千锋教育
WWW.QFEDU.COM

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 9.0.3.6, 规则： 10344
扫描开始时间： 2018/10/23 15:18:46

目录

介绍

摘要

按问题类型分类的问题

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：	3
中等严重性问题：	1
低严重性问题：	23
参考严重性问题：	3
报告中包含的严重性问题总数：	30
扫描中发现的严重性问题总数：	30

常规信息

扫描文件名称：	192.168.106.134-yangge2
扫描开始时间：	2018/10/23 15:18:46
测试策略：	Default

主机	testhtml5.vulnweb.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：	
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 13

TOC

	问题类型	问题的数量
高	已解密的登录请求	1
高	跨站点脚本编制	2
中	通过框架钓鱼	1
低	SRI (Subresource Integrity) 的检查	1
低	不安全的第三方链接 (target="_blank")	3
低	检测到隐藏目录	2
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
低	自动填写未对密码字段禁用的 HTML 属性	1
低	过度许可的 CORS 访问测试	1
参	HTML 注释敏感信息泄露	2
参	应用程序错误	1

有漏洞的 URL 10

TOC

	URL	问题的数量
高	http://testhtml5.vulnweb.com/login	6
低	http://testhtml5.vulnweb.com/	6
低	http://testhtml5.vulnweb.com/logout	1
低	http://testhtml5.vulnweb.com/cgi-bin/	1
低	http://testhtml5.vulnweb.com/static/	1
低	http://testhtml5.vulnweb.com/static/app/app.js	3
低	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js	3
低	http://testhtml5.vulnweb.com/static/app/libs/sessvars.js	3
低	http://testhtml5.vulnweb.com/static/app/post.js	3

低	http://testhtml5.vulnweb.com/static/app/services/itemsService.js	3

修订建议 12

TOC

	修复任务	问题的数量
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	1
高	查看危险字符注入的可能解决方案	3
低	修改“Access-Control-Allow-Origin”头以仅获取允许的站点	1
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	2
低	将“autocomplete”属性正确设置为“off”	1
低	将属性 rel = "noopener noreferrer" 添加到带有 target="_blank" 的每个元素	3
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	将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。	1
低	除去 HTML 注释中的敏感信息	2
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	1

安全风险 8

TOC

	风险	问题的数量
高	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	1
高	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	2
中	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	20
低	在第三方服务器被破坏的情况下，站点的内容/行为将更改。	1
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	2
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
低	可能会绕开 Web 应用程序的认证机制	1
参	可能会收集敏感的调试信息	1

原因 9

TOC

	原因	问题的数量
高	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	1
高	未对用户输入正确执行危险字符清理	3
低	不支持子资源完整性。	1
低	链接元素中的 rel 属性未设置为“noopener noreferrer”。	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	2
低	Web 应用程序编程或配置不安全	17
参	程序员在 Web 页面上留下调试信息	2
参	未对入局参数值执行适当的边界检查	1
参	未执行验证以确保用户输入与预期的数据类型匹配	1

WASC 威胁分类

TOC

威胁	问题的数量
传输层保护不足	1
信息泄露	22
内容电子欺骗	1
功能滥用	3
跨站点脚本编制	2
远程文件包含	1

按问题类型分类的问题

高 已解密的登录请求 1 TOC

问题 1 / 1 TOC

已解密的登录请求	
严重性：	高
CVSS 分数：	8.5
URL：	http://testhtml5.vulnweb.com/login
实体：	password (Parameter)
风险：	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因：	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值：	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

推理： AppScan 识别了不是通过 SSL 发送的密码参数。

原始请求

```
...
POST /login HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Host: testhtml5.vulnweb.com
Content-Length: 24
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

username=admin&password=

HTTP/1.1 302 FOUND
Location: http://testhtml5.vulnweb.com/
Connection: keep-alive
Server: nginx/1.4.1
Content-Length: 209
Set-Cookie: username=admin; Path=/
Date: Mon, 22 Jun 1970 15:42:03 GMT
Content-Type: text/html; charset=utf-8

...
```

高 跨站点脚本编制 2 TOC

问题 1 / 2 TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://testhtml5.vulnweb.com/login
实体：	login (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：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应：

```
...

username=%3E%22%27%3E%3Cscript%3Ealert%28158%29%3C%2Fscript%3E&password=%3E%22%27%3E%3Cscript%3Ealert%28158%29%3C%2Fscript%3E

HTTP/1.1 302 FOUND
Location: http://testhtml5.vulnweb.com/
Connection: keep-alive
Server: nginx/1.4.1
Content-Length: 209
Set-Cookie: username=">\"'><script>alert(158)</script>"; Path=/
Date: Mon, 22 Jun 1970 16:05:41 GMT
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a href="/">/</a>.  If not click the
link.

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/login

...

...

            <p class="navbar-text pull-right">

                Welcome <b>>"'><script>alert(158)</script></b> | <a href='/logout'>Logout</a>
```

```
            </p>
        </div>
    </div>
</div>
...
```

问题 2 / 2

TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://testhtml5.vulnweb.com/login
实体：	username (Parameter)
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：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

未经处理的测试响应：

```
...

username=<script>alert(276)</script>&password=

HTTP/1.1 302 FOUND
Location: http://testhtml5.vulnweb.com/
Connection: keep-alive
Server: nginx/1.4.1
Content-Length: 209
Set-Cookie: username="<script>alert(276)</script>"; Path=/
Date: Mon, 22 Jun 1970 16:07:21 GMT
Content-Type: text/html; charset=utf-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a href="/">/</a>.  If not click the
link.

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/login

...

...

            <p class="navbar-text pull-right">

                Welcome <b><script>alert(276)</script></b> | <a href='/logout'>Logout</a>

            </p>
        </div>
    </div>
```

```
</div>
...
```

中 通过框架钓鱼 1 TOC

问题 1 / 1 TOC

通过框架钓鱼	
严重性：	中
CVSS 分数：	6.4
URL：	http://testhtml5.vulnweb.com/login
实体：	username (Parameter)
风险：	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：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

推理： 测试结果似乎指示存在脆弱性，因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

低 SRI (Subresource Integrity) 的检查 1

TOC

问题 1 / 1

TOC

SRI (Subresource Integrity) 的检查	
严重性:	低
CVSS 分数:	5.0
URL:	http://testhtml5.vulnweb.com/
实体:	(Page)
风险:	在第三方服务器被破坏的情况下，站点的内容/行为将更改。
原因:	不支持子资源完整性。
固定值:	将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。

推理: 第三方链接/脚本没有浏览器的完整性属性来确认它们未被破坏。

未经处理的测试响应:

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/logout
Host: testhtml5.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Connection: keep-alive

...
```

低 不安全的第三方链接 (target="_blank") 3

TOC

问题 1 / 3

TOC

不安全的第三方链接 (target="_blank")

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/login
实体：	login (Page)
风险：	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：	链接元素中的 rel 属性未设置为“noopener noreferrer”。
固定值：	将属性 rel = "noopener noreferrer" 添加到带有 target="_blank" 的每个元素

推理： 带有 target="_blank" 属性且不带有 rel="noopener noreferrer" 属性的第三方链接允许链接的页面部分访问链接页面窗口对象

未经处理的测试响应：

```
...

                    <li class="nav-header">Acunetix</li>
                    <li><a target="_blank" href="http://www.acunetix.com/">Website</a></li>
                    <li><a target="_blank" href="http://www.acunetix.com/blog/">Blog</a></li>
                    <li><a target="_blank" href="http://www.facebook.com/Acunetix">Facebook</a>
</li>
                    <li><a target="_blank" href="http://www.twitter.com/acunetix/">Twitter</a>
</li>
                </ul>
            </div><!--/.well -->
        </div><!--/span-->
        <div class="span10">
            <div class="row-fluid">
                <div ng-view></div>
            </div><!--/row-->
        </div><!--/span-->
    </div><!--/row-->
...
```

问题 2 / 3

TOC

不安全的第三方链接 (target="_blank")

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/logout
实体：	logout (Page)
风险：	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：	链接元素中的 rel 属性未设置为“noopener noreferrer”。
固定值：	将属性 rel = "noopener noreferrer" 添加到带有 target="_blank" 的每个元素

推理： 带有 target="_blank" 属性且不带有 rel="noopener noreferrer" 属性的第三方链接允许链接的页面部分访问链接页面窗口对象

未经处理的测试响应：

```
...
                    <li class="nav-header">Acunetix</li>
                    <li><a target="_blank" href="http://www.acunetix.com/">Website</a></li>
                    <li><a target="_blank" href="http://www.acunetix.com/blog/">Blog</a></li>
                    <li><a target="_blank" href="http://www.facebook.com/Acunetix">Facebook</a>
</li>
                    <li><a target="_blank" href="http://www.twitter.com/acunetix/">Twitter</a>
</li>
                </ul>
            </div><!--/.well -->
        </div><!--/span-->
        <div class="span10">
            <div class="row-fluid">
                <div ng-view></div>
            </div><!--/row-->
        </div><!--/span-->
    </div><!--/row-->
...
```

问题 3 / 3

TOC

不安全的第三方链接 (target="_blank")

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/
实体：	(Page)
风险：	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：	链接元素中的 rel 属性未设置为“noopener noreferrer”。
固定值：	将属性 rel = "noopener noreferrer" 添加到带有 target="_blank" 的每个元素

推理： 带有 target="_blank" 属性且不带有 rel="noopener noreferrer" 属性的第三方链接允许链接的页面部分访问链接页面窗口对象

未经处理的测试响应：

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/logout
Host: testhtml5.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Connection: keep-alive

...
```

低 检测到隐藏目录 2 TOC

问题 1 / 2 TOC

检测到隐藏目录	
严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/cgi-bin/
实体：	cgi-bin/ (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 /cgi-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/logout
Host: testhtml5.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx/1.4.1
Vary: Accept-Encoding
Content-Length: 263
Date: Mon, 22 Jun 1970 16:11:46 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
...
```

问题 2 / 2 TOC

检测到隐藏目录

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/
实体：	static/ (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 /static/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/logout
Host: testhtml5.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx/1.4.1
Content-Length: 168
Date: Mon, 22 Jun 1970 16:16:23 GMT
Content-Type: text/html

<html>
<head><title>403 Forbidden</title></head>
<body bgcolor="white">

...
```

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://testhtml5.vulnweb.com/static/app/app.js
实体：	app.js (Page)
风险：	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 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：	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 /static/app/app.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 2 / 5

TOC

缺少“Content-Security-Policy”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/post.js
实体：	post.js (Page)
风险：	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 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：	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 /static/app/post.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 3 / 5

TOC

缺少“Content-Security-Policy”头	
严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/services/itemsService.js
实体：	itemsService.js (Page)
风险：	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 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：	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 /static/app/services/itemsService.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 4 / 5

TOC

缺少“Content-Security-Policy”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/libs/sessvars.js
实体：	sessvars.js (Page)
风险：	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 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：	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 /static/app/libs/sessvars.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 5 / 5

TOC

缺少“Content-Security-Policy”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js
实体：	controllers.js (Page)
风险：	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 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：	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 /static/app/controllers/controllers.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

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://testhtml5.vulnweb.com/static/app/app.js
实体：	app.js (Page)
风险：	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 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：	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 /static/app/app.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 2 / 5

TOC

缺少“X-Content-Type-Options”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/post.js
实体：	post.js (Page)
风险：	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 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：	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 /static/app/post.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 3 / 5

TOC

缺少“X-Content-Type-Options”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/services/itemsService.js
实体：	itemsService.js (Page)
风险：	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 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：	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 /static/app/services/itemsService.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 4 / 5

TOC

缺少“X-Content-Type-Options”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/libs/sessvars.js
实体：	sessvars.js (Page)
风险：	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 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：	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 /static/app/libs/sessvars.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 5 / 5

TOC

缺少“X-Content-Type-Options”头	
严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js
实体：	controllers.js (Page)
风险：	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 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：	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 /static/app/controllers/controllers.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

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://testhtml5.vulnweb.com/static/app/app.js
实体：	app.js (Page)
风险：	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 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：	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 /static/app/app.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 2 / 5

TOC

缺少“X-XSS-Protection”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/post.js
实体：	post.js (Page)
风险：	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 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：	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 /static/app/post.js HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 3 / 5

TOC

缺少“X-XSS-Protection”头	
严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/services/itemsService.js
实体：	itemsService.js (Page)
风险：	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 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：	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 /static/app/services/itemsService.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 4 / 5

TOC

缺少“X-XSS-Protection”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/libs/sessvars.js
实体：	sessvars.js (Page)
风险：	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 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：	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 /static/app/libs/sessvars.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

问题 5 / 5

TOC

缺少“X-XSS-Protection”头

严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js
实体：	controllers.js (Page)
风险：	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 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：	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 /static/app/controllers/controllers.js HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/
Connection: keep-alive
Host: testhtml5.vulnweb.com
Accept: */*
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK

...
```

低 自动填写未对密码字段禁用的 HTML 属性 1 TOC

问题 1 / 1 TOC

自动填写未对密码字段禁用的 HTML 属性	
严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/
实体：	(Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

推理： AppScan 发现密码字段没有强制禁用自动填写功能。
未经处理的测试响应：

```
...

            <div class="control-group">
                <!-- Password-->
                <label class="control-label" for="password">Password</label>
                <div class="controls">
                    <input type="password" id="password" name="password" placeholder="" class="input-xlarge">
                </div>
            </div>
...
```

低 过度许可的 CORS 访问测试 1 TOC

问题 1 / 1 TOC

过度许可的 CORS 访问测试	
严重性：	低
CVSS 分数：	5.0
URL：	http://testhtml5.vulnweb.com/
实体：	(Page)
风险：	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 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：	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

推理： AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

未经处理的测试响应：

```
...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://testhtml5.vulnweb.com/logout
Host: testhtml5.vulnweb.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Connection: keep-alive

...
```

参 HTML 注释敏感信息泄露 2 TOC

问题 1 / 2 TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://testhtml5.vulnweb.com/
实体：	Username (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...

<!-- Modal -->
<div id="myModal" class="modal hide fade" tabindex="-1" role="dialog" aria-
labelledby="myModalLabel" aria-hidden="true">
    <form class="modal-body" action="/login" method="POST" id="loginForm">
    <div class="modal-header">
        <button type="button" class="close" data-dismiss="modal" aria-hidden="true">×</button>
        <h3 id="myModalLabel">Login</h3>
    </div>
    <div class="modal-body">
            <div class="control-group">
                <!-- Username -->
                <label class="control-label"  for="username">Username</label>
                <div class="controls">
                    <input type="text" id="username" name="username" placeholder="" class="input-
xlarge" value="admin">
                </div>
            </div>
...
```

问题 2 / 2 TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://testhtml5.vulnweb.com/
实体：	Password (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：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

原始响应

```
...

            <div class="control-group">
                <!-- Password-->
                <label class="control-label" for="password">Password</label>
                <div class="controls">
                    <input type="password" id="password" name="password" placeholder=""
class="input-xlarge">
                </div>
            </div>
...
```

参 应用程序错误 1

TOC

问题 1 / 1

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://testhtml5.vulnweb.com/login
实体：	username (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

Referer: http://testhtml5.vulnweb.com/
Host: testhtml5.vulnweb.com
Content-Length: 22
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

username=%00&password=

HTTP/1.1 502 Bad Gateway
Connection: keep-alive
Server: nginx/1.4.1
Content-Length: 172
Date: Mon, 22 Jun 1970 16:07:02 GMT
Content-Type: text/html

<html>
<head><title>502 Bad Gateway</title></head>
<body bgcolor="white">

...
```