



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: 2019/9/18 13:55:50

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

- 客户端 (JavaScript) Cookie 引用 ①
- 发现电子邮件地址模式 ①
- 发现可能的服务器路径泄露模式 ②
- 发现内部 IP 泄露模式 ①
- 缺少“X-XSS-Protection”头 ⑤
- 缺少“X-Content-Type-Options”头 ⑤
- 缺少“Content-Security-Policy”头 ⑤
- 检测到隐藏目录 ①
- 跨站点请求伪造 ①
- IPSwitch Imail Imonitor 拒绝服务 ①

修订建议

- 升级至 IPSwitch Imail IMONITOR 的最新版本，或者安装最新更新的补丁
- 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

- 为 Web 服务器或 Web 应用程序下载相关的安全补丁
- 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去
- 将您的服务器配置为使用“Content-Security-Policy”头
- 将您的服务器配置为使用“X-Content-Type-Options”头
- 将您的服务器配置为使用“X-XSS-Protection”头
- 除去 Web 站点中的内部 IP 地址
- 除去 Web 站点中的电子邮件地址
- 除去客户端中的业务逻辑和安全逻辑

咨询

- 客户端（JavaScript）Cookie 引用
- 发现电子邮件地址模式
- 发现可能的服务器路径泄露模式
- 发现内部 IP 泄露模式
- 缺少“X-XSS-Protection”头
- 缺少“X-Content-Type-Options”头
- 缺少“Content-Security-Policy”头
- 检测到隐藏目录
- 跨站点请求伪造
- IPSwitch Imail Imonitor 拒绝服务

介绍

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

高严重性问题:	1
中等严重性问题:	1
低严重性问题:	16
参考严重性问题:	5
报告中包含的严重性问题总数:	23
扫描中发现的严重性问题总数:	23

常规信息

扫描文件名称: 信息联动2
扫描开始时间: 2019/9/18 13:55:50
测试策略: Default

主机 192.168.11.210
端口 0
操作系统: 未知
Web 服务器: 未知
应用程序服务器: JavaAppServer

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: <http://192.168.11.210/informationLinkage/>
<http://192.168.11.210/server/user/getVerifyCode>

<http://192.168.11.210/server/user/login>
<http://192.168.11.210/server/user/login>
http://192.168.11.210/civil/information_linkage/content/pageFindContent

摘要










问题类型 10

TOC

问题类型		问题的数量
参	客户端（JavaScript）Cookie 引用	1 
参	发现电子邮件地址模式	1 
参	发现可能的服务器路径泄露模式	2 
参	发现内部 IP 泄露模式	1 
低	缺少“X-XSS-Protection”头	5 
低	缺少“X-Content-Type-Options”头	5 
低	缺少“Content-Security-Policy”头	5 
低	检测到隐藏目录	1 
中	跨站点请求伪造	1 
高	IPSwitch Imail Imonitor 拒绝服务	1 

有漏洞的 URL 12

TOC

URL		问题的数量
参	http://192.168.11.210/informationLinkage/assets/js/chunk-65f44854.8f446a02.js	1 
参	http://192.168.11.210/informationLinkage/assets/js/chunk-074e1af5.862c9280.js	2 
参	http://192.168.11.210/informationLinkage/assets/js/chunk-vendors.5ed272ce.js	1 
参	http://192.168.11.210/civil/information_linkage/content/pageFindContent	1 
中	http://192.168.11.210/civil/information_linkage/column/pageQueryColumn	4 
低	http://192.168.11.210/civil/ueditor/ueditorConfig	3 
低	http://192.168.11.210/informationLinkage/layui/layui.js	3 
低	http://192.168.11.210/server/user/getVerifyCode	2 
低	http://192.168.11.210/server/user/login	3 

低	http://192.168.11.210/informationLinkage/	1	<div></div>
低	http://192.168.11.210/informationLinkage/assets/	1	<div></div>
高	http://192.168.11.210/	1	<div></div>

修订建议 10

TOC

修复任务	问题的数量
高 升级至 IPSwitch Imail IMONITOR 的最新版本，或者安装最新更新的补丁	1 <div></div>
中 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	1 <div></div>
低 为 Web 服务器或 Web 应用程序下载相关的安全补丁	2 <div></div>
低 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去	1 <div></div>
低 将您的服务器配置为使用“Content-Security-Policy”头	5 <div></div>
低 将您的服务器配置为使用“X-Content-Type-Options”头	5 <div></div>
低 将您的服务器配置为使用“X-XSS-Protection”头	5 <div></div>
低 除去 Web 站点中的内部 IP 地址	1 <div></div>
低 除去 Web 站点中的电子邮件地址	1 <div></div>
低 除去客户端中的业务逻辑和安全逻辑	1 <div></div>

安全风险 7

TOC

风险	问题的数量
高 可能会阻止 Web 应用程序服务其他用户（拒绝服务）	1 <div></div>
中 可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	1 <div></div>
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 <div></div>
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	15 <div></div>
低 可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点	1 <div></div>
参 此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色	1 <div></div>
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	2 <div></div>



原因 5

TOC

原因		问题的数量
参	Cookie 是在客户端创建的	1 
低	Web 应用程序编程或配置不安全	17 
高	未安装第三方产品的最新补丁或最新修订程序	3 
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 
中	应用程序使用的认证方法不充分	1 

WASC 威胁分类

TOC

威胁	问题的数量
信息泄露	21 
拒绝服务	1 
跨站点请求伪造	1 

按问题类型分类的问题

客户端（JavaScript）Cookie 引用	
严重性:	参考
CVSS 分数:	0.0
URL:	http://192.168.11.210/informationLinkage/assets/js/chunk-65f44854.8f446a02.js
实体:	(window["webpackJsonp"]=window["webpackJsonp"] []).push([["chunk-65f44854"],{"044b":function(e,t){ (Page)
风险:	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因:	Cookie 是在客户端创建的
固定值:	除去客户端中的业务逻辑和安全逻辑

推理: AppScan 在 JavaScript 中找到对 cookie 的引用。
原始响应

```
...
....isString(o)&&a.push("path="+o),r.isString(i)&&a.push("domain="+i),!0===s&&a.push("secure"),do
cument.cookie=a.join("; "),read:function(e){var t=document.cookie.match(new RegExp("(^|;\\s*)
(\\+e+)=([^\s]*)"));re...
...

```

发现电子邮件地址模式

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://192.168.11.210/informationLinkage/assets/js/chunk-074e1af5.862c9280.js>

实体: chunk-074e1af5.862c9280.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:**

```

...
...l_information_linkage\\\\node_modules\\\\browserify-sign", "author": {"name": "Fedor
Indutny", "email": "fedor@indutny.com"}, "bugs":
{"url": "https://github.com/indutny/elliptic/issues"}, "bundleDependencies": false, "dependenc...

...

...cense": "MIT", "main": "lib/elliptic.js", "name": "elliptic", "repository":
{"type": "git", "url": "git+ssh://git@github.com:indutny/elliptic.git"}, "scripts": {"jscs": "jscs
benchmarks/*.js lib/*.js lib/**/*.js lib/**/*.js ...

...

...
...on(e) {
/*!
* The buffer module from node.js, for the browser.
*
* @author Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
* @license MIT
*/
var i=r("1fb5"),n=r("9152"),a=r("e3db");function f(){try{...

...

```

参

发现可能的服务器路径泄露模式 2

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://192.168.11.210/informationLinkage/assets/js/chunk-074e1af5.862c9280.js>

实体: chunk-074e1af5.862c9280.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订程序

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:

```
...
...-
6.5.0.tgz", "_shasum": "2b8ed4c891b7de3200e14412a5b8248c7af505ca", "_spec": "elliptic@^6.0.0", "_where
": "D:\\\\project\\\\ä¿;æ`èà"\\
```

问题 2 / 2

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://192.168.11.210/informationLinkage/assets/js/chunk-vendors.5ed272ce.js>

实体: chunk-vendors.5ed272ce.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订程序

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:

```
...
GET /informationLinkage/assets/js/chunk-vendors.5ed272ce.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.210
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Wed, 18 Sep 2019 01:56:52 GMT
```

...

参

发现内部 IP 泄露模式 1

TOC

问题 1 / 1

TOC

发现内部 IP 泄露模式

严重性:

参考

CVSS 分数: 0.0

URL: http://192.168.11.210/civil/information_linkage/content/pageFindContent

实体: pageFindContent (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:

```
...

"source": "",
"website": "",
...t-skin imgClass video-js\" controls=\"\" preload=\"none\" width=\"420\" height=\"280\"
src=\"http://192.168.11.210:9999/files/605e35ab-f153-4a00-8e46-e23a25d496a8.mp4\"><source
src=\"http://1...
"imgUrl": "",
"videoUrl": "",
"status": 4,
"reason": "张莉>>>通过",
"reviewer": "张莉",
"happenTime": "2019-09-18",
"publishTime": "2019-09-18 13:48:46",
"processDefinitionId": "KEY_NEWS_1568008953210:1:322514",
"loginName": "ZhangYanPing",

...

...

"website": "",
...baidu.com\" target=\"_self\">超链接</a></p></li></ul><p style=\"text-align:center\"><img
src=\"http://--begin_highlight_tag--192.168.11.210:9999/files/328c566f-57b7-4829-a9f7-
3ce7f088398b.jpg\" title=\"\" alt=\"\"/></p><p>gsdg<img src=\"ht...
"imgUrl": "",
"videoUrl": "",
"status": 4,
"reason": "张莉>>>通过",
```

```

...

...

    "2"
  ],
  "columnId": "2",
  "columnDTO": null,
  "description": "",
  "sketchPath": "",
  "source": "",
  "website": "",
  "content": "<p style='line-height: 16px;'><img
src='/informationLinkage/Ueditor/dialogs/attachment/fileTypeImages/icon_doc.gif'><a
title='47880581-ceb9-46a9-aeb5-0d956d94957e.doc' style='color: rgb(0, 102, 204); font-size:
12px;' href='http://192.168.11.210:9999/files/47880581-ceb9-46a9-aeb5-
0d956d94957e.doc'>47880581-ceb9-46a9-aeb5-0d956d94957e.doc</a></p><p style='text-align:
center;'><video class='edui-upload-video vjs-default-skin imgClass video-js' controls='\"
preload='none' width='420' height='280' src='http://192.168.11.210:9999/files/bd990754-
27c2-4244-b21e-88f30ceeb0ef.mp4'><source src='http://192.168.11.210:9999/files/bd990754-27c2-
4244-b21e-88f30ceeb0ef.mp4' type='video/mp4'></video></p><p><img title='正在上传...'
class='loadingclass' id='loading_k0m2a5ij'
src='/informationLinkage/Ueditor/themes/default/images/spacer.gif'>&nbsp;</p><p><br></p><p>
'15:03:56</p><table><tbody><tr class='firstRow'><td width='645' valign='top' style='-ms-
word-break: break-all;'>34<br></td><td width='645' valign='top' style='-ms-word-break:
break-all;'>34<br></td><tr><td width='645' valign='top' style='-ms-word-break: break-
all;'>34<br></td><td width='645' valign='top' style='-ms-word-break: break-all;'>34<br>
</td></tr><tr><td width='645' valign='top' style='-ms-word-break: break-all;'>34<br></td>
<td width='645' valign='top' style='-ms-word-break: break-all;'><br></td></tr></tbody>
</table><p><span style='color: rgb(255, 192, 0);'>34</span></p>,
  "imgUrl": "",
  "videoUrl": "",
  "status": 4,
  "reason": "张莉>>>通过吗通过吗通过吗通过吗通过吗通过吗通过吗通过吗通过吗通过吗通过吗通过吗通
过吗通过",
  "reviewer": "张莉",

...

```

低

缺少“X-XSS-Protection”头 5

TOC

问题 1 / 5

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/informationLinkage/layui/layui.js>

实体: layui.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 /informationLinkage/layui/layui.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.210
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Wed, 18 Sep 2019 01:56:52 GMT
...
```

问题 2 / 5

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/server/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:

```
...  
  
Content-Length: 88  
Pragma: no-cache  
  
{  
  "param1": "zhangyanping",  
  "param2": "e10adc3949ba59abbe56e057f20f883e",  
  "imageCode": "6558"  
}  
  
HTTP/1.1 200  
Transfer-Encoding: chunked  
Connection: keep-alive  
Server: nginx/1.15.8  
Date: Wed, 18 Sep 2019 06:02:28 GMT  
Content-Type: application/json; charset=UTF-8  
  
{  
  "code": 20016,  
  "msg": "验证码输入错误",  
  "data": null  
}  
...
```

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://192.168.11.210/civil/ueditor/ueditorConfig>

实体: ueditorConfig (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 /civil/ueditor/ueditorConfig?action=config&noCache=1568786093746 HTTP/1.1
Accept-Language: zh-cn
Referer: http://192.168.11.210/informationLinkage/#/login?
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: */*
Host: 192.168.11.210

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Set-Cookie: JSESSIONID=915272C1691EFE06F9C3C4676297F566; Path=/civil; HttpOnly
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json;charset=ISO-8859-1

{
  "videoMaxSize": 102400000,
  "videoActionName": "uploadvideo",
  "fileActionName": "uploadfile",
  "fileManagerListPath": "/ueditor/jsp/upload/file/",
  "imageCompressBorder": 1600,
  "imageManagerAllowFiles": [
    ".png",
    ".jpg",
    ".jpeg",
  ]
}
```


缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/server/user/getVerifyCode>

实体: getVerifyCode (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:

```
...

Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: application/json, text/plain, */*
Host: 192.168.11.210
Content-Length: 0
Pragma: no-cache

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 1,
  "msg": "成功",
  "data":
    "data:image/jpeg;base64,iVBORw0KGgoAAAANSUhEUgAAAEgAAAAeCAYAAACPOlitAAAIc01EQVR42p3a21oURxQFYn4jb
    5Cr\nPINfbvMEuRWEiUSDCkFEVAgMCeqHnAwHg8hr5SQYUEAJKagCCkKMREH1LOgI4hCBpMPawy52VVcP\nnJBfLbrp7wvi7an
    cPJCiQKsoxklM9QdvMvlXXubGL+RTzeGviA9r+2BCpjklNNGnX5H+b5gwc6KeY\nnr5/KXrMG54rGKijma4JlA47t/e+W4v47e
    742oqC2zUF6Kz46vjevnIfPgWSErcz96QS1n9fdqaDk\nnNUACKPlaGSBhy1DI3ScF2jU1B2rUvgkGKHktkMJ9PzPzecUEhP3A
    0HHX+ZHy...
  ...
}
```

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: http://192.168.11.210/civil/information_linkage/column/pageQueryColumn

实体: pageQueryColumn (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:

```
...

Host: 192.168.11.210
Content-Length: 20
Pragma: no-cache

{
  "page": 1,
  "rows": 10
}

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "total": 5,
  "rows": [
    {
      "id": 15,
      "createTime": "2019-09-18 14:02:28",
      "updateTime": "2019-09-18 14:02:28",
      "name": "栏目1",
      "description": "栏目描述",
      "hide": null,
    }
  ]
}

...
```

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://192.168.11.210/informationLinkage/layui/layui.js>

实体: layui.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 /informationLinkage/layui/layui.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.210
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Wed, 18 Sep 2019 01:56:52 GMT
...
```

问题 2 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/server/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:

```

...
Content-Length: 88
Pragma: no-cache

{
  "param1": "zhangyanping",
  "param2": "e10adc3949ba59abbe56e057f20f883e",
  "imageCode": "6558"
}

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 20016,
  "msg": "验证码输入错误",
  "data": null
}
...

```

问题 3 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/civil/ueditor/ueditorConfig>

实体: ueditorConfig (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 /civil/ueditor/ueditorConfig?action=config&noCache=1568786093746 HTTP/1.1
Accept-Language: zh-cn
Referer: http://192.168.11.210/informationLinkage/#/login?
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: */*
Host: 192.168.11.210

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Set-Cookie: JSESSIONID=915272C1691EFE06F9C3C4676297F566; Path=/civil; HttpOnly

```

```
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json; charset=ISO-8859-1

{
  "videoMaxSize": 102400000,
  "videoActionName": "uploadvideo",
  "fileActionName": "uploadfile",
  "fileManagerListPath": "/ueditor/jsp/upload/file/",
  "imageCompressBorder": 1600,
  "imageManagerAllowFiles": [
    ".png",
    ".jpg",
    ".jpeg",
    ...
  ]
}
```

问题 4 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/server/user/getVerifyCode>

实体: getVerifyCode (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:

```
...

Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: application/json, text/plain, */*
Host: 192.168.11.210
Content-Length: 0
Pragma: no-cache

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json; charset=UTF-8

{
  "code": 1,
  "msg": "成功",
  "data":
    "data:image/jpeg;base64,iVBORw0KGgoAAAANSUhEUgAAAEgAAAAeCAYAAACPOLitAAAIc01EQVR42p3a21oURxQFYn4jb5Cr\nnPINFbvMEuRWEiUSDCkFEVAgMCEqHnAwHg8hr5SQYUEAJKAgCCKKMREH1LOgI4hCBpMPawy52VVcP\nnJBfLbrp7wvi7an
```

```
cPJCIqKsoxk1M9QdvMvlXXubGL+RTzeGviA9r+2BCpjklnNgN5H+b5gwc6KeY\nr5/KXrMG54rGKijma4JlA47t/e+W4v47e
742oqC2zUF6Kz46vjevnIfPgwsErcz96QSl9fdqaDk\nNUACkPlaGSBhy1DI3ScF2jU1B2rUvgkGKHktkMJ9PzPzecUEhP3A
0HHX+ZHy...
...
```

问题 5 / 5

TOC

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: http://192.168.11.210/civil/information_linkage/column/pageQueryColumn

实体: pageQueryColumn (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:

```
...
Host: 192.168.11.210
Content-Length: 20
Pragma: no-cache

{
  "page": 1,
  "rows": 10
}

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "total": 5,
  "rows": [
    {
      "id": 15,
      "createTime": "2019-09-18 14:02:28",
      "updateTime": "2019-09-18 14:02:28",
      "name": "栏目1",
      "description": "栏目描述",
      "hide": null,
    }
  ]
}
...
```

低

缺少“Content-Security-Policy”头 5

TOC

问题 1 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/informationLinkage/layui/layui.js>

实体: layui.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 /informationLinkage/layui/layui.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.210
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Wed, 18 Sep 2019 01:56:52 GMT
...
```

问题 2 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/server/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:

```
...  
  
Content-Length: 88  
Pragma: no-cache  
  
{  
  "param1": "zhangyanping",  
  "param2": "e10adc3949ba59abbe56e057f20f883e",  
  "imageCode": "6558"  
}  
  
HTTP/1.1 200  
Transfer-Encoding: chunked  
Connection: keep-alive  
Server: nginx/1.15.8  
Date: Wed, 18 Sep 2019 06:02:28 GMT  
Content-Type: application/json; charset=UTF-8  
  
{  
  "code": 20016,  
  "msg": "验证码输入错误",  
  "data": null  
}  
...
```


缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: http://192.168.11.210/civil/information_linkage/column/pageQueryColumn

实体: pageQueryColumn (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:

```
...  
  
Host: 192.168.11.210  
Content-Length: 20  
Pragma: no-cache  
  
{  
  "page": 1,  
  "rows": 10  
}  
  
HTTP/1.1 200  
Transfer-Encoding: chunked  
Connection: keep-alive  
Server: nginx/1.15.8  
Date: Wed, 18 Sep 2019 06:02:28 GMT  
Content-Type: application/json; charset=UTF-8  
  
{  
  "total": 5,  
  "rows": [  
    {  
      "id": 15,  
      "createTime": "2019-09-18 14:02:28",  
      "updateTime": "2019-09-18 14:02:28",  
      "name": "栏目1",  
      "description": "栏目描述",  
      "hide": null,  
    }  
  ]  
}  
...
```

缺少“Content-Security-Policy”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://192.168.11.210/civil/ueditor/ueditorConfig>

实体: ueditorConfig (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 /civil/ueditor/ueditorConfig?action=config&noCache=1568786093746 HTTP/1.1
Accept-Language: zh-cn
Referer: http://192.168.11.210/informationLinkage/#/login?
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: */*
Host: 192.168.11.210

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.15.8
Set-Cookie: JSESSIONID=915272C1691EFE06F9C3C4676297F566; Path=/civil; HttpOnly
Date: Wed, 18 Sep 2019 06:02:28 GMT
Content-Type: application/json;charset=ISO-8859-1

{
  "videoMaxSize": 102400000,
  "videoActionName": "uploadvideo",
  "fileActionName": "uploadfile",
  "fileManagerListPath": "/ueditor/jsp/upload/file/",
  "imageCompressBorder": 1600,
  "imageManagerAllowFiles": [
    ".png",
    ".jpg",
    ".jpeg",
  ]
}
```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.210/informationLinkage/>

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 /informationLinkage/ HTTP/1.1
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: */*
Host: 192.168.11.210

HTTP/1.1 200 OK
Last-Modified: Wed, 18 Sep 2019 01:56:52 GMT
x-ua-compatible: IE=edge
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1950
ETag: "5d818ee4-79e"
Date: Wed, 18 Sep 2019 06:02:27 GMT
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,in...

...
```

低

检测到隐藏目录 1

TOC

问题 1 / 1

TOC

检测到隐藏目录

严重性: **低**

CVSS 分数: 5.0

URL: <http://192.168.11.210/informationLinkage/assets/>

实体: assets/ (Page)

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

原因: Web 服务器或应用程序服务器是以不安全的方式配置的

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

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

未经处理的测试响应:

```
...
GET /informationLinkage/assets/ HTTP/1.1
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: */*
Host: 192.168.11.210

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx/1.15.8
Content-Length: 153
Date: Wed, 18 Sep 2019 06:02:42 GMT
Content-Type: text/html

<html>
<head><title>403 Forbidden</title></head>
<body>

...
```

问题 1 / 1

TOC

跨站点请求伪造

严重性: 中

CVSS 分数: 6.4

URL: http://192.168.11.210/civil/information_linkage/column/pageQueryColumn

实体: pageQueryColumn (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 1 / 1

TOC

IPSwitch Imail Imonitor 拒绝服务

严重性: 高

CVSS 分数: 7.8

URL: <http://192.168.11.210/>

实体: status.cgi (Page)

风险: 可能会阻止 Web 应用程序服务其他用户（拒绝服务）

原因: 未安装第三方产品的最新补丁或最新修订程序

固定值: 升级至 IPSwitch Imail IMONITOR 的最新版本，或者安装最新更新的补丁

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。

未经处理的测试响应:

```
...

Accept-Language: zh-CN
Referer: http://192.168.11.210/informationLinkage/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Accept: application/json, text/plain, */*
Host: 192.168.11.210
Pragma: no-cache

HTTP/1.1 200 OK
Connection: keep-alive
Server: nginx/1.15.8
Content-Length: 757
Date: Wed, 18 Sep 2019 06:02:43 GMT
Content-Type: text/xml

<?xml-stylesheet type="text/xsl" href="stat.xsl" ?>
<rtmp>
  <nginx_version>1.15.8</nginx_version>
  <nginx_rtmp_version>1.1.4</nginx_rtmp_version>
  <compiler>gcc 4.8.5 20150623 (Red Hat 4.8.5-36) (GCC) </compiler>
  <built>Jun 3 2019 02:07:34</built>
  <pid>7771</pid>
  <uptime>775257</uptime>
  <naccepted>18</naccepted>
  <bw_in>0</bw_in>

...
```

修订建议

高

升级至 IPSwitch IMail IMONITOR 的最新版本，或者安装最新更新的补丁

TOC

该任务修复的问题类型

- IPSwitch IMail Imonitor 拒绝服务

常规

升级值 iMail 7.0.6，位置如下：

<http://www.ipswitch.com/Support/IMail/patch-upgrades.html>

中

验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

TOC

该任务修复的问题类型

- 跨站点请求伪造

常规

有多种减轻威胁的技巧：

[1] 策略：库或框架

使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。

例如，使用能防御 CSRF 的软件包，例如 OWASP CSRFGuard -

[http://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)_Prevention_Cheat_Sheet](http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)

另一个示例为“ESAPI 会话管理”控件，其中包括针对 CSRF 的组件 -

<http://www.owasp.org/index.php/ESAPI>

[2] 确保应用程序中没有跨站点脚本编制问题 (CWE-79)，因为通过使用攻击者控制的脚本可绕过大部分 CSRF 防御。

[3] 为每个表单生成唯一的现时标志，将现时标志放到表单中，并在接收表单时验证现时标志。请确保现时标志是不可预测的 (CWE-330) -

<http://www.cgisecurity.com/articles/csrf-faq.shtml>

请注意，通过使用 XSS (CWE-79) 可绕过这一点。

[4] 识别特别危险的操作。在用户执行危险操作时，发送单独的确认请求以确保是用户自己希望执行该操作。请注意，通过使用 XSS (CWE-79) 可绕过这一点。

[5] 使用“两次提交的 cookie”方法，如 Felten 和 Zeller 所述：

在用户访问站点时，该站点应生成伪随机值，并将其设置为用户机器上的 cookie。站点应要求每次表单提交都包括该值作为表单和 cookie 值。向站点发送 POST 请求时，只有表单和 cookie 值相同时才应将该请求视为有效。

由于同源策略，攻击者无法读取或修改 cookie 中存储的值。要以用户的身份成功提交表单，攻击者必须正确猜出伪随机值。如果伪随机值的保密性很强，这将是极端困难的。此技巧需要 JavaScript，因此对于禁用了 JavaScript 的浏览器可能无效 -

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.1445>

请注意，使用 XSS (CWE-79) 有可能绕过这一点，或者在使用支持攻击者从 HTTP 请求中读取原始头的 Web 技术时也有可能绕过这一点。

[6] 请勿对触发状态更改的任何请求使用 GET 方法。

[7] 检查 HTTP Referer 头以查看请求是否源自预期的页面。这可能会破坏合法功能，因为用户或代理可能已出于隐私原因而禁止发送 Referer。请注意，通过使用 XSS (CWE-79) 可绕过这一点。

攻击者可能使用 XSS 来生成欺骗性的 Referer，或从允许使用其 Referer 的页面生成恶意请求。

低

为 Web 服务器或 Web 应用程序下载相关的安全补丁

TOC

该任务修复的问题类型

- 发现可能的服务器路径泄露模式

常规

下载相关的安全补丁，这会随着 Web 服务器或 Web 应用程序上现有的问题而不同。

低

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

TOC

该任务修复的问题类型

- 检测到隐藏目录

常规

如果不需要禁止的资源，请将其从站点中除去。

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

该任务修复的问题类型

- 缺少“Content-Security-Policy”头

常规

将您的服务器配置为发送“Content-Security-Policy”头。对于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

对于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

对于 nginx，请参阅：

http://nginx.org/en/docs/http/nginx_headers_module.html

该任务修复的问题类型

- 缺少“X-Content-Type-Options”头

常规

将您的服务器配置为在所有传出请求上发送值为“nosniff”的“X-Content-Type-Options”头。对于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

对于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

对于 nginx，请参阅：

http://nginx.org/en/docs/http/nginx_headers_module.html

该任务修复的问题类型

- 缺少“X-XSS-Protection”头

常规

将您的服务器配置为在所有传出请求上发送值为“1”（例如已启用）的“X-XSS-Protection”头。对于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html

对于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

对于 nginx，请参阅：

http://nginx.org/en/docs/http/nginx_http_headers_module.html

低

除去 Web 站点中的内部 IP 地址

TOC

该任务修复的问题类型

- 发现内部 IP 泄露模式

常规

内部 IP 通常显现在 Web 应用程序/服务器所生成的错误消息中，或显现在 HTML/JavaScript 注释中。

[1] 关闭 Web 应用程序/服务器中有问题的详细错误消息。

[2] 确保已安装相关的补丁。

[3] 确保内部 IP 信息未留在 HTML/JavaScript 注释中。

低

除去 Web 站点中的电子邮件地址

TOC

该任务修复的问题类型

- 发现电子邮件地址模式

常规

从 Web 站点中除去任何电子邮件地址，以便其不会被恶意用户利用。

低

除去客户端中的业务逻辑和安全逻辑

TOC

该任务修复的问题类型

- 客户端 (JavaScript) Cookie 引用

常规

[1] 避免在客户端放置业务/安全逻辑。

[2] 查找并除去客户端不安全的 JavaScript 代码，该代码可能会对站点造成安全威胁。

咨询

客户端（JavaScript）Cookie 引用

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Cookie 是在客户端创建的

安全性风险：

此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色

受影响产品：

CWE:

602

X-Force:

52514

引用：

WASC 威胁分类：信息泄露

技术描述：

cookie 是一则信息，通常由 Web 服务器创建并存储在 Web 浏览器中。

web 应用程序主要（但不只是）使用 cookie 包含的信息来识别用户并维护用户的状态。

AppScan 检测到客户端上的 JavaScript 代码用于操控（创建或修改）站点的 cookie。

攻击者有可能查看此代码、了解其逻辑并根据所了解的知识将其用于组成其自己的 cookie，或修改现有 cookie。

攻击者可能导致的损坏取决于应用程序使用其 cookie 的方式或应用程序存储在这些 cookie 中的信息内容。

此外，cookie 操控还可能导致会话劫持或特权升级。

由 cookie 毒害导致的其他漏洞包含 SQL 注入和跨站点脚本编制。

发现电子邮件地址模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

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

受影响产品：

CWE:

359

X-Force:

52584

引用：

Spambot 的定义（维基百科）

技术描述：

Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。

AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。

而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

发现可能的服务器路径泄露模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因:

未安装第三方产品的最新补丁或最新修订程序

安全性风险:

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

受影响产品:

CWE:

200

X-Force:

52839

技术描述:

AppScan 检测到含有文件绝对路径（例如：Windows 的 c:\dir\file，Unix 的 /dir/file）的响应。
攻击者也许能够利用这项信息，从而访问到关于服务器机器目录结构的敏感信息，因而能够进一步攻击站点。

发现内部 IP 泄露模式

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

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

受影响产品:

CWE:

200

X-Force:

52657

技术描述:

AppScan 检测到包含内部 IP 地址的响应。

内部 IP 定义为以下 IP 范围内的 IP:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

内部 IP 公开对于攻击者非常有价值，因为它揭示了内部网络的 IP 联网模式。获知内部网络的 IP 联网模式可能会帮助攻击者计划针对内部网络的进一步攻击。

缺少“X-XSS-Protection”头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

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

受影响产品:

CWE:

200

引用:

有用 HTTP 头的列表

IE XSS 过滤器

技术描述:

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

缺少“X-Content-Type-Options”头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

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

受影响产品:

CWE:

200

引用:

有用 HTTP 头的列表

减小 MIME 类型安全性风险

技术描述:

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

缺少“Content-Security-Policy”头

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

Web 应用程序编程或配置不安全

安全性风险:

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

受影响产品：

CWE:

200

引用：

有用 HTTP 头的列表
内容安全策略的简介

技术描述：

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

检测到隐藏目录

TOC

测试类型：

基础结构测试

威胁分类：

信息泄露

原因：

Web 服务器或应用程序服务器是以不安全的方式配置的

安全性风险：

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

受影响产品：

CWE:

200

X-Force:

52599

技术描述：

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

跨站点请求伪造

TOC

测试类型：

应用程序级别测试

威胁分类：

跨站点请求伪造

原因：

应用程序使用的认证方法不充分

安全性风险：

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

受影响产品：

CWE:

352

X-Force:

6784

引用：

跨站点伪造请求 [Wiki 页面](#)

“JavaScript 劫持”，作者：Fortify

跨站点请求伪造培训模块

技术描述：

即使是格式正确、有效且一致的请求也可能已在用户不知情的情况下发送。因此，**Web** 应用程序应检查所有请求以发现其不合法的迹象。此测试的结果指示所扫描的应用程序没有执行此操作。此脆弱性的严重性取决于受影响应用程序的功能。例如，对搜索页面的 **CSRF** 攻击的严重性低于对转账或概要文件更新页面的 **CSRF** 攻击。如果某个 **Web** 服务器设计为接收客户机的请求时无任何机制来验证该请求是否确实是客户机发送的，那么攻击者就有可能诱导客户机向该 **Web** 服务器误发请求，而该请求将视为真实请求。这可通过 **URL**、图像装入、**XMLHttpRequest** 等来完成，并可导致数据暴露或意外的代码执行。如果用户当前已登录到受害者站点，请求将自动使用用户的凭证（包括会话 **cookie**、**IP** 地址和其他浏览器认证方法）。通过使用此方法，攻击者可伪造受害者的身份，并以其身份提交操作。

IPSwitch Imail Imonitor 拒绝服务

TOC

测试类型:

基础结构测试

威胁分类:

拒绝服务

原因:

未安装第三方产品的最新补丁或最新修订程序

安全性风险:

可能会阻止 **Web** 应用程序服务其他用户（拒绝服务）

受影响产品:

CWE:

119

X-Force:

3874

引用:

FrontPage 服务器扩展: 安全考虑

BugTraq BID: 3430

USSR advisory

技术描述:

status.cgi 脚本的设计不正确，在后续多个请求之后，会使服务器崩溃。利用的样本如下：
相对 **IPMonitor** 端口（通常是 **8181**），执行下列请求若干次：

GET /status.cgi HTTP/1.0

若干次之后，服务器会崩溃，造成拒绝服务。