

深信服成都安全运营中心

综合评估报告



**深信服科技股份有限公司**

**2024年09月**

* 文档说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文档名称 | 深信服成都安全运营中心综合评估报告 | | | |
| 文档管理编号 | SFSS-VS-R0101 | | | |
| 保密级别 | 商业秘密 | 文档版本号 | | V1.0 |
| 制作人 | 深信服安全服务团队 | 制作日期 | | 2024-09-24 |
| 复审人 | 深信服安全服务团队 | 复审日期 | | 2024-09-24 |
| 扩散范围 | 限“深信服科技股份有限公司项目组”、深信服成都安全运营中心 | | | |
| 分发控制 | 深信服：创建、修改、读取 | | 深信服成都安全运营中心项目组：读取 | |

* 适用范围

本次漏洞扫描是由深信服成都安全运营中心授权，由深信服科技股份有限公司（以下简称“深信服”）对深信服成都安全运营中心授权资产进行的漏洞扫描评估，根据评估结果所提交的技术报告，用于对评估范围内资产的安全状况做出安全评估和加固建议，仅限于“深信服”、深信服成都安全运营中心内部人员传阅。

本报告结论的有效性建立在被评估单位提供相关证据的真实性基础之上。本报告中给出的评估结论仅对被评估的资产当时的安全状态有效，当资产发生涉及到的系统构成组件（或子系统）变更时本报告不再适用。

* 版本变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| 修改日期 | 版本 | 说明 | 修改人 |
| 2024-09-24 | V1.0 | 创建文档 |  |
|  |  |  |  |

* 版本声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属深信服所有，受到有关产权及版权法保护。任何个人、机构未经深信服的书面授权许可，不得以任何方式复制或引用本文的任何片段。

目录

[1 漏洞综述 1](#_Toc82094111)

[1.1 漏洞风险等级分布 1](#_Toc82094112)

[1.2 资产风险等级分布 2](#_Toc82094113)

[1.3 漏洞威胁分布 2](#_Toc82094114)

[1.4 急需修复漏洞 3](#_Toc82094115)

[2 资产风险概览 3](#_Toc82094116)

[3 漏洞列表概览 3](#_Toc82094117)

[4 资产风险详情 4](#_Toc82094118)

[4.1 高危风险资产详情 4](#_Toc82094119)

[4.2 中危风险资产详情 5](#_Toc82094120)

[4.3 低危风险资产详情 6](#_Toc82094121)

[4.4 信息风险资产详情 7](#_Toc82094122)

[5 主机服务探测 8](#_Toc82094123)

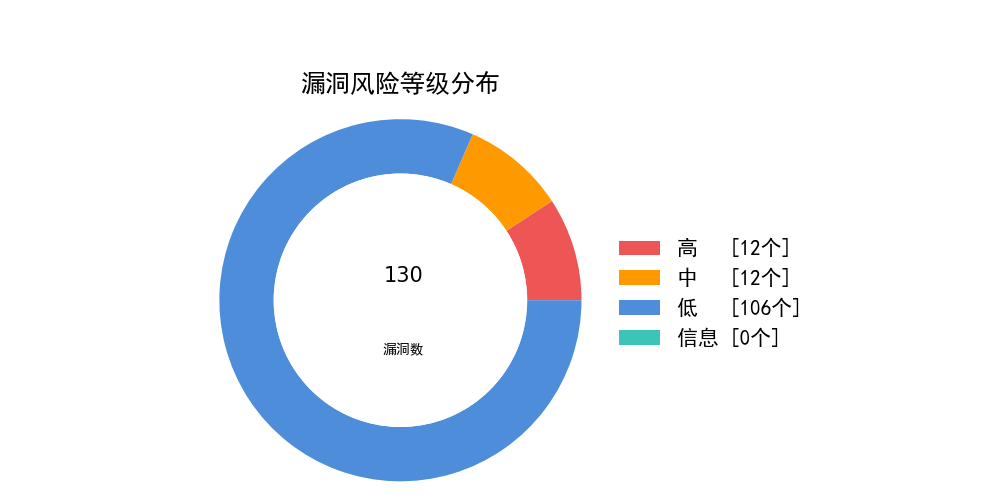
[6 参考标准 9](#_Toc82094124)

[7 了解更多 10](#_Toc82094125)

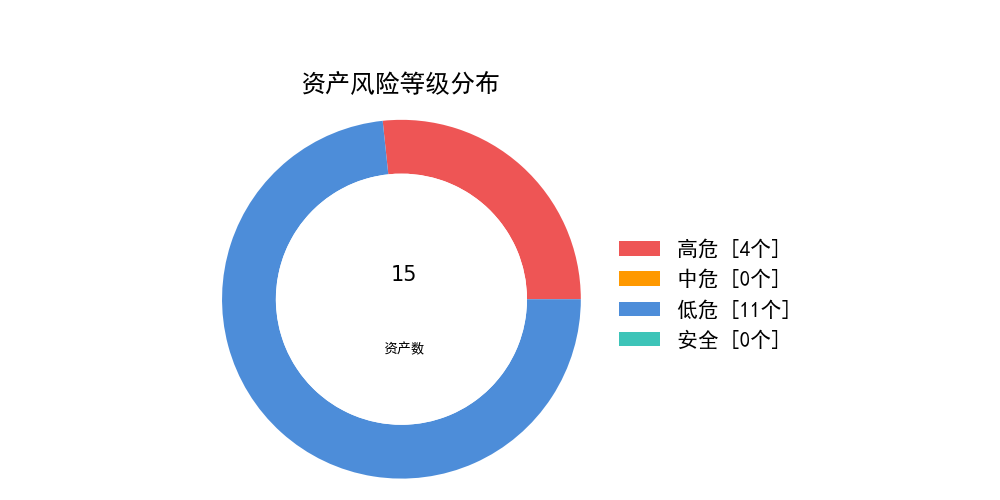
# 漏洞综述

本次评估资产30个，其中存活资产15个。共发现高危漏洞12个，中危漏洞12个，低危漏洞106个，其中高危资产4个，建议优先修复危害高的漏洞。

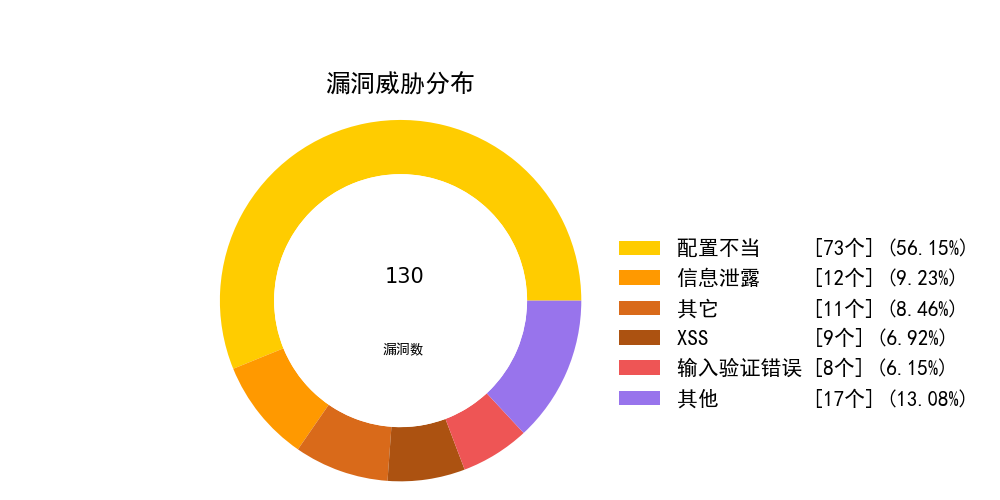
## 漏洞风险等级分布



## 资产风险等级分布



## 漏洞威胁分布



# 资产风险概览

本次评估服务，我们对您的信息资产进行了全面的评估扫描，发现风险的资产如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | IP/URL | 高 | 中 | 低 | 信息 | 总计 | 资产风险等级 |
| 1 | https://dxclouds.yangzhouyiyuan.com:8091 | 5 | 6 | 5 | 0 | 16 | 高危 |
| 2 | https://dxclouds.yangzhouyiyuan.com:8083 | 5 | 6 | 2 | 0 | 13 | 高危 |
| 3 | https://meal.yangzhouyiyuan.com | 1 | 0 | 8 | 0 | 9 | 高危 |
| 4 | https://dxclouds.yangzhouyiyuan.com:8999 | 1 | 0 | 5 | 0 | 6 | 高危 |
| 5 | https://dxclouds.yangzhouyiyuan.com:8010 | 0 | 0 | 10 | 0 | 10 | 低危 |
| 6 | http://dxclouds.yangzhouyiyuan.com:27003 | 0 | 0 | 10 | 0 | 10 | 低危 |
| 7 | https://dxclouds.yangzhouyiyuan.com:81/ | 0 | 0 | 9 | 0 | 9 | 低危 |
| 8 | https://dxclouds.yangzhouyiyuan.com:10130 | 0 | 0 | 9 | 0 | 9 | 低危 |
| 9 | https://dxclouds.yangzhouyiyuan.com:8090 | 0 | 0 | 8 | 0 | 8 | 低危 |
| 10 | https://dxclouds.yangzhouyiyuan.com:5003 | 0 | 0 | 8 | 0 | 8 | 低危 |
| 11 | https://dxclouds.yangzhouyiyuan.com:5000 | 0 | 0 | 8 | 0 | 8 | 低危 |
| 12 | https://dxclouds.yangzhouyiyuan.com:18090 | 0 | 0 | 8 | 0 | 8 | 低危 |
| 13 | http://dxclouds.yangzhouyiyuan.com:27002 | 0 | 0 | 8 | 0 | 8 | 低危 |
| 14 | https://dxclouds.yangzhouyiyuan.com:1443/ | 0 | 0 | 5 | 0 | 5 | 低危 |
| 15 | https://dxclouds.yangzhouyiyuan.com:8088 | 0 | 0 | 3 | 0 | 3 | 低危 |

# 漏洞列表概览

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **漏洞名称** | **漏洞等级** | **出现次数** |
| 1 | Apache Tomcat 拒绝服务漏洞(CVE-2022-29885) | 高 | 2 |
| 2 | Apache Tomcat 注入漏洞(CVE-2022-45143) | 高 | 2 |
| 3 | Apache Tomcat 信息泄露漏洞 (CVE-2023-28708) | 高 | 2 |
| 4 | Apache Tomcat 拒绝服务漏洞(CVE-2023-24998) | 高 | 2 |
| 5 | Apache Tomcat 输入验证错误漏洞(CVE-2023-46589) | 高 | 2 |
| 6 | CORS(跨站资源共享)原始验证失败 | 高 | 1 |
| 7 | SSL/TLS协议信息泄露漏洞(CVE-2016-2183) | 高 | 1 |
| 8 | Apache Tomcat 跨站脚本漏洞(CVE-2022-34305) | 中 | 2 |
| 9 | Apache Tomcat 安全漏洞(CVE-2023-42795) | 中 | 2 |
| 10 | Apache Tomcat 输入验证错误漏洞(CVE-2023-41080) | 中 | 2 |
| 11 | Apache Tomcat 输入验证错误漏洞(CVE-2023-45648) | 中 | 2 |
| 12 | Apache Tomcat 输入验证错误漏洞(CVE-2024-24549) | 中 | 2 |
| 13 | Apache Tomcat 安全漏洞(CVE-2024-23672) | 中 | 2 |
| 14 | 未设置Content-Security-Policy响应头 | 低 | 13 |
| 15 | 未设置Referrer-Policy响应头 | 低 | 13 |
| 16 | 未设置Strict-Transport-Security响应头 | 低 | 12 |
| 17 | 未设置X-Download-Options响应头 | 低 | 12 |
| 18 | 未设置X-Permitted-Cross-Domain-Policies响应头 | 低 | 12 |
| 19 | 未设置X-Content-Type-Options响应头 | 低 | 10 |
| 20 | 未设置X-XSS-Protection响应头 | 低 | 9 |
| 21 | 点击劫持:无X-Frame-Options头信息 | 低 | 8 |
| 22 | general 未设置cookie的Secure标志位 | 低 | 7 |
| 23 | cookie 没有设置httponly标志位 | 低 | 5 |
| 24 | Apache Tomcat 竞争条件问题漏洞(CVE-2021-43980) | 低 | 2 |
| 25 | Apache Tomcat HTTP请求走私漏洞(CVE-2022-42252) | 低 | 2 |
| 26 | OPTIONS方法启用 | 低 | 1 |

# 资产风险详情

## 高危风险资产详情

### 资产: https://dxclouds.yangzhouyiyuan.com:8083

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 拒绝服务漏洞(CVE-2022-29885)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-29885 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | Apache Tomcat 存在拒绝服务漏洞，该漏洞是由于Tomcat开启集群配置中存在缺陷，攻击者可利用该漏洞在未权限的情况下，构造恶意数据造成拒绝服务，最终导致目标服务器拒绝服务。 | |
| 风险影响： | 未配置 EncryptInterceptor 则全版本受影响,配置 EncryptInterceptor 如下版本受影响：,10.1.0-M1 ≤ Apache Tomcat ≤ 10.1.0-M14,10.0.0-M1 ≤ Apache Tomcat ≤ 10.0.20,9.0.13 ≤ Apache Tomcat ≤ 9.0.62,8.5.38 ≤ Apache Tomcat ≤ 8.5.78 | |
| 解决方案： | 当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：https://tomcat.apache.org/security-10.html、https://tomcat.apache.org/security-9.html、https://tomcat.apache.org/security-8.html | |
| 参考资料： | https://lists.apache.org/thread/2b4qmhbcyqvc7dyfpjyx54c03x65vhcv https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2022\_04969&lang=ZH-CN https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-13796 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 注入漏洞(CVE-2022-45143)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-45143 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat 8.5.83版本、9.0.40版本至9.0.68版本、10.1.0-M1版本至10.1.1版本存在注入漏洞，该漏洞源于JsonErrorReportValve没有转义类型、消息或描述值。 | |
| 风险影响： | 影响Tomcat:10.1.0版本(含)到10.1.1版本(含),9.0.40版本(含)到9.0.68版本(含),8.5.83版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj | |
| 参考资料： | https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15166 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 信息泄露漏洞 (CVE-2023-28708)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-28708 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 当使用RemoteIpFilter接受携带X-Forwarded-Proto请求头的通过反向代理的HTTP协议被设置为HTTPS时，Tomcat 创建的会话 cookie 不包括安全属性。这可能会导致用户代理将Cookie或Session通过不安全的隧道传输 | |
| 风险影响： | 影响apache tomcat: 8.5.0版本(含)至8.5.85版本(含),9.0.0-M1版本(含)至9.0.71版本(含),10.1.0-M1版本(含)至10.1.5版本(含),11.0.0-M1版本(含)至11.0.0-M2版本(含) | |
| 解决方案： | 目前厂商已发布修复漏洞的最新版本，请及时下载安装安全版本：https://tomcat.apache.org/tomcat-11.0-doc/index.html | |
| 参考资料： | https://tomcat.apache.org/security-11.html https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15391 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 拒绝服务漏洞(CVE-2023-24998)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-24998 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat使用Apache Commons FileUpload的打包重命名副本来提供Jakarta Servlet规范中定义的文件上传功能。因此，Apache Tomcat也容易受到Apache Commons FileUpload漏洞CVE-2023-24998的攻击，因为处理的请求部分数量没有限制。这导致攻击者有可能通过恶意上传或一系列上传触发DoS。 | |
| 风险影响： | 影响tomcat:10.1.0版本(含)到10.1.4版本(含),9.0.0版本(含)到9.0.70版本(含),8.5.0版本(含)到8.5.84版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tomcat.apache.org/security-9.html | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15700 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2023-46589)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-46589 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。Apache Tomcat存在输入验证错误漏洞，该漏洞源于存在不正确的输入验证漏洞，可能会导致将单个请求视为多个请求，从而在反向代理后面出现请求走私。 | |
| 风险影响： | 影响Tomcat:8.5.0版本(含)到8.5.95版本(含),9.0.1版本(含)到9.0.82版本(含),10.1.1版本(含)到10.1.15版本(含),11.0.0-M1版本(含)到11.0.0-M10版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr | |
| 参考资料： | https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-17201 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 跨站脚本漏洞(CVE-2022-34305)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-34305 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。Apache Tomcat 存在跨站脚本漏洞，该漏洞源于示例 Web 应用程序中表单身份验证示例对于用户提供的数据未进行过滤。 | |
| 风险影响： | 影响Tomcat:8.5.50版本(含)到8.5.81版本(含),9.0.30版本(含)到9.0.64版本(含),10.0.0-M1版本(含)到10.0.22版本(含),10.1.0-M1版本(含)到10.1.0-M16版本(含) | |
| 解决方案： | 厂商补丁: 请关注厂商公告，下载修复版本进行升级进行防护，下载链接：https://hadoop.apache.org/releases.html https://tomcat.apache.org/download-10.cgi https://tomcat.apache.org/download-9.cgi https://tomcat.apache.org/download-8.cgi | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-14342 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 安全漏洞(CVE-2024-23672)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2024-23672 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在安全漏洞，该漏洞源于不完全清理，会导致拒绝服务。 | |
| 风险影响： | 影响tomcat:8.5.0版本(含)到8.5.98版本(含),9.0.0.M1版本(含)到9.0.85版本(含),10.1.0.M1版本(含)到10.1.18版本(含),11.0.0.M1版本(含)到11.0.0.M16版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2024-23672 | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-19941 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2024-24549)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2024-24549 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在输入验证错误漏洞，该漏洞源于HTTP/2请求的输入验证不正确，会导致拒绝服务。 | |
| 风险影响： | 影响tomcat:8.5.0版本(含)到8.5.98版本(含),9.0.0.M1版本(含)到9.0.85版本(含),10.1.0.M1版本(含)到10.1.18版本(含),11.0.0.M1版本(含)到11.0.0.M16版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2024-24549 | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-19940 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2023-45648)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-45648 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。\nApache Tomcat存在安全漏洞，该漏洞源于没有正确解析HTTP尾部标头，导致攻击者可以利用特制的尾部标头造成反向代理走私。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M11版本，10.1.0-M1至10.1.13版本，9.0.0.M1至9.0.81版本，8.5.0至8.5.93版本。 | |
| 风险影响： | 影响Tomcat:8.5.85版本(含)到8.5.94版本,9.0.1版本(含)到9.0.81版本,10.1.1版本(含)到10.1.14版本,11.0.0-M1版本(含)到11.0.0-M10版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-16753 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2023-41080)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-41080 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。\nApache Tomcat存在输入验证错误漏洞，该漏洞源于FORM身份验证功能存在开放重定向漏洞，允许攻击者将URL重定向到不受信任站点。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M10版本，10.1.0-M1至10.1.12版本，9.0.0-M1至9.0.79版本，8.5.0 至8.5.92版本。 | |
| 风险影响： | 影响Tomcat:8.5.0版本(含)到8.5.92版本(含),9.0.0版本(含)到9.0.79版本(含),10.1.0版本(含)到10.1.12版本(含),11.0.0-M1版本(含)到11.0.0-M10版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-16752 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 安全漏洞(CVE-2023-42795)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-42795 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。\nApache Tomcat存在安全漏洞，该漏洞源于回收内部对象时存在安全漏洞，导致请求/响应信息泄露。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M11版本，10.1.0-M1至10.1.13版本，9.0.0-M1至9.0.80版本，8.5.0至8.5.93版本。 | |
| 风险影响： | 影响Tomcat:8.5.85版本(含)到8.5.94版本,9.0.1版本(含)到9.0.81版本,10.1.1版本(含)到10.1.14版本,11.0.0-M1版本(含)到11.0.0-M11版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-16751 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 竞争条件问题漏洞(CVE-2021-43980)【低可信】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2021-43980 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在安全漏洞，该漏洞源于阻塞读写的简化实现，存在并发错误，该错误可能导致客户端连接共享一个Http11Processor实例，从而导致响应或者部分响应，由错误的客户接收。以下产品和版本受到影响：Tomcat 10.1.0-M1至10.1.0-M12版本、10.0.0-M1至10.0.18版本、9.0.0-M1至9.0.60版本、8.5.0至8.5.77版本。 | |
| 风险影响： | 影响Tomcat:10.1.0-M1版本(含)到10.1.0-M12版本(含),10.0.0版本(含)到10.0.18版本(含),9.0.0版本(含)到9.0.60版本(含),8.5.0版本(含)到8.5.77版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3 | |
| 参考资料： | https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3 | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15167 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat HTTP请求走私漏洞(CVE-2022-42252)【低可信】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-42252 | |
| 端口(服务)： | 8083(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】2022年11月1日，深信服安全团队监测到一则Apache Tomcat组件存在HTTP请求走私漏洞的信息，漏洞编号：CVE-2022-42252，漏洞威胁等级：低危。在关闭rejectIllegalHeader的条件下，攻击者可利用该漏洞构造恶意HTTP Header在未授权的情况执行钓鱼攻击。 | |
| 风险影响： | 影响Tomcat: 8.5.0版本(含)到8.5.82版本(含),9.0.0版本(含)到9.0.67版本(含),10.1.0版本(含)到10.1.0-M20版本(含),10.0.0版本(含)到10.0.26版本(含) | |
| 解决方案： | 当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下： Apache Tomcat系列10 https://tomcat.apache.org/download-10.cgi Apache Tomcat系列9 https://tomcat.apache.org/download-90.cgi Apache Tomcat系列8 https://tomcat.apache.org/download-80.cgi | |
| 参考资料： | https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-14697 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:8091

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2023-46589)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-46589 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。Apache Tomcat存在输入验证错误漏洞，该漏洞源于存在不正确的输入验证漏洞，可能会导致将单个请求视为多个请求，从而在反向代理后面出现请求走私。 | |
| 风险影响： | 影响Tomcat:8.5.0版本(含)到8.5.95版本(含),9.0.1版本(含)到9.0.82版本(含),10.1.1版本(含)到10.1.15版本(含),11.0.0-M1版本(含)到11.0.0-M10版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr | |
| 参考资料： | https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-17201 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 拒绝服务漏洞(CVE-2023-24998)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-24998 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat使用Apache Commons FileUpload的打包重命名副本来提供Jakarta Servlet规范中定义的文件上传功能。因此，Apache Tomcat也容易受到Apache Commons FileUpload漏洞CVE-2023-24998的攻击，因为处理的请求部分数量没有限制。这导致攻击者有可能通过恶意上传或一系列上传触发DoS。 | |
| 风险影响： | 影响tomcat:10.1.0版本(含)到10.1.4版本(含),9.0.0版本(含)到9.0.70版本(含),8.5.0版本(含)到8.5.84版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tomcat.apache.org/security-9.html | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15700 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 信息泄露漏洞 (CVE-2023-28708)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-28708 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 当使用RemoteIpFilter接受携带X-Forwarded-Proto请求头的通过反向代理的HTTP协议被设置为HTTPS时，Tomcat 创建的会话 cookie 不包括安全属性。这可能会导致用户代理将Cookie或Session通过不安全的隧道传输 | |
| 风险影响： | 影响apache tomcat: 8.5.0版本(含)至8.5.85版本(含),9.0.0-M1版本(含)至9.0.71版本(含),10.1.0-M1版本(含)至10.1.5版本(含),11.0.0-M1版本(含)至11.0.0-M2版本(含) | |
| 解决方案： | 目前厂商已发布修复漏洞的最新版本，请及时下载安装安全版本：https://tomcat.apache.org/tomcat-11.0-doc/index.html | |
| 参考资料： | https://tomcat.apache.org/security-11.html https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15391 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 注入漏洞(CVE-2022-45143)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-45143 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat 8.5.83版本、9.0.40版本至9.0.68版本、10.1.0-M1版本至10.1.1版本存在注入漏洞，该漏洞源于JsonErrorReportValve没有转义类型、消息或描述值。 | |
| 风险影响： | 影响Tomcat:10.1.0版本(含)到10.1.1版本(含),9.0.40版本(含)到9.0.68版本(含),8.5.83版本 | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj | |
| 参考资料： | https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15166 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 拒绝服务漏洞(CVE-2022-29885)【低可信】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-29885 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | Apache Tomcat 存在拒绝服务漏洞，该漏洞是由于Tomcat开启集群配置中存在缺陷，攻击者可利用该漏洞在未权限的情况下，构造恶意数据造成拒绝服务，最终导致目标服务器拒绝服务。 | |
| 风险影响： | 未配置 EncryptInterceptor 则全版本受影响,配置 EncryptInterceptor 如下版本受影响：,10.1.0-M1 ≤ Apache Tomcat ≤ 10.1.0-M14,10.0.0-M1 ≤ Apache Tomcat ≤ 10.0.20,9.0.13 ≤ Apache Tomcat ≤ 9.0.62,8.5.38 ≤ Apache Tomcat ≤ 8.5.78 | |
| 解决方案： | 当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：https://tomcat.apache.org/security-10.html、https://tomcat.apache.org/security-9.html、https://tomcat.apache.org/security-8.html | |
| 参考资料： | https://lists.apache.org/thread/2b4qmhbcyqvc7dyfpjyx54c03x65vhcv https://sec.sangfor.com.cn/security-vulnerability/detail?vuln\_sfv=SF\_2022\_04969&lang=ZH-CN https://tomcat.apache.org/security-10.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-13796 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 跨站脚本漏洞(CVE-2022-34305)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-34305 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。Apache Tomcat 存在跨站脚本漏洞，该漏洞源于示例 Web 应用程序中表单身份验证示例对于用户提供的数据未进行过滤。 | |
| 风险影响： | 影响Tomcat:8.5.50版本(含)到8.5.81版本(含),9.0.30版本(含)到9.0.64版本(含),10.0.0-M1版本(含)到10.0.22版本(含),10.1.0-M1版本(含)到10.1.0-M16版本(含) | |
| 解决方案： | 厂商补丁: 请关注厂商公告，下载修复版本进行升级进行防护，下载链接：https://hadoop.apache.org/releases.html https://tomcat.apache.org/download-10.cgi https://tomcat.apache.org/download-9.cgi https://tomcat.apache.org/download-8.cgi | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-14342 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 安全漏洞(CVE-2023-42795)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-42795 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。\nApache Tomcat存在安全漏洞，该漏洞源于回收内部对象时存在安全漏洞，导致请求/响应信息泄露。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M11版本，10.1.0-M1至10.1.13版本，9.0.0-M1至9.0.80版本，8.5.0至8.5.93版本。 | |
| 风险影响： | 影响Tomcat:8.5.85版本(含)到8.5.94版本,9.0.1版本(含)到9.0.81版本,10.1.1版本(含)到10.1.14版本,11.0.0-M1版本(含)到11.0.0-M11版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-16751 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2023-41080)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-41080 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。\nApache Tomcat存在输入验证错误漏洞，该漏洞源于FORM身份验证功能存在开放重定向漏洞，允许攻击者将URL重定向到不受信任站点。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M10版本，10.1.0-M1至10.1.12版本，9.0.0-M1至9.0.79版本，8.5.0 至8.5.92版本。 | |
| 风险影响： | 影响Tomcat:8.5.0版本(含)到8.5.92版本(含),9.0.0版本(含)到9.0.79版本(含),10.1.0版本(含)到10.1.12版本(含),11.0.0-M1版本(含)到11.0.0-M10版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-16752 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2023-45648)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2023-45648 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。\nApache Tomcat存在安全漏洞，该漏洞源于没有正确解析HTTP尾部标头，导致攻击者可以利用特制的尾部标头造成反向代理走私。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M11版本，10.1.0-M1至10.1.13版本，9.0.0.M1至9.0.81版本，8.5.0至8.5.93版本。 | |
| 风险影响： | 影响Tomcat:8.5.85版本(含)到8.5.94版本,9.0.1版本(含)到9.0.81版本,10.1.1版本(含)到10.1.14版本,11.0.0-M1版本(含)到11.0.0-M10版本(含) | |
| 解决方案： | 厂商补丁:目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp | |
| 参考资料： |  | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-16753 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 安全漏洞(CVE-2024-23672)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2024-23672 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在安全漏洞，该漏洞源于不完全清理，会导致拒绝服务。 | |
| 风险影响： | 影响tomcat:8.5.0版本(含)到8.5.98版本(含),9.0.0.M1版本(含)到9.0.85版本(含),10.1.0.M1版本(含)到10.1.18版本(含),11.0.0.M1版本(含)到11.0.0.M16版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2024-23672 | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-19941 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 输入验证错误漏洞(CVE-2024-24549)【低可信】 | |
| 风险等级： | 中 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2024-24549 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在输入验证错误漏洞，该漏洞源于HTTP/2请求的输入验证不正确，会导致拒绝服务。 | |
| 风险影响： | 影响tomcat:8.5.0版本(含)到8.5.98版本(含),9.0.0.M1版本(含)到9.0.85版本(含),10.1.0.M1版本(含)到10.1.18版本(含),11.0.0.M1版本(含)到11.0.0.M16版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg | |
| 参考资料： | https://nvd.nist.gov/vuln/detail/CVE-2024-24549 | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-19940 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat HTTP请求走私漏洞(CVE-2022-42252)【低可信】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2022-42252 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】2022年11月1日，深信服安全团队监测到一则Apache Tomcat组件存在HTTP请求走私漏洞的信息，漏洞编号：CVE-2022-42252，漏洞威胁等级：低危。在关闭rejectIllegalHeader的条件下，攻击者可利用该漏洞构造恶意HTTP Header在未授权的情况执行钓鱼攻击。 | |
| 风险影响： | 影响Tomcat: 8.5.0版本(含)到8.5.82版本(含),9.0.0版本(含)到9.0.67版本(含),10.1.0版本(含)到10.1.0-M20版本(含),10.0.0版本(含)到10.0.26版本(含) | |
| 解决方案： | 当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下： Apache Tomcat系列10 https://tomcat.apache.org/download-10.cgi Apache Tomcat系列9 https://tomcat.apache.org/download-90.cgi Apache Tomcat系列8 https://tomcat.apache.org/download-80.cgi | |
| 参考资料： | https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-14697 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8091 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8091User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | Apache Tomcat 竞争条件问题漏洞(CVE-2021-43980)【低可信】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2021-43980 | |
| 端口(服务)： | 8091(Tomcat) | |
| 风险描述： | 【该漏洞通过版本比较方式检测，结果可能不准确，需要根据实际情况确认。】Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在安全漏洞，该漏洞源于阻塞读写的简化实现，存在并发错误，该错误可能导致客户端连接共享一个Http11Processor实例，从而导致响应或者部分响应，由错误的客户接收。以下产品和版本受到影响：Tomcat 10.1.0-M1至10.1.0-M12版本、10.0.0-M1至10.0.18版本、9.0.0-M1至9.0.60版本、8.5.0至8.5.77版本。 | |
| 风险影响： | 影响Tomcat:10.1.0-M1版本(含)到10.1.0-M12版本(含),10.0.0版本(含)到10.0.18版本(含),9.0.0版本(含)到9.0.60版本(含),8.5.0版本(含)到8.5.77版本(含) | |
| 解决方案： | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3 | |
| 参考资料： | https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3 | |
| 协议类型： | http | |
| 风险举证: | Tomcat: 9.0.59 | |
| 漏洞ID： | SF-0005-15167 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | cookie 没有设置httponly标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 为SetCookie配置HttpOnly属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8091 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8091User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00870 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8091 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8091User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:8999

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | CORS(跨站资源共享)原始验证失败【原理扫描】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | CORS漏洞是当前服务器对跨源资源的配置不当，导致允许任意源来共享服务器资源，从而导致用户数据泄露、客户端缓存中毒或者服务端缓存中毒。 | |
| 风险影响： | 1、获取用户数据,2、客户端缓存中毒：这种配置允许攻击者利用其他的漏洞，更改没有验证的字段，看是否正常回显。比如，一个应用返回数据报文头部中包含“X-User”这个字段，这个字段的值没有经过验证就直接输出到返回页面上，此时就可以结合XSS漏洞来利用。,3、服务端缓存中毒：利用CORS的错误配置注入HTTP头部，这可能会被服务器端缓存下来，比如制造存储型xss | |
| 解决方案： | 非必要不建议开启cors跨域资源共享功能，如需开启，请严格限制Origin值为需要资源共享的子域，或者当前主域。 | |
| 参考资料： |  | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8999 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8999User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveOrigin: https://www.evil.com |
| 漏洞ID： | SF-2023-00249 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8999 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8999User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8999 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8999User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8999 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8999User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8999 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8999User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8999 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8999User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

### 资产: https://meal.yangzhouyiyuan.com

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】 | |
| 风险等级： | 高 | |
| 高可利用： | 否 | |
| CVE编号： | CVE-2016-2183 | |
| 端口(服务)： | 443(SSL) | |
| 风险描述： | OpenSSL是Openssl团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。TLS、SSH和IPSec协议和其它协议及产品中使用的DES和Triple DES密码算法存在信息泄露漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。 | |
| 风险影响： | TLS、SSH 和 IPSec 协议以及其他协议和产品中使用的 DES 和 Triple DES 密码的生日限制约为 40 亿个块，这使得远程攻击者更容易通过生日攻击获取明文数据长时间的加密会话，如 CBC 模式下使用 Triple DES 的 HTTPS 会话所示，也称为“Sweet32”攻击 | |
| 解决方案： | 禁用DES和Triple DES加密算法 | |
| 参考资料： | https://www.cnnvd.org.cn/home/globalSearch?keyword=CNNVD-201608-448 https://sweet32.info/ http://www.securitytracker.com/id/1036696 | |
| 协议类型： | - | |
| 风险举证: | 通过nmap探测发现存在DES相关加密算法响应如下:b'Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-23 20:46 CST\nNmap scan report for meal.yangzhouyiyuan.com (58.220.99.162)\nHost is up (0.029s latency).\n\nPORT STATE SERVICE\n443/tcp open https\n| ssl-enum-ciphers: \n| TLSv1.0: \n| ciphers: \n| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (ecdh\_x25519) - A\n| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (ecdh\_x25519) - A\n| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048) - A\n| TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (rsa 2048) - C\n| compressors: \n| NULL\n| cipher preference: server\n| warnings: \n| 64-bit block cipher 3DES vulnerable to SWEET32 attack\n| TLSv1.1: \n| ciphers: \n| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (ecdh\_x25519) - A\n| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (ecdh\_x25519) - A\n| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048) - A\n| TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (rsa 2048) - C\n| compressors: \n| NULL\n| cipher preference: server\n| warnings: \n| 64-bit block cipher 3DES vulnerable to SWEET32 attack\n| TLSv1.2: \n| ciphers: \n| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (ecdh\_x25519) - A\n| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (ecdh\_x25519) - A\n| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (ecdh\_x25519) - A\n| TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (ecdh\_x25519) - A\n| TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (ecdh\_x25519) - A\n| TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048) - A\n| TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048) - A\n| TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (rsa 2048) - C\n| compressors: \n| NULL\n| cipher preference: server\n| warnings: \n| 64-bit block cipher 3DES vulnerable to SWEET32 attack\n|\_ least strength: C\n\nNmap done: 1 IP address (1 host up) scanned in 3.90 seconds\n' | |
| 漏洞ID： | SF-2022-00961 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://meal.yangzhouyiyuan.com | |
| 请求： | GET / HTTP/1.1Host: meal.yangzhouyiyuan.com:443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

## 低危风险资产详情

### 资产: http://dxclouds.yangzhouyiyuan.com:27002

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27002 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27002User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

### 资产: http://dxclouds.yangzhouyiyuan.com:27003

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | cookie 没有设置httponly标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 为SetCookie配置HttpOnly属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00870 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | http://dxclouds.yangzhouyiyuan.com:27003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:27003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:10130

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | cookie 没有设置httponly标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 为SetCookie配置HttpOnly属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00870 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:10130 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:10130User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:1443/

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:1443/ | |
| 请求： | GET /UniExServices/user/toLogin.html HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:1443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveCookie: JSESSIONID=F6D5AA4B39B627CC1E01EDDC9C455DE7; JSESSIONID=DB4B7EC49CA014E9C42AAA29982FACED |
| 漏洞ID： | SF-2024-00154 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:1443/ | |
| 请求： | GET /UniExServices/user/toLogin.html HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:1443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveCookie: JSESSIONID=F6D5AA4B39B627CC1E01EDDC9C455DE7; JSESSIONID=DB4B7EC49CA014E9C42AAA29982FACED |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:1443/ | |
| 请求： | GET /UniExServices/user/toLogin.html HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:1443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveCookie: JSESSIONID=F6D5AA4B39B627CC1E01EDDC9C455DE7; JSESSIONID=DB4B7EC49CA014E9C42AAA29982FACED |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:1443/ | |
| 请求： | GET /UniExServices/user/toLogin.html HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:1443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveCookie: JSESSIONID=F6D5AA4B39B627CC1E01EDDC9C455DE7; JSESSIONID=DB4B7EC49CA014E9C42AAA29982FACED |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:1443/ | |
| 请求： | GET /UniExServices/user/toLogin.html HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:1443User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveCookie: JSESSIONID=F6D5AA4B39B627CC1E01EDDC9C455DE7; JSESSIONID=DB4B7EC49CA014E9C42AAA29982FACED |
| 漏洞ID： | SF-2022-00439 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:18090

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:18090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:18090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:5000

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5000 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5000User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:5003

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:5003 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:5003User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:8010

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | cookie 没有设置httponly标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 为SetCookie配置HttpOnly属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00870 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8010 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8010User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:8088

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8088 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8088User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8088 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8088User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | OPTIONS方法启用【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 此Web服务器上启用了HTTP OPTIONS方法。 OPTIONS方法提供了Web服务器支持的方法列表，它表示对有关由Request-URI标识的请求/响应链上可用的通信选项的信息的请求。 | |
| 风险影响： | OPTIONS方法可能会公开敏感信息，这些信息可能有助于恶意用户准备更高级的攻击。 | |
| 解决方案： | 建议在Web服务器上禁用OPTIONS方法。 | |
| 参考资料： | https://www.owasp.org/index.php/Testing\_for\_HTTP\_Methods\_and\_XST\_(OWASP-CM-008) | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8088 | |
| 请求： | OPTIONS / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8088User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-aliveContent-Length: 0 |
| 漏洞ID： | SF-2022-00754 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:8090

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | cookie 没有设置httponly标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | HttpOnly 主要是为了限制web页面程序的browser端script程序读取cookie，防止恶意代码获取客户的敏感信息。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 为SetCookie配置HttpOnly属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00870 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:8090 | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:8090User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

### 资产: https://dxclouds.yangzhouyiyuan.com:81/

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Referrer-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效。 当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也成为了一个不安全的因素，所以就有了 Referrer-Policy，用于过滤 Referrer 报头内容，其可选的项有： no-referrer no-referrer-when-downgrade origin origin-when-cross-origin same-origin strict-origin strict-origin-when-cross-origin unsafe-url 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Referrer-Policy，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Referrer-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00436 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 点击劫持:无X-Frame-Options头信息【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 目标服务器没有返回一个X-Frame-Options头。攻击者可以使用一个透明的、不可见的iframe，覆盖在目标网页上，然后诱使用户在该网页上进行操作，此时用户将在不知情的情况下点击透明的iframe页面。通过调整iframe页面的位置，可以诱使用户恰好点击iframe页面的一些功能性按钮上，导致被劫持。 | |
| 风险影响： | 可能会导致点击劫持漏洞 | |
| 解决方案： | 修改web服务器配置，添加X-frame-options响应头。赋值有如下三种：（1）DENY：不能被嵌入到任何iframe或frame中。（2）SAMEORIGIN：页面只能被本站页面嵌入到iframe或者frame中。（3）ALLOW-FROM uri：只能被嵌入到指定域名的框架中。也可在代码中加入，在PHP中加入：header('X-Frame-Options: deny'); | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00874 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Strict-Transport-Security响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置Strict-Transport-Security响应标头。HTTP严格传输安全（HSTS）强制执行到服务器的安全（HTTP over SSL / TLS）连接。这可以减少网络应用程序中的漏洞通过cookie和外部链接泄漏会话数据的影响，并抵御中间人攻击。 HSTS还禁止用户忽略SSL协商警告的能力。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下标题：Strict-Transport-Security：max-age = 16070400;请注意，当您设置此标头时，您需要在端口443上运行的Web服务器。如果你没有它并且应用这个修复你的网站将不再可用 | |
| 参考资料： | http://en.wikipedia.org/wiki/Strict-Transport-Security | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00873 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-XSS-Protection响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程Web应用程序没有设置X-XSS-Protection响应头。 此标题使最近的Web浏览器中内置的跨站点脚本（XSS）过滤器成为可能。 它通常默认情况下是启用的，所以如果用户禁用了这个标头，这个标头的作用是重新启用这个特定网站的过滤器。此标头在IE 8+和Chrome中支持（不确定哪些版本）。在Chrome 4中添加了反XSS筛选器。如果该版本符合此标题，则不详。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以下响应头：X-XSS-Protection：1; mode=block | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00872 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Content-Type-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程网络应用程序没有设置X-Content-Options响应头。X-Content-Options是Microsoft提出的一种缓解MIME类型攻击的方式，并且已经在Chrome和Safari中实现。 | |
| 风险影响： | 远程攻击者可以利用此漏洞获取敏感信息 | |
| 解决方案： | 需要在Web应用程序的所有页面上设置以返回头：X-Content-Type-Options：nosniff | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2021-00871 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | general 未设置cookie的Secure标志位【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 通用型(general)漏洞并不针对某一系统，其在各类系统中都有可能存在。Cookie Without Secure Flag Set是指服务器Set-Cookie消息头中未设置可选属性Secure，如果服务器设置这个属性，那么cookie只能在HTTPS请求中提交。 | |
| 风险影响： | 影响所有Set-Cookie消息头中未设置可选属性Secure的系统 | |
| 解决方案： | 为cookie设置Secure属性 | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2016-00025 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Download-Options响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Download-Options响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Download-Options | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00438 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置X-Permitted-Cross-Domain-Policies响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置X-Permitted-Cross-Domain-Policies响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2022-00439 | |

|  |  |  |
| --- | --- | --- |
| 漏洞名称 | 未设置Content-Security-Policy响应头【原理扫描】 | |
| 风险等级： | 低 | |
| 高可利用： | 否 | |
| CVE编号： | - | |
| 端口(服务)： | - | |
| 风险描述： | 远程主机上的web应用没有设置未设置Content-Security-Policy响应头 | |
| 风险影响： | 远程攻击者可以利用此漏洞进行信息收集，方便下一步的攻击行为 | |
| 解决方案： | 修改服务端程序，给 HTTP 响应头加上 Content-Security-Policy | |
| 参考资料： | 暂无 | |
| 协议类型： | - | |
| 风险举证： | https://dxclouds.yangzhouyiyuan.com:81/ | |
| 请求： | GET / HTTP/1.1Host: dxclouds.yangzhouyiyuan.com:81User-Agent: python-requests/2.23.0Accept-Encoding: gzip, deflateAccept: \*/\*Connection: keep-alive |
| 漏洞ID： | SF-2024-00154 | |

# 主机服务探测

和业务不相关端口的开放，是潜在的风险点，建议关闭不使用的端口，服务器的服务及端口开放和分布情况如下：

|  |  |  |
| --- | --- | --- |
| **主机名** | **端口** | **开启服务** |
| http://dxclouds.yangzhouyiyuan.com:27002 | 27002 | http |
| http://dxclouds.yangzhouyiyuan.com:27003 | 27003 | http |
| https://dxclouds.yangzhouyiyuan.com:10130 | 10130 | https |
| https://dxclouds.yangzhouyiyuan.com:1443/ | 1443 | https |
| https://dxclouds.yangzhouyiyuan.com:18090 | 18090 | https |
| https://dxclouds.yangzhouyiyuan.com:5000 | 5000 | https |
| https://dxclouds.yangzhouyiyuan.com:5003 | 5003 | https |
| https://dxclouds.yangzhouyiyuan.com:8010 | 8010 | https |
| https://dxclouds.yangzhouyiyuan.com:8083 | 8083 | http |
| 8083 | https |
| https://dxclouds.yangzhouyiyuan.com:8088 | 8088 | https |
| https://dxclouds.yangzhouyiyuan.com:8090 | 8090 | https |
| https://dxclouds.yangzhouyiyuan.com:8091 | 8091 | http |
| 8091 | https |
| https://dxclouds.yangzhouyiyuan.com:81/ | 81 | https |
| https://dxclouds.yangzhouyiyuan.com:8999 | 8999 | https |
| https://meal.yangzhouyiyuan.com | 443 | https |

# 参考标准

|  |
| --- |
| 单一系统漏洞风险等级评定标准 |

|  |  |  |
| --- | --- | --- |
| 危险程度 | 危险值区域 | 危险程度说明 |
| 高危 | 7 <= 漏洞风险值 <= 10 | 攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。 |
| 中危 | 4 <= 漏洞风险值 < 7 | 攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。 |
| 低危 | 1 <= 漏洞风险值 < 4 | 攻击者可以获取某些敏感的系统、服务信息，或读取系统文件和数据。 |
| 信息 | 漏洞风险值 = 0 | 攻击者可以获取系统、服务的信息，如服务软件、版本、以及运行信息。 |

|  |
| --- |
| 单一Web漏洞风险等级评定标准 |

|  |  |  |
| --- | --- | --- |
| 危险程度 | 危险值区域 | 危险程度说明 |
| 高危 | 7 <= 漏洞风险值 <= 10 | 攻击者可以远程操作系统文件、读写后台数据库、执行任意命令或进行远程拒绝服务攻击。 |
| 中危 | 4 <= 漏洞风险值 < 7 | 攻击者可以利用web应用系统攻击其他用户，读取系统文件或后台数据。 |
| 低危 | 1 <= 漏洞风险值 < 4 | 攻击者可以获取某些系统、文件的信息或冒用身份以及存在敏感词。 |
| 信息 | 漏洞风险值 = 0 | 存在如邮件地址、电话等明文，存在信息泄露的可能性。 |

|  |
| --- |
| 单一资产风险等级评定标准 |

|  |  |
| --- | --- |
| 危险程度 | 危险程度说明 |
| 高危 | 资产存在高危风险的漏洞，风险等级为高风险，建议优先关注。 |
| 中危 | 资产只发现中危以下风险等级的漏洞，风险等级为中风险。 |
| 低危 | 资产只发现低危风险的漏洞，风险值等级较低。 |
| 安全 | 不存在高中低风险的漏洞，不存在脆弱性风险。 |

# 了解更多

了解更多安全信息，或关于本文出现的漏洞、攻击方式等详细介绍与建议，可查看深信服安全中心的威胁维基或关注深信服科技公众号了解最新的威胁情报。

威胁维基：<http://sec.sangfor.com.cn/vulns/lst.html>

