



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: 2019/9/19 11:10:09

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 ①
- 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: 3
报告中包含的严重性问题总数: 19
扫描中发现的严重性问题总数: 19

常规信息

扫描文件名称: 信息登陆
扫描开始时间: 2019/9/19 11:10:09
测试策略: Default

主机: xizang.sccddw.com
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: createUserId:null|roleName": "超级管理员
跟踪或会话标识 cookie:
跟踪或会话标识参数:
登陆序列:
http://xizang.sccddw.com/userRole
http://xizang.sccddw.com/userRole/
http://xizang.sccddw.com/server/user/getVerifyCode

<http://xizang.sccddw.com/server/user/login>
<http://xizang.sccddw.com/server/user/findUserPage>
<http://xizang.sccddw.com/server/role/pageRole>
<http://xizang.sccddw.com/server/role/pageRole>
<http://xizang.sccddw.com/server/user/findUserPage>
<http://xizang.sccddw.com/server/role/pageRole>

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	1 
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 8

TOC

URL	问题的数量
高 http://xizang.sccddw.com/	1 
低 http://xizang.sccddw.com/userRole/browser/check.js	3 
低 http://xizang.sccddw.com/userRole/js/app.a55d1c1e.js	3 
低 http://xizang.sccddw.com/userRole/js/role.d97565c5.js	2 
低 http://xizang.sccddw.com/userRole/js/user.a0fe66cf.js	3 
低 http://xizang.sccddw.com/userRole/static/layui-src/dist/layui.js	3 
低 http://xizang.sccddw.com/userRole/js/myCenter.d68f75fc.js	1 
参 http://xizang.sccddw.com/userRole/js/chunk-vendors.e58e5a19.js	3 

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	<div></div>
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	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 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	<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	16	<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>
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	<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>

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	2	<div></div>
低	Web 应用程序编程或配置不安全	16	<div></div>
参	Cookie 是在客户端创建的	1	<div></div>

WASC 威胁分类

TOC

威胁	问题的数量
信息泄露	18
拒绝服务	1

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://xizang.sccddw.com/
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: en-US,en;q=0.8
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Origin: http://xizang.sccddw.com
Connection: keep-alive
Accept: */*
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Connection: keep-alive
Server: nginx/1.15.8
Content-Length: 774
Date: Thu, 19 Sep 2019 03:23:29 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>3186242</uptime>  
<naccepted>387</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://xizang.sccddw.com/userRole/browser/check.js>

实体: check.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 /userRole/browser/check.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzdWIiOiIxODY2IiwiaWY2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxRbxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: xizang.sccddw.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1680
ETag: "5d7a12b7-690"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript
```

```
function getBrowserInfo() {
    var agent = navigator.userAgent.toLowerCase();
    var regStr_ie = /msie [\d.]+;/gi;
    var regStr_ff = /firefox\/[\d.]+/gi;
    var regStr_chrome = /chrome\/[\d.]+/gi;
    var regStr_saf = /safari\/[\d.]+/gi;
    var isIE = agent.indexOf("compatible") > -1 && agent.indexOf("msie") > -1; //判断是否IE<11浏览器
    var isEdge = agent.indexOf("edge") > -1 && !isIE; //判断是否IE的Edge浏览器
```

```

var isIE11 = agent.indexOf('trident') > -1 && agent.indexOf("rv:11.0") > -1;
if (isIE) {
...

```

问题 2 / 5

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/static/layui-src/dist/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 /userRole/static/layui-src/dist/layui.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzdWIiOiIxODY2Iiwia2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxRbxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: xizang.sccddw.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 6675
ETag: "5d7a12b7-1a13"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

/** layui-v2.5.4 MIT License By https://www.layui.com */
;!function(e){ "use strict";var t=document,o={modules:{},status:{},timeout:10,event:
{}},n=function(...
...

```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/app.a55d1c1e.js>

实体: app.a55d1c1e.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 /userRole/js/app.a55d1c1e.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzdWIiOiIxODY2Iiwia2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxRbxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 17762
ETag: "5d7a12b7-4562"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(function(e){function t(t){for(var n,a,i=t[0],c=t[1],l=t[2],u=0,f=
[];u<i.length;u++)a=i[u],s[a]&&f.push(s[a][0]),s[a]=0;for(n in c)Object.prototype.hasOwnPropertyPr...
...

```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/user.a0fe66cf.js>

实体: user.a0fe66cf.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 /userRole/js/user.a0fe66cf.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2IiwiaWY2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 15690
ETag: "5d7a12b7-3d4a"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["user"],{"0d63":function(e,t,a){"use
strict";var i=a("fa99"),l=a.n(i);l.a},"6afe":function(e,t,a)...

...
```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/role.d97565c5.js>

实体: role.d97565c5.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 /userRole/js/role.d97565c5.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2IiwiaWY2xpZW50X3R5cGUjEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 13329
ETag: "5d7a12b7-3411"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["role"],{2511:function(e,t,a){
"use strict";var i=a("d94d"),n=a.n(i);n.a,"695c":function(e,t,a){"...
...
```

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://xizang.sccddw.com/userRole/browser/check.js>

实体: check.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 /userRole/browser/check.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzdWIiOiIxODY2IiwiaWY2xpZW50X3R5cGUiojEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcFfXRBxJtRtWDMZeau9Lukq-swW35q52YOPkJp_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: xizang.sccddw.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1680
ETag: "5d7a12b7-690"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

function getBrowserInfo() {
    var agent = navigator.userAgent.toLowerCase();
    var regStr_ie = /msie [\d.]+;/gi;
    var regStr_ff = /firefox\/[\d.]+/gi;
    var regStr_chrome = /chrome\/[\d.]+/gi;
    var regStr_saf = /safari\/[\d.]+/gi;
    var isIE = agent.indexOf("compatible") > -1 && agent.indexOf("msie") > -1; //判断是否IE<11浏览
器
    var isEdge = agent.indexOf("edge") > -1 && !isIE; //判断是否IE的Edge浏览器
    var isIE11 = agent.indexOf('trident') > -1 && agent.indexOf("rv:11.0") > -1;
    if (isIE) {
        ...
    }
}
```

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/static/layui-src/dist/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 /userRole/static/layui-src/dist/layui.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2IiwiaWY2xpZW50X3R5cGUjEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: xizang.sccddw.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 6675
ETag: "5d7a12b7-1a13"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

/** layui-v2.5.4 MIT License By https://www.layui.com */
;!function(e){ "use strict";var t=document,o={modules:{},status:{},timeout:10,event:
{}},n=function(...
...
```


缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/user.a0fe66cf.js>

实体: user.a0fe66cf.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 /userRole/js/user.a0fe66cf.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2Iiwia2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 15690
ETag: "5d7a12b7-3d4a"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["user"],{"0d63":function(e,t,a){"use
strict";var i=a("fa99"),l=a.n(i);l.a},"6afe":function(e,t,a)...

...
```

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/app.a55d1c1e.js>

实体: app.a55d1c1e.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 /userRole/js/app.a55d1c1e.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2IiwiaWY2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 17762
ETag: "5d7a12b7-4562"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(function(e){function t(t){for(var n,a,i=t[0],c=t[1],l=t[2],u=0,f=
[];u<i.length;u++)a=i[u],s[a]&&f.push(s[a][0]),s[a]=0;for(n in c)Object.prototype.hasOwnPr...
...

```

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/role.d97565c5.js>

实体: role.d97565c5.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 /userRole/js/role.d97565c5.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2IiwiaWY2xpZW50X3R5cGUjEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 13329
ETag: "5d7a12b7-3411"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["role"],{2511:function(e,t,a){
"use strict";var i=a("d94d"),n=a.n(i);n.a,"695c":function(e,t,a){"...
...

```

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://xizang.sccddw.com/userRole/browser/check.js>

实体: check.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 /userRole/browser/check.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzdWIiOiIiODY2IiwiaWY2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxRbxJtRtWDMZeau9Lukq-swW35q52YOPkjp_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: xizang.sccddw.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1680
ETag: "5d7a12b7-690"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

function getBrowserInfo() {
    var agent = navigator.userAgent.toLowerCase();
    var regStr_ie = /msie [\d.]+;/gi;
    var regStr_ff = /firefox\/[\d.]+/gi;
    var regStr_chrome = /chrome\/[\d.]+/gi;
    var regStr_saf = /safari\/[\d.]+/gi;
    var isIE = agent.indexOf("compatible") > -1 && agent.indexOf("msie") > -1; //判断是否IE<11浏览
器
    var isEdge = agent.indexOf("edge") > -1 && !isIE; //判断是否IE的Edge浏览器
    var isIE11 = agent.indexOf('trident') > -1 && agent.indexOf("rv:11.0") > -1;
    if (isIE) {
        ...
    }
}
```

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/static/layui-src/dist/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 /userRole/static/layui-src/dist/layui.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXZzaW9uX25vIjoxLCJzdWIiOiIiX2Iiwia2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkjp_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: xizang.sccddw.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 6675
ETag: "5d7a12b7-1a13"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

/** layui-v2.5.4 MIT License By https://www.layui.com */
;!function(e){"use strict";var t=document,o={modules:{},status:{},timeout:10,event:
{}},n=function(...
...
```

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/user.a0fe66cf.js>

实体: user.a0fe66cf.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 /userRole/js/user.a0fe66cf.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZW50X3R5cGUjEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 15690
ETag: "5d7a12b7-3d4a"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["user"],{"0d63":function(e,t,a){"use
strict";var i=a("fa99"),l=a.n(i);l.a},"6afe":function(e,t,a)...

...
```

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/app.a55d1c1e.js>

实体: app.a55d1c1e.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 /userRole/js/app.a55d1c1e.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzZWl0IiIxODY2IiwiaWY2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxBxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 17762
ETag: "5d7a12b7-4562"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(function(e){function t(t){for(var n,a,i=t[0],c=t[1],l=t[2],u=0,f=
[];u<i.length;u++)a=i[u],s[a]&&f.push(s[a][0]),s[a]=0;for(n in c)Object.prototype.hasOwnPropertyPr...

...
```

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://xizang.sccddw.com/userRole/js/myCenter.d68f75fc.js>

实体: myCenter.d68f75fc.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 /userRole/js/myCenter.d68f75fc.js HTTP/1.1
x-access-token:
eyJhbGciOiJIUzI1NiJ9.eyJ2ZXJzaW9uX25vIjoxLCJzdWIiOiIiXODY2IiwiaWY2xpZW50X3R5cGUiOiJEsImV4cCI6MTU2ODk0
ODU2MSwiaWF0IjoxNTY4ODYyMTYxfQ.wCzcfFxRbxJtRtWDMZeau9Lukq-swW35q52YOPkJP_U
Accept-Language: en-US
Referer: http://xizang.sccddw.com/userRole/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: xizang.sccddw.com

HTTP/1.1 200 OK
Last-Modified: Thu, 12 Sep 2019 09:41:11 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 13968
ETag: "5d7a12b7-3690"
Date: Thu, 19 Sep 2019 03:23:21 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["myCenter"],{"6afe":function(e,t,s)
{"use strict";s.d(t,"i",function(){return n}),s.d(t,"c",functi...

...

```


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://xizang.sccddw.com/userRole/js/chunk-vendors.e58e5a19.js>

实体: chunk-vendors.e58e5a19.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:

```

...
...d 0!=e)return e[r]||e["@@iterator"]||o[i(e)]},2801:function(e){e.exports={_args:
[["elliptic@6.4.1","G:\projects\cddw\xizang\web_civil_education"],_development:!0,_from:"ell
iptic@6.4.1",_id:"elliptic...

...

...
...resolved:"http://registry.npm.taobao.org/elliptic/download/elliptic-
6.4.1.tgz",_spec:"6.4.1",_where:"G:\projects\cddw\xizang\web_civil_education",author:
{name:"Fedor Indutny",email:"fedor@indutny.com"...

...

...
...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",...

...

...
...focus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|readonly|required|scope
d",_s="[\\x20\\t\\n\\f]",N="(?:\\\\.|[\\w-]|[\x00--begin_highlig...

...

...
... (?: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-\u00ff0-9]+?) * [a-z\u00a1-\u00ff0-9]+) (?:\\. (?:[a-z\u00a1--b...

...

```

```
...
...G[W]WWE", /\d{4}W\d{3}/], ["GGGG[W]WW", /\d{4}W\d{2}/, !1], ["YYYYDDD", /\d{7}/]], Dn=
[["HH:mm:ss.SSSS", /\d\d:\d\d:\d\d\.\d+/, ["HH:mm:ss.SSSS", /\d--begin_highlight_ta...
...
```

参

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:

<http://xizang.sccddw.com/userRole/js/chunk-vendors.e58e5a19.js>

实体:

chunk-vendors.e58e5a19.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:

```
...
...6.4.1", _where: "G:\\projects\\cddw\\xizang\\web_civil_education", author: {name: "Fedor
Indutny", email: "fedor@indutny.com"}, bugs:
{url: "https://github.com/indutny/elliptic/issues"}, dependencies: {"bn.js": "^4.4.0", brorand: "^...

...

...graphy"], license: "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 test...

...

...
...on(e) {
/*!
* The buffer module from node.js, for the browser.
*
* @author Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
* @license MIT
*/
var i=n("1fb5"),r=n("9152"),o=n("e3db");function a(){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://xizang.sccddw.com/userRole/js/chunk-vendors.e58e5a19.js>

实体: (window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["chunk-vendors"],{"00dc":function(e,t,n){... (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(r)&&s.push("path="+r),i.isString(o)&&s.push("domain="+o),!0===a&&s.push("secure"),do
cument.cookie=s.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

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

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

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

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

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

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。