



# 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: 2019/9/17 13:55:53

# 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

- IPSwitch Imail Imonitor 拒绝服务 ①
- 缺少“Content-Security-Policy”头 ⑤
- 缺少“X-Content-Type-Options”头 ⑤
- 缺少“X-XSS-Protection”头 ⑤
- 发现可能的服务器路径泄露模式 ②
- 发现电子邮件地址模式 ①
- 客户端（JavaScript）Cookie 引用 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
- 为 Web 服务器或 Web 应用程序下载相关的安全补丁
- 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 站点中的电子邮件地址
- 除去客户端中的业务逻辑和安全逻辑

## 咨询

- IPSwitch Imail Imonitor 拒绝服务
- 缺少“Content-Security-Policy”头
- 缺少“X-Content-Type-Options”头
- 缺少“X-XSS-Protection”头
- 发现可能的服务器路径泄露模式
- 发现电子邮件地址模式
- 客户端（JavaScript）Cookie 引用

# 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
低严重性问题:	15
参考严重性问题:	4
报告中包含的严重性问题总数:	20
扫描中发现的严重性问题总数:	20

## 常规信息

扫描文件名称:	test
扫描开始时间:	2019/9/17 13:55:53
测试策略:	Default
主机	192.168.11.206
端口	0
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
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 7

TOC

问题类型		问题的数量
高	IPSwitch Imail Imonitor 拒绝服务	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	发现可能的服务器路径泄露模式	2
参	发现电子邮件地址模式	1
参	客户端（JavaScript）Cookie 引用	1

## 有漏洞的 URL 9

TOC

URL		问题的数量
高	http://192.168.11.206/	1
低	http://192.168.11.206/informationLinkage/	1
低	http://192.168.11.206/informationLinkage/assets/js/chunk-39b04568.0bf56b6f.js	3
低	http://192.168.11.206/informationLinkage/assets/js/chunk-65f44854.8f446a02.js	4
低	http://192.168.11.206/informationLinkage/assets/js/chunk-6e2855ec.1ca313ea.js	3
低	http://192.168.11.206/informationLinkage/layui/layui.js	3
低	http://192.168.11.206/server/user/getVerifyCode	2
参	http://192.168.11.206/informationLinkage/assets/js/chunk-074e1af5.862c9280.js	2
参	http://192.168.11.206/informationLinkage/assets/js/chunk-vendors.5ed272ce.js	1

## 修订建议 7

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
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	2
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	除去 Web 站点中的电子邮件地址	1
低	除去客户端中的业务逻辑和安全逻辑	1

## 安全风险 5

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
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	16
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
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
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

## 原因 3

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订程序	3
低	Web 应用程序编程或配置不安全	16
参	Cookie 是在客户端创建的	1

## WASC 威胁分类

TOC

威胁	问题的数量
信息泄露	19



# 按问题类型分类的问题

高

IPSwitch Imail Imonitor 拒绝服务 ①

TOC

问题 1 / 1

TOC

## IPSwitch Imail Imonitor 拒绝服务

严重性: 高

CVSS 分数: 7.8

URL: <http://192.168.11.206/>

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:**

```
...
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Connection: keep-alive
Host: 192.168.11.206
Accept: application/json, text/plain, */*
Origin: http://192.168.11.206
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Connection: keep-alive
Server: nginx/1.15.8
Content-Length: 774
Date: Tue, 17 Sep 2019 05:57:14 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  5 2019 22:19:02</built>  
<pid>96905</pid>  
<uptime>3022667</uptime>  
<naccepted>384</naccepted>  
<bw_in>0</bw_in>
```

...

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://192.168.11.206/informationLinkage/assets/js/chunk-39b04568.0bf56b6f.js>

实体: chunk-39b04568.0bf56b6f.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/assets/js/chunk-39b04568.0bf56b6f.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 4956
ETag: "5d78905f-135c"
Date: Tue, 17 Sep 2019 05:57:09 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-39b04568"],
{"1c0c":function(e,t,r){},c639:function(e,t,r){},ccd9:function(e,t,r){"use stri...
...

```

**缺少“Content-Security-Policy”头****严重性:** 低**CVSS 分数:** 5.0**URL:** <http://192.168.11.206/informationLinkage/assets/js/chunk-6e2855ec.1ca313ea.js>**实体:** chunk-6e2855ec.1ca313ea.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/assets/js/chunk-6e2855ec.1ca313ea.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 8538
ETag: "5d78905f-215a"
Date: Tue, 17 Sep 2019 05:57:09 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-6e2855ec"],
{"0278":function(t,e,a){"use strict";var n=function(){var t=this,e=t.$createEle...

...

```

## 缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/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
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
```

...

## 问题 4 / 5

TOC

## 缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/informationLinkage/assets/js/chunk-65f44854.8f446a02.js>

实体: chunk-65f44854.8f446a02.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/assets/js/chunk-65f44854.8f446a02.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
```

```
...
```

## 问题 5 / 5

TOC

### 缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/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
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 192.168.11.206
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
Last-Modified: Wed, 11 Sep 2019 06:12:47 GMT
x-ua-compatible: IE=edge
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1950
ETag: "5d78905f-79e"
Date: Tue, 17 Sep 2019 05:57:09 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

## 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://192.168.11.206/informationLinkage/assets/js/chunk-39b04568.0bf56b6f.js>

实体: chunk-39b04568.0bf56b6f.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/assets/js/chunk-39b04568.0bf56b6f.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 4956
ETag: "5d78905f-135c"
Date: Tue, 17 Sep 2019 05:57:09 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-39b04568"],
{"1c0c":function(e,t,r){},c639:function(e,t,r){},ccd9:function(e,t,r){use stri...
...

```

## 缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/informationLinkage/assets/js/chunk-6e2855ec.1ca313ea.js>

实体: chunk-6e2855ec.1ca313ea.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/assets/js/chunk-6e2855ec.1ca313ea.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 8538
ETag: "5d78905f-215a"
Date: Tue, 17 Sep 2019 05:57:09 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-6e2855ec"],
{"0278":function(t,e,a){"use strict";var n=function(){var t=this,e=t.$createEle...

...

```

## 缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/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
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
...
```

## 问题 4 / 5

TOC

## 缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/informationLinkage/assets/js/chunk-65f44854.8f446a02.js>

实体: chunk-65f44854.8f446a02.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/assets/js/chunk-65f44854.8f446a02.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT

...

```

## 问题 5 / 5

TOC

### 缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/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:**

```

...
POST /server/user/getVerifyCode HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Connection: keep-alive
Host: 192.168.11.206
Content-Length: 0
Accept: application/json, text/plain, */*
Origin: http://192.168.11.206
Accept-Language: en-US,en;q=0.8

...

```

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://192.168.11.206/informationLinkage/assets/js/chunk-39b04568.0bf56b6f.js>**实体:** chunk-39b04568.0bf56b6f.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/assets/js/chunk-39b04568.0bf56b6f.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 4956
ETag: "5d78905f-135c"
Date: Tue, 17 Sep 2019 05:57:09 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-39b04568"],
{"1c0c":function(e,t,r){},c639:function(e,t,r){},ccd9:function(e,t,r){"use stri...

...

```

## 缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/informationLinkage/assets/js/chunk-6e2855ec.1ca313ea.js>

实体: chunk-6e2855ec.1ca313ea.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/assets/js/chunk-6e2855ec.1ca313ea.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 8538
ETag: "5d78905f-215a"
Date: Tue, 17 Sep 2019 05:57:09 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-6e2855ec"],
{"0278":function(t,e,a){"use strict";var n=function(){var t=this,e=t.$createEle...

...

```

## 缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/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
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
...
```

## 问题 4 / 5

TOC

## 缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/informationLinkage/assets/js/chunk-65f44854.8f446a02.js>

实体: chunk-65f44854.8f446a02.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/assets/js/chunk-65f44854.8f446a02.js HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Host: 192.168.11.206
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: Wed, 11 Sep 2019 06:12:47 GMT
```

...

## 问题 5 / 5

TOC

### 缺少“X-XSS-Protection”头

严重性:  低

CVSS 分数: 5.0

URL: <http://192.168.11.206/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:**

```
...
POST /server/user/getVerifyCode HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://192.168.11.206/informationLinkage/
Connection: keep-alive
Host: 192.168.11.206
Content-Length: 0
Accept: application/json, text/plain, */*
Origin: http://192.168.11.206
Accept-Language: en-US,en;q=0.8
```

...

## 问题 1 / 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://192.168.11.206/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:\\\\projec\\\\\\\\ä¿;æ`èä"\\
```

## 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:	<a href="http://192.168.11.206/informationLinkage/assets/js/chunk-vendors.5ed272ce.js">http://192.168.11.206/informationLinkage/assets/js/chunk-vendors.5ed272ce.js</a>
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:	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:

```
...
... (?:1?\\d{1,2}|2[0-4]\\d{25[0-5]}){2}(?:\\. (?:[0-9]\\d?|1\\d\\d|2[0-4]\\d{25[0-4]})| (?:?:[a-
z\\u00a1-\\uffff0-9]+-?) * [a-z\\u00a1-\\uffff0-9]+) (?:\\. (?:[a-z\\u00a1-b...

...

...
...nction(e){return e.trim()}).filter(function(e){return e}).some(function(e)
{return/\\.+$/ .test(e)?r==e:/\\*$/ .test(e)?
o===e.replace(/\\/\\*$/,""):!!/^[/\\+\\/[/\\+$/ .test(e)&n===e)}}):this.$emit("file",...

...
```

## 发现电子邮件地址模式 ①

## TOC

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:	<a href="http://192.168.11.206/informationLinkage/assets/js/chunk-074e1af5.862c9280.js">http://192.168.11.206/informationLinkage/assets/js/chunk-074e1af5.862c9280.js</a>
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": {"jscss": "jscss
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{...
```

问题 1 / 1

TOC

客户端（JavaScript）Cookie 引用	
严重性:	参考
CVSS 分数:	0.0
URL:	http://192.168.11.206/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...  
  
...
```

# 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>

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

将您的服务器配置为使用“Content-Security-Policy”头

TOC

## 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](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](http://nginx.org/en/docs/http/nginx_headers_module.html)

低

将您的服务器配置为使用“X-Content-Type-Options”头

TOC

## 该任务修复的问题类型

- 缺少“X-Content-Type-Options”头

### 常规

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

[http://httpd.apache.org/docs/2.2/mod/mod\\_headers.html](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](http://nginx.org/en/docs/http/nginx_headers_module.html)

低

将您的服务器配置为使用“X-XSS-Protection”头

TOC

## 该任务修复的问题类型

- 缺少“X-XSS-Protection”头

### 常规

将您的服务器配置为在所有传出请求上发送值为“1”（例如已启用）的“X-XSS-Protection”头。对于 Apache，请参阅：

[http://httpd.apache.org/docs/2.2/mod/mod\\_headers.html](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](http://nginx.org/en/docs/http/nginx_headers_module.html)

## 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

## 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。

## 缺少“Content-Security-Policy”头

TOC

### 测试类型:

应用程序级别测试

### 威胁分类:

信息泄露

### 原因:

Web 应用程序编程或配置不安全

### 安全性风险:

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

### 受影响产品:

### CWE:

200

### 引用:

有用 HTTP 头的列表  
内容安全策略的简介

### 技术描述:

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

## 缺少“X-Content-Type-Options”头

TOC

### 测试类型:

应用程序级别测试

### 威胁分类:

信息泄露

### 原因:

Web 应用程序编程或配置不安全

### 安全性风险:

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

### 受影响产品:

### CWE:

200

### 引用:

有用 HTTP 头的列表

减小 MIME 类型安全性风险

### 技术描述:

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

## 缺少“X-XSS-Protection”头

TOC

### 测试类型:

应用程序级别测试

### 威胁分类:

信息泄露

### 原因:

Web 应用程序编程或配置不安全

### 安全性风险:

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

### 受影响产品:

### CWE:

200

引用:

有用 HTTP 头的列表  
IE XSS 过滤器

技术描述:

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

## 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。

## 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** 操控还可能導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。