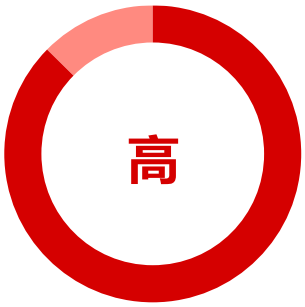
三零卫士

# 综合报告




## Acunetix 威胁等级 3

扫描程序发现了一个或多个高危类型漏洞。恶意用户可以利用这些漏洞并破坏后端数据库和/或损坏您的网站。

## 扫描详情

| | |
|---|---|
| 目标 | http://10.101.59.207:8070/jointframe/login |
| 扫描类型 | Full Scan |
| 开始时间 | Jul 7, 2023, 1:54:52 PM GMT+8 |
| 扫描持续时间 | 32 minutes |
| 请求 | 49155 |
| 平均响应时间 | 1ms |
| 最大响应时间 | 3021ms |


高

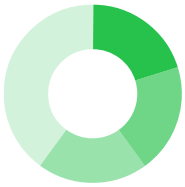

中


低


信息性

| 严重性 | 漏洞 | 实例 |
|---|---|---|
| 高 | 1 | 1 |
| 中 | 2 | 2 |
| 低 | 1 | 1 |
| 信息性 | 4 | 5 |
| 总计 | 8 | 9 |

## 信息性



| | 实例 |
|---|---|
| Subresource Integrity (SRI) 未实施 | 1 |
| 未实施内容安全策略 (CSP) | 1 |
| 无 HTTP 重定向 | 1 |
| Others | 2 |

## 低危

| | 实例 |
|---|---|
| 点击劫持：X-Frame-Options 报头缺失 | 1 |

## 中危

| | 实例 |
|---|---|
| 未加密的连接 | 1 |
| 应用程序错误消息 | 1 |

## 高危

| | 实例 |
|---|---|
| web.xml 配置文件披露 | 1 |

# 影响

| 严重性 | 影响 | |
|---|---|---|
| 高 | 1 | **web.xml 配置文件披露** |
| 中 | 1 | **未加密的连接** |
| 中 | 1 | **应用程序错误消息** |
| 低 | 1 | **点击劫持：X-Frame-Options 报头缺失** |
| 信息性 | 1 | **未实施内容安全策略 (CSP)** |
| 信息性 | 1 | **无 HTTP 重定向** |
| 信息性 | 2 | **已过时的 JavaScript 库** |
| 信息性 | 1 | **Subresource Integrity (SRI) 未实施** |

# web.xml 配置文件披露

**WEB-INF/web.xml** 部署描述符文件描述如何在 servlet 容器（如 Tomcat）中部署 Web 应用程序。通常，此文件应不可访问。但是，Acunetix WS 能够使用各种编码和目录穿越变体来读取此文件的内容。

## 影响

配置文件会泄露敏感信息，这些信息将帮助恶意用户准备更高级的攻击。

---

## http://10.101.59.207:8070/jointframe/web/WEB-INF/web.xml

找到模式：

```
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://xmlns.jcp.org/xml/ns/javaee"
xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee/web-app_2_5.xsd"
id="scplatform" version="2.5">
<display-name>/</display-name>

<welcome-file-list>
<welcome-file>index.html</welcome-file>
</welcome-file-list>

<!-- 400 é□□è¯¯é¡µé□¢é□□ç½® -->
<error-page>
<error-code>400</error-code>
<location>/index.html</location>
</error-page>
<!-- 404 é¡µé□¢ä¸□å□å□¨é□□ç½® -->
<error-page>
<error-code>404</error-code>
<location>/index.html</location>
</error-page>
</web-app>
```

### 请求

```
GET /jointframe/web/./WEB-INF/web.xml HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
```

```
Connection: Keep-alive
```

### 推荐

限制对此文件的访问。

# 未加密的连接

此扫描目标通过未加密的连接进行连接。潜在攻击者可以拦截并修改往返此站点的数据。

### 影响

可能出现信息披露。

---

**http://10.101.59.207:8070/** 已验证

### 请求

```
GET /jointframe/login HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/login
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

### 推荐

此站点应通过安全的 (HTTPS) 连接发送和接收数据。

# 应用程序错误消息

此警报需要手动确认

Acunetix 发现了一个或多个错误/警告消息。应用程序错误或警告消息可能会将有关应用程序内部工作的敏感信息泄露给攻击者。

这些消息还可能包含产生了未处理异常的文件的位置。
请查阅“攻击详情”部分，以获取有关受影响页面的更多信息。

## 影响

错误消息可能会泄露可用于实施进一步攻击的敏感信息。

---

### http://10.101.59.207:8070/

应用程序错误消息：

- http://10.101.59.207:8070/jointframe/web/cdn/log.json
  **org.apache.coyote.http11.Http11InputBuffer.parseRequestLine(Http11InputBuffer.java:494)**
  **org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:271)**
  **org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63)**
  **org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:926)**
  **org.apache.tomcat.util.net.Nio2Endpoint$SocketProcessor.doRun(Nio2Endpoint.java:1710)**
  **org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)**
  **org.apache.tomcat.util.net.AbstractEndpoint.processSocket(AbstractEndpoint.java:1265)**
  **org.apache.tomcat.util.net.Nio2Endpoint$Nio2SocketWrapper$2.completed(Nio2Endpoint.java:641)**
  **org.apache.tomcat.util.net.Nio2Endpoint$Nio2SocketWrapper$2.completed(Nio2Endpoint.java:619)**
  **sun.nio.ch.Invoker.invokeUnchecked(Invoker.java:126)**
  **sun.nio.ch.UnixAsynchronousSocketChannelImpl.finishRead(UnixAsynchronousSocketChannelImpl.java:430)**
  **sun.nio.ch.UnixAsynchronousSocketChannelImpl.finish(UnixAsynchronousSocketChannelImpl.java:191)**
  **sun.nio.ch.UnixAsynchronousSocketChannelImpl.onEvent(UnixAsynchronousSocketChannelImpl.java:213)**
  **sun.nio.ch.EPollPort$EventHandlerTask.run(EPollPort.java:293)**
  **sun.nio.ch.AsynchronousChannelGroupImpl$1.run(AsynchronousChannelGroupImpl.java:112)**
  **java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)**
  **java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)**
  **java.lang.Thread.run(Thread.java:748)**

- http://10.101.59.207:8070/
  **org.apache.coyote.http11.Http11InputBuffer.parseRequestLine(Http11InputBuffer.java:502)**
  **org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:271)**
  **org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63)**
  **org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:926)**
  **org.apache.tomcat.util.net.Nio2Endpoint$SocketProcessor.doRun(Nio2Endpoint.java:1710)**
  **org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)**
  **org.apache.tomcat.util.net.AbstractEndpoint.processSocket(AbstractEndpoint.java:1265)**
  **org.apache.tomcat.util.net.Nio2Endpoint$Nio2SocketWrapper$2.completed(Nio2Endpoint.java:641)**
  **org.apache.tomcat.util.net.Nio2Endpoint$Nio2SocketWrapper$2.completed(Nio2Endpoint.java:619)**
  **sun.nio.ch.Invoker.invokeUnchecked(Invoker.java:126)**
  **sun.nio.ch.UnixAsynchronousSocketChannelImpl.finishRead(UnixAsynchronousSocketChannelImpl.java:430)**
  **sun.nio.ch.UnixAsynchronousSocketChannelImpl.finish(UnixAsynchronousSocketChannelImpl.java:191)**
  **sun.nio.ch.UnixAsynchronousSocketChannelImpl.onEvent(UnixAsynchronousSocketChannelImpl.java:213)**
  **sun.nio.ch.EPollPort$EventHandlerTask.run(EPollPort.java:293)**
  **sun.nio.ch.AsynchronousChannelGroupImpl$1.run(AsynchronousChannelGroupImpl.java:112)**

java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
java.lang.Thread.run(Thread.java:748)

- http://10.101.59.207:8070/
  org.apache.coyote.http11.Http11InputBuffer.parseRequestLine(Http11InputBuffer.java:502)
  org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:271)
  org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63)
  org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:926)
  org.apache.tomcat.util.net.Nio2Endpoint$SocketProcessor.doRun(Nio2Endpoint.java:1710)
  org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
  org.apache.tomcat.util.net.AbstractEndpoint.processSocket(AbstractEndpoint.java:1265)
  org.apache.tomcat.util.net.Nio2Endpoint$Nio2SocketWrapper$2.completed(Nio2Endpoint.java:641)
  org.apache.tomcat.util.net.Nio2Endpoint$Nio2SocketWrapper$2.completed(Nio2Endpoint.java:619)
  sun.nio.ch.Invoker.invokeUnchecked(Invoker.java:126) sun.nio.ch.Invoker$2.run(Invoker.java:218)
  sun.nio.ch.AsynchronousChannelGroupImpl$1.run(AsynchronousChannelGroupImpl.java:112)
  java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
  java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
  java.lang.Thread.run(Thread.java:748)

- http://10.101.59.207:8070/
  org.apache.coyote.http11.Http11InputBuffer.parseRequestLine(Http11InputBuffer.java:502)
  org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:271)
  org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63)
  org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:926)
  org.apache.tomcat.util.net.Nio2Endpoint$SocketProcessor.doRun(Nio2Endpoint.java:1710)
  org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
  org.apache.tomcat.util.net.AbstractEndpoint.processSocket(AbstractEndpoint.java:1265)
  org.apache.tomcat.util.net.Nio2Endpoint.setSocketOptions(Nio2Endpoint.java:339)
  org.apache.tomcat.util.net.Nio2Endpoint$Nio2Acceptor.completed(Nio2Endpoint.java:479)
  org.apache.tomcat.util.net.Nio2Endpoint$Nio2Acceptor.completed(Nio2Endpoint.java:415)
  sun.nio.ch.Invoker.invokeUnchecked(Invoker.java:126) sun.nio.ch.Invoker.invokeDirect(Invoker.java:157)
  sun.nio.ch.Invoker.invoke(Invoker.java:185)
  sun.nio.ch.UnixAsynchronousServerSocketChannelImpl.onEvent(UnixAsynchronousServerSocketChannelImpl
  .java:193) sun.nio.ch.EPollPort$EventHandlerTask.run(EPollPort.java:293)
  sun.nio.ch.AsynchronousChannelGroupImpl$1.run(AsynchronousChannelGroupImpl.java:112)
  java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
  java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
  java.lang.Thread.run(Thread.java:748)

- http://10.101.59.207:8070/
  org.apache.coyote.http11.Http11InputBuffer.parseRequestLine(Http11InputBuffer.java:502)
  org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:271)
  org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63)
  org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:926)
  org.apache.tomcat.util.net.Nio2Endpoint$SocketProcessor.doRun(Nio2Endpoint.java:1710)
  org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)

org.apache.tomcat.util.net.AbstractEndpoint.processSocket(AbstractEndpoint.java:1265)
org.apache.tomcat.util.net.Nio2Endpoint.setSocketOptions(Nio2Endpoint.java:339)
org.apache.tomcat.util.net.Nio2Endpoint$Nio2Acceptor.completed(Nio2Endpoint.java:479)
org.apache.tomcat.util.net.Nio2Endpoint$Nio2Acceptor.completed(Nio2Endpoint.java:415)
sun.nio.ch.Invoker.invokeUnchecked(Invoker.java:126) sun.nio.ch.Invoker$2.run(Invoker.java:218)
sun.nio.ch.AsynchronousChannelGroupImpl$1.run(AsynchronousChannelGroupImpl.java:112)
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
java.lang.Thread.run(Thread.java:748)

### 请求

```
GET /jointframe/web/cdn/log.json?_t=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27' HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/login
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

## 推荐

验证这些页面是否披露错误或警告消息，并适当配置应用程序以将错误记录到文件，而不是将错误显示给用户。

## 描述

尽管信息披露漏洞不能被攻击者直接利用，但它们可以帮助攻击者了解特定于系统的信息。以下是攻击者可能从应用程序错误披露获取的**部分**信息列表。

内部 IP 地址
机密（密码、密钥、令牌...）
操作系统版本
软件版本号
缺失的安全补丁
应用程序堆栈跟踪
SQL 语句
敏感文件（备份、临时文件...）的位置
敏感资源（数据库、缓存、代码存储库...）的位置

## 参考

PHP Runtime Configuration
https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors

Improper Error Handling

https://www.owasp.org/index.php/Improper_Error_Handling

# 点击劫持：X-Frame-Options 报头缺失

点击劫持（用户界面矫正攻击、UI 矫正攻击、UI 矫正）是一种恶意技术，诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制 。

服务器未返回 X-Frame-Options **报头，这意味着此网站存在遭受点击劫持攻击的风险。X-Frame-Options HTTP 响应报头可被用于指示是否应允许浏览器在框架或 iframe 内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。**

## 影响

影响取决于受影响的 Web 应用程序。

---

### http://10.101.59.207:8070/

不包含 XFO 报头的路径：

- http://10.101.59.207:8070/jointframe/login
- http://10.101.59.207:8070/jointframe/
- http://10.101.59.207:8070/jointframe/web/
- http://10.101.59.207:8070/jointframe/appmain/
- http://10.101.59.207:8070/jointframe/static/fonts/
- http://10.101.59.207:8070/jointframe/static/
- http://10.101.59.207:8070/jointframe/static/img/
- http://10.101.59.207:8070/
- http://10.101.59.207:8070/jointframe/static/css/
- http://10.101.59.207:8070/jointframe/web/WEB-INF/
- http://10.101.59.207:8070/jointframe/web/fonts/
- http://10.101.59.207:8070/jointframe/web/img/

- http://10.101.59.207:8070/jointframe/static/js/
- http://10.101.59.207:8070/jointframe/web/cdn/
- http://10.101.59.207:8070/jointframe/web/js/
- http://10.101.59.207:8070/jointframe/web/css/

### 请求

```
GET /jointframe/login HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/login
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

### 推荐

配置您的 Web 服务器，使其包含 X-Frame-Options 报头和带有 frame-ancestors 指令的 CSP 报头。有关该报头可能值的更多信息，请查阅 Web 参考资料。

### 参考

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking
https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

# 未实施内容安全策略 (CSP)

内容安全策略 (CSP) 增加了额外的安全层，有助于检测和缓解某些类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击。

内容安全策略 (CSP) 可通过添加 **Content-Security-Policy** 报头实施。此报头的值是一个字符串，其中包含描述内容安全策略的策略指令。要实施 CSP，您应该为站点使用的所有资源类型定义允许的来源列表。例如，如果您有一个简单的站点，需要从 CDN 加载本地托管和 jQuery 库中的脚本、样式表和图像，则 CSP 报头可能如下所示：

```
Content-Security-Policy: default-src 'self'; script-src 'self'
https://code.jquery.com;
```

检测到您的 Web 应用程序未实施内容安全策略 (CSP)，因为响应中缺少 CSP 报头。建议在您的 Web 应用程序中实施内容安全策略 (CSP)。

## 影响

CSP 可用于预防和/或缓解涉及内容/代码注入的攻击，例如跨站脚本/XSS 攻击、需要嵌入恶意资源的攻击、涉及恶意使用 iframe 的攻击（例如点击劫持攻击）等。

---

## http://10.101.59.207:8070/

不包含 CSP 报头的路径：

- http://10.101.59.207:8070/jointframe/login
- http://10.101.59.207:8070/jointframe/
- http://10.101.59.207:8070/jointframe/web/
- http://10.101.59.207:8070/jointframe/appmain/
- http://10.101.59.207:8070/jointframe/static/fonts/
- http://10.101.59.207:8070/jointframe/static/
- http://10.101.59.207:8070/jointframe/static/img/
- http://10.101.59.207:8070/
- http://10.101.59.207:8070/jointframe/static/css/
- http://10.101.59.207:8070/jointframe/web/WEB-INF/
- http://10.101.59.207:8070/jointframe/web/fonts/
- http://10.101.59.207:8070/jointframe/web/img/
- http://10.101.59.207:8070/jointframe/static/js/

- http://10.101.59.207:8070/jointframe/web/cdn/
- http://10.101.59.207:8070/jointframe/web/js/
- http://10.101.59.207:8070/jointframe/web/css/

### 请求

```
GET /jointframe/login HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/login
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

## 推荐

建议在您的 Web 应用程序中实施内容安全策略 (CSP)。配置内容安全策略涉及添加 **Content-Security-Policy** HTTP 报头到 Web 页面并为其赋值，以控制允许用户代理为该页面加载的资源。

## 参考

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

# 无 HTTP 重定向

检测到您的 Web 应用程序使用 HTTP 协议，但未自动将用户重定向到 HTTPS。

## 影响

在某些情况下，其可用于中间人 (MitM) 攻击

---

**http://10.101.59.207:8070/**

### 请求

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

### 推荐

建议在您的 Web 应用程序中实施 HTTP 重定向最佳实践。请查询网络参考文件以了解更多信息

### 参考

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

# 已过时的 JavaScript 库

您使用的是已过时的一个或多个 JavaScript 库版本。有最新版本可用。虽然未发现您的版本受任何安全漏洞影响，但仍建议将库更新到最新版本。

### 影响

更多信息，请查阅参考资料。

---

**http://10.101.59.207:8070/** 信心: 95%

- **jQuery Validation 1.15.0**
  - URL：http://10.101.59.207:8070/jointframe/appmain/jquery.validate.js
  - 检测方法：The library's name and version were determined based on the file's contents.
  - 参考文献：
    - https://github.com/jquery-validation/jquery-validation/tags

### 请求

```
GET /jointframe/appmain/jquery.validate.js HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
```

```
Host: 10.101.59.207:8070
Connection: Keep-alive
```

---

### http://10.101.59.207:8070/ 信心: 95%

- **Vue.js 2.6.12**
  - URL：http://10.101.59.207:8070/jointframe/static/js/chunk-vendors.6f6739a1.js
  - 检测方法：The library's name and version were determined based on the file's contents.
  - 参考文献：
    - https://github.com/vuejs/vue/releases

#### 请求

```
GET /jointframe/static/js/chunk-vendors.6f6739a1.js HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

#### 推荐

升级至最新版本。

## Subresource Integrity (SRI) 未实施

Subresource Integrity (SRI) 是一个安全功能，使浏览器可以验证是否已交付获取的第三方资源（例如，从 CDN 中获取）且没有意外的操作。它允许开发人员提供获取的文件必须匹配的加密哈希。

可以对第三方资源（如脚本和样式表）进行操作。访问或攻击主机 CDN 的攻击者可以操作或替换文件。SRI 允许开发人员对要加载的资源指定 base64-encoded 加密哈希。然后，会将包含哈希的 integrity 属性添加至 <script> HTML 元素标签。integrity 字符串包含 base64-encoded 哈希，后面的后缀取决于哈希算法。此后缀可能是 sha256、sha384 或 sha512。

从“详细信息”部分中指定的外部 URL 加载的脚本未实施 Subresource Integrity (SRI)。建议为从外部主机加载的所有脚本实施 Subresource Integrity (SRI)。

### 影响

具有访问权限或已入侵托管 CDN 的攻击者可以操纵或替换文件。

## http://10.101.59.207:8070/jointframe/

未实施 SRI 的页面：

- http://10.101.59.207:8070/jointframe/
  脚本 SRC：**http://1.1.1.2:89/cookie/flash.js**

### 请求

```
GET /jointframe/ HTTP/1.1
Referer: http://10.101.59.207:8070/jointframe/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4512.0 Safari/537.36
Host: 10.101.59.207:8070
Connection: Keep-alive
```

## 推荐

使用 SRI Hash Generator 链接（从参考文献部分）以生成 <script> 元素，该元素实施 Subresource Integrity (SRI)。

例如，您可以使用以下 <script> 元素来告知浏览器，在执行 https://example.com/example-framework.js 脚本前，浏览器必须先将脚本与期望哈希进行比较，并验证两者之间存在匹配。

```
<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

## 参考

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

# 网站结构

- http://10.101.59.207:8070
  - jointframe
    - appmain
      - appcore.js
      - jquery-migrate.js
      - jquery.js
      - jquery.metadata.js
      - jquery.notify.js
      - jquery.qtip.js
      - jquery.ui.js
      - jquery.validate.js
      - jsloader.js
    - static
      - css
        - app.29c5b1d7.css
        - chunk-0c1798a4.cc286625.css
        - chunk-21c08efc.85d8c4f8.css
        - chunk-409de44a.e23895ba.css
        - chunk-a42a9526.cf5b5965.css
        - chunk-d909c2c8.f3ad5f77.css
        - chunk-vendors.463d3173.css
      - fonts
      - img
      - js
        - app.dbc6c573.js
        - chunk-0c1798a4.97f1fbbf.js
        - chunk-21c08efc.6c58b167.js
        - chunk-2d0cc5e5.55067036.js
        - chunk-2d0e95df.bf07591b.js
        - chunk-2d225a07.754b8e7c.js
        - chunk-409de44a.09d6f698.js

- chunk-a42a9526.79ee72d9.js
- chunk-d909c2c8.a6291d05.js
- chunk-vendors.6f6739a1.js
- web
  - #fragments
    - /
    - /auto-monitor/data-monitor-part
    - /common-iframe
    - /data-mark
    - /electro-sys/base
  - cdn
    - ctc.css
    - log.json
      - Inputs
        - GET _t
    - xlsx.full.min.js
  - css
    - app.1e028156.css
    - chunk-0c87c79f.4957c2fc.css
    - chunk-0ca6d247.27bec6af.css
    - chunk-0e54f612.680c3ed9.css
    - chunk-0ebe6f49.51668101.css
    - chunk-119ec906.687408d4.css
    - chunk-142a2a2a.1520d336.css
    - chunk-1af3ba1f.3f19076e.css
    - chunk-1b8e9a2a.c509c7ec.css
    - chunk-2bf3b704.84e39023.css
    - chunk-2f16563b.b4c615ce.css
    - chunk-32ca071e.c73a9487.css
    - chunk-40d7181b.4d05a7a7.css
    - chunk-41eec72e.1e2cc737.css
    - chunk-43fa51e2.305353b7.css
    - chunk-455cc484.680c3ed9.css

chunk-4950af26.2433024c.css
chunk-4da6b414.946d745c.css
chunk-570360fa.f3354957.css
chunk-611f22f9.f3354957.css
chunk-66948282.4178a5bd.css
chunk-66e06bb0.92485a1e.css
chunk-798e4358.0161de4d.css
chunk-7a8a9a88.ee90d7cb.css
chunk-7edc7add.4025f61a.css
chunk-a77c2d46.ee90d7cb.css
chunk-b28f5dba.d66361be.css
chunk-be549874.bf309466.css
chunk-c2a45496.935316ee.css
chunk-df028686.47cf110e.css
chunk-e7de4770.3facd174.css
chunk-f73151ac.bd77b1f8.css
chunk-fe02c1e0.3730ef4c.css
chunk-vendors.6343d127.css
CommonIframe.5f9e2cd1.css
dataMarkRoute.19081dad.css
dataMonitorCarbonRoute.c1621c8c.css
dataMonitorRoute.d95598af.css
emissionStandard.26d19242.css
gisRoute.984d5ec2.css
gkMonitorRoute.6077972d.css
radixListRoute.39698747.css
sysManageRoute.32436332.css
fonts
img
js
app.659c5bca.js
chunk-02b64e91.1599aeb5.js
chunk-0b640e8f.9cc4ba6b.js

chunk-0c87c79f.4e116899.js
chunk-0ca6d247.a0eb5eb8.js
chunk-0e54f612.def05fd6.js
chunk-0ebe6f49.bb3393ee.js
chunk-119ec906.affea1b0.js
chunk-142a2a2a.e538b506.js
chunk-16f4e816.e3d85e18.js
chunk-1af3ba1f.7638656e.js
chunk-1b8e9a2a.886d15e2.js
chunk-22576578.9bedad1e.js
chunk-2bf3b704.250977cb.js
chunk-2d2107f0.6447fce8.js
chunk-2f16563b.b0717c36.js
chunk-32be34e0.02fd8a2c.js
chunk-32ca071e.89e5fa55.js
chunk-40d7181b.d1caee79.js
chunk-41eec72e.ed13a0ad.js
chunk-43fa51e2.19f37abe.js
chunk-455cc484.50d12dc7.js
chunk-4950af26.5a78f1ea.js
chunk-4da6b414.03ccac7d.js
chunk-570360fa.40513d65.js
chunk-611f22f9.af4c7d7d.js
chunk-66948282.d229d4c2.js
chunk-66e06bb0.acb3b486.js
chunk-798e4358.4f196e12.js
chunk-7a8a9a88.b30e34da.js
chunk-7edc7add.b32ac48a.js
chunk-a77c2d46.e603e089.js
chunk-b28f5dba.c73fe146.js
chunk-be549874.e2d1738b.js
chunk-c2a45496.bd284408.js
chunk-df028686.cb42ba36.js

- chunk-e7de4770.c111206b.js
- chunk-f73151ac.02d982c7.js
- chunk-fe02c1e0.9b40bf16.js
- chunk-vendors.ff6ccc60.js
- CommonIframe.9853540d.js
- dataMarkRoute.d502fdda.js
- dataMonitorCarbonRoute.067f186e.js
- dataMonitorRoute.4fe24247.js
- deviceStatsRoute.ce85d3be.js
- emissionStandard.fd124e3a.js
- gisRoute.383d12cc.js
- gkMonitorRoute.09db5925.js
- radixListRoute.7ee06b0e.js
- stander-mod-record.bceb891d.js
- sysManageRoute.52495563.js
- WEB-INF
  - web.xml
- config.env.js
- ctcConfig.js
- login