



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: 2017/4/17 9:23:23

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

- 发现 Web 应用程序源代码泄露模式 ①
- 查询中接受的主体参数 ①
- 缺少“Content-Security-Policy”头 ⑤
- 缺少“X-Content-Type-Options”头 ⑤
- 缺少“X-XSS-Protection”头 ⑤
- 发现电子邮件地址模式 ①
- 应用程序错误 ②
- 整数溢出 ②

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。

低严重性问题: 17
参考严重性问题: 5
报告中包含的严重性问题总数: 22
扫描中发现的严重性问题总数: 22

常规信息

扫描文件名称: 安全扫描
扫描开始时间: 2017/4/17 9:23:23
测试策略: Default

主机: 101.37.20.178
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:

摘要











问题类型 8

TOC

问题类型	问题的数量
低 发现 Web 应用程序源代码泄露模式	1 
低 查询中接受的主体参数	1 
低 缺少“Content-Security-Policy”头	5 
低 缺少“X-Content-Type-Options”头	5 
低 缺少“X-XSS-Protection”头	5 
参 发现电子邮件地址模式	1 
参 应用程序错误	2 
参 整数溢出	2 








有漏洞的 URL 10

TOC

URL	问题的数量
低 http://101.37.20.178/Content/template.js	1 
低 http://101.37.20.178/PC/Member/CheckImgCode	1 
低 http://101.37.20.178/	3 
低 http://101.37.20.178/Admin/User/Login	3 
低 http://101.37.20.178/Admin/User/Tip	3 
低 http://101.37.20.178/Areas/Admin/Content/login/js/login.js	3 
低 http://101.37.20.178/Areas/PC/Content/lib/con_js.6.23.js	3 
参 http://101.37.20.178/Areas/Mobile/Content/lib/judge.js	1 
参 http://101.37.20.178/Mobile/Member/Protocol	2 
参 http://101.37.20.178/PC/Member/Protocol	2 





修订建议 7

TOC

修复任务		问题的数量
低	将您的服务器配置为使用“Content-Security-Policy”头	5 
低	将您的服务器配置为使用“X-Content-Type-Options”头	5 
低	将您的服务器配置为使用“X-XSS-Protection”头	5 
低	请勿接受在查询字符串中发送的主体参数	1 
低	除去 Web 站点中的电子邮件地址	1 
低	除去 web-server 中的源代码文件并应用任何相关补丁	1 
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	4 

安全风险 4

TOC

风险		问题的数量
低	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	1 
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	17 
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	16 
参	可能会收集敏感的调试信息	4 

原因 6

TOC

原因		问题的数量
低	未安装第三方产品的最新补丁或最新修订程序	1 
低	在生产环境中留下临时文件	1 
低	程序员在 Web 页面上留下调试信息	1 
低	Web 应用程序编程或配置不安全	17 
参	未对入局参数值执行适当的边界检查	4 
参	未执行验证以确保用户输入与预期的数据类型匹配	4 

WASC 威胁分类

TOC

威胁	问题的数量
信息泄露	20 
整数溢出	2 

按问题类型分类的问题

低

发现 Web 应用程序源代码泄露模式 1

TOC

问题 1 / 1

TOC

发现 Web 应用程序源代码泄露模式	
严重性:	低
CVSS 分数:	5.0
URL:	http://101.37.20.178/Content/template.js
实体:	template.js (Page)
风险:	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因:	未安装第三方产品的最新补丁或最新修订程序 在生产环境中留下临时文件 程序员在 Web 页面上留下调试信息
固定值:	除去 web-server 中的源代码文件并应用任何相关补丁

推理： 响应包含可能会泄露有关站点和应用程序逻辑的敏感信息的脚本文件源代码。

未经处理的测试响应：

```
...
...b,{filename:a}):g(a,b)};d.version="3.0.0",d.config=function(a,b){e[a]=b};var e=d.defaults={
openTag:"<",closeTag:">",escape:!0,cache:!0,compress:!1,parser:null},f=d.cache=
{};d.render=function(a,b){retu...
...

```

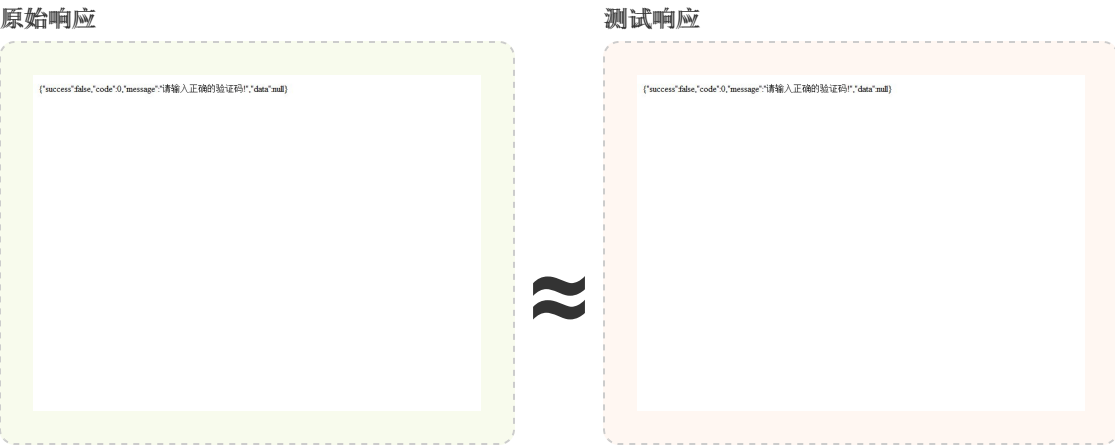
低

查询中接受的主体参数 1

TOC

查询中接受的主体参数	
严重性:	低
CVSS 分数:	5.0
URL:	http://101.37.20.178/PC/Member/CheckImgCode
实体:	CheckImgCode (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。



缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/>

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

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

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: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Content-Length: 490
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html>

<html>
<head>
  <meta name="viewport" content="width=device-width" />
  <title>页面跳转</title>
</head>
```

```
...
```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: http://101.37.20.178/Areas/PC/Content/lib/con_js.6.23.js

实体: con_js.6.23.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: 将您的服务器配置为使用“Content-Security-Policy”头

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

未经处理的测试响应:

```
...
GET /Areas/PC/Content/lib/con_js.6.23.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://101.37.20.178/PC/Home
Host: 101.37.20.178
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 24 Mar 2017 08:20:15 GMT
Server: Microsoft-IIS/7.5
Accept-Ranges: bytes
Content-Length: 27938
X-Powered-By: ASP.NET
ETag: "e7b1eb7677a4d21:0"
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: application/x-javascript

//公共函数库---基于属性驱动方式--需要页面加载完毕的方法
...
```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Areas/Admin/Content/login/js/login.js>

实体: login.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: 将您的服务器配置为使用“Content-Security-Policy”头

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

未经处理的测试响应:

```
...
GET /Areas/Admin/Content/login/js/login.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://101.37.20.178/Admin/User/Login
Host: 101.37.20.178
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 24 Mar 2017 08:20:04 GMT
...
```

问题 4 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Admin/User/Login>

实体: Login (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: 将您的服务器配置为使用“Content-Security-Policy”头

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

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://101.37.20.178/Admin/User/Tip?state=0
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
x-ua-compatible: ie=11.0000
Server: Microsoft-IIS/7.5
Content-Length: 1767
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8

<!doctype html >
<html>
<head>
  <meta content="ie=11.0000" http-equiv="x-ua-compatible">
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="generator" content="mshtml 11.00.9600.17496">
  <title>拇指物联后台管理系统</title>
  <link href="/Areas/Admin/Content/login/css/animate.min.css" rel="stylesheet" />
  <link href="/Areas/Admin/Content/login/css/login.css" rel="stylesheet" />
</head>
...

```

问题 5 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Admin/User/Tip>

实体: Tip (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: 将您的服务器配置为使用“Content-Security-Policy”头

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

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://101.37.20.178/
Connection: keep-alive

```

```
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Content-Length: 1045
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<meta name="viewport" content="width=device-width" />
```

```
<title>Tip</title>
```

```
<script src="/Areas/Admin/Content/easyui/jquery.min.js"></script>
```

```
<script type="text/javascript">
```

```
...
```

低

缺少“X-Content-Type-Options”头 5

TOC

问题 1 / 5

TOC

缺少“X-Content-Type-Options”头

严重性:

低

CVSS 分数: 5.0

URL: <http://101.37.20.178/>

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: 将您的服务器配置为使用“X-Content-Type-Options”头

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

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: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Content-Length: 490
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html>

<html>
<head>
  <meta name="viewport" content="width=device-width" />
  <title>页面跳转</title>
</head>

...
```

问题 2 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: **低**

CVSS 分数: 5.0

URL: http://101.37.20.178/Areas/PC/Content/lib/con_js.6.23.js

实体: con_js.6.23.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: 将您的服务器配置为使用“X-Content-Type-Options”头

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

未经处理的测试响应:

```
...
GET /Areas/PC/Content/lib/con_js.6.23.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://101.37.20.178/PC/Home
Host: 101.37.20.178
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Last-Modified: Fri, 24 Mar 2017 08:20:15 GMT
Server: Microsoft-IIS/7.5
Accept-Ranges: bytes
Content-Length: 27938
X-Powered-By: ASP.NET
ETag: "e7b1eb7677a4d21:0"
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: application/x-javascript

//公共函数库---基于属性驱动方式--需要页面加载完毕的方法
...
```

问题 3 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Areas/Admin/Content/login/js/login.js>

实体: login.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: 将您的服务器配置为使用“X-Content-Type-Options”头

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

未经处理的测试响应:

```
...
GET /Areas/Admin/Content/login/js/login.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://101.37.20.178/Admin/User/Login
Host: 101.37.20.178
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 24 Mar 2017 08:20:04 GMT
...
```

问题 4 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Admin/User/Login>

实体: Login (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: 将您的服务器配置为使用“X-Content-Type-Options”头

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

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://101.37.20.178/Admin/User/Tip?state=0
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
x-ua-compatible: ie=11.0000
Server: Microsoft-IIS/7.5
Content-Length: 1767
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8

<!doctype html >
<html>
<head>
  <meta content="ie=11.0000" http-equiv="x-ua-compatible">
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="generator" content="mshtml 11.00.9600.17496">
  <title>拇指联联后台管理系统</title>
  <link href="/Areas/Admin/Content/login/css/animate.min.css" rel="stylesheet" />
  <link href="/Areas/Admin/Content/login/css/login.css" rel="stylesheet" />
</head>

...
```


缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Admin/User/Tip>

实体: Tip (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: 将您的服务器配置为使用“X-Content-Type-Options”头

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

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://101.37.20.178/
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Content-Length: 1045
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<meta name="viewport" content="width=device-width" />
```

```
<title>Tip</title>
```

```
<script src="/Areas/Admin/Content/easyui/jquery.min.js"></script>
```

```
<script type="text/javascript">
```

```
...
```

低

缺少“X-XSS-Protection”头 5

TOC

缺少“X-XSS-Protection”头**严重性:** 低**CVSS 分数:** 5.0**URL:** <http://101.37.20.178/>**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:** 将您的服务器配置为使用“X-XSS-Protection”头

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
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: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Content-Length: 490
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html>

<html>
<head>
  <meta name="viewport" content="width=device-width" />
  <title>页面跳转</title>
</head>

...
```

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: http://101.37.20.178/Areas/PC/Content/lib/con_js.6.23.js

实体: con_js.6.23.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: 将您的服务器配置为使用“X-XSS-Protection”头

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
未经处理的测试响应:

```
...
GET /Areas/PC/Content/lib/con_js.6.23.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://101.37.20.178/PC/Home
Host: 101.37.20.178
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 24 Mar 2017 08:20:15 GMT
Server: Microsoft-IIS/7.5
Accept-Ranges: bytes
Content-Length: 27938
X-Powered-By: ASP.NET
ETag: "e7bleb7677a4d21:0"
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: application/x-javascript

//公共函数库---基于属性驱动方式--需要页面加载完毕的方法
...
```

问题 3 / 5

TOC

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://101.37.20.178/Areas/Admin/Content/login/js/login.js>

实体: login.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: 将您的服务器配置为使用“X-XSS-Protection”头

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
未经处理的测试响应：

```
...
GET /Areas/Admin/Content/login/js/login.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://101.37.20.178/Admin/User/Login
Host: 101.37.20.178
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Last-Modified: Fri, 24 Mar 2017 08:20:04 GMT

...
```

缺少“X-XSS-Protection”头	
严重性:	低
CVSS 分数:	5.0
URL:	http://101.37.20.178/Admin/User/Login
实体:	Login (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:	将您的服务器配置为使用“X-XSS-Protection”头

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
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://101.37.20.178/Admin/User/Tip?state=0
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
x-ua-compatible: ie=11.0000
Server: Microsoft-IIS/7.5
Content-Length: 1767
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8
```

```

<!doctype html >
<html>
<head>
  <meta content="ie=11.0000" http-equiv="x-ua-compatible">
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="generator" content="mshtml 11.00.9600.17496">
  <title>拇指联联后台管理系统</title>
  <link href="/Areas/Admin/Content/login/css/animate.min.css" rel="stylesheet" />
  <link href="/Areas/Admin/Content/login/css/login.css" rel="stylesheet" />
</head>

...

```

问题 5 / 5

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://101.37.20.178/Admin/User/Tip>

实体: Tip (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: 将您的服务器配置为使用“X-XSS-Protection”头

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
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://101.37.20.178/
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Content-Length: 1045
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:29:45 GMT
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>

<html>
<head>
  <meta name="viewport" content="width=device-width" />

```

```
<title>Tip</title>  
<script src="/Areas/Admin/Content/easyui/jquery.min.js"></script>  
<script type="text/javascript">
```

...

问题 1 / 1

TOC

发现电子邮件地址模式

严重性: 参考

CVSS 分数: 0.0

URL: <http://101.37.20.178/Areas/Mobile/Content/lib/judge.js>

实体: judge.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

原因: Web 应用程序编程或配置不安全

固定值: 除去 Web 站点中的电子邮件地址

推理: 响应包含可能是专用的电子邮件地址。**未经处理的测试响应:**

```
...  
  
/**  
 * Created by trigkit4 on 16/1/17.  
 * judge.js < https://github.com/hawx1993/judge >  
 * @author trigkit4 <trigkit@163.com>  
 */  
;(function (root,factory) {console.log("judge加载");  
  //support requirejs && amd  
  if(typeof define === 'function' && define.amd){  
    define(function () {  
      return judge = factory();  
    });  
    //CommonJS  
  }else if(typeof exports === 'object'){  
    ...  
  }  
})
```

应用程序错误**严重性:** [参考](#)**CVSS 分数:** 0.0**URL:** <http://101.37.20.178/PC/Member/Protocol>**实体:** ID (Parameter)**风险:** 可能会收集敏感的调试信息**原因:** 未对入局参数值执行适当的边界检查
未执行验证以确保用户输入与预期的数据类型匹配**固定值:** 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常**推理:** 应用程序以错误消息响应,表示可能会泄露敏感信息的未定义状态。**未经处理的测试响应:**

```
...

Referer: http://101.37.20.178/PC/Member/Login
Cookie: ASP.NET_SessionId=ovz2kz3bjlrvphbat02diws2
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/7.5
Content-Length: 298
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:30:34 GMT
Content-Type: text/html; charset=utf-8

...
```


应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://101.37.20.178/Mobile/Member/Protocol>

实体: ID (Parameter)

风险: 可能会收集敏感的调试信息

原因: 未对入局参数值执行适当的边界检查
未执行验证以确保用户输入与预期的数据类型匹配

固定值: 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理: 应用程序以错误消息响应, 表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应:

```
...

Referer: http://101.37.20.178/Mobile/Member/Register
Cookie: ASP.NET_SessionId=ovz2kz3bjlrphbat02diws2
Connection: keep-alive
Host: 101.37.20.178
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/7.5
Content-Length: 298
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Cache-Control: private
X-Powered-By: ASP.NET
Date: Mon, 17 Apr 2017 01:30:34 GMT
Content-Type: text/html; charset=utf-8

...
```

参

整数溢出 **2**

TOC

问题 1 / 2

TOC

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://101.37.20.178/Mobile/Member/Protocol>

实体: ID (Parameter)

风险: 可能会收集敏感的调试信息

原因: 未对入局参数值执行适当的边界检查
未执行验证以确保用户输入与预期的数据类型匹配

固定值: 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理: 应用程序以错误消息响应, 表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应:

```
...  
  
Referer: http://101.37.20.178/Mobile/Member/Register  
Cookie: ASP.NET_SessionId=ovz2kz3bj1rvphbat02diws2  
Connection: keep-alive  
Host: 101.37.20.178  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 500 Internal Server Error  
Server: Microsoft-IIS/7.5  
Content-Length: 298  
X-AspNetMvc-Version: 5.2  
X-AspNet-Version: 4.0.30319  
Cache-Control: private  
X-Powered-By: ASP.NET  
Date: Mon, 17 Apr 2017 01:30:34 GMT  
Content-Type: text/html; charset=utf-8
```

```
...
```

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://101.37.20.178/PC/Member/Protocol>

实体: ID (Parameter)

风险: 可能会收集敏感的调试信息

原因: 未对入局参数值执行适当的边界检查
未执行验证以确保用户输入与预期的数据类型匹配

固定值: 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理: 应用程序以错误消息响应, 表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应:

```
...  
  
Referer: http://101.37.20.178/PC/Member/Login  
Cookie: ASP.NET_SessionId=ovz2kz3bjlrphbat02diws2  
Connection: keep-alive  
Host: 101.37.20.178  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 500 Internal Server Error  
Server: Microsoft-IIS/7.5  
Content-Length: 298  
X-AspNetMvc-Version: 5.2  
X-AspNet-Version: 4.0.30319  
Cache-Control: private  
X-Powered-By: ASP.NET  
Date: Mon, 17 Apr 2017 01:30:34 GMT  
Content-Type: text/html; charset=utf-8
```

```
...
```