



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 10:51:23

目录

介绍

- 常规信息
- 登陆设置

摘要

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- 缺少“Content-Security-Policy”头 5
- 缺少“X-Content-Type-Options”头 5
- 缺少“X-XSS-Protection”头 5
- 发现内部 IP 泄露模式 2
- 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

- 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

- 缺少“Content-Security-Policy”头
- 缺少“X-Content-Type-Options”头
- 缺少“X-XSS-Protection”头
- 发现内部 IP 泄露模式
- 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。

低严重性问题: 15
参考严重性问题: 5
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: 教育系统5
扫描开始时间: 2019/9/19 10:51:23
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
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	发现内部 IP 泄露模式	2 
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
低	http://192.168.11.206/education/browser/check.js	3 
低	http://192.168.11.206/education/js/app.ad4c5c09.js	3 
低	http://192.168.11.206/education/js/course.84892b10.js	3 
低	http://192.168.11.206/education/js/courseManagement.d1ba65b7.js	3 
低	http://192.168.11.206/education/static/layui-src/dist/layui.js	3 
参	http://192.168.11.206/education/js/myQuestionBank.c5a0dcd2.js	1 
参	http://192.168.11.206/education/js/videoCourseCreateSuccess.500afeb0.js	1 
参	http://192.168.11.206/education/js/chunk-vendors.46d31dc3.js	3 

修订建议 7

TOC

修复任务	问题的数量
------	-------

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 站点中的内部 IP 地址	2	<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 4

TOC

风险	问题的数量
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	18 <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
低 Web 应用程序编程或配置不安全	18 <div></div>
参 未安装第三方产品的最新补丁或最新修订程序	1 <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	20 <div></div>

按问题类型分类的问题

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/education/js/course.84892b10.js>

实体:

course.84892b10.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 /education/js/course.84892b10.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 14370
ETag: "5d710e00-3822"
Date: Thu, 19 Sep 2019 02:52:33 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["course"],{"01f9":function(t,e,n){
"strict";var r=n("2d00"),o=n("5ca1"),s=n("2aba"),a=n("32e9"...
```

...

问题 2 / 5

TOC

缺少“Content-Security-Policy”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://192.168.11.206/education/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 /education/browser/check.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.206
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1680
ETag: "5d710e00-690"
Date: Thu, 19 Sep 2019 02:52:34 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“Content-Security-Policy”头**严重性:** 低**CVSS 分数:** 5.0**URL:** <http://192.168.11.206/education/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 /education/static/layui-src/dist/layui.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.206
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 6675
ETag: "5d710e00-1a13"
Date: Thu, 19 Sep 2019 02:52:34 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://192.168.11.206/education/js/app.ad4c5c09.js>

实体: app.ad4c5c09.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 /education/js/app.ad4c5c09.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 28269
ETag: "5d710e00-6e6d"
Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

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

```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/education/js/courseManagement.d1ba65b7.js>

实体: courseManagement.d1ba65b7.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 /education/js/courseManagement.d1ba65b7.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 16662
ETag: "5d710e00-4116"
Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["courseManagement"],
{"1af6":function(t,e,a){var n=a("63b6");n(n.S,"Array",{isArray:a("9003")})},"...
...

```

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/education/js/course.84892b10.js>

实体: course.84892b10.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 /education/js/course.84892b10.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 14370
ETag: "5d710e00-3822"
Date: Thu, 19 Sep 2019 02:52:33 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["course"],{"01f9":function(t,e,n){ "use
strict";var r=n("2d00"),o=n("5ca1"),s=n("2aba"),a=n("32e9"...

...
```

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/education/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 /education/browser/check.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.206
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1680
ETag: "5d710e00-690"
Date: Thu, 19 Sep 2019 02:52:34 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://192.168.11.206/education/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 /education/static/layui-src/dist/layui.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.206
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 6675
ETag: "5d710e00-1a13"
Date: Thu, 19 Sep 2019 02:52:34 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://192.168.11.206/education/js/app.ad4c5c09.js>

实体: app.ad4c5c09.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 /education/js/app.ad4c5c09.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 28269
ETag: "5d710e00-6e6d"
Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

(function(e){function t(t){for(var r,n,i=t[0],c=t[1],u=t[2],l=0,d=
[];l<i.length;l++)n=i[l],o[n]&&d.push(o[n][0]),o[n]=0;for(r in c)Object.prototype.hasOwnProperty.Pr...

...
```

缺少“X-Content-Type-Options”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/education/js/courseManagement.d1ba65b7.js>

实体: courseManagement.d1ba65b7.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 /education/js/courseManagement.d1ba65b7.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 16662
ETag: "5d710e00-4116"
Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["courseManagement"],
{"1af6":function(t,e,a){var n=a("63b6");n(n.S,"Array",{isArray:a("9003")})},"...
...

```

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://192.168.11.206/education/js/course.84892b10.js>

实体: course.84892b10.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 /education/js/course.84892b10.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 14370
ETag: "5d710e00-3822"
Date: Thu, 19 Sep 2019 02:52:33 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["course"],{"01f9":function(t,e,n){"use
strict";var r=n("2d00"),o=n("5ca1"),s=n("2aba"),a=n("32e9"...

...
```

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://192.168.11.206/education/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 /education/browser/check.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.206
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 1680
ETag: "5d710e00-690"
Date: Thu, 19 Sep 2019 02:52:34 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://192.168.11.206/education/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 /education/static/layui-src/dist/layui.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 192.168.11.206
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 6675
ETag: "5d710e00-1a13"
Date: Thu, 19 Sep 2019 02:52:34 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://192.168.11.206/education/js/courseManagement.d1ba65b7.js>

实体: courseManagement.d1ba65b7.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 /education/js/courseManagement.d1ba65b7.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 16662
ETag: "5d710e00-4116"
Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["courseManagement"],
{"1af6":function(t,e,a){var n=a("63b6");n(n.S,"Array",{isArray:a("9003")}}),"...

...
```

缺少“X-XSS-Protection”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://192.168.11.206/education/js/app.ad4c5c09.js>

实体: app.ad4c5c09.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 /education/js/app.ad4c5c09.js HTTP/1.1
Accept-Language: en-US
Referer: http://192.168.11.206/education/
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: 192.168.11.206

HTTP/1.1 200 OK
Last-Modified: Thu, 05 Sep 2019 13:30:40 GMT
Connection: keep-alive
Server: nginx/1.15.8
Accept-Ranges: bytes
Content-Length: 28269
ETag: "5d710e00-6e6d"
Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

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

...
```

问题 1 / 2

TOC

发现内部 IP 泄露模式

严重性: 参考

CVSS 分数: 0.0

URL: <http://192.168.11.206/education/js/myQuestionBank.c5a0dcd2.js>

实体: myQuestionBank.c5a0dcd2.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:

```
...
...Visible:!1,newSubject:"",pagination:{size:6,current:1,total:0}},copySubjects:
({},templateUrl:"http://192.168.11.206:9999/files/éçâ°æ"iæç-ç°è²ää%ääçâ;«.xlsx"}},watch:
{excelName:function(t,e){this.$refs["ru...
...
```

问题 2 / 2

TOC

发现内部 IP 泄露模式

严重性: 参考

CVSS 分数: 0.0

URL: <http://192.168.11.206/education/js/videoCourseCreateSuccess.500afeb0.js>

实体: videoCourseCreateSuccess.500afeb0.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:

```

Date: Thu, 19 Sep 2019 02:52:34 GMT
Content-Type: application/javascript

(window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["videoCourseCreateSuccess"],
{"35b9":function(t,e,s){},a63b:function(t,e,s){return s("div",{staticClass:"content"},[t._m(0),l===t.type?s("div",{staticStyle:{color:"#a2a2a2"}},{s("div",{staticClass:"paddingTB10"},[t._v("\n\n你的课程已经上传完成.\n\n"))]),s("div",{staticStyle:{color:"#a2a2a2"}},{t._m(1)},s("div",[t._v("\n\n播放地址为: "+t._s(t.liveUrl)+"\n\n")),s("div",{staticClass:"paddingTB10"},[t._v("\n\n请使用OBS进行推流, ")])],s("span",{staticClass:"blue",on:{click:t.goOBSDoc}},[t._v("OBS使用说明")])]),s("div",[s("span",{staticClass:"blue",on:{click:t.goBack}}),[t._v("继续创建课程")])])]),a=[function(){var t=this,e=t.$createElement,s=t._self._c||e;return s("div",{staticClass:"el-icon-circle-check green"}),s("span",{staticStyle:{margin-left:"15px"}},[t._v("已成功! ")])}],function(){var t=this,e=t.$createElement,s=t._self._c||e;return s("div",{s("div",{staticStyle:{padding-top:"10px"}},[t._v("\n\n你的直播已经创建.\n\n"))]),s("div",{staticClass:"paddingTB10"},[t._v("\n\n您可以在开课前10分钟进入课堂准备直播\n\n"))])}),n={name:"videoCourseCreateSuccess",data:function(){return{type:l,liveUrl:"rtmp://192.168.11.206/hls/as1s2ac"}},mounted:function(){var t=this,$route=query,console.log(t),this.type=t.type,this.streamPwd=t.streamPwd,this.liveUrl=t.liveUrl,methods:{goBack:function(){this.$router.go(-1)},goOBSDoc:function(){this.$router.push({path:"/OBSDoc"})}},c=n,o=(s("a63b"),s("2877")),r=Object(o["a"])(c,i,a,!1,null,"4e30469b",null);e["default"]=r.exports}}];
//# sourceMappingURL=videoCourseCreateSuccess.500afeb0.js.map

```

发现可能的服务器路径泄露模式 ①

TOC

问题 1 / 1

TOC

发现可能的服务器路径泄露模式

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://192.168.11.206/education/js/chunk-vendors.46d31dc3.js>

实体: chunk-vendors.46d31dc3.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", $="[\x20\t\r\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-\uffff0-9]+)?*[a-z\u00a1-\uffff0-9]+)(?:\\.([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\d/],["HH:mm:ss.SSSS",/\d--begin_highlight_ta...

...
```

参

发现电子邮件地址模式 1

TOC

发现电子邮件地址模式

严重性: 参考

CVSS 分数: 0.0

URL: <http://192.168.11.206/education/js/chunk-vendors.46d31dc3.js>

实体: chunk-vendors.46d31dc3.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:{jscs:"jscs
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{...
```

参

客户端 (JavaScript) Cookie 引用 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/education/js/chunk-vendors.46d31dc3.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"),document.cookie=s.join("; "),read:function(e){var t=document.cookie.match(new RegExp("(^|;\\s*)(\"+e+\")=([^\"]*)"));re...
...
```

修订建议

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_http_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/ngx_http_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/ngx_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

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。

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。