山西省生态环境厅

重点污染源自动监控与基础数据库系统

漏洞扫描报告

山西云时代政务云技术有限公司

本报告生成于 2025 年 3 月

1 综述

本次评估的总体安全等级为**高危** 。

资产情况如下：

- 存活资产 1 个，其中，存在风险的资产 1 个。

攻击面情况如下：

- 漏洞共 38 个，其中严重 0 个，高危 6 个，中危 15 个，低危 17 个。
- 登录入口共 1 个，其中，web 登录入口 0 个，系统登录入口 1 个。

若存在严重或高危风险，建议您重点关注并及时修复。

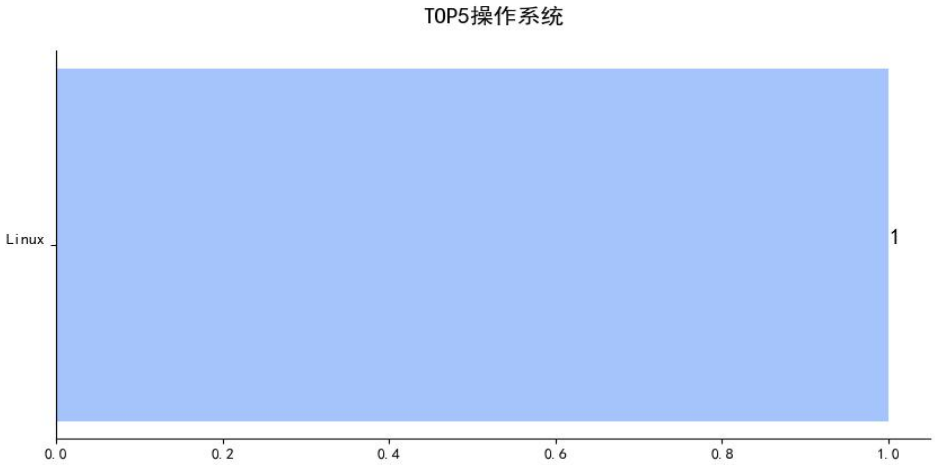
2 资产统计

2.1 资产基本信息

本次共检测到存活资产 1 个，其中，主机资产 1 个，网站资产 0 个。

主机资产的设备类型统计情况如下图所示：

存活资产中使用最多的操作系统是 Linux，TOP5 操作系统统计如下图所示：

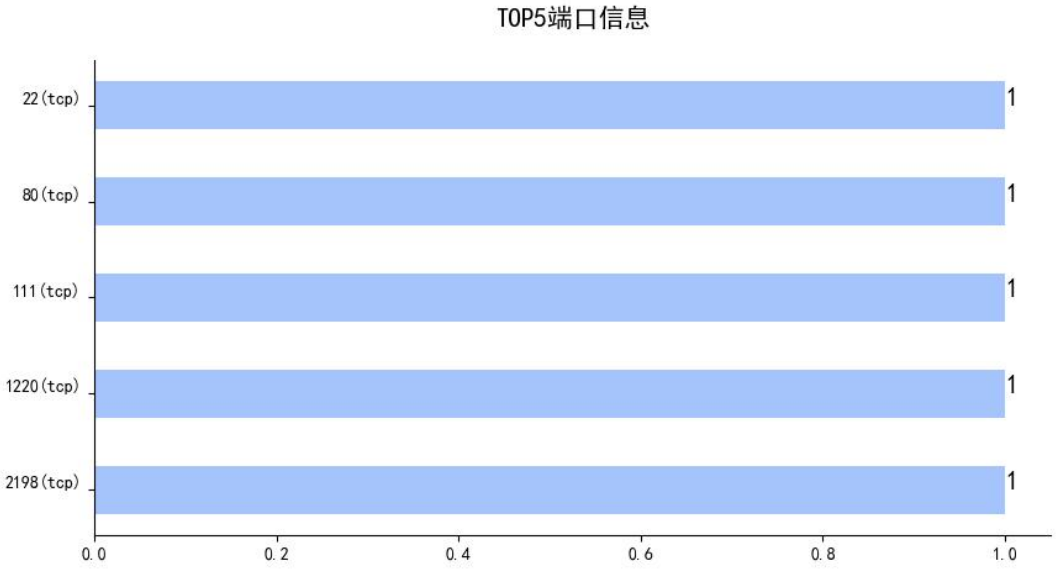


资产基本信息情况如下表所示：

序号	IP/URL	设备类型	操作系统	资产名称	是否核心	责任人	业务组
1	17.167.7.7	服务器设备	Linux(Linux)		否		

2.2 资产端口信息

存在端口开放的资产共 1 个，开放最多的端口为 22(tcp)，开放端口数量最多的资产为 17.167.7.7。TOP5 端口使用情况如下图所示：



资产端口信息如下表所示：

序号	IP/URL	端口数	端口	协议	服务	软件

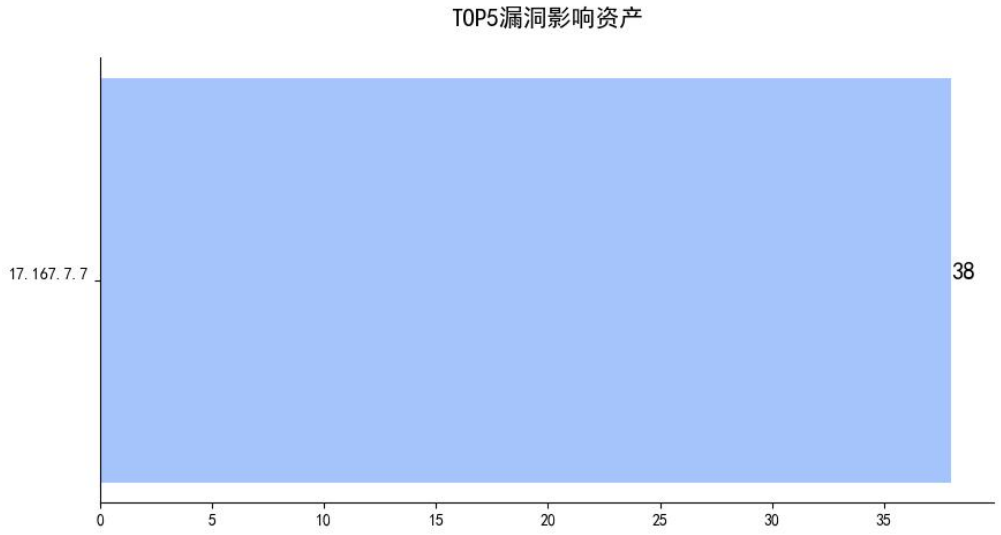
1	17.167.7.7	29	22	tcp	ssh	OpenSSH
			80	tcp	http	nginx
			111	tcp	rpcbind	rpcbind
			1220	tcp	http	http
			2198	tcp	onehome-remote	onehome-remote
			7080	tcp	http	http
			7081	tcp	http	JointFrame Platform Server
			7082	tcp	http	http
			7083	tcp	http	http
			8080	tcp	http	http
			8081	tcp	http	JointFrame Platform Server
			8188	tcp	http	http
			8586	tcp	http	http
			12008	tcp	http	http
			12300	tcp	http	nginx
			12301	tcp	http	http
			12325	tcp	http	http
			12333	tcp	http	http
			12345	tcp	http	http
			12378	tcp	http	http
			12407	tcp	http	http
			12409	tcp	http	http
			12410	tcp	http	http
			12411	tcp	http	http
			123	udp	ntp	NTP
			5355	udp	tcpwrapped	tcpwrapped
			18088	tcp	http	http
			40002	tcp	unknown	unknown

			61616	tcp	apachemq	ActiveMQ OpenWire transport

2.3 资产风险信息

2.3.1 漏洞

存在漏洞风险的资产共 1 个，其中风险数量最多的资产 TOP5 如下图所示：



资产的漏洞风险情况如下表所示：

序号	IP/URL	严重	高	中	低	总计
1	17.167.7.7	0	6	15	17	38

2.3.2 登录入口

存在登录入口风险的资产共 1 个，资产的登录入口风险情况如下表所示：

序号	IP/URL	Web 登录入口	系统登录入口	总计
1	17.167.7.7	0	1	1

3 资产详情

3.1 17.167.7.7

3.1.1 资产基本信息

资产	17.167.7.7
是否核心	否
资产名称	
业务组	
责任人	
所属部门	
联系电话	
MAC 地址	
操作系统	Linux(Linux)
设备类型	服务器设备
设备小类	其它
厂商和型号	-

3.1.2 资产端口信息

序号	开放端口	协议	开放服务	软件信息	网站 URL	网站标题
1	22	tcp	ssh	OpenSSH		
2	80	tcp	http	nginx	http://17.167.7.7:80/	Welcome to nginx!
3	111	tcp	rpcbind	rpcbind		
4	1220	tcp	http	http	http://17.167.7.7:1220/	HTTP Status 404 - Not Found
5	2198	tcp	onehome-remote	onehome-remote		

6	7080	tcp	http	http	http://17.167.7.7:7080/	HTTP 状态 404 - 未找到
7	7081	tcp	http	JointFrame Platform Server		
8	7082	tcp	http	http	http://17.167.7.7:7082/	
9	7083	tcp	http	http		
10	8080	tcp	http	http		
11	8081	tcp	http	JointFrame Platform Server		
12	8188	tcp	http	http	http://17.167.7.7:8188/	
13	8586	tcp	http	http	http://17.167.7.7:8586/	HTTP Status 404 - Not Found
14	12008	tcp	http	http	http://17.167.7.7:12008/	
15	12300	tcp	http	nginx	http://17.167.7.7:12300/	Welcome to nginx!
16	12301	tcp	http	http	http://17.167.7.7:12301/	HTTP Status 404 - Not Found
17	12325	tcp	http	http	http://17.167.7.7:12325/	HTTP Status 404 - Not Found
18	12333	tcp	http	http	http://17.167.7.7:12333/	
19	12345	tcp	http	http	http://17.167.7.7:12345/	HTTP Status 404 - Not Found
20	12378	tcp	http	http	http://17.167.7.7:12378/	
21	12407	tcp	http	http	http://17.167.7.	HTTP Status 404 - Not

					7:12407/	Found
22	12409	tcp	http	http	http://17.167.7.7:12409/	HTTP Status 404 - Not Found
23	12410	tcp	http	http	http://17.167.7.7:12410/	HTTP Status 404 - Not Found
24	12411	tcp	http	http	http://17.167.7.7:12411/	HTTP Status 404 - Not Found
25	123	udp	ntp	NTP		
26	5355	udp	tcpwrapped	tcpwrapped		
27	18088	tcp	http	http	http://17.167.7.7:18088/	
28	40002	tcp	unknown	unknown		
29	61616	tcp	apachemq	ActiveMQ OpenWire transport		

3.1.3 资产风险信息

该资产总体安全等级为**高危** ，不同类型的风险分布如下：

风险类型	严重	高	中	低	总计
系统漏洞	0	3	14	3	20
web 漏洞	0	3	1	14	18
弱口令	0	0	0	0	0
web 登录入口	0	0	0	0	0
系统登录入口	0	0	0	1	1
总计	**0**	**6**	**15**	**18**	39

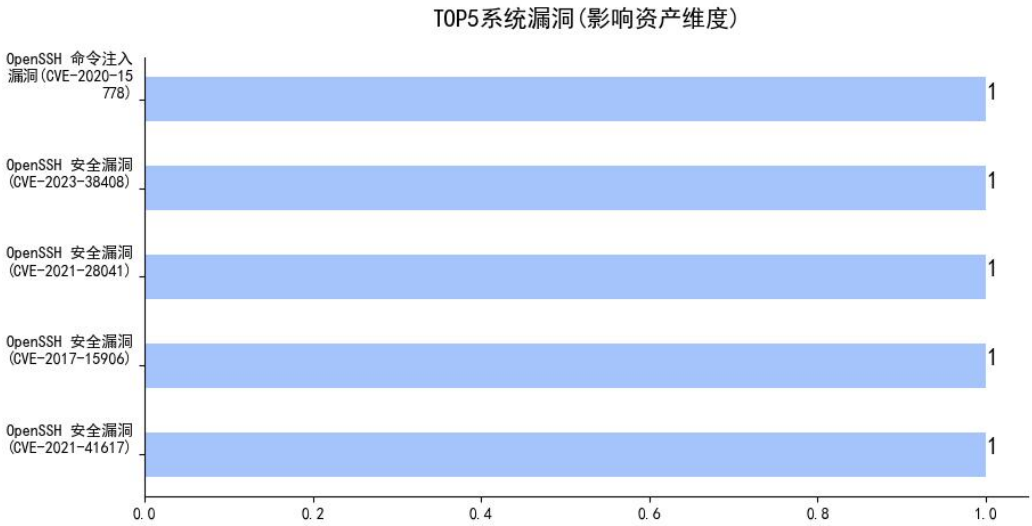
4 风险统计

4.1 系统漏洞影响分析

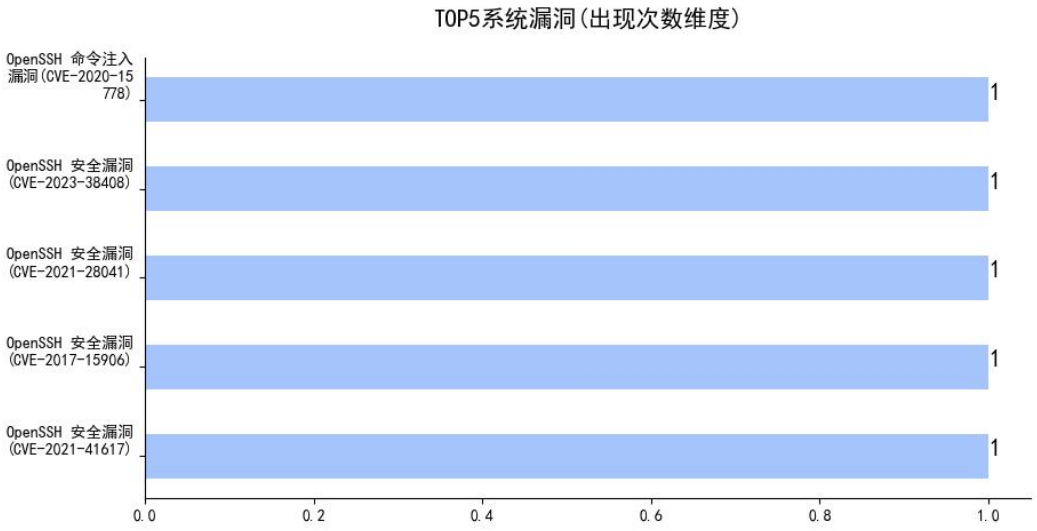
4.1.1 风险等级分析

4.1.2 影响资产分析

系统漏洞影响资产数量 TOP5 统计如下：



出现次数指的是每个漏洞影响的端口或页面数量，系统漏洞出现次数 TOP５统计如下：



TOP100 系统漏洞影响资产情况如下表所示：

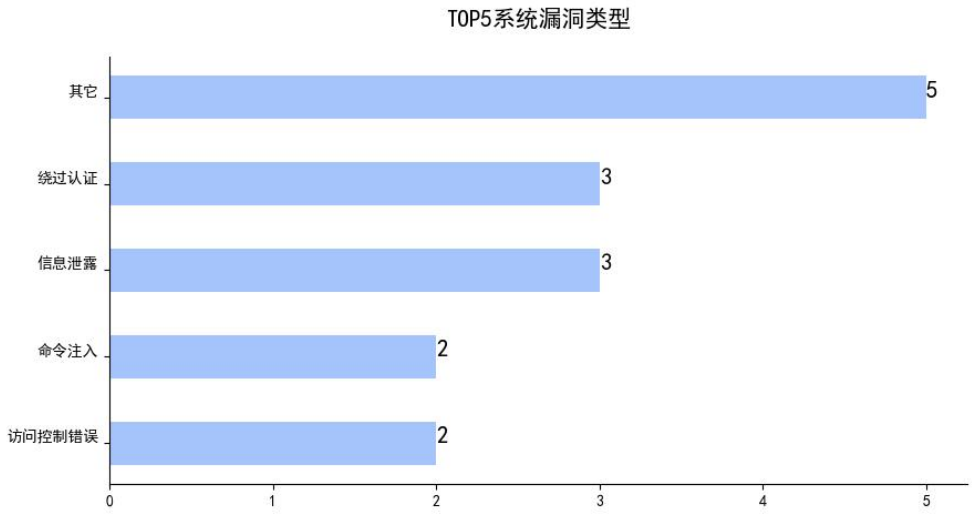
注：此处仅展示 TOP100 系统漏洞及其影响资产情况，每个漏洞影响的资产最多展示 10 个，更多信息请登录平台查看，或者下载 excel/html 报告查看。

序号	系统漏洞名称	风险等级	影响资产（仅展示 10 个）	影响资产数	出现次数
1	OpenSSH 命令注入漏洞(CVE-2020-15778)	高	17.167.7.7	1	1
2	OpenSSH 安全漏洞(CVE-2023-38408)	高	17.167.7.7	1	1
3	OpenSSH 安全漏洞(CVE-2021-28041)	高	17.167.7.7	1	1
4	OpenSSH 安全漏洞(CVE-2017-15906)	中	17.167.7.7	1	1
5	OpenSSH 安全漏洞(CVE-2021-41617)	中	17.167.7.7	1	1
6	OpenSSH 安全漏洞(CVE-2023-48795)	中	17.167.7.7	1	1
7	OpenSSH 访问控制错误漏洞(CVE-2019-6110)	中	17.167.7.7	1	1
8	OpenSSH 安全漏洞(CVE-2016-20012)	中	17.167.7.7	1	1
9	OpenSSH 信息泄漏漏洞(CVE-2018-15919)	中	17.167.7.7	1	1
10	OpenSSH 安全漏洞(CVE-2023-51767)	中	17.167.7.7	1	1
11	OpenSSH 访问控制错误漏洞(CVE-2019-6109)	中	17.167.7.7	1	1
12	OpenSSH 安全漏洞(CVE-2023-51384)	中	17.167.7.7	1	1
13	OpenSSH 用户枚举漏洞(CVE-2018-15473)	中	17.167.7.7	1	1
14	OpenSSH 输入验证错误漏洞	中	17.167.7.7	1	1

	(CVE-2019-6111)				
15	OpenSSH 访问限制绕过漏洞(CVE-2018-20685)	中	17.167.7.7	1	1
16	OpenSSH 安全漏洞(CVE-2023-51385)	中	17.167.7.7	1	1
17	OpenSSH 信息泄露漏洞(CVE-2020-14145)	中	17.167.7.7	1	1
18	SSH 服务器支持的算法发现【原理扫描】	低	17.167.7.7	1	1
19	OpenSSH 授权问题漏洞(CVE-2021-36368)	低	17.167.7.7	1	1
20	OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)【原理扫描】	低	17.167.7.7	1	1

4.1.3 漏洞类别分析

系统漏洞类别 TOP５统计如下：



系统漏洞类别统计列表如下：

序号	漏洞名称	出现次数
1	其它	5
2	绕过认证	3
3	信息泄露	3
4	命令注入	2
5	访问控制错误	2
6	信息发现	1
7	登录入口	1

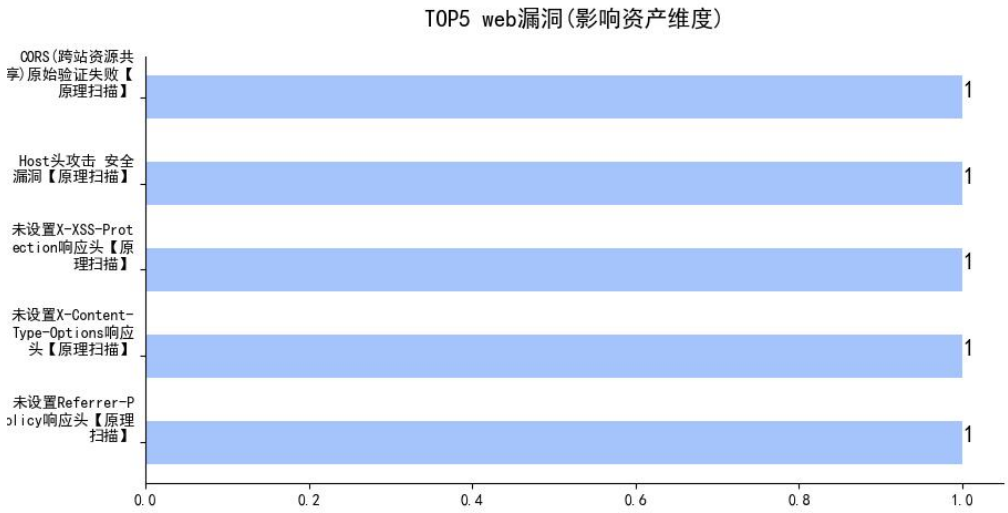
8	授权问题	1
9	输入验证错误	1
10	代码注入	1
11	权限提升	1

4.2 Web 漏洞影响分析

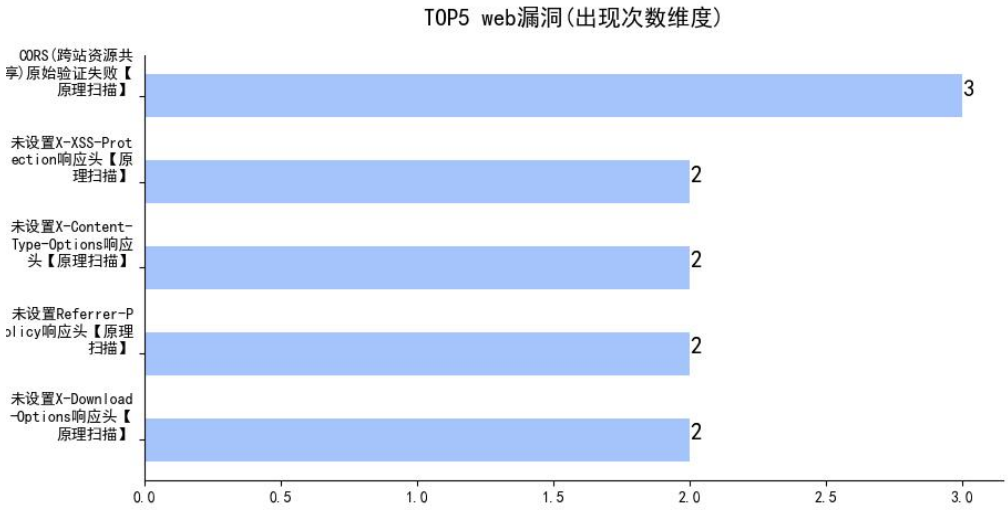
4.2.1 风险等级统计

4.2.2 影响资产分析

Web 漏洞影响资产数量 TOP5 统计如下：



出现次数指的是每个漏洞影响的端口或页面数量，系统漏洞出现次数 TOP５统计如下：



TOP100web 漏洞影响资产情况如下表所示：

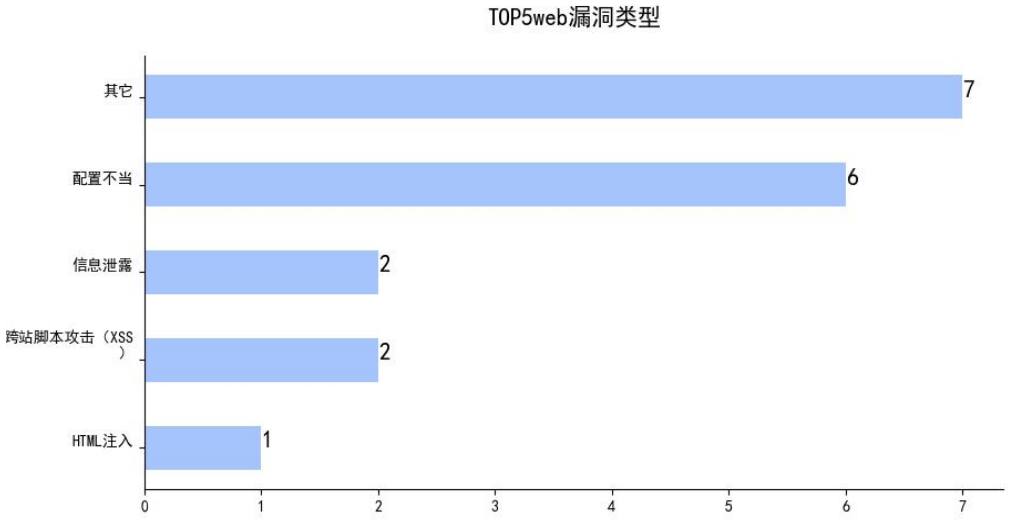
注：此处仅展示 TOP100web 漏洞及其影响资产情况，每个漏洞影响的资产最多展示 10 个，更多信息请登录平台查看，或者下载 excel/html 报告查看。

序号	Web 漏洞名称	风险等级	影响资产（仅展示 10 个）	影响资产数	出现次数
1	CORS(跨站资源共享)原始验证失败【原理扫描】	高	17.167.7.7	1	3
2	Host 头攻击 安全漏洞【原理扫描】	中	17.167.7.7	1	1
3	未设置 X-XSS-Protection 响应头【原理扫描】	低	17.167.7.7	1	2
4	未设置 X-Content-Type-Options 响应头【原理扫描】	低	17.167.7.7	1	2

5	未设置 Referrer-Policy 响应头【原理扫描】	低	17.167.7.7	1	2
6	未设置 X-Download-Options 响应头【原理扫描】	低	17.167.7.7	1	2
7	未设置 X-Permitted-Cross-Domain-Policies 响应头【原理扫描】	低	17.167.7.7	1	2
8	点击劫持:无 X-Frame-Options 头信息【原理扫描】	低	17.167.7.7	1	2
9	未设置 Strict-Transport-Security 响应头【原理扫描】	低	17.167.7.7	1	2

4.2.3 漏洞类别分析

web 漏洞类别 TOP５统计如下：



web 漏洞类别统计列表如下：

序号	漏洞名称	出现次数
1	其它	7
2	配置不当	6
3	信息泄露	2
4	跨站脚本攻击（XSS）	2
5	HTML 注入	1

4.3 弱口令影响分析

4.3.1 影响资产分析

未发现存在弱口令影响的资产。

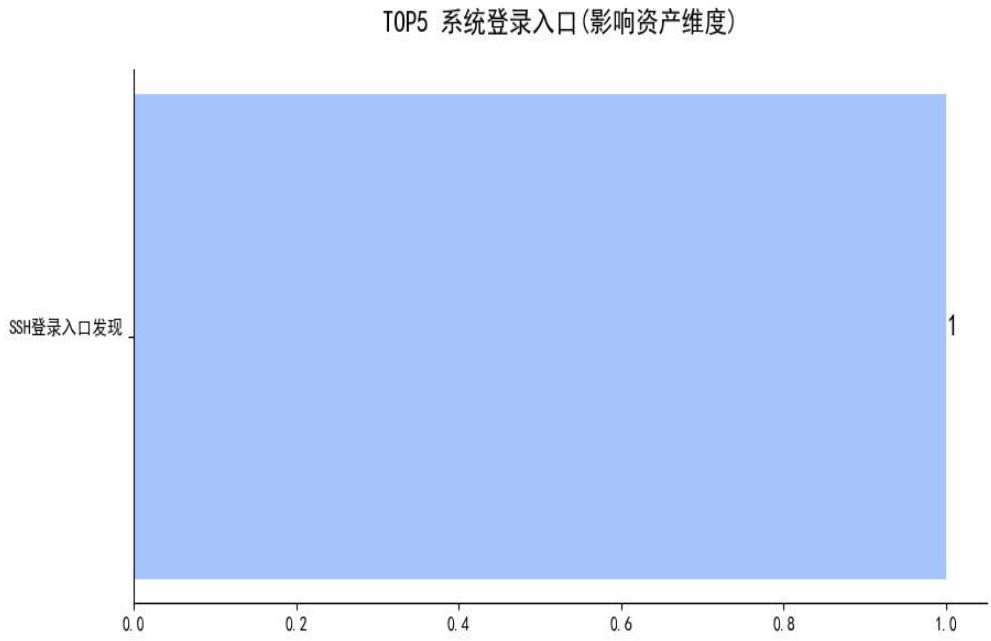
4.4 登录入口影响分析

4.4.1 Web 登录入口影响资产分析

未发现存在 web 登录入口影响的资产。

4.4.2 系统登录入口影响资产分析

系统登录入口影响资产数量 TOP5 统计如下：



TOP100 系统登录入口影响资产情况如下表所示：

注：此处仅展示 TOP100 系统登录入口及其影响资产情况，每个系统登录入口影响的资产最多展示 10 个，更多信息请登录平台查看，或者下载 excel/html 报告查看。

序号	系统登录入口名称	影响资产（仅展示 10 个）	影响资产数	出现次数

1	SSH 登录入口发现	17.167.7.7	1	1

5 风险详情

5.1 17.167.7.7

5.1.1 系统漏洞

1	OpenSSH 命令注入漏洞(CVE-2020-15778)
风险等级	高
深信服漏洞编号	SF-0005-02635
CVE 编号	CVE-2020-15778
CNNVD 编号	CNNVD-202007-1519
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 8.3p1 及之前版本中的 scp 的 scp.c 文件存在命令注入漏洞。该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。
风险影响	影响 OpenSSH:8.4p1 以下版本(含)
解决方案	可以禁用 scp，改用 rsync 等缓解风险（可能会导致小文件机器内拷贝变慢）
风险举证	OpenSSH:7.4

2	OpenSSH 安全漏洞(CVE-2023-38408)
风险等级	高
深信服漏洞编号	SF-0005-17300
CVE 编号	CVE-2023-38408
CNNVD 编号	CNNVD-202307-1721

CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.3p2 之前版本存在安全漏洞，该漏洞源于 ssh-agent 的 PKCS11 功能存在安全问题。攻击者可利用该漏洞执行远程代码。
风险影响	影响 OpenSSH:9.3p2 版本以下版本
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://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8
风险举证	OpenSSH:7.4

3	**OpenSSH 安全漏洞(CVE-2021-28041)**
风险等级	高
深信服漏洞编号	SF-0005-06510
CVE 编号	CVE-2021-28041
CNNVD 编号	CNNVD-202103-527
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。OpenSSH before 8.5 存在安全漏洞，攻击者可利用该漏洞在遗留操作系统上不受约束的代理套接字访问。
风险影响	影响 OpenSSH:8.5 以下版本
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://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db
风险举证	OpenSSH:7.4

4	**OpenSSH 安全漏洞(CVE-2017-15906)**
风险等级	中
深信服漏洞编号	SF-0005-06522
CVE 编号	CVE-2017-15906

CNNVD 编号	CNNVD-201710-1230
CNVD 编号	CNVD-2017-36017
Bugtraq 编号	101552
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。OpenSSH 7.6 之前的版本中的 sftp-server.c 文件的‘process_open’函数存在安全漏洞，该漏洞源于程序在只读模式下没有正确的阻止写入操作。攻击者可利用该漏洞创建长度为零的文件。
风险影响	影响 OpenSSH:7.6 以下版本
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://www.openssh.com/txt/release-7.6
风险举证	OpenSSH:7.4

5	**OpenSSH 安全漏洞(CVE-2021-41617)**
风险等级	中
深信服漏洞编号	SF-0005-10928
CVE 编号	CVE-2021-41617
CNNVD 编号	CNNVD-202109-1695
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。OpenSSH 6.2 到 8.8 之前版本存在安全漏洞。该漏洞源于允许权限提升，因为补充组未按预期初始化。
风险影响	影响 OpenSSH:6.2 版本(含)到 8.8 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://www.openssh.com/security.html
风险举证	OpenSSH:7.4

6	**OpenSSH 安全漏洞(CVE-2023-48795)**
风险等级	中
深信服漏洞编号	SF-0005-17304
CVE 编号	CVE-2023-48795

CNNVD 编号	CNNVD-202312-1668
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.6 之前版本存在安全漏洞，该漏洞源于允许远程攻击者绕过完整性检查，从而省略某些数据包。
风险影响	影响 OpenSSH:9.6 版本以下版本
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://www.openssh.com/openbsd.html
风险举证	OpenSSH:7.4

7	**OpenSSH 访问控制错误漏洞(CVE-2019-6110)**
风险等级	中
深信服漏洞编号	SF-0005-00643
CVE 编号	CVE-2019-6110
CNNVD 编号	CNNVD-201901-468
CNVD 编号	
Bugtraq 编号	106836
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。SCP（Secure Copy Protocol）是一个远程文件复制协议。OpenSSH 中的 SCP 客户端实用程序存在安全漏洞。攻击者可利用该漏洞伪造被显示的文件名。
风险影响	影响 OpenSSH:7.9 以下版本(含)
解决方案	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://www.openssh.com/
风险举证	OpenSSH:7.4

8	**OpenSSH 安全漏洞(CVE-2016-20012)**
风险等级	中
深信服漏洞编号	SF-0005-10926

CVE 编号	CVE-2016-20012
CNNVD 编号	CNNVD-202109-1073
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。OpenSSH 8.7 之前版本存在安全漏洞，允许远程攻击者怀疑 SSH 服务器知道用户名和公钥的特定组合，以测试这种怀疑是否正确。 发生这种情况是因为仅当该组合对登录会话有效时才会发送质询。
风险影响	影响 OpenSSH:8.7 版本(含)以下版本
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://github.com/openssh/openssh-portable/pull/270
风险举证	OpenSSH:7.4

9	**OpenSSH 信息泄漏漏洞(CVE-2018-15919)**
风险等级	中
深信服漏洞编号	SF-0005-00645
CVE 编号	CVE-2018-15919
CNNVD 编号	CNNVD-201808-902
CNVD 编号	
Bugtraq 编号	105163
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.8 及之前版本中的 auth-gss2.c 文件存在信息泄漏漏洞。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。*重点:使用 GSS2 时会存在漏洞
风险影响	影响 OpenSSH:5.9 版本(含)到 7.8 版本(含)
解决方案	建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：https://www.openssh.com/
风险举证	OpenSSH:7.4

10	**OpenSSH 安全漏洞(CVE-2023-51767)**

风险等级	中
深信服漏洞编号	SF-0005-17308
CVE 编号	CVE-2023-51767
CNNVD 编号	CNNVD-202312-2216
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.6 及之前版本存在安全漏洞，该漏洞源于当使用常见类型的 DRAM 时，mm_answer_authpassword 中已验证的整数值不能抵抗单个比特的翻转，导致攻击者可以绕过身份验证。
风险影响	影响 OpenSSH:9.6 版本(含)以下版本
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://www.openssh.com/txt/release-9.6
风险举证	OpenSSH:7.4

11	**OpenSSH 访问控制错误漏洞(CVE-2019-6109)**
风险等级	中
深信服漏洞编号	SF-0005-00642
CVE 编号	CVE-2019-6109
CNNVD 编号	CNNVD-201901-467
CNVD 编号	
Bugtraq 编号	106843
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 中存在安全漏洞，该漏洞源于程序没有对字符进行编码。攻击者可利用该漏洞伪造被显示的文件名。
风险影响	影响 OpenSSH:7.9 以下版本(含)
解决方案	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://www.openssh.com/
风险举证	OpenSSH:7.4

12	OpenSSH 安全漏洞(CVE-2023-51384)
风险等级	中
深信服漏洞编号	SF-0005-17307
CVE 编号	CVE-2023-51384
CNNVD 编号	CNNVD-202312-1662
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.6 之前版本存在安全漏洞,该漏洞源于当在添加 PKCS11 托管私钥的过程中指定目标约束时，这些约束仅应用于第一个密钥。
风险影响	影响 OpenSSH:9.6 版本以下版本
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://www.openssh.com/txt/release-9.6
风险举证	OpenSSH:7.4

13	OpenSSH 用户枚举漏洞(CVE-2018-15473)
风险等级	中
深信服漏洞编号	SF-0005-17302
CVE 编号	CVE-2018-15473
CNNVD 编号	CNNVD-201808-536
CNVD 编号	CNVD-2018-20960
Bugtraq 编号	105140
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 7.7 及之前版本存在一个用户枚举漏洞，原因是在完全解析含有请求的报文之前不能推迟对无效验证用户的救助。此漏洞与 auth2-gss.c、auth2-hostbased.c 和 auth2-pubkey 相关。
风险影响	影响 OpenSSH:7.7 版本(含)以下版本

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://www.openssh.com/txt/release-9.6
风险举证	OpenSSH:7.4

14	OpenSSH 输入验证错误漏洞(CVE-2019-6111)
风险等级	中
深信服漏洞编号	SF-0005-00644
CVE 编号	CVE-2019-6111
CNNVD 编号	CNNVD-201901-767
CNVD 编号	CNVD-2019-02499
Bugtraq 编号	106741
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 中的 scp client 实用程序存在安全漏洞，该漏洞源于程序错误的验证了对象名称。攻击者可利用该漏洞覆盖文件。
风险影响	影响 OpenSSH:7.9 以下版本(含)
解决方案	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： https://www.openssh.com/
风险举证	OpenSSH:7.4

15	OpenSSH 访问限制绕过漏洞(CVE-2018-20685)
风险等级	中
深信服漏洞编号	SF-0005-13834
CVE 编号	CVE-2018-20685
CNNVD 编号	CNNVD-201901-347
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。OpenSSH 7.9 版本，scp 客户端的 scp.c 文件存在安全漏洞。远程攻击者可借助.文件名或空文件名，利用该漏洞绕过访问限制。

风险影响	影响 OpenSSH:8.0 版本以下版本
解决方案	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2
风险举证	OpenSSH:7.4

16	OpenSSH 安全漏洞(CVE-2023-51385)
风险等级	中
深信服漏洞编号	SF-0005-17305
CVE 编号	CVE-2023-51385
CNNVD 编号	CNNVD-202312-1665
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.6 之前版本存在安全漏洞，该漏洞源于存在操作系统命令注入漏洞。
风险影响	影响 OpenSSH:9.6 版本以下版本
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://www.openssh.com/txt/release-9.6
风险举证	OpenSSH:7.4

17	OpenSSH 信息泄露漏洞(CVE-2020-14145)
风险等级	中
深信服漏洞编号	SF-0005-10927
CVE 编号	CVE-2020-14145
CNNVD 编号	CNNVD-202006-1822
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于

	安全访问远程计算机的连接工具。OpenSSH 5.7 至 8.3 版本的客户端存在信息泄露漏洞。该漏洞产生的原因是 OpenSSH 客户端中的可观察到的差异会导致算法协商过程中的信息泄露。中间人攻击者可利用该漏洞攻击初始连接尝试。
风险影响	影响 OpenSSH:5.7 版本(含)到 8.4 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：http://www.openbsd.org/security.html
风险举证	OpenSSH:7.4

18	SSH 服务器支持的算法发现【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-01026
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	用来获取 SSH 服务器支持的算法列表
风险影响	
解决方案	无影响
风险举证	-

19	OpenSSH 授权问题漏洞(CVE-2021-36368)
风险等级	低
深信服漏洞编号	SF-0005-11776
CVE 编号	CVE-2021-36368
CNNVD 编号	CNNVD-202203-1230
CNVD 编号	
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。 OpenSSH 8.9 之前的版本中存在安全漏洞。该漏洞源于客户端使用带代理转发但没有 -oLogLevel=verbose

	的公钥身份验证。
风险影响	影响 OpenSSH:8.9 版本以下版本
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://www.openssh.com/security.html
风险举证	OpenSSH:7.4

20	**OpenSSH CBC 模式信息泄露漏洞(CVE-2008-5161)【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00587
CVE 编号	CVE-2008-5161
CNNVD 编号	CNNVD-200811-32
CNVD 编号	CNVD-2009-12630
Bugtraq 编号	
风险端口	22
风险描述	OpenSSH（OpenBSD Secure Shell）是 OpenBSD 计划组所维护的一套用于安全访问远程计算机的连接工具。如果配置为 CBC 模式的话，OpenSSH 没有正确地处理分组密码算法加密的 SSH 会话中所出现的错误，导致可能泄露密文中任意块最多 32 位纯文本。在以标准配置使用 OpenSSH 时，攻击者恢复 32 位纯文本的成功概率为 2^{-18}，此外另一种攻击变种恢复 14 位纯文本的成功概率为 2^{-14}。
风险影响	攻击者可以利用该信息进行下一步攻击。
解决方案	在 SSH 会话中仅使用 CTR 模式加密算法，如 AES-CTR。
风险举证	当前 openssh 为 CBC 模式，成功读取到泄露文本，检测存在漏洞

5.1.2 web 漏洞

1	**CORS(跨站资源共享)原始验证失败【原理扫描】**
风险等级	高
深信服漏洞编号	SF-2022-00935
CVE 编号	-
CNNVD 编号	
CNVD 编号	

Bugtraq 编号	
风险端口	12008
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。
风险举证	举证描述： - 页面：17.167.7.7 请求： GET / HTTP/1.1 Host: 17.167.7.7:12008 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Origin: https://www.evil.com 响应： HTTP/1.1 404 Access-Control-Allow-Origin: https://www.evil.com Access-Control-Allow-Credentials: true Access-Control-Allow-Methods: POST, PUT, GET, OPTIONS, DELETE Access-Control-Allow-Headers: Authorization, Content-Type,X-Requested-With Access-Control-Max-Age: 3600 Vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers Content-Type: application/json Date: Tue, 25 Mar 2025 10:12:08 GMT Connection: close

	{"timestamp":"2025-03-25T10:12:08.896+00:00","status":404,"error":"Not Found","path":"/"}

2	CORS(跨站资源共享)原始验证失败【原理扫描】
风险等级	高
深信服漏洞编号	SF-2022-00935
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12378
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。
风险举证	举证描述： - 页面：17.167.7.7 请求： GET / HTTP/1.1 Host: 17.167.7.7:12378 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Origin: https://www.evil.com

	响应： HTTP/1.1 404 Access-Control-Allow-Origin: https://www.evil.com Access-Control-Allow-Credentials: true Access-Control-Allow-Methods: POST, PUT, GET, OPTIONS, DELETE Access-Control-Allow-Headers: Authorization, Content-Type,X-Requested-With Access-Control-Max-Age: 3600 Vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers Content-Type: application/json Date: Tue, 25 Mar 2025 10:14:43 GMT Connection: close {"timestamp":"2025-03-25T18:14:44.864+08:00","status":404,"error":"Not Found","path":"/"}

3	**CORS(跨站资源共享)原始验证失败【原理扫描】**
风险等级	高
深信服漏洞编号	SF-2022-00935
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12333
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。
风险举证	举证描述： -

	页面：17.167.7.7 请求： GET / HTTP/1.1 Host: 17.167.7.7:12333 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive Origin: https://www.evil.com 响应： HTTP/1.1 404 Access-Control-Allow-Origin: https://www.evil.com Access-Control-Allow-Credentials: true Access-Control-Allow-Methods: POST, PUT, GET, OPTIONS, DELETE Access-Control-Allow-Headers: Authorization, Content-Type,X-Requested-With Access-Control-Max-Age: 3600 Vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers Content-Type: application/json Date: Tue, 25 Mar 2025 10:11:22 GMT Connection: close {"timestamp":"2025-03-25T10:11:23.123+00:00","status":404,"error":"Not Found","path":"/"}

4	**Host 头攻击 安全漏洞【原理扫描】**
风险等级	中
深信服漏洞编号	SF-2019-00222
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	8080
风险描述	主机头攻击：许多 web 服务器都会在同一主机上托管多个 web 应用程序（虚拟主机），web 服务将根据用户 HTTP 请求中的 host 头来判断该请求

	应交由哪个 web 应用处理，HTTP 请求头是用户可控的，一般当用户输入了不在 web 服务配置中的 host 头时，web 服务会默认由配置中的第一个 web 应用处理，此时就将错误的 host 头传入到了 web 应用之中，若 web 应用在运行过程中需要使用 host 头，将会导致非预期的行为，这包括： 1. 缓存中毒：若主机部署在缓存设备(如 CDN)之后，攻击使用恶意的 HOST 头访问目标站点能导致错误的内容被缓存，其他正常的用户访问站点时将获取到错误的数据，包括有危害的攻击数据。 2. 任意重定向：恶意攻击者将使用户被重定向到任何恶意的网站。 3. 密码重置：在重置密码时，网站通常会根据自身地址生成一个带有随机 TOKEN 的重置链接，并将其发送到用户邮箱，当存在漏洞时攻击者能控制链接的域名，用户点击重置链接将跳转到用户控制的网站，攻击者能因此获取随机 token 重置受害者密码。 需要注意不只 HOST 头可能受影响，X-Forwarded-Host 可能会覆盖 HOST 的值，从而导致 HOST 头攻击。
风险影响	可能导致 HTML 注入，XSS 漏洞等。
解决方案	在代码里正确验证用户提供的输入，不直接使用用户的请求头部，例如 PHP 代码在获取自身 URL 时不使用 _SERVER['HOST'] 而使用 $_SERVER['SERVER_NAME'] 正确配置 web 服务，将所有预期外的 HOST 头部全部交由一个无用的虚拟主机处理，注意一般该主机配置应该放在第一个位置上。对于 nginx 可参考：https://www.nginx.com/resources/wiki/start/topics/examples/server_blocks/ ，对于 apache 可参考：http://httpd.apache.org/docs/trunk/vhosts/examples.html#defaultallports。其他 web 服务请查阅官方手册进行配置。
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: www.sangfor.com.cn:45904 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive X-Forwarded-Host: 17.167.7.7 响应： HTTP/1.1 302

	X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: http://www.sangfor.com.cn:45904/jointos/app Content-Type: text/html;charset=ISO-8859-1 Content-Length: 0 Date: Tue, 25 Mar 2025 10:12:01 GMT Connection: keep-alive Keep-Alive: timeout=50

5	**未设置 X-XSS-Protection 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00872
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12300
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive

	响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

6	**未设置 X-Content-Type-Options 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00871

CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	80
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:12:52 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title>

	<style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

7	**未设置 Referrer-Policy 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2022-00436
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12300
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

	For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

8	**未设置 X-Content-Type-Options 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00871
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12300
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应：

	HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

9	**未设置 X-Download-Options 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2022-00438
CVE 编号	-
CNNVD 编号	
CNVD 编号	

Bugtraq 编号	
风险端口	80
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:12:52 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body>

	Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

10	**未设置 X-Download-Options 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2022-00438
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12300
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive

	响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

11	未设置 X-Permitted-Cross-Domain-Policies 响应头【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00439
CVE 编号	-
CNNVD 编号	

CNVD 编号	
Bugtraq 编号	
风险端口	80
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:12:52 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; }

	</style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

12	**点击劫持:无 X-Frame-Options 头信息【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00874
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	80
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');
风险举证	举证描述： - 页面：17.167.7.7

请求：

```
GET  HTTP/1.1
Host: 17.167.7.7:80
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

响应：

```
HTTP/1.1 200 OK
Server: nginx/1.23.3
Date: Tue, 25 Mar 2025 10:12:52 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT
Connection: keep-alive
ETag: "64a61be7-267"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully
installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
```

	</body> </html>

13	未设置 Referrer-Policy 响应头【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00436
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	80
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive

	响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:12:52 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

14	**未设置 Strict-Transport-Security 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00873
CVE 编号	-
CNNVD 编号	

CNVD 编号	
Bugtraq 编号	
风险端口	12300
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head>

	<title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

15	点击劫持:无 X-Frame-Options 头信息【原理扫描】
风险等级	低
深信服漏洞编号	SF-2021-00874
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12300
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');
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to

	nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

16	未设置 X-Permitted-Cross-Domain-Policies 响应头【原理扫描】
风险等级	低
深信服漏洞编号	SF-2022-00439
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	12300
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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:12300 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:15:03 GMT

	Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

17	**未设置 X-XSS-Protection 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00872
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	80

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
风险举证	举证描述： - 页面：17.167.7.7 请求： GET HTTP/1.1 Host: 17.167.7.7:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:12:52 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style>

	</head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

18	**未设置 Strict-Transport-Security 响应头【原理扫描】**
风险等级	低
深信服漏洞编号	SF-2021-00873
CVE 编号	-
CNNVD 编号	
CNVD 编号	
Bugtraq 编号	
风险端口	80
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
风险举证	举证描述： - 页面：17.167.7.7 请求：

	GET HTTP/1.1 Host: 17.167.7.7:80 User-Agent: python-requests/2.23.0 Accept-Encoding: gzip, deflate Accept: */* Connection: keep-alive 响应： HTTP/1.1 200 OK Server: nginx/1.23.3 Date: Tue, 25 Mar 2025 10:12:52 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Thu, 06 Jul 2023 01:41:59 GMT Connection: keep-alive ETag: "64a61be7-267" Accept-Ranges: bytes <!DOCTYPE html> <html> <head> <title>Welcome to nginx!</title> <style> html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style> </head> <body> Welcome to nginx! If you see this page, the nginx web server is successfully installed and working. Further configuration is required. For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com. Thank you for using nginx. </body> </html>

5.1.3 弱口令

该资产不存在弱口令风险。

5.1.4 登录入口

该资产不存在 web 登录入口。
系统登录入口详情如下：

序号	登录入口名称	端口	弱口令数	漏洞数
1	SSH 登录入口发现	22	0	20

6 参考标准

6.1 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
严重	9 <= 漏洞风险值 <= 10	漏洞可能导致系统崩溃、数据泄露等严重后果，易受攻击，影响范围广，修复难度大，需要立即修复。
高危	7 <= 漏洞风险值 < 9	漏洞可能导致系统受到攻击或数据被盗取，易受攻击，影响范围较广，修复难度较大，需要尽快修复。
中危	4 <= 漏洞风险值 < 7	漏洞可能导致系统受到攻击或数据泄露，易受攻击，影响范围较小，修复难度一般，需要在合理的时间内修复。
低危	0 <= 漏洞风险值 < 4	漏洞可能导致系统受到攻击或数据泄露的风险较小，不易受攻击，修复难度较小，可以在合理的时间内修复。

6.2 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
严重	9 <= 漏洞风险值 <= 10	漏洞可能导致系统崩溃、数据泄露等严重后果，易受攻击，影响范围广，修复难度大，需要立即修复。
高危	7 <= 漏洞风险值 < 9	漏洞可能导致系统受到攻击或数据被盗取，易受攻击，影响范围较广，修复难度较大，需要尽快修复。
中危	4 <= 漏洞风险值 < 7	漏洞可能导致系统受到攻击或数据泄露，易受攻击，影响范围较小，修复难度一般，需要在合理的时间内修复。
低危	0 <= 漏洞风险值 < 4	漏洞可能导致系统受到攻击或数据泄露的风险较小，不易受攻击，修复难度较小，可以在合理的时间内修复。

6.3 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	资产只发现中危及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

6.4 安全建议

2017 年 6 月 1 日起《中华人民共和国网络安全法》（下文简称《网络安全法》）正式实施。这意味着网络运营者（指网络的所有者、管理者和网络服务提供者）必须担负起履行网络安全的法律责任。

随着网络安全技术的不断发展，道高一尺魔高一丈，网络安全的本质就是人与人的对抗和博弈，没有百分之百的安全，也没有百分之百的成功入侵，但网络安全的门槛永远是可以不断提高的。外网安全防护只是网络运营企业网络安全的第一道防线，真正的对抗仍然是发生在具有核心业务系统及核心业务数据的内网，内网才是真正的主战场。近几年，各大网络安全事件无不印证此观点，无论是国内 CSDN、163、12306 等用户个人信息泄漏事件，还是境外针对全球特定目标的 APT 攻击，如：“丰收行动”、摩诃草事件、震网病毒事件等，都是突破外网安全防护的第一道防线，长期潜伏于内网而未被及时检测和发现导致的。

因此，外网安全防护是网络安全的第一道防线，真正的网络安全主战场仍然是内网网络安全。针对内网安全，我们建议采用如下措施来降低内网安全风险：

- 内网业务系统在设计阶段，需要考虑安全机制、安全设备和安全管理等因素
- 内网安全域划分，对内网不同业务系统，按照安全风险等级要求进行安全域划分

- 请专业人员定期对内网进行渗透测试，发现安全漏洞，及时修复
- 请专业人员定期对内网弱口令进行排查，加强弱口令安全管理，对业务系统密码复杂度进行要求，如：长度至少 8 位，包含字母、数字、特殊字符等
- 对内部人员进行安全意识培训，通过管理手段和安全意识培训降低内网安全风险事件的发生
- 对关键业务系统进行定期备份