分数:	7.5
URL:	http://192.168.1.1/aoaform/url_filter_show.cgi
实体:	url_filter_show.cgi (Global)
风险:	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
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

推理: 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

测试响应

{ "retcode":"0", "data":{"URL_filter_enable_checkbox":"0","ExcludeMode_select":"1","SeW_list":
[{"indexid":"2","URLAddress":"WFXSSProbe"},{"indexid":"3","URLAddress":"AB"},
{"indexid":"4","URLAddress":"/../WEB-INF/web.xml"},{"indexid":"5","URLAddress":"/WEB-
INF/web.xml"},{"indexid":"6","URLAddress":"|id"},{"indexid":"7","URLAddress":"&&id"},
{"indexid":"8","URLAddress":"||id"},{"indexid":"9","URLAddress":"id"},
{"indexid":"10","URLAddress":"
{"indexid":"11","URLAddress":"
{"indexid":"12","URLAddress":"
{"indexid":"13","URLAddress":"
varId=904"},
{"indexid":"14","URLAddress":"
varId=905"},{"indexid":"15","U
varId=906"},{"indexid":"16","U
varId=907"},{"indexid":"17","U
{"indexid":"18","URLAddress":"
+"},{"indexid":"20","URLAddres
{"indexid":"22","URLAddress":"
{"indexid":"24","URLAddress":""},{"
{"indexid":"26","URLAddress":"ping.953_4
762ec551e2f7.securityip.appsechcl.com"},{"
856f-48f5-848c-762ec551e2f7.securityip.appsechcl.com"},
{"indexid":"28","URLAddress":"http://@ping.955_4bb69525-856f-48f5-848c-
762ec551e2f7.securityip.appsechcl.com"},{"indexid":"29","URLAddress":";"},
{"indexid":"30","URLAddress":")"},{"indexid":"31","URLAddress":"javascript:alert(957)"}]} }



模拟当在浏览器中打开该页面时会出现的弹出窗口

未经处理的测试响应：

```
...

Host: 192.168.1.1
X-Forwarded-For: '
X-Requested-With: XMLHttpRequest
Content-Length: 0
Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 1935
Content-Type: text/html

{
    "retcode":"0",
    "data":{"URL_filter_enable_checkbox":"0","ExcludeMode_select":"1","SeW_list":
[{"indexid":"2","URLAddress":"WFXSSProbe"},{"indexid":...

...

...


{
    "retcode":"0",
    "data":{"URL_filter_enable_checkbox":"0","ExcludeMode_select":"1","SeW_list":
[{"indexid":"2","URLAddress":"WFXSSProbe"},{"indexid":"3","URLAddress":"AB"},
{"indexid":"4","URLAddress":"/../WEB-INF/web.xml"},{"indexid":"5","URLAddress":"/WEB-
INF/web.xml"},{"indexid":"6","URLAddress":"|id"},{"indexid":"7","URLAddress":"&&id"},
{"indexid":"8","URLAddress":"||id"},{"indexid":"9","URLAddress":"id"},{"...
```

```
}
...
```

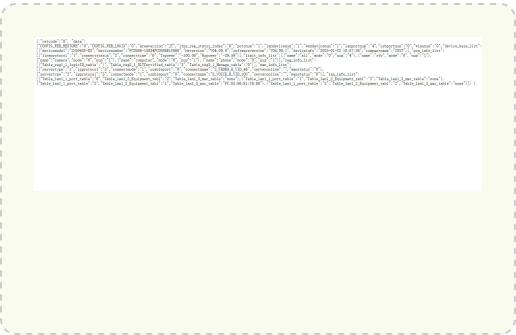
中 跨站点请求伪造 8 TOC

问题 1 / 8 TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/aoaform/device_basic_show.cgi
实体：	device_basic_show.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

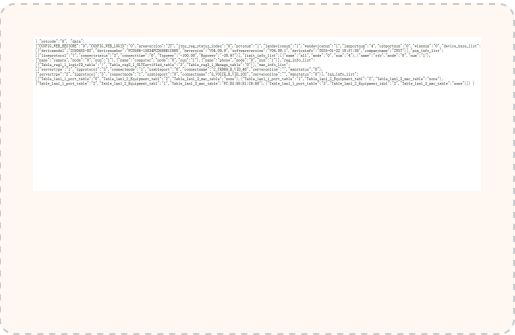
推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应



≈

测试响应



问题 2 / 8 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/boaform/login_user_index_show.cgi
实体：	login_user_index_show.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应

≈

测试响应

问题 3 / 8

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/boaform/web_loid_auth_show.cgi
实体：	web_loid_auth_show.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应

≈

测试响应

问题 4 / 8

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/aoaform/wan_connect_show.cgi
实体：	wan_connect_show.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应

≈

测试响应

问题 5 / 8

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	web_loid_auth_ext.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应

≈

测试响应

问题 6 / 8

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/js/common.js
实体：	common.js (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

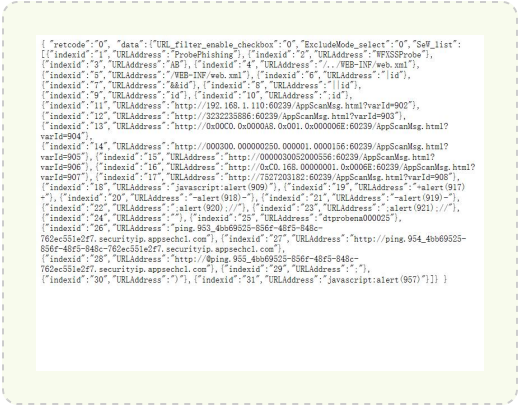
问题 7 / 8

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/aoaform/url_filter_show.cgi
实体：	url_filter_show.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

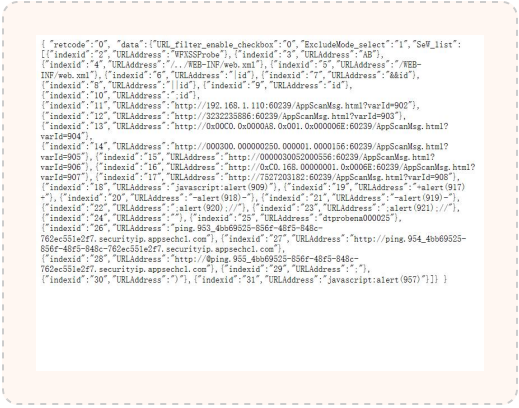
推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应


{"retcode":"0","data":{"URL_filter_enable_checkbox":"0","ExcludeMode_select":"0","SeW_list":[{"indexid":"1","URLAddress":"ProbePhishing"},{"indexid":"2","URLAddress":"WFSSProbe"},{"indexid":"3","URLAddress":"AB"},{"indexid":"4","URLAddress":"/../WEB-INF/web.xml"},{"indexid":"5","URLAddress":"/WEB-INF/web.xml"},{"indexid":"6","URLAddress":"|id"},{"indexid":"7","URLAddress":"&&id"},{"indexid":"8","URLAddress":"||id"},{"indexid":"9","URLAddress":"id"},{"indexid":"10","URLAddress":";id"},{"indexid":"11","URLAddress":"http://192.168.1.110:60239/AppScanMsg.html?varId=902"},{"indexid":"12","URLAddress":"http://3232233886:60239/AppScanMsg.html?varId=903"},{"indexid":"13","URLAddress":"http://0x00C0.0x000A8.0x001.0x000006E:60239/AppScanMsg.html?varId=904"},{"indexid":"14","URLAddress":"http://000300.000000250.000001.0000156:60239/AppScanMsg.html?varId=905"},{"indexid":"15","URLAddress":"http://0000030052000556:60239/AppScanMsg.html?varId=906"},{"indexid":"16","URLAddress":"http://0xC0.168.00000001.0x0006E:60239/AppScanMsg.html?varId=907"},{"indexid":"17","URLAddress":"http://7527203182:60239/AppScanMsg.html?varId=908"},{"indexid":"18","URLAddress":"javascript:alert(909)"},{"indexid":"19","URLAddress":"+alert(917)+"},{"indexid":"20","URLAddress":"-alert(918)-"},{"indexid":"21","URLAddress":"-alert(919)-"},{"indexid":"22","URLAddress":";alert(920)://"},{"indexid":"23","URLAddress":";alert(921)://"},{"indexid":"24","URLAddress":";"},{"indexid":"25","URLAddress":"dtprobena000025"},{"indexid":"26","URLAddress":"ping.953_4bb69525-856f-48f8-848c-762ec351e2f7.securityip.appsechcl.com"},{"indexid":"27","URLAddress":"http://ping.954_4bb69525-856f-48f8-848c-762ec351e2f7.securityip.appsechcl.com"},{"indexid":"28","URLAddress":"http://@ping.955_4bb69525-856f-48f8-848c-762ec351e2f7.securityip.appsechcl.com"},{"indexid":"29","URLAddress":":"},{"indexid":"30","URLAddress":")"},{"indexid":"31","URLAddress":"javascript:alert(957)"}]} }

≈

测试响应


{"retcode":"0","data":{"URL_filter_enable_checkbox":"0","ExcludeMode_select":"1","SeW_list":[{"indexid":"2","URLAddress":"WFSSProbe"},{"indexid":"3","URLAddress":"AB"},{"indexid":"4","URLAddress":"/../WEB-INF/web.xml"},{"indexid":"5","URLAddress":"/WEB-INF/web.xml"},{"indexid":"6","URLAddress":"|id"},{"indexid":"7","URLAddress":"&&id"},{"indexid":"8","URLAddress":"||id"},{"indexid":"9","URLAddress":"id"},{"indexid":"10","URLAddress":";id"},{"indexid":"11","URLAddress":"http://192.168.1.110:60239/AppScanMsg.html?varId=902"},{"indexid":"12","URLAddress":"http://3232233886:60239/AppScanMsg.html?varId=903"},{"indexid":"13","URLAddress":"http://0x00C0.0x000A8.0x001.0x000006E:60239/AppScanMsg.html?varId=904"},{"indexid":"14","URLAddress":"http://000300.000000250.000001.0000156:60239/AppScanMsg.html?varId=905"},{"indexid":"15","URLAddress":"http://0000030052000556:60239/AppScanMsg.html?varId=906"},{"indexid":"16","URLAddress":"http://0xC0.168.00000001.0x0006E:60239/AppScanMsg.html?varId=907"},{"indexid":"17","URLAddress":"http://7527203182:60239/AppScanMsg.html?varId=908"},{"indexid":"18","URLAddress":"javascript:alert(909)"},{"indexid":"19","URLAddress":"+alert(917)+"},{"indexid":"20","URLAddress":"-alert(918)-"},{"indexid":"21","URLAddress":"-alert(919)-"},{"indexid":"22","URLAddress":";alert(920)://"},{"indexid":"23","URLAddress":";alert(921)://"},{"indexid":"24","URLAddress":";"},{"indexid":"25","URLAddress":"dtprobena000025"},{"indexid":"26","URLAddress":"ping.953_4bb69525-856f-48f8-848c-762ec351e2f7.securityip.appsechcl.com"},{"indexid":"27","URLAddress":"http://ping.954_4bb69525-856f-48f8-848c-762ec351e2f7.securityip.appsechcl.com"},{"indexid":"28","URLAddress":"http://@ping.955_4bb69525-856f-48f8-848c-762ec351e2f7.securityip.appsechcl.com"},{"indexid":"29","URLAddress":":"},{"indexid":"30","URLAddress":")"},{"indexid":"31","URLAddress":"javascript:alert(957)"}]} }

问题 8 / 8

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/aoaform/url_filter_set.cgi
实体：	url_filter_set.cgi (Page)
风险：	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
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

原始响应

≈

测试响应

低 “Content-Security-Policy”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_exe.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

X-Requested-With: XMLHttpRequest
Content-Length: 103
Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

web_login_name=user&web_login_password=002699af2eb4727ac636c4acbdf3ed95d25b66b59165f85bfec5514033
510da2

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=g815Xv7DL7OetkM5RKV6LIW4BsOqTp2; path=/
Content-Type: text/html

{
    "retcode":"1",
    "data":{"result":"success_useradmin"}
}
...
```

问题 2 / 5

TOC

“Content-Security-Policy”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/js/main.js
实体：	main.js (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/welcome.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 22405
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

/*
 页面加载完成执行
*/
$(document).ready(function(){
...
```

问题 3 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/welcome.html
实体：	welcome.html (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Referer: http://192.168.1.1/
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: keep-alive
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 4829
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>中国联通智能网关</title>
 <link href="/css/basic.css?v=20250122105705" rel="stylesheet">
 <link href="/css/operator.css?v=20250122105705" rel="stylesheet">
...
```

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/js/aes_1.js
实体：	aes_1.js (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/welcome.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 19061
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
  if(passwd_key.charCodeAt(i) < 16){
   key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
  }
  else{
   key += (passwd_key.charCodeAt(i)).toString(16);
  }
...
```

问题 5 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	(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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/admin/help.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 4330
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>中国联通智能网关</title>
 <link href="/css/basic.css?v=20250122105705" rel="stylesheet">
 <link href="/css/operator.css?v=20250122105705" rel="stylesheet">
...
```

低 “X-Content-Type-Options”头缺失或不安全 5

TOC

问题 1 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	(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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/admin/help.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 4330
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>中国联通智能网关</title>
 <link href="/css/basic.css?v=20250122105705" rel="stylesheet">
 <link href="/css/operator.css?v=20250122105705" rel="stylesheet">
...
```

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_exe.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

X-Requested-With: XMLHttpRequest
Content-Length: 103
Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

web_login_name=user&web_login_password=002699af2eb4727ac636c4acbdf3ed95d25b66b59165f85bfec5514033
510da2

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=g815Xv7DL7OetkM5RKV6LIW4BsOqTp2; path=/
Content-Type: text/html

{
    "retcode":"1",
    "data":{"result":"success_useradmin"}
}
...
```

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/js/main.js
实体：	main.js (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/welcome.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 22405
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

/*
 页面加载完成执行
*/
$(document).ready(function(){
...
```

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/welcome.html
实体：	welcome.html (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Referer: http://192.168.1.1/
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: keep-alive
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 4829
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>中国联通智能网关</title>
 <link href="/css/basic.css?v=20250122105705" rel="stylesheet">
 <link href="/css/operator.css?v=20250122105705" rel="stylesheet">
...
```

问题 5 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/js/aes_1.js
实体：	aes_1.js (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/welcome.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 19061
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
  if(passwd_key.charCodeAt(i) < 16){
   key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
  }
  else{
   key += (passwd_key.charCodeAt(i)).toString(16);
  }
...
```

低 “X-XSS-Protection”头缺失或不安全 5

TOC

问题 1 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_exe.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

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

未经处理的测试响应：

```
...

X-Requested-With: XMLHttpRequest
Content-Length: 103
Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

web_login_name=user&web_login_password=002699af2eb4727ac636c4acbdf3ed95d25b66b59165f85bfec5514033
510da2

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=g815Xv7DL7OetkM5RKV6LIW4BsOqTp2; path=/
Content-Type: text/html

{
    "retcode":"1",
    "data":{"result":"success_useradmin"}
}
...
```

问题 2 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	(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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

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

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/admin/help.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 4330
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>中国联通智能网关</title>
 <link href="/css/basic.css?v=20250122105705" rel="stylesheet">
 <link href="/css/operator.css?v=20250122105705" rel="stylesheet">
...
```

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/js/main.js
实体：	main.js (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

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

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/welcome.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 22405
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

/*
 页面加载完成执行
*/
$(document).ready(function(){
...
```

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/welcome.html
实体：	welcome.html (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

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

未经处理的测试响应：

```
...

Referer: http://192.168.1.1/
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: keep-alive
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 4829
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
 <title>中国联通智能网关</title>
 <link href="/css/basic.css?v=20250122105705" rel="stylesheet">
 <link href="/css/operator.css?v=20250122105705" rel="stylesheet">
...
```

问题 5 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/js/aes_1.js
实体：	aes_1.js (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

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

未经处理的测试响应：

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.1.1/welcome.html
Cookie: Token=1hW2xq5N65eBNkgtI2DHd25WZtUJIUQ
Connection: Keep-Alive
Host: 192.168.1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 19061
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

var passwd_key = ""
function encryted_pwd(pwd){
 var key = "";
 for(var i = 0; i < passwd_key.length; i++){
  if(passwd_key.charCodeAt(i) < 16){
   key += ("0" + (passwd_key.charCodeAt(i)).toString(16));
  }
  else{
   key += (passwd_key.charCodeAt(i)).toString(16);
  }
...
```

低 Microsoft IIS 缺少 Host 头信息泄露 1

TOC

问题 1 / 1

TOC

Microsoft IIS 缺少 Host 头信息泄露

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	/ (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：	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：	根据 Q218180 应用配置更改

推理： 测试响应在“Location”或“Content-Location”HTTP 头中包含内部 IP 地址，此地址可用于进一步针对站点进行攻击。

未经处理的测试响应：

```
...
GET / HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.0 302 Moved Temporarily
Location: http://192.168.1.1:80/pon_err.html
Connection: close
Server: HSANHomeGateway
Content-Type: text/html

HTTP/1.0 200 OK
Server: HSANHomeGateway
Connection: close
Content-Length: 4330
Content-Type: text/html

...
```

低 查询中接受的主体参数 2

TOC

问题 1 / 2

TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	web_loid_auth_ext.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	请勿接受在查询字符串中发送的主体参数

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

原始响应

≈

测试响应

问题 2 / 2

TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/aoaform/url_filter_set.cgi
实体：	url_filter_set.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	请勿接受在查询字符串中发送的主体参数

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

原始响应

≈

测试响应

低 跨帧脚本编制防御缺失或不安全 5 TOC

问题 1 / 5 TOC

跨帧脚本编制防御缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_exe.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

web_login_name=user&web_login_password=002699af2eb4727ac636c4acbdf3ed95d25b66b59165f85bfec5514033
510da2

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=BFGrbcFm1VEu6bC61g71kT5aJZLE45S; path=/
Content-Type: text/html
```

```
{
    "retcode":"1",
    "data":{"result":"success_useradmin"}
}
...
```

问题 2 / 5

TOC

跨帧脚本编制防御缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/login_user_index_show.cgi
实体：	login_user_index_show.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 52
Content-Type: text/html

{
    "retcode":"0",
    "data":{"user_index":"1"}
}
...
```

问题 3 / 5

TOC

跨帧脚本编制防御缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_loid_auth_show.cgi
实体：	web_loid_auth_show.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击
未经处理的测试响应：

```
...

Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 287
Content-Type: text/html

{
    "retcode":"0",
    "data":
{"login_name":")","login_password_enable":"0","login_password":"","web_ucStatus":"99","web_ucResu
lt":"99","web_loidplan":"20","web_service_current":"","web_service_plan":"","web_service_count":"
0","web_device_type":"0","web_uplink_type":"7","times":"0"}
}
...
```

问题 4 / 5

TOC

跨帧脚本编制防御缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/aoaform/device_basic_show.cgi
实体：	device_basic_show.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Accept: */*
Origin: http://192.168.1.1
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 1597
Content-Type: text/html

{
    "retcode":"0",
    "data":
{"CONFIG_WEB_RESTORE":"0","CONFIG_WEB_LOGIN":"0","areaversion":"JT","itms_reg_status_index":"0","
potsnum":"1","landevicenum":"1","wandevicenum":"1","lanportnum":"4","usbportnum":"0","wlannum":"0
","device_base_list":[{"devicemodel":"ZN504XG-D2","devicenumber":"FCD586-
15834FCD586E1C660","hwversion":"V04.00.0","softwareversion":"V04.00.1","deviceinfo":"2025-01-22
10:57:36","companyname":"ZNXT"}],"pon_info_list":
[{"lineprotocol":"7","connectstatus":"2","connecttime":"0","Txpower":"-100.00","Rxpower":"-
30.97"}],"limit_info_list":[{"name":"all","mode":"0","num":"4"},
{"name":"stb","mode":"0","num":"1"},{"name":"camera","mode":"0","num":"1"},
{"name":"computer","mode":"0","num":"1"},{"name":"phone","mode":"0","num":"1"}],"reg_info_list":
[{"Table_reg1_1_logic...
...
```

问题 5 / 5

TOC

跨帧脚本编制防御缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	web_loid_auth_ext.cgi (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 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
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

未经处理的测试响应：

```
...

Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

login_name=&login_password=

HTTP/1.0 200 OK
```

```
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

{
    "retcode":"1",
    "data":{"param":"all","errinfo":"null error"}
}
...
```

参 发现可能的服务器路径泄露模式 1

TOC

问题 1 / 1

TOC

发现可能的服务器路径泄露模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://192.168.1.1/js/jquery.js
实体：	jquery.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...

var whitespace = "[\\x20\\t\\r\\n\\f]";
...

...

 // https://www.w3.org/TR/css-syntax-3/#ident-token-diagram
 identifier = "(?:\\\\[\\da-fA-F]{1,6}" + whitespace +
  "?|\\\\[^\\r\\n\\f]|[\\w-]|[^\0-\\x7f])+",
...
```

参 发现内部 IP 泄露模式 2

TOC

问题 1 / 2

TOC

发现内部 IP 泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://192.168.1.1/aoaform/admin/url_filter_show.cgi
实体：	url_filter_show.cgi (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：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的内部 IP 地址

推理： AppScan 在响应中发现了看似为内部 IP 地址的内容。
未经处理的测试响应：

```
...

Connection: close
Server: HSANHomeGateway
Content-Length: 1935
Content-Type: text/html

...id":"9","URLAddress":"id"},{"indexid":"10","URLAddress":";id"},
{"indexid":"11","URLAddress":"http://192.168.1.110:60239/AppScanMsg.html?varId=902"},
{"indexid":"12","URLAddress":"http://3232235886:60239/AppScanMsg....

...
```

问题 2 / 2

TOC

发现内部 IP 泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://192.168.1.1/aoaform/url_filter_show.cgi
实体：	url_filter_show.cgi (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：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的内部 IP 地址

推理： AppScan 在响应中发现了看似为内部 IP 地址的内容。
未经处理的测试响应：

```
...

Connection: close
Server: HSANHomeGateway
Content-Length: 1935
```

```
Content-Type: text/html

...id":"9","URLAddress":"id"},{"indexid":"10","URLAddress":";id"},
{"indexid":"11","URLAddress":"http://192.168.1.110:60239/AppScanMsg.html?varId=902"},
{"indexid":"12","URLAddress":"http://3232235886:60239/AppScanMsg....

...
```