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： 2025/2/17 10:55:26

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

- Linux 中的 Oracle WebLogic 服务器远程命令执行 1
- Parameter Command Injection 8
- Windows 中的 Oracle WebLogic 服务器远程命令执行 1
- ADNS 盲 SSRF 8
- 跨站点请求伪造 4
- “Content-Security-Policy”头缺失或不安全 5
- “X-Content-Type-Options”头缺失或不安全 5
- “X-XSS-Protection”头缺失或不安全 5
- 查询中接受的主体参数 1
- 发现潜在注册信息 1
- 跨帧脚本编制防御缺失或不安全 3
- 发现可能的服务器路径泄露模式 1

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：	10
中等严重性问题：	12
低严重性问题：	20
参考严重性问题：	1
报告中包含的严重性问题总数：	43
扫描中发现的严重性问题总数：	43

常规信息

扫描文件名称： user1g-2

扫描开始时间： 2025/2/17 10:55:26

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/boaform/web_login_exe.cgi
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 12

TOC

	问题类型	问题的数量
高	Linux 中的 Oracle WebLogic 服务器远程命令执行	1
高	Parameter Command Injection	8
高	Windows 中的 Oracle WebLogic 服务器远程命令执行	1
中	ADNS 盲 SSRF	8
中	跨站点请求伪造	4
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	查询中接受的主体参数	1
低	发现潜在注册信息	1
低	跨帧脚本编制防御缺失或不安全	3
参	发现可能的服务器路径泄露模式	1

有漏洞的 URL 10

TOC

	URL	问题的数量
高	http://192.168.1.1/	6
高	http://192.168.1.1/boaform/web_login_exe.cgi	9
高	http://192.168.1.1/boaform/web_loid_auth_ext.cgi	7
高	http://192.168.1.1/js/aes_1.js	5
高	http://192.168.1.1/js/bigInt.js	3
高	http://192.168.1.1/js/jquery.js	3
高	http://192.168.1.1/js/main.js	2
中	http://192.168.1.1/boaform/web_loid_auth_show.cgi	2
低	http://192.168.1.1/boaform/login_user_index_show.cgi	3
低	http://192.168.1.1/welcome.html	3

修订建议 11

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	8
高	升级至 Oracle WebLogic 服务器组件的最新版本，或者应用最新的补丁	2
中	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	4
中	验证和清理所有外部提供的数据。验证访问控制机制。	8
低	不要在可以轻易猜测到的文件名中保存敏感信息，或者限制对它们的访问	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	3
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	1
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 6

TOC

	风险	问题的数量
高	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容	10
中	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。	8
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	4
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	20
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	19
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	未安装第三方产品的最新补丁或最新修补程序	3	
高	Sanitation of hazardous characters was not performed correctly on user input	8	
中	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI	8	
中	应用程序使用的认证方法不充分	4	
低	Web 应用程序编程或配置不安全	20	

WASC 威胁分类

TOC

威胁	问题的数量
操作系统命令	10
服务器端请求伪造	8
跨站点请求伪造	4
信息泄露	21

按问题类型分类的问题

高 Linux 中的 Oracle WebLogic 服务器远程命令执行 1 TOC

问题 1 / 1 TOC

Linux 中的 Oracle WebLogic 服务器远程命令执行

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/
实体：	aes_1.js (Page)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
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：	升级至 Oracle WebLogic 服务器组件的最新版本，或者应用最新的补丁

推理：

未经处理的测试响应：

```
HTTP/1.0 400 Bad Request
Connection: close
Server: HSANHomeGateway
Content-Type: text/html

<HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
<BODY><H1>400 Bad Request</H1>
Your client has issued a malformed or illegal request.
</BODY></HTML>...
```

高 Parameter Command Injection 8 TOC

问题 1 / 8

TOC

Parameter Command Injection

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	login_name (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

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

问题 2 / 8

TOC

Parameter Command Injection

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	login_password (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
```

```
Content-Length: 72
Content-Type: text/html

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

问题 3 / 8

TOC

Parameter Command Injection	
严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/js/aes_1.js
实体：	v (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：
未经处理的测试响应：

```
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);
                }
        }
 if (key.length > 64){
         key = key.slice(0,64);
...
```

问题 4 / 8

TOC

Parameter Command Injection

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/js/jquery.js
实体：	v (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：
未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 285313
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

/*!
 * jQuery JavaScript Library v3.7.1
 * https://jquery.com/
 *
 * Copyright OpenJS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2023-08-28T13:37Z
 */
( function( global, factory ) {
...
```

问题 5 / 8

TOC

Parameter Command Injection

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_password (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：
未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

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

问题 6 / 8

TOC

Parameter Command Injection	
严重性:	高
CVSS 分数:	10.0
URL:	http://192.168.1.1/js/bigInt.js
实体:	v (Parameter)
风险:	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因:	Sanitation of hazardous characters was not performed correctly on user input
固定值:	查看危险字符注入的可能解决方案

推理:

未经处理的测试响应:

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 46521
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

////////////////////////////////////////////////////////////////////////////////////
// header
////////////////////////////////////////////////////////////////////////////////////
var __BIGINT_RADIX = 10;

var __BIGINT_POWER = 7;

var __BIGINT_UNIT = Math.pow( __BIGINT_RADIX, __BIGINT_POWER );
var __BIGINT_UNIT_MINUS_1 = __BIGINT_UNIT - 1;
var __BIGINT_HALF_UNIT = __BIGINT_UNIT / 2;

var __BIGINT_JS_INT_MAX = Math.pow(2, 53);// 90 0719925 4740992

...
```

问题 7 / 8

TOC

Parameter Command Injection

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/js/main.js
实体：	v (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：
未经处理的测试响应：

```
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 8 / 8

TOC

Parameter Command Injection

严重性：	高
CVSS 分数：	10.0
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_name (Parameter)
风险：	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
原因：	Sanitation of hazardous characters was not performed correctly on user input
固定值：	查看危险字符注入的可能解决方案

推理：
未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html
```

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

高 Windows 中的 Oracle WebLogic 服务器远程命令执行 1 TOC

问题 1 / 1 TOC

Windows 中的 Oracle WebLogic 服务器远程命令执行

严重性:	高
CVSS 分数:	10.0
URL:	http://192.168.1.1/
实体:	aes_1.js (Page)
风险:	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容
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:	升级至 Oracle WebLogic 服务器组件的最新版本，或者应用最新的补丁

推理:
未经处理的测试响应:

```
HTTP/1.0 400 Bad Request
Connection: close
Server: HSANHomeGateway
Content-Type: text/html

<HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
<BODY><H1>400 Bad Request</H1>
Your client has issued a malformed or illegal request.
</BODY></HTML>...
```

中 ADNS 盲 SSRF 8 TOC

问题 1 / 8 TOC

ADNS 盲 SSRF	
严重性:	中
CVSS 分数:	5.9
URL:	http://192.168.1.1/js/aes_1.js
实体:	v (Parameter)
风险:	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因:	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值:	验证和清理所有外部提供的数据。验证访问控制机制。

推理:

未经处理的测试响应:

```
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);
                }
        }
 if (key.length > 64){
         key = key.slice(0,64);
...
```

问题 2 / 8 TOC

ADNS 盲 SSRF

严重性：	中
CVSS 分数：	5.9
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	login_name (Parameter)
风险：	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因：	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值：	验证和清理所有外部提供的数据。验证访问控制机制。

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

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

问题 3 / 8

TOC

ADNS 盲 SSRF

严重性：	中
CVSS 分数：	5.9
URL：	http://192.168.1.1/boaform/web_loid_auth_ext.cgi
实体：	login_password (Parameter)
风险：	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因：	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值：	验证和清理所有外部提供的数据。验证访问控制机制。

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
```

```
Content-Length: 72
Content-Type: text/html

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

问题 4 / 8

TOC

ADNS 盲 SSRF	
严重性：	中
CVSS 分数：	5.9
URL：	http://192.168.1.1/js/bigInt.js
实体：	v (Parameter)
风险：	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因：	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值：	验证和清理所有外部提供的数据。验证访问控制机制。

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 46521
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

////////////////////////////////////////////////////////////////////////////////////
// header
////////////////////////////////////////////////////////////////////////////////////
var __BIGINT_RADIX = 10;

var __BIGINT_POWER = 7;

var __BIGINT_UNIT = Math.pow( __BIGINT_RADIX, __BIGINT_POWER );
var __BIGINT_UNIT_MINUS_1 = __BIGINT_UNIT - 1;
var __BIGINT_HALF_UNIT = __BIGINT_UNIT / 2;

var __BIGINT_JS_INT_MAX = Math.pow(2, 53);// 90 0719925 4740992

...
```

问题 5 / 8

TOC

ADNS 盲 SSRF

严重性：	中
CVSS 分数：	5.9
URL：	http://192.168.1.1/js/main.js
实体：	v (Parameter)
风险：	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因：	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值：	验证和清理所有外部提供的数据。验证访问控制机制。

推理：

未经处理的测试响应：

```
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 6 / 8

TOC

ADNS 盲 SSRF

严重性：	中
CVSS 分数：	5.9
URL：	http://192.168.1.1/js/jquery.js
实体：	v (Parameter)
风险：	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因：	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值：	验证和清理所有外部提供的数据。验证访问控制机制。

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
```

```
Connection: close
Server: HSANHomeGateway
Content-Length: 285313
Cache-control: public,max-age=86400
Content-Type: application/x-javascript

/*!
 * jQuery JavaScript Library v3.7.1
 * https://jquery.com/
 *
 * Copyright OpenJS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2023-08-28T13:37Z
 */
( function( global, factory ) {
...
```

问题 7 / 8

TOC

ADNS 盲 SSRF

严重性:	中
CVSS 分数:	5.9
URL:	http://192.168.1.1/boaform/web_login_exe.cgi
实体:	web_login_name (Parameter)
风险:	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因:	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值:	验证和清理所有外部提供的数据。验证访问控制机制。

推理:

未经处理的测试响应:

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

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

问题 8 / 8

TOC

ADNS 盲 SSRF

严重性：	中
CVSS 分数：	5.9
URL：	http://192.168.1.1/boaform/web_login_exe.cgi
实体：	web_login_password (Parameter)
风险：	攻击者可以检索未授权的资源，并且影响这些资源的完整性。可以使用应用程序的服务器对包括内部网络在内的不同网络进行扫描，这些服务器可以放入各种黑名单中。
原因：	Incorrect processing, sanitation, or validation of user input that contain elements later joined with URI
固定值：	验证和清理所有外部提供的数据。验证访问控制机制。

推理：

未经处理的测试响应：

```
HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 72
Content-Type: text/html

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

中 跨站点请求伪造 4 TOC

问题 1 / 4 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 2 / 4

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 3 / 4

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://192.168.1.1/js/bigInt.js
实体：	bigInt.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。

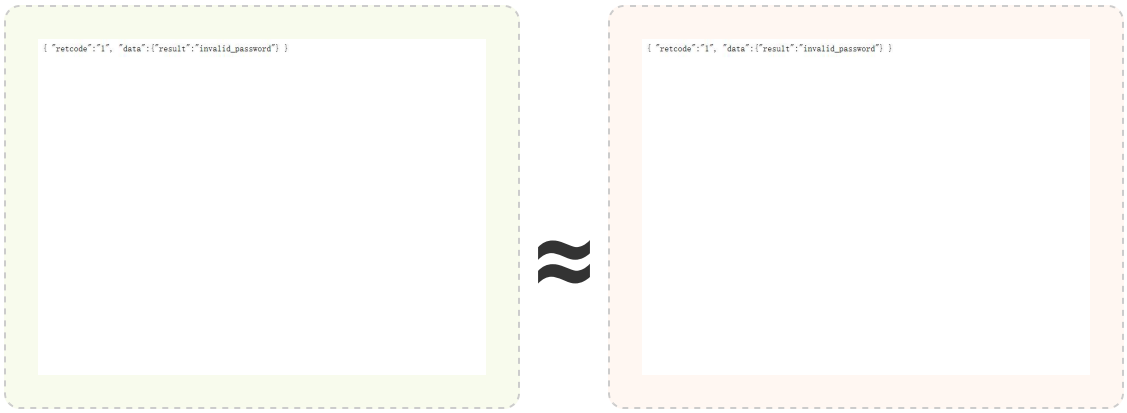
问题 4 / 4

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_login_exe.cgi
实体：	web_login_password (Parameter)
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 CSRF 令牌。

原始响应 **测试响应**


{ "retcode":"1", "data":{"result":"invalid_password"} }
≈
{ "retcode":"1", "data":{"result":"invalid_password"} }

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/
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：

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
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: 4587
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=IGILGIHKHLGMGG" rel="stylesheet">
 <link href="/css/operator.css?v=IGILGIHKHLGMGG" rel="stylesheet">
...
```

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/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：

```
...

Connection: keep-alive
Host: 192.168.1.1
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: 36
Content-Type: text/html

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

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/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=ifFGctB33Z6XO8fV8iC2250JiF8Za91
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);
  }
...
```

“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=6e282cd8b4b1790065fa81175d8716c200aef99df6a78c79097900dbcf
96ac01

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=wS1ekpEUfZK0fYlJ8inL1IT9p8sY1oJ; path=/
Content-Type: text/html

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

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/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=ifFGctB33Z6XO8fV8iC2250JiF8Za9l
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: 5050
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=IGILGIHKHLGMGG" rel="stylesheet">
 <link href="/css/operator.css?v=IGILGIHKHLGMGG" 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/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=6e282cd8b4b1790065fa81175d8716c200aef99df6a78c79097900dbcf
96ac01

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=wS1ekpEUfZK0fYlJ8inL1IT9p8sY1oJ; path=/
Content-Type: text/html

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

问题 2 / 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/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“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：

```
...

Connection: keep-alive
Host: 192.168.1.1
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: 36
Content-Type: text/html

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

“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：

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
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: 4587
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=IGILGIHKHLGMGG" rel="stylesheet">
 <link href="/css/operator.css?v=IGILGIHKHLGMGG" rel="stylesheet">
...
```

问题 4 / 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/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=ifFGctB33Z6XO8fV8iC2250JiF8Za91
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: 5050
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=IGILGIHKHLGMGG" rel="stylesheet">
 <link href="/css/operator.css?v=IGILGIHKHLGMGG" 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/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=ifFGctB33Z6XO8fV8iC2250JiF8Za91
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=6e282cd8b4b1790065fa81175d8716c200aef99df6a78c79097900dbcf
96ac01

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=wS1ekpEUfZK0fYlJ8inL1IT9p8sY1oJ; 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/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“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：

```
...

Connection: keep-alive
Host: 192.168.1.1
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: 36
Content-Type: text/html

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

问题 3 / 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：

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
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: 4587
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=IGILGIHKHLGMGG" rel="stylesheet">
 <link href="/css/operator.css?v=IGILGIHKHLGMGG" rel="stylesheet">
...
```

问题 4 / 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/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=ifFGctB33Z6XO8fV8iC2250JiF8Za91
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: 5050
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=IGILGIHKHLGMGG" rel="stylesheet">
 <link href="/css/operator.css?v=IGILGIHKHLGMGG" 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=ifFGctB33Z6XO8fV8iC2250JiF8Za91
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 查询中接受的主体参数 1

TOC

问题 1 / 1

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

低 发现潜在注册信息 1

TOC

问题 1 / 1

TOC

发现潜在注册信息

严重性：	低
CVSS 分数：	5.0
URL：	http://192.168.1.1/
实体：	register.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
原因：	Web 应用程序编程或配置不安全
固定值：	不要在可以轻易猜测到的文件名中保存敏感信息，或者限制对它们的访问

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

测试请求：

测试响应

```
GET /register.html?v=IGILGIHKHLG
MGG HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: http://192.168.1.1/
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US
```

```
...
GET /register.html?v=IGILGIHKHLG
MGG HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: http://192.168.1.1/
Connection: keep-alive
Host: 192.168.1.1
Accept: */*
Accept-Language: en-US


HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 7564
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="utf-8">
...

...

<body>
 <div class="main">
  <div class="login-header">
   <div class="pad">
    <div class="logo"></div>
   </div>
  </div>
  <a href="/cu.html" style="posi
tion: relative; top: 100px">返回
登录页面</a>
  <div class="login_center" id="
loid_register_input_div">
    <img src="/image/welcome_oth
erusers_default.png">
    <p>逻辑ID注册</p>
    <div class="login">
     <input type="text" name="lo
gin_name" placeholder="逻辑ID">
     <img src="/image/login_phon
e.png">
    </div>
    <div class="login">
     <input type="text" name="lo
gin_password" placeholder="密码">
     <img src="/image/login_pass
word.png">
     <button onclick="saveApply(
)" id="do_register">注册</button>
...
```

低 跨帧脚本编制防御缺失或不安全 3 TOC

问题 1 / 3 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=6e282cd8b4b1790065fa81175d8716c200aef99df6a78c79097900dbcf
96ac01

HTTP/1.0 200 OK
Connection: close
Server: HSANHomeGateway
Content-Length: 64
Set-Cookie: Token=ysTZB3i85d666cJh8933983sSsayEq3; path=/
Content-Type: text/html

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

问题 2 / 3 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"}
}
...
```

问题 3 / 3

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":"5","times":"0"}
}
...
```

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])+",
...
```