忻州市生态环境局
网络安全检查报告

山西护网信息科技有限公司

2024 年 11 月

声　明

本报告是对忻州市生态环境局进行网络安全检查基础上得出的客观评估结果。

本报告作为本次检查结果，仅对检查时间段内被指定范围的信息系统现有的状况有效，检查后系统出现任何变更，本报告的结果不再适用。

考虑到检查工作的时间、范围限制以及检查技术的局限性，被检查信息系统可能仍存在未发现的安全风险。

山西护网信息科技有限公司

2024 年 11 月 26 日

概　要

受中共忻州市委网络安全和信息化委员会办公室委托，山西护网信息科技有限公司于2024年11月19日对忻州市生态环境局开展了网络安全检查工作。本次检查工作目的是增强网络安全意识、识别网络安全风险、指导网络安全建设、提高网络安全管理水平、提升网络安全技术能力。

经过多年的发展，忻州市生态环境局的信息化建设已经取得了显著成效，特别是在重点污染源自动监控与基础数据库系统方面，极大地提升了忻州市生态环境局的信息化管理水平和工作效率。然而，在本次网络安全检查中，发现这些系统还存在着一些潜在的安全风险，需要进一步优化和加固，以确保系统的稳定性和安全性。本次检查过程中发现的主要安全问题如下:

（1）网络安全符合性检查：

符合性检查项目共40项，其中符合项共28项，部分符合项共5项，**不符合项共7项，不涉及项共0项。符合率为82.50%。**符合性检查发现的问题主要集中在:

①未明确网络安全和数据安全的职能部门和相应岗位;

②未定期对管理制度进行评审和修订;

③未配备网络安全专职人员;

④未建立第三方人员的安全管理细则，明确第三方人员职责、保

密、考核细则等管理要求。

（2）网络安全技术检查:

主机漏洞检查: 发现主机安全漏洞共 0 个，包括可利用紧急漏洞 0 个，包括高危安全漏洞 0 个，中危漏洞 0 个，低危漏洞 0 个。相关信息详见附件 1《主机漏洞检查报告》。

网站漏洞检查: 发现**网站安全漏洞共 14 个，包括高危安全漏洞 0 个，中危漏洞 2 个，低危漏洞 10 个，信息漏洞 2 个。**系统存在紧急和高危安全漏洞可能导致黑客攻击从外网控制服务器，造成网络安全事件的发生。相关信息详见附件 2《网站漏洞检查报告》。

基线配置检查: 发现 **156 个高危项，80 个中危项。**相关信息详见附件 3《基线配置检查报告》。

建议忻州市生态环境局根据本检查评估报告中的修复建议及时进行整改，提高忻州市生态环境局的网络安全防护水平。

目　录

第 1 章　检查任务概述

1.1 检查对象

本次网络安全检查的对象是忻州市生态环境局，具体包括网络设备、安全防护设备、服务器、终端设备以及相关业务系统等。

1.2 检查目的

通过开展网络安全检查工作，全面准确掌握网络安全工作现状。科学评估面临的网络安全风险，以查促管、以查促防、以查促改、以查促建。增强安全意识，落实安全责任，系统评估安全状况，安全排查安全隐患，完善安全防护措施，预防和减少网络安全事件的发生，保障重要网络与信息系统的政治安全、运行安全和数据安全。

1.3 检查原则

为保障现场检查工作能顺利有效开展，现场检查过程将遵循以下工作原则：

表 1-1 网络安全检查原则

序号	原则	具体说明
1	规范性原则	根据本项目工作方案，在实施过程中对人员、质量、时间进度进行严格管控。
2	标准化原则	严格遵守国家和行业的相关法律法规、标准，并参考国际的标准来实施
3	整体性原则	包括测试内容完整性和测试流程整体性和完整性
4	保密性原则	在进行信息安全测试的过程中，严格遵守保密原则，确保所涉及的任何用户保密信息，不会泄露给第三方单位和个人，不利用这些信息损害用户利益。
5	敏感信息保护原则	对于检查中涉及的敏感信息，做到不扩散、不破坏，避免对被检查单位造成不良影响。

6	交互性原则	在进行信息安全测试过程中，保持与受检查方相关负责人员进行沟通交流，共同挖掘系统存在的安全漏洞和管理漏洞，从而保证项目执行的效果并提高受测试方的安全技能和安全意识。
7	最小影响原则	测试方将从项目管理和技术应用的层面，与受检查方进行充分沟通，考虑测试对目标系统的正常运行可能产生的不利影响，将风险降到最低，在不影响目标系统正常运行的情况下同时保证项目实施的有效性。
8	可控性原则	实施检查的人员为本单位的正式员工，实施检查的工具全部经过安全测试验证，保证检查的安全可控。

1.4 检查依据

①《信息安全技术信息安全检查规范》（GB/T20984-2007）

②《信息安全技术信息安全检查实施指南》（GB/T31509-2015）

③《信息安全技术信息安全风险管理指南》（GB/Z24364-2009）

④《信息安全技术主机安全加固系统安全技术要求》(GA/T1393-2017)

⑤《计算机信息系统 安全保护等级划分准则》（GB17859-1999）

⑥《信息安全技术信息系统安全管理要求》（GB/T20269-2006）

⑦《信息安全技术信息系统安全管理评估要求》（GB/T28453-2012）

⑧《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

⑨《信息安全技术信息安全事件分类分级指南》（GB/Z20986-2007）

⑩《计算机场地通用规范》（GB/T2887-2011）

⑪《计算机场地安全要求》（GB/T9361-2011）

1.5 检查时间

2024 年 11 月 19 日

1.6 检查人员

表 1-2 检查人员清单

姓名	职务	职责
高宏伟	组长	负责检查全面工作、综合协调
许茂州	组员	符合性检查、制度检查、人员访谈
李安栋	组员	技术检查

第 2 章　网络拓扑图

图 2-1 忻州市生态环境局网络拓扑图

该省级网络系统采用多层分级架构，以省、市两级为单位。省级网络与市级政务外网互联，承载省级数据和应用；市级网络承载本地政务数据，连接省级网络和互联网。设有市级数据共享交换平台和视频应用服务器，分别用于数据管理和视频监控业务。网络接入提供无线连接，支持移动设备和远程传输。互联网用于有限访问和数据共享。视频监控系统负责捕获并传输实时画面至服务器或共享平台。总体特点为政务外网隔离、数据集中共享。

第 3 章　被检查系统情况

3.1 被检查系统描述

重点污染源自动监控与基础数据库系统：该系统分为两部分，基础数据库系统主要用于企业基本信息的录入和管理，新建用户和给用户授权企业信息等。污染源自动监控系统主要用于企业数据的查看、数据修约、监控点设备验收信息录入和企业停运录入超标和异常的汇总。

3.2 定级备案情况

经确认受检单位名称受检单位名称定级备案情况为：

重点污染源自动监控与基础数据库系统：☐4 级、☐3 级、☑2 级、☐尚未定级

第 4 章　设备资产情况

本次网络安全检查涉及的设备资产包括服务器 6 台。详情见附件 1《主机漏洞检查报告》、附件 2《网站漏洞检查报告》、附件 3《基线配置检查报告》。

第 5 章　检查内容与方法

5.1 检查内容

本次网络安全检查主要包括符合性检查和网络安全技术检查两部分。符合性检查主要是通过对安全管理机构、人员安全管理、系统运维安全、物理安全、基础网络安全、应用安全、安全漏洞扫描、系统建设安全、供应链安全、云计算服务安全等 10 大项适用项进行现场检查，全面分析管理制度和网络安全防护中的薄弱环节。技术检查主要是通过漏洞扫描、日志查看、流量分析等技术手段，发现信息系统存在的安全漏洞。综合评估关键信息基础设施管理和技术两方面存在的安全风险和隐患，提出整改建议和意见，推动该单位完善关键信息基础设施网络安全责任制和防范体系。

5.2 检查方法

本次网络安全检查的方法包括人员访谈、文档查验、技术检查等。

①人员访谈：检查人员通过对被测系统管理、开发、运维等人员进行访谈，核实规章制度落实、安全手段实施、应急处理等方面是否存在薄弱环节。

②文档查验：检查人员通过查阅规章制度、日常运维材料等文档，核对安全管理是否满足相关政策和标准要求，是否存在安全隐患。

③技术检查：检查人员通过技术手段，验证网络设备、安全设备、主机系统、数据库、应用系统在安全配置、安全管理、安全防护措施等方面是否存在安全漏洞和隐患。

5.3 技术检查流程

本次网络安全技术检查流程定义为如下阶段。

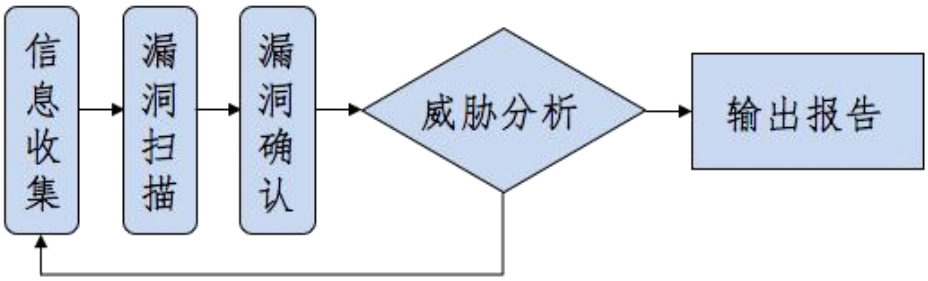


图 5-1 网络安全技术检查流程

①信息收集:此阶段中,检查人员进行必要的信息收集,如 IP 地址、DNS 记录、软件版本信息、IP 段、互联网中的公开信息等。

②漏洞扫描: 此阶段中，检查人员通过漏洞扫描工具，对指定的信息系统的安全脆弱性进行检查，发现可利用漏洞和缺陷。

③漏洞确认: 此阶段中，检查人员尝试确认漏洞扫描阶段发现的可利用漏洞和缺陷。在时间许可的情况下，必要时从第一阶段重新进行。

④威胁分析: 此阶段中，检查人员对发现的上述问题进行威胁分类和分析其影响。

⑤输出报告: 此阶段中，检查人员根据检查和分析的结果编写直观的技术检查报告。

5.4 检查工具

表 5-1 检查工具列表

常用工具名称	工具描述
NSFOCUS RSAS	全方位检查 IT 系统存在的各类脆弱性风险，发现系统存在的安全漏洞、安全配置问题，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计。
Nessus	目前全球流行的系统漏洞扫描与分析软件，它可同时在本机或远程进行系统的漏洞分析扫描。
Metasploit	开源的安全漏洞检查工具。它是一个功能强大的开源平台，可以自由

	获取的渗透测试框架软件，供开发，测试和使用恶意代码。渗透测试人员利用这个框架可以进行灵活的渗透测试。
Nmap	用来探测计算机网络上的主机和服务的一种安全扫描器。它能够用来探测目标主机所开放的端口，通过对设备或者防火墙的探测来审计它的安全性。
AWVS	知名的 Web 网络漏洞扫描工具，它通过网络爬虫测试网站的安全，检查系统中存在的安全漏洞。
Burp suite	用于攻击 Web 应用程序的渗透测试集成平台。Burp 套件允许一个攻击者将人工的和自动的技术结合起来，以列举、分析、攻击 Web 应用程序，或利用这些程序的漏洞。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。
sqlmap	一款用来检查和利用 SQL 注入漏洞的开源工具。
Navicat Premium	它是一个可多重链接的数据库管理工具，可以单一程序同时连接到 MySQL、Oracle、PostgreSQL、SQLite 及 SQL Server 数据库，使管理不同类型的数据库更加方便。
IT 及工控系统安全配置核查系统	一款用于 IT 基础设备脆弱性检查的扫描工具。具有远程和本地对 IT 设备进行安全配置检查的能力，能够检查信息系统中的主机操作系统、数据库、网络设备、应用服务等。
Superscan	Windows 平台下快速的端口扫描工具，可以快速扫描服务器开放 TCP 端口/UDP 端口。除此之外，它还附带了一些其他功能，比如 ip 域名相互转换、Ping 功能、验证服务器提供的服务类别等。
Hscan	运行在 Windows NT/2000/XP 下多线程方式对指定 IP 段(指定主机)，或主机列表，进行漏洞、弱口令账号、匿名用户检查的工具。
Solarwinds	基于 SNMP 网络管理协议的管理软件，可监控任何 SNMP 指标。
Okscan	集攻击面管理、资产探测与管理、脆弱性风险发现、威胁诱捕、主机安全、流量监测等能力于一体

【注】以上所列检查工具仅为常用工具，实际检查过程不限于以上工具。

第 6 章　检查结果

6.1 符合性检查结果

检查小组通过查验文档、人员访谈、现场检查等方式，从网络安全责任制落实情况、网络安全日常管理情况、网络安全技术防护情况、网络安全应急工作情况、网络安全教育培训情况、技术检查及网络安全事件情况等方面对忻州市生态环境局进行了评估，现场评估结果如下：

表 6-1 网络安全符合项检查表

序号	检查项目	检查内容	检查内容描述
1	安全管理机构	1. 组织架构设置、岗位设置（需要明确网络安全和数据安全的职能部门和相应岗位）	不符合
		2. 人员配备：应配备系统管理员、审计管理员和安全管理员并明确各岗位人员配备情况	部分符合（无审计管理员和安全管理员）
		3. 管理制度建立和落实：建立由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系，覆盖机房安全管理、办公环境安全管理、网络和系统安全管理供应商管理、变更管理、备份和恢复管理、软件开发管理等方面，并配套制定相应的操作表单，做好日常操作记录	符合
		4. 管理制度评审和修订：应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订	符合
		5. 合作方管理：应建立第三方合作单位管理制度，明确保密、安全责任等管理内容。建立并及时更新外联单位联系列表，包括外	部分符合（无相关

		联单位名称、合作内容、联系人和联系方式等信息	文件）
2	人员安全管理	1.本单位人员管理制度：应建立本单位从业人员安全管理细则，明确岗位职责、考核细则等管理要求	符合
		2.人员配置:应配备网络安全专职人员，不可兼任	不符合
		3.安全培训:应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训	符合
		4.外部人员管理：应建立第三方人员的安全管理细则，明确第三方人员职责、保密、考核细则等管理要求，并加强外部人员现场管理	不符合
3	系统运维安全	1.风险预警管理：应采取必要的措施识别安全风险，及时发布风险预警	符合
		2.环境管理：应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定	符合
		3.漏洞和事件管理：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患进行修补，或评估可能的影响后进行修补；应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题，应制定安全事件报告和处置管理制度	不符合
		4.网络和系统安全管理：运维变更记录，严格管理、做好记录；无违反规定的上网行为管理；委托第三方对系统进行测试，出具安全测试报告。	部分符合（无安全测评报告）
		5.备份与恢复管理：应规定备份信息的备份方式、备份频度、存储介质、保存期等	不符合
		6.应急预案管理：应急预案是否制定，且内容齐全，是否对系统相关人员进行了应急预案的培训，和定期演练	符合
		7.定期开展安全检查：系统日常运行、系统漏洞和数据备份等情况；何时检查的，发现的问题，以及整改情况	不符合
		8.定期开展一致性检查：安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	不符合

		9. 运维工具管控措施：运维工具是什么，是否合规，工具是否经过合规审批或是控制，运维完成后是否删除敏感数据	符合
		10. 运行监控措施：网络链路、安全设备、网络设备、服务器等是否有运行监控措施。	符合
		11. 外部人员接入网络管理措施：管理制度中明确外部人员接入受控网络访问系统的申请、审批流程，以及相关安全控制要求，且可记录并提供外部人员接入受控网络访问系统的申请、审批等相关记录证据；管理制度中规定外部连接的授权和审批流程，也要求定期进行相关的巡检，并通过技术手段对违规上网及其他违反网络安全策略的行为进行有效控制、检查、阻断	部分符合（无相关记录留存）
4	物理安全	1. 物理位置合理性：具体物理机房位置，云计算服务商具体名称	符合
5	基础网络安全	1. 网络架构：是否定期更新网络拓扑图，是否分区分域，重要区域是否做安全隔离手段	符合
		2. 网络设备业务处理能力：核心交换机、核心路由器、边界防火墙是否满足业务高峰需求，性能指标在 80%以下	符合
		3. 通信网络:应采用密码技术保证通信过程中数据的完整性/保密性	符合
		4. 边界防护:需对内部外联至外部的网络进行检查或限制，需保障无线网络受控后进行连接	符合
		5. 防护措施：在网络节点处限制网络攻击行为；需对恶意代码和垃圾邮件进行检查清除。是否设置相关策略	符合
		6. 是否有安全审计措施，日志是否全面，时间是否满足 180 天	符合
6	应用安全	1. 系统默认账号要重命名、修改弱口令、删除离职人员账户，或是由专人管理，是否关闭不必要的服务、端口	符合
		2. 开启安全审计功能，对用户行为和事件进行审计。	符合
		3. 是否进行漏洞测试，进行修补，且进行数据备份。	符合
		4. 开源软件使用：系统开发者、运维者是否使用了开源代码管理平台或产品，是否修改了默认配置和访问控制策略	符合

7	安全漏洞扫描	1.主机扫描：服务器、中间件、数据库等的安全漏洞扫描	完成
		2.口令扫描：弱口令扫描	完成
		3.Web 扫描：发现网站存在的 SQL 注入、网页木马等安全漏洞	完成
		4.安全配置核查：对操作系统、中间件、主机等开展策略、账号、口令、授权、日志、IP 协议等有关的安全特性	完成
8	系统建设安全	1.产品采购和使用：应确保网络安全产品采购和使用符合国家的有关规定	符合
		2.外包软件开发：开发单位需提供源代码，进行代码审计，确认后门和漏洞	符合
		3.测试验收:上线前必须做安全检查，出具安全测试报告，报告须包含密码应用安全性测试内容	符合
9	供应链安全	1.核心软硬件产品和服务：检查所使用的核心软硬件产品和服务是否有未公开的功能、隐蔽链接、协议端口，核心软硬件产品和服务是否有断供风险	符合
		2.开源软件使用：系统开发人员和运维人员是否使用了开源代码平台，是否修改了默认配置	符合
		3.开发商管理：是否对核心软硬件产品和服务和供应商进行审查，在采购合同中是否体系安全性要求；是否对开发商人员进行审查，包括不限于背景审查相关证明，提供证明文件	部分符合（无相关文件）
10	云计算服务安全	1. 虚拟机监控机制：应支持虚拟机之间、虚拟机与宿主机之间的隔离。应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机 与外部网络之间的安全访问控制	符合
		2. 虚拟化管理平台安全：应保证每个虚拟机能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保某个虚拟机崩溃 后不影响虚拟机监控器及其他虚拟机；应保证不同虚拟机之间的内存隔离，内存被释放或再分配给其他虚拟机前得到完全释放	符合
		3. 安全审计：审计范围应覆盖到服务器上的每个操作系统用户和数据库用户，审计记录应包括事件的日期、时间、类型、主体	符合

		标识、客体标识和结果等	

6.2 网络安全技术检查结果

6.2.1 主机漏洞检查

通过本次技术检查，检查人员未发现服务器存在漏洞，服务器较为安全。相关信息详见附件 1《主机漏洞检查报告》。

表 6-2 主机漏扫检查结果

存活主机数量	弱口令	可入侵	高危	中危	低危
6	0	0	0	0	0

6.2.2 网站漏洞检查

通过本次网络安全技术检查，发现**网站安全漏洞共 14 个，其中中危漏洞 2 个，低危漏洞 10 个，信息 2 个。**相关信息详见附件 2《网站漏洞检查报告》。

表 6-3 网站漏洞检查结果

网站数量	弱口令	可利用	高危	中危	低危	信息
1	0	0	0	2	10	2

【注】：高中危漏洞以国内外权威的 CVE 漏洞库和国家互联网应急中心 CNVD 漏洞库为基本判断依据；对于高危 Web 安全隐患，以国际上公认的开放式 Web 应用程序安全项目（OWASP，Open Web Application Security Project）确定的最新 Top10 中所列的 WEB 安全隐患判断作为判断依据。

6.2.3 基线配置检查

通过本次基线配置检查，发现 **156 个高危项，80 个中危项。**相关信息详见附件 3《基线配置检查报告》。

表 6-4 基线配置检查结果

序号	IP	高危项	中危项	低危项	小计
1	10.0.248.202	26	14	0	40
2	10.0.248.199	26	14	0	40

3	10.0.248.201	26	14	0	40
4	10.0.248.198	26	13	0	39
5	10.0.248.203	26	13	0	39
6	10.0.248.200	26	12	0	38
7	合计	156	80	0	236

6.2.4 风险程度说明

表 6-5 风险程度说明

风险程度	风险程度说明
高危风险	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。
中危风险	攻击者可以利用 Web 网站攻击其他用户，读取系统文件或后台数据库。
低危风险	攻击者可以获取某些系统、网站、文件的信息或冒用身份。
信息风险	攻击者可以获取网站相关信息，可能是非敏感信息。

6.2.5 接入点信息

表 6-6 网络安全检查接入点信息

IP 地址	10.0.248.202、10.0.248.203
网关	2.0.1.154
子网掩码	255.0.0.0
物理位置	忻州市生态环境局
是否允许直接访问	否

第 7 章　整改建议

7.1 符合性检查建议

序号	不符合项	整改建议
1	组织架构设置、岗位设置（需要明确网络安全和数据安全的职能部门和相应岗位）	明确网络安全和数据安全的职能部门，设立专门的网络安全和数据安全岗位。制定岗位说明书，明确各岗位的职责和要求。
2	人员配置:应配备网络安全专职人员，不可兼任	配备专职的网络安全人员，确保他们不兼任其他可能存在利益冲突的岗位。供必要的培训和资源，以确保网络安全人员能够胜任工作。
3	外部人员管理：应建立第三方人员的安全管理细则，明确第三方人员职责、保密、考核细则等管理要求，并加强外部人员现场管理	制定第三方人员安全管理细则，包括职责、保密协议、考核标准等。 加强对外部人员现场活动的监督和管理，确保他们遵守安全规定。
4	漏洞和事件管理：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患进行修补，或评估可能的影响后进行修补；应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题，应制定安全事件报告和处置管理制度	实施定期的安全漏洞扫描和隐患排查。对发现的安全漏洞和隐患及时进行修补，或在评估影响后制定修补计划。定期进行安全测评，形成报告，并根据报告采取措施。制定并实施安全事件报告和处置管理制度。
5	备份与恢复管理：应规定备份信息的备份方式、备份频度、存储介质、保存期等	规定备份信息的备份方式（如全备份、增量备份等）。确定备份频度（如每日、每周等）。选择合适的存储介质（如云存储、外部硬盘等）。 明确备份数据的保存期限。
6	定期开展安全检查：系统日常运行、系统漏洞和数据备份等情况；何时检查的，发	制定安全检查计划，包括检查时间、内容和责任人。检查系统日常运行状况、

	现的问题，以及整改情况	系统漏洞和数据备份情况。 记录检查结果，包括检查时间、发现的问题和整改情况。
7	定期开展一致性检查：安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	定期评估安全技术措施的有效性。 检查安全配置是否与安全策略保持一致。监督安全管理制度的执行情况，确保所有规定得到遵守。这些整改建议旨在帮助组织加强网络安全和数据安全，确保符合相关标准和法规要求。

7.2 网站漏洞检查建议

序号	网站	漏洞详情	解决方案	漏洞链接
1	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	此 Web 服务器支持通过 TLS 1.0 加密。TLS 1.0 不被认为是“强密码术”。根据 PCI 数据安全标准 3.2(.1)的定义和要求，在保护从网站往返的敏感信息时，TLS 1.0 并不被认为是"强加密"。根据 PCI，"2018 年 6 月 30 日是禁用 SSL/早前 TLS 并实施更安全的加密协议 TLS 1.1 或更高版本（强烈建议 TLS v1.2）的最后期限，以便满足 PCI 数据安全标准(PCI DSS)，保障支付数据的安全。 攻击者可能能够利用此问题实施中间人攻击，以及解密受影响的服务与客户端之间的通信。	建议禁用 TLS 1.0 并替换为 TLS 1.2 或更高版本。	漏洞链接 1:https://124.163.201.106:9999/
2	https://124.163.201.106:9999/amOnline/zdjk-company-base/logi	此 Web 服务器支持通过 TLS 1.1 加密。当目标是支付卡行业(PCI)数据安全标准(DSS)合规性时，建议（尽管在当时或书面上并不需要）使	建议禁用 TLS 1.1 并替换为 TLS 1.2 或更高版本。	漏洞链接 1:https://124.163.201.106:9999/

	n	用 TLS 1.2 或更高版本。根据 PCI，"2018 年 6 月 30 日是禁用 SSL/早前 TLS 并实施更安全的加密协议 TLS 1.1 或更高版本（强烈建议 TLS v1.2）的最后期限，以便满足 PCI 数据安全标准(PCI DSS)，保障支付数据的安全。 攻击者可能能够利用此问题实施中间人攻击，以及解密受影响的服务与客户端之间的通信。		
3	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	点击劫持（用户界面矫正攻击、UI 矫正攻击、UI 矫正）是一种恶意技术，诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制。服务器在 Content-Security-Policy 报头中未返回 frame-ancestors 指令，这意味着此网站存在遭受点击劫持攻击的风	配置您的 Web 服务器，使其包含带有 frame-ancestors 指令的 CSP 报头和 X-Frame-Options 报头。有关该报头可能值的更多信息，请查阅 Web 参考资料。	漏洞链接 1:https://124.163.201.106:9999/

		险。frame-ancestors 指令可被用于指示是否应允许浏览器在框架内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。 影响取决于受影响的 Web 应用程序。		
4	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	HTTP Cross-Origin-Embedder-Policy(COEP)响应标头可防止文档加载未明确授予文档权限(通过 CORP(en-US)或者 CORS)的任何跨域资源。	语法： Cross-Origin-Embedder-Policy:unsafe-none|require-corp。 unsafe-none：这是默认值。允许文档获取跨源资源，而无需通过 CORS 协议或 Cross-Origin-Resource-Policy 头。 require-corp：文档只能从相同的源加载资源，或显式标记为可从另一个源加载的资源。如果跨源资源支持 CORS，则 crossorigin 属性或 Cross-Origin-Resource-Policy 头必须使用它来加载资源，而不会被 COEP 阻止。	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login

5	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	HTTP Cross-Origin-Opener-Policy（COOP）响应标头允许您确保顶级文档不会与跨来源文档共享浏览上下文组。COOP 将处理隔离您的文档，如果潜在攻击者在弹出窗口中打开您的全局对象，他们将无法访问该对象，从而防止一系列被称为 XS-Leaks 的跨源攻击。	支持语法：Cross-Origin-Opener-Policy:unsafe-noneCross-Origin-Opener-Policy:same-origin-allow-popupsCross-Origin-Opener-Policy:same-origin	漏洞链接1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login
6	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	Cross-Origin-Resource-Policy 响应头会指示浏览器阻止对指定资源的无源跨域/跨站点请求。注意设置 Cross-Origin-Resource-Policy（跨域资源策略）可能会使文件下载失败：当从设置了 CORP 请求头的资源服务器下载资源时，浏览器会阻止用户使用“保存”或“另存为”按钮将文件保存到本地。在决定生产环境中是否使用这一特性（CORP）之前需要	支持语法：Cross-Origin-Resource-Policy:same-site|same-origin	漏洞链接1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login

		慎重考虑。		
7	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	Clear-Site-Data 响应头，表示清除当前请求网站有关的浏览器数据（cookie，存储，缓存）。它让 Web 开发人员对浏览器本地存储的数据有更多控制能力。	支持语法：//单个参数 Clear-Site-Data:cache //多个参数(用逗号分隔)Clear-Site-Data:cache,cookies//通配 Clear-Site-Data:*	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login
8	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	HTTP Permissions Policy 标头提供了一种机制，在文档中或文档中的任何<iframe>元素中可以允许或拒绝使用浏览器功能。	支持语法：Cross-Origin-Resource-Policy:same-site|same-origin|cross-origin	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login
9	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	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	1）修改服务端程序，给 HTTP 响应头加上 Referrer-Policy 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(Referrer-Policy,value) 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(Referrer-Policy:value)如果是 asp 服务端，可以使用如下方式	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login

		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。	添加 HTTP 响应头 Response.AddHeader Referrer-Policy,value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response=HttpResponse()response[Referrer-Policy]=value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response=make_response()response.headers[Referrer-Policy]=value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 Referrer-Policy 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：add_header Referrer-Policy value;如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：	

			Header add Referrer-Policy value。	
10	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	Web 服务器对于 HTTP 请求的响应头中缺少 Strict-Transport-Security，这将导致浏览器提供的安全特性失效。当 Web 服务器的 HTTP 头中包含 Strict-Transport-Security 头时，浏览器将持续使用 HTTPS 来访问 Web 站点，可以用来对抗协议降级攻击和 Cookie 劫持攻击。其可选的值有：max-age=SECONDS，表示本次命令在未来的生效时间 includeSubDomains，可以用来指定是否对子域名生效漏洞危害：Web 服务器对于 HTTP 请求的响应头中缺少 Strict-Transport-Security，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。	1）修改服务端程序，给 HTTP 响应头加上 Strict-Transport-Security 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(Strict-Transport-Security,value)如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(Strict-Transport-Security:value)如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader Strict-Transport-Security,value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response=HttpResponse()response[Strict-Transport-Security]=value 如果是 python flask	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login

			服务端，可以使用如下方式添加 HTTP 响应头 response=make_response()response.headers[Strict-Transport-Security]=value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 Strict-Transport-Security 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：add_header Strict-Transport-Security value;如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：Header add Strict-Transport-Security value。	
11	https://124.163.201.106:9999/amOnline/zdjk-company-base/logi	Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，这将导致浏览器提供的安全特性失效。漏洞危害:Web 服务器对于 HTTP	1）修改服务端程序，给 HTTP 响应头加上 X-Download-Options 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login

	n	请求的响应头中缺少 X-Download-Options，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。	response.setHeader(X-Download-Options,value)如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(X-Download-Options:value)如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader X-Download-Options,value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response=HttpResponse()response[X-Download-Options]=value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response=make_response()response.headers[X-Download-Options]=value；2）修改负载均衡或反向代理服务器,给 HTTP 响应头加上 X-Download-Options 如果使用 Nginx、Tengine、	

			Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：add_header X-Download-Options value;如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：Header add X-Download-Options value。	
12	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	Web 服务器对于 HTTP 请求的响应头中缺少 X-Permitted-Cross-Domain-Policies，这将导致浏览器提供的安全特性失效。当一些在线的 Web Flash 需要加载其他域的内容时，很多 Web 会通过设置一个 crossdomain.xml 文件的方式来控制其跨域方式。很有可能有些开发者并没有修改 crossdomain.xml 文件的权限，但是又有和跨域的 Flash 共享数据的需求，这时候可以通过	1）修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(X-Permitted-Cross-Domain-Policies,value)如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(X-Permitted-Cross-Domain-Policies:value)如果是 asp 服务端，可以使用如下方式添	漏洞链接 1:https://124.163.201.106:9999/amOnline/zdjk-company-base/login

		设置 X-Permitted-Cross-Domain-Policies 头的方式来替代 crossdomain.xml 文件，其可选的值有：none master-only by-content-type by-ftp-filename all 漏洞危害：Web 服务器对于 HTTP 请求的响应头中缺少 X-Permitted-Cross-Domain-Policies，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。	加 HTTP 响应头 Response.AddHeader X-Permitted-Cross-Domain-Policies,value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response=HttpResponse()response[X-Permitted-Cross-Domain-Policies]=value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response=make_response()response.headers[X-Permitted-Cross-Domain-Policies]=value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：add_header X-Permitted-Cross-Dom	

			ain-Policies value;如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头：Header add X-Permitted-Cross-Domain-Policies value。	
13	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	在此页面上找到了一个匹配内部 IPv4 地址的字符串。这可能会披露有关内部网络的 IP 寻址方案的信息。此信息可用于进一步攻击。 存在敏感信息泄露的风险	防止此信息公开显示。	漏洞链接1:https://124.163.201.106:9999/
14	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	您使用的是已过时的一个或多个 JavaScript 库版本。有最新版本可用。虽然未发现您的版本受任何安全漏洞影响，但仍建议将库更新到最新版本。 更多信息，请查阅参考资料。	升级至最新版本。	漏洞链接1:https://124.163.201.106:9999/

7.3 基线配置检查建议

序号	脆弱点	整改建议
1	检查密码复杂度策略中设置的小写字母个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件, Suse9：修改/etc/pam.d/passwd 文件， Ubuntu,Suse10,Suse11,Suse12：修改 /etc/pam.d/common-password 文件， 在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数
2	syslog 是否启用记录 cron 行为日志功能	配置: cron.* /var/log/cron ， 其中/var/log/cron 为日志文件。 如果该文件不存在，则创建该文件，命令为： touch /var/log/cron，并修改权限为 775.命令为：chmod 775 /var/log/cron.
3	rsyslog 是否配置远程日志功能	在/etc/syslog-ng/syslog-ng.conf 中配置 destination logserver { udp("10.10.10.10" port(514)); }; log { source(src); destination(logserver); }; 可以将此处 10.10.10.10 替换为实际的 IP
4	syslog-ng 是否配置远程日志功能	修改配置文件 vi /etc/syslog.conf， 加上这一行： *.* @192.168.0.1 可以将"*.*"替换为你实际需要的日志信息。比如： kern.* ; mail.* 等等。

		可以将此处 192.168.0.1 替换为实际的 IP 或域名(域名格式形如：www.oksec.com,根据具体情况填写)。"
5	syslog 是否配置远程日志功能	修改配置文件 vi /etc/syslog.conf， 加上这一行： *.* @192.168.0.1 可以将"*.*"替换为你实际需要的日志信息。比如： kern.* ; mail.* 等等。 可以将此处 192.168.0.1 替换为实际的 IP 或域名(域名格式形如：www.oksec.com,根据具体情况填写)。
6	检查 syslog 是否配置安全事件日志	编辑/etc/syslog.conf 配置： *.err;kern.debug;daemon.notice /var/adm/messages 其中/var/adm/messages 为日志文件。 如果该文件不存在，则创建该文件，命令为： touch /var/adm/messages，并修改权限为 666.命令为： chmod 666 /var/adm/messages. 重启日志服务： #/etc/init.d/syslog restart 或者 service syslog restart
7	检查 syslog-ng 是否配置安全事件日志	编辑/etc/syslog-ng/syslog-ng.conf 配置： filter f_msgs { level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice); }; destination msgs { file("/var/adm/msgs"); }; log { source(src); filter(f_msgs); destination(msgs); }; 其中/var/adm/msgs 为日志文件。

		如果该文件不存在，则创建该文件，命令为： touch /var/adm/msgs，并修改权限为 666.命令为：chmod 666 /var/adm/msgs. 重启日志服务： #/etc/init.d/syslog restart 或者 service syslog restart
8	检查 rsyslog 是否配置安全事件日志	编辑/etc/rsyslog.conf 配置： *.err;kern.debug;daemon.notice /var/adm/messages 其中/var/adm/messages 为日志文件。 如果该文件不存在，则创建该文件，命令为： touch /var/adm/messages，并修改权限为 666.命令为：chmod 666 /var/adm/messages. 重启日志服务： #/etc/init.d/rsyslog restart 或者 service rsyslog restart
9	检查系统 openssh 安全配置	1.确保/etc/ssh/sshd_config 或 /etc/ssh2/sshd2_config 文件存在。如果不存在，则忽略下面配置步骤。 2.在 sshd_config 或 sshd2_config 中配置：Protocol 2 3.在 sshd_config 或 sshd2_config 中配置：PermitRootLogin no 或 PermitRootLogin NO
10	检查配置文件 /etc/snmp/snmpd.conf 是否存在	如果系统安装了 snmp 服务，请确保该文件存在。如果不存在，则在/etc/snmp/目录下创建该文件。
11	对于使用 IP 协议进行远程维护的设备,应禁止使用 telnet 协议	利用命令 rpm -qa |grep telnet 查看是否安装 telnet 和 telnet server 如果安装的话 1、编辑/etc/xinetd.d/telnet, 修改 disable = yes。

		2.激活 xinetd 服务。命令如下： # service xinetd restart 如果没安装则说明禁用 telnet 服务
12	检查是否配置账户认证失败次数限制	Redhat,CentOS,Fedora: 编辑/etc/pam.d/system-auth 文件 配置: auth required pam_tally.so deny=5 unlock_time=600 account required pam_tally.so Suse9: 编辑/etc/pam.d/passwd 文件 配置: auth required pam_tally.so deny=5 unlock_time=600 account required pam_tally.so Ubuntu,Suse10,Suse11,Suse12: 编辑/etc/pam.d/common-auth 文件 配置:auth required pam_tally.so deny=5 unlock_time=600 编辑/etc/pam.d/common-account 文件 配置:account required pam_tally.so 参数说明： deny #连续认证失败次数超过的次数 unlock_time #锁定的时间，单位为秒
13	检查是否配置关闭 IP 伪装	编辑/etc/host.conf 文件： nospoof on #关闭 IP 伪装

		补充操作说明 Redhat 默认没有/etc/host.conf 文件，要先新建一个 host.conf 文件
14	检查是否配置关闭多 IP 绑定	编辑/etc/host.conf 文件： multi off　　#关闭多 IP 绑定 补充操作说明 Redhat 默认没有/etc/host.conf 文件，要先新建一个 host.conf 文件
15	检查 /etc/hosts.allow 配置	编辑/etc/hosts.allow 增加一行 <service>: 允许访问的 IP；举例如下： all:192.168.4.44:allow #允许单个 IP； sshd:192.168.1.:allow #允许 192.168.1 的整个网段的 PC 通过 SSH 来访问本机 重启进程： #/etc/init.d/xinetd restart 或者 service xinetd restart
16	检查/etc/hosts.deny 配置	编辑/etc/hosts.deny 增加一行 all:all
17	检查 send_redirects 配置	执行命令 #sysctl -w net.ipv4.conf.all.send_redirects="0" 修改后可查看文件 cat /proc/sys/net/ipv4/conf/all/send_redirects 的值为 0 注：修改只能当次生效，重启系统需重新修改
18	是否禁止 icmp 重定向报文	执行命令 #sysctl -w net.ipv4.conf.all.accept_redirects="0" 修改后可查看文件 cat /proc/sys/net/ipv4/conf/all/accept_redirects 的值为 0

		注：修改只能当次生效，重启系统需重新修改
19	启用屏幕锁定	在屏幕上面的面板中，打开“系统”-->“首选项”-->“屏幕保护程序”； 或使用命令： gconftool-2 --direct \ 此处为回车换行 --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \ 此处为回车换行 --type bool \ 此处为回车换行 --set /apps/gnome-screensaver/lock_enabled true
20	检查密码复杂度策略中设置的数字个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件, Suse9：修改/etc/pam.d/passwd 文件， Ubuntu,Suse10,Suse11,Suse12：修改 /etc/pam.d/common-password 文件， 在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数
21	检查密码复杂度策略中设置的特殊字符个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件, Suse9：修改/etc/pam.d/passwd 文件， Ubuntu,Suse10,Suse11,Suse12：修改 /etc/pam.d/common-password 文件， 在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，

		添加到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数
22	检查密码复杂度策略中设置的大写字母个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件, Suse9：修改/etc/pam.d/passwd 文件， Ubuntu,Suse10,Suse11,Suse12：修改 /etc/pam.d/common-password 文件， 在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数
23	在/etc/login.defs 中设置口令最小长度	在文件/etc/login.defs 中设置 PASS_MIN_LEN 不小于标准值
24	检查口令更改最小间隔天数	在文件/etc/login.defs 中设置 PASS_MIN_DAYS 不小于标准值
25	检查口令过期前警告天数	在文件/etc/login.defs 中设置 PASS_WARN_AGE 不小于标准值
26	检查口令生存周期	在文件/etc/login.defs 中设置 PASS_MAX_DAYS 不大于标准值,PASS_MAX_DAYS 90，如果该文件不存在，则创建并按照要求进行编辑
27	检查是否按用户分配账号	为用户创建账号：#useradd username #创建账号#passwd username#设置密码修改权限#chmod 750 directory #其中 755 为设置的权限，可根据实际情况设置相应的权限，

		directory 是要更改权限的目录)使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。
28	检查是否限制FTP用户登录后能访问的目录	1.vsftp 修改/etc/vsftpd.conf(或者/etc/vsfptd/vsftpd.conf) #vi /etc/vsftpd.conf 确保以下行未被注释掉，如果没有该行，请添加： chroot_local_user=YES 重启网络服务 #/etc/init.d/vsftpd restart 2.pure-ftp 修改/etc/pure-ftpd/pure-ftpd.conf #vi /etc/pure-ftpd/pure-ftpd.conf 确保以下行未被注释掉（并且值为以下值），如果没有该行，请添加： ChrootEveryone yes AllowUserFXP no AllowAnonymousFXP no 重启 ftp 服务 #/etc/init.d/pure-ftpd restart
29	检查是否配置NTP服务器地址	编辑 ntp 的配置文件： #vi /etc/ntp.conf, 配置：server IP 地址（提供 ntp 服务的机器） 如：server 192.168.1.1 开启 ntp 服务： Redhat 为：/etc/init.d/ntpd start 或者 service ntpd start suse9 为：/etc/init.d/xntpd start suse10,11,12,Ubuntu,Fedora 为:/etc/init.d/ntp start

		centos 为：systemctl start ntpd
30	检查 ntp 服务是否开启	1.如果未安装 ntp 服务，请先安装 ntp 服务 2.如果 ntp 服务未开启，开启 ntp 服务： Redhat 为：/etc/init.d/ntpd start 或者 service ntpd start suse9 为：/etc/init.d/xntpd start suse10,11,12,Ubuntu,Fedora 为:/etc/init.d/ntp start centos 为：systemctl start ntpd
31	检查是否禁止 root 用户远程 ssh 登录	修改/etc/ssh/sshd_config 文件,配置 PermitRootLogin no。重启服务，/etc/init.d/sshd restart 或者 service sshd restart
32	检查是否使用 PAM 认证模块禁止 wheel 组之外的用户 su 为 root	编辑 su 文件(vi /etc/pam.d/su)，在开头添加下面两行： auth sufficient pam_rootok.so 和 auth required pam_wheel.so group=wheel 这表明只有 wheel 组的成员可以使用 su 命令成为 root 用户。 你可以把用户添加到 wheel 组，以使它可以使用 su 命令成为 root 用户。 添加方法为：usermod -G wheel username
33	/etc/rc.d/init.d/文件权限是否符合规范	chmod 750 /etc/rc.d/init.d/
34	/etc/xinetd.conf 文件权限是否符合规范	chmod 600 /etc/xinetd.conf 补充说明：低版本的 Linux 系统采用 inetd.conf 配置文件，执行命令:chmod 600 /etc/inetd.conf
35	/etc/security 目录权限是否符合规范	chmod 600 /etc/security
36	检查/etc/passwd 文件属性	执行 chattr +i /etc/passwd 如果不支持 chattr,编辑/etc/fstab 在相应的 reiserfs 系统的选项中添加 "user_xattr,attrs"这两个选项，然后重启主机。

37	检查/etc/group 文件属性	执行 chattr +i /etc/group 如果不支持 chattr,编辑/etc/fstab 在相应的 reiserfs 系统的选项中添加 "user_xattr,attrs"这两个选项，然后重启主机。
38	检查/etc/gshadow 文件属性	执行 chattr +i /etc/gshadow 如果不支持 chattr,编辑/etc/fstab 在相应的 reiserfs 系统的选项中添加 "user_xattr,attrs"这两个选项，然后重启主机。
39	检查 /var/log/localmessages 文件是否 other 用户不可写	执行命令：chmod 775 /var/log/localmessages
40	检查/var/log/mail 文件是否 other 用户不可写	执行命令：chmod 775 /var/log/mail

附件 1 主机漏洞检查报告

一. 任务概述

1.1 任务信息

任务名称	生态环保数据库（可入侵漏扫/版本漏扫/弱口令扫描/常规端口） 生态环保 1（可入侵漏扫/版本漏扫/弱口令扫描/常规端口） 生态环保 3（可入侵漏扫/版本漏扫/弱口令扫描/常规端口）
扫描目标	10.0.248.202-203；59.195.68.71；59.195.68.72-74
存活主机数	6
开始时间	2024-11-19 16:49:34
结束时间	2024-11-19 17:01:16
系统版本信息	2.0.270

1.2 风险综述

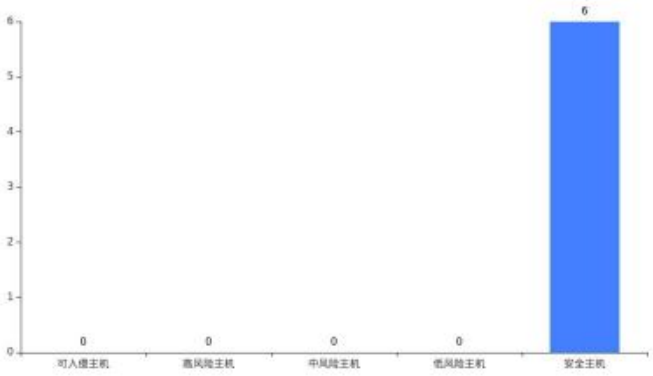
存活主机数量	弱口令	可入侵漏洞	高风险	中风险	低风险	小计
6	0	0	0	0	0	0

本次评估共发现存活主机 6 个，其中发现可入侵漏洞 0 个，高风险漏洞 0 个，弱口令 0 个，风险综述如下所示：

1.3 主机风险等级分布

本次评估的 6 个主机中，存在可入侵漏洞主机 0 个，存在高风险漏洞主机 0 个，如下所示：

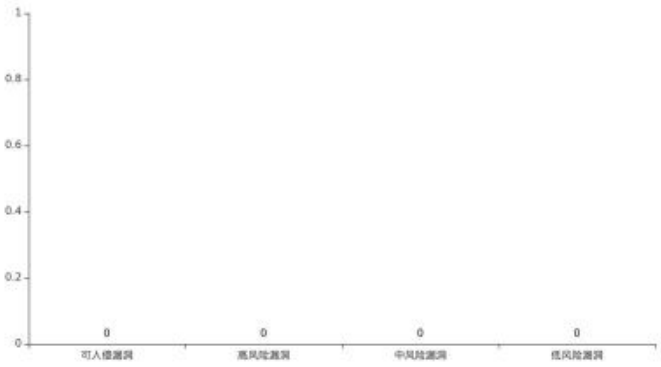
可入侵主机	0
高风险主机	0
中风险主机	0
低风险主机	0
安全主机	6



1.4 漏洞风险分布

本次评估的 6 个主机中，存在可入侵风险漏洞 0 个，存在高风险漏洞 0 个，如下所示：

可入侵漏洞	0
高风险漏洞	0
中风险漏洞	0
低风险漏洞	0



1.5 漏洞应用分类

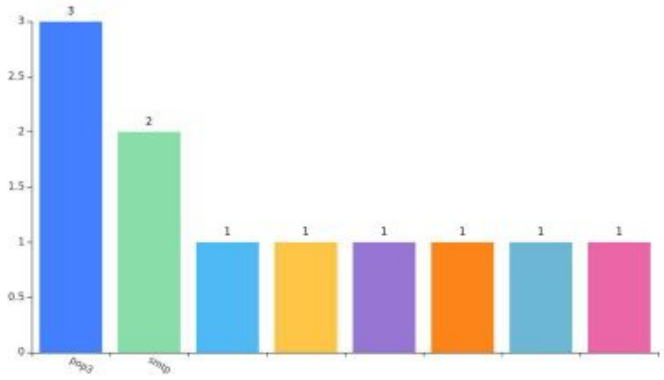
应用	高风险	中风险	低风险	合计
暂未发现漏洞				

1.6 Top10 漏洞

序号	漏洞名称	风险等级	数量	影响资产
暂未发现漏洞				

1.7 Top10 服务

序号	端口	服务	描述	数量	存在主机
1	110	pop3		3	59.195.68.73 59.195.68.72 59.195.68.74
2	25	smtp		2	59.195.68.73 59.195.68.74
3	25			1	59.195.68.71
4	110			1	59.195.68.71
5	22022			1	10.0.248.202
6	10009			1	59.195.68.73
7	800			1	59.195.68.73
8	5003			1	59.195.68.74



二. 主机风险等级列表

序号	IP 地址	操作系统	端口数	可入侵漏洞	高风险	中风险	低风险	弱口令	小计
1	59.195.68.71		2	0	0	0	0	0	0
2	10.0.248.202		1	0	0	0	0	0	0
3	10.0.248.203		0	0	0	0	0	0	0
4	59.195.68.73	linux	4	0	0	0	0	0	0
5	59.195.68.74	embedded	3	0	0	0	0	0	0
6	59.195.68.72	linux	1	0	0	0	0	0	0

三. 漏洞风险列表

3.1 可入侵漏洞分析

可入侵漏洞是指有公开利用方法，已验证可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，或可获取重要敏感数据。此部分漏洞基于漏洞原理验证识别，在漏洞名称中，会标识【原理扫描】。

对主机资产脆弱性进行分析，共发现存在 0 个可入侵漏洞，漏洞种类涉及 0 种，详情请查阅 Excel 报表附件。

序号	漏洞名称	风险等级	加固建议	影响资产
暂未发现漏洞				

3.2 版本漏洞分析

此部分漏洞主要是通过服务版本识别，以及根据权威漏洞库数据，判断资产是否在漏洞影响范围内，从而检测出相关漏洞。

请根据漏洞分类，针对受影响的资产，升级到相关应用的最新版本即可修复此类漏洞。

具体的漏洞详情请参见对应 Excel 报表附件。

序号	漏洞类型	高风险	中风险	低风险	影响资产
暂未发现漏洞					

3.2.1 高风险

序号	漏洞名称	风险等级	加固建议	影响资产
暂未发现漏洞				

3.2.2 中风险

序号	漏洞名称	风险等级	加固建议	影响资产
暂未发现漏洞				

3.2.3 低风险

序号	漏洞名称	风险	加固建议	影响资产

		等级		
暂未发现漏洞				

3.3 弱口令列表

序号	IP 地址	端口	类型	用户名	口令
暂未发现弱口令					

附录 A 附录

A.1 漏洞风险说明

漏洞是与信息资产有关的弱点或安全隐患。漏洞本身并不对资产构成危害，但是在一定条件得到满足时，漏洞会被威胁加以利用来对信息资产造成危险！本报告的漏洞共分了以下 4 种漏洞风险等级。

危险程度	危险程度说明
可入侵漏洞（严重）	有公开利用方法，已验证可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，或可获取重要敏感数据。此部分漏洞基于漏洞原理验证识别，在漏洞名称中，会标识【原理扫描】。
高	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，或可获取重要敏感数据。此部分漏洞主要通过服务版本识别，可能会有一定的误报。
中	攻击者可以远程创建、修改、删除部分文件或数据，或对普通服务进行拒绝服务攻击。此部分漏洞主要通过服务版本识别，可能会有一定的误报。
低	攻击者可以获取某些系统、服务的信息，或读取某些系统文件和数据。此部分漏洞主要通过服务版本识别，可能会有一定的误报。

A.2 主机漏洞加固策略

基于多年的安全整改经验，提供了以下 5 种安全加固整改策略，并对不同整改建议的有效防护度、整改困难度作了评级参考，有效防护度越高则表示加固效果越好，整改困难度越高则表示整改方案实施越难。您可以根据实际的业务情况，参考以下表，选择加固整改策略。

序号	加固整改策略	有效防护度	整改困难度
1	根据漏洞整改建议打补丁或者修改配置进行安全加固，加固前建议作好相关备份以便回退；建议所有 Windows 系统使用"Windows Update"进行更新。	高	高
2	若存在漏洞的应用服务平时不需要使用，建议关闭这些不必要的服务或应用。	高	低
3	若存在漏洞的应用服务不需要对外开放或者只对部分用户开放，建议在主机防火墙上进行访问控制，限定只有合法 IP 才能访问此应用。	中	低
4	若不便在主机防火墙上配置，建议在网络/出口防火墙上做白名单访问控制。	低	低
5	建议修改应用的 banner 信息，隐藏应用名称、版本号等信息，让攻击者无法识别目标系统，使之难以进行针对性的攻击入侵。	低	中

附件 2 网站漏洞检查报告

一. 任务概述

1.1 任务信息

任务名称	生态环保网站（全量漏洞扫描/中速/探测次数 12640/扫描链接数 5）
网站数量	1
开始时间	2024-11-19 16:54:58
结束时间	2024-11-19 17:02:20
系统版本信息	2.0.270

1.2 风险综述

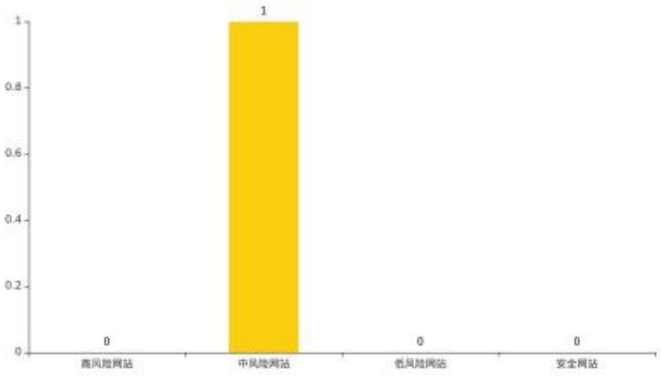
本次评估共对 1 个站点进行网站漏洞扫描，发现高风险漏洞 0 个，中风险漏洞 2 个，风险综述如下所示：

网站数量	高风险	中风险	低风险	信息风险	小计
1	0	2	10	2	14

1.3 网站风险等级分布

本次评估的 1 个网站中，存在高风险网站 0 个，存在中风险网站 1 个，如下所示：

高风险网站	0
中风险网站	1
低风险网站	0
安全网站	0



1.4 漏洞风险分布

本次评估的 1 个网站中，存在高风险漏洞 0 个，中风险漏洞 2 个，如下所示：

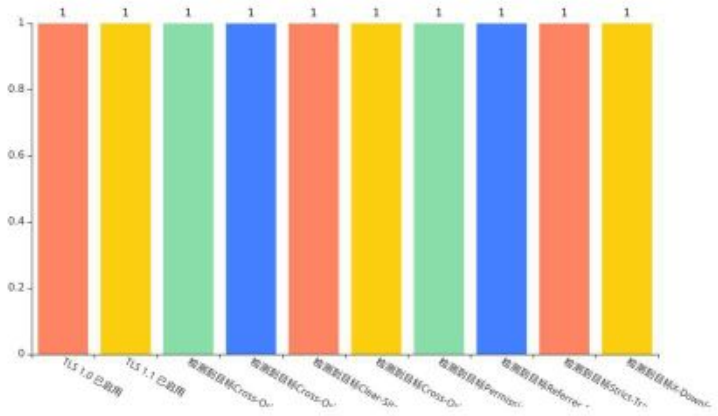
高风险漏洞	0
中风险漏洞	2
低风险漏洞	10
信息风险	2

1.5 高中风险漏洞类型分类

应用	高风险	中风险	低风险	合计
TLS 1.0 已启用	0	1	0	1
TLS 1.1 已启用	0	1	0	1
检测到目标 Cross-Origin-Embedder-Policy 响应头缺失	0	0	1	1
检测到目标 Cross-Origin-Opener-Policy 响应头缺失	0	0	1	1
检测到目标 Clear-Site-Data 响应头缺失	0	0	1	1
检测到目标 Cross-Origin-Resource-Policy 响应头缺失	0	0	1	1
检测到目标 Permissions-Policy 响应头缺失	0	0	1	1
检测到目标 Referrer-Policy 响应头缺失	0	0	1	1
检测到目标 Strict-Transport-Security 响应头缺失	0	0	1	1
检测到目标 X-Download-Options 响应头缺失	0	0	1	1
检测到目标 X-Permitted-Cross-Domain-Policies 响应头缺失	0	0	1	1
点击劫持：CSP frame-ancestors 缺失	0	0	1	1
合计	0	2	10	12

1.6 Top10 高危漏洞

序号	漏洞名称	风险等级	数量	漏洞详情
1	TLS 1.0 已启用	中风险	1	漏洞详情-1：https://124.163.201.106:9999/
2	TLS 1.1 已启用	中风险	1	漏洞详情-1：https://124.163.201.106:9999/
3	检测到目标 Cross-Origin-Embedder-Policy 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
4	检测到目标 Cross-Origin-Opener-Policy 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
5	检测到目标 Clear-Site-Data 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
6	检测到目标 Cross-Origin-Resource-Policy 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
7	检测到目标 Permissions-Policy 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
8	检测到目标 Referrer-Policy 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
9	检测到目标 Strict-Transport-Security 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login
10	检测到目标 X-Download-Options 响应头缺失	低风险	1	漏洞详情-1：https://124.163.201.106:9999/amOnline/zdjk-company-base/login



二. 网站风险等级列表

任务名称	网址	中间件	高风险	中风险	低风险	信息风险	小计
生态环保网站	https://124.163.201.106:9999/amOnline/zdjk-company-base/login		0	2	10	2	14

三. 漏洞风险列表

3.1 中风险

3.1.1 TLS 1.0 已启用

漏洞详情:

此 Web 服务器支持通过 TLS 1.0 加密。TLS 1.0 不被认为是"强密码术"。根据 PCI 数据安全标准 3.2(.1) 的定义和要求，在保护从网站往返的敏感信息时，TLS 1.0 并不被认为是

"强加密"。根据 PCI，"2018 年 6 月 30 日是禁用 SSL/早前 TLS 并实施更安全的加密协议 TLS 1.1 或更高版本（强烈建议 TLS v1.2）的最后期限，以便满足 PCI 数据安全标准 (PCI DSS)，保障支付数据的安全。

解决方案:

建议禁用 TLS 1.0 并替换为 TLS 1.2 或更高版本。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/	

3.1.2 TLS 1.1 已启用

漏洞详情:

此 Web 服务器支持通过 TLS 1.1 加密。当目标是支付卡行业 (PCI) 数据安全标准 (DSS) 合规性时，建议（尽管在当时或书面上并不需要）使用 TLS 1.2 或更高版本。根据 PCI，"2018 年 6 月 30 日是禁用 SSL/早前 TLS 并实施更安全的加密协议 TLS 1.1 或更高版本（强烈建议 TLS v1.2）的最后期限，以便满足 PCI 数据安全标准 (PCI DSS)，保障支付数据的安全。

解决方案:

建议禁用 TLS 1.1 并替换为 TLS 1.2 或更高版本。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/	

3.2 低风险

3.2.1 检测到目标 Cross-Origin-Embedder-Policy 响应头缺失

漏洞详情:

HTTP Cross-Origin-Embedder-Policy (COEP) 响应标头可防止文档加载未明确授予文档权限 (通过 CORP (en-US) 或者 CORS) 的任何跨域资源。

解决方案:

语法：Cross-Origin-Embedder-Policy: unsafe-none | require-corp。unsafe-none：这是默认值。允许文档获取跨源资源，而无需通过 CORS 协议或 Cross-Origin-Resource-Policy 头。require-corp：文档只能从相同的源加载资源，或显式标记为可从另一个源加载的资源。如果跨源资源支持 CORS，则 crossorigin 属性或 Cross-Origin-Resource-Policy 头必须使用它来加载资源，而不会被 COEP 阻止。

漏洞链接：

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/anOnline/zdjk-company-base/login	

3.2.2 检测到目标 Cross-Origin-Opener-Policy 响应头缺失

漏洞详情：

HTTP Cross-Origin-Opener-Policy（COOP）响应标头允许您确保顶级文档不会与跨来源文档共享浏览上下文组。COOP 将处理隔离您的文档，如果潜在攻击者在弹出窗口中打开您的全局对象，他们将无法访问该对象，从而防止一系列被称为 XS-Leaks 的跨源攻击。

解决方案：

支持语法：Cross-Origin-Opener-Policy: unsafe-noneCross-Origin-Opener-Policy: same-origin-allow-popupsCross-Origin-Opener-Policy: same-origin

漏洞链接：

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/anOnline/zdjk-company-base/login	

3.2.3 检测到目标 Clear-Site-Data 响应头缺失

漏洞详情：

Clear-Site-Data 响应头，表示清除当前请求网站有关的浏览器数据（cookie，存储，缓存）。它让 Web 开发人员对浏览器本地存储的数据有更多控制能力。

解决方案：

支持语法：// 单个参数 Clear-Site-Data: cache// 多个参数 (用逗号分隔)Clear-Site-Data: cache, cookies// 通配 Clear-Site-Data: *

漏洞链接：

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	

3.2.4 检测到目标 Cross-Origin-Resource-Policy 响应头缺失

漏洞详情：

Cross-Origin-Resource-Policy 响应头会指示浏览器阻止对指定资源的无源跨域/跨站点请求。注意设置 Cross-Origin-Resource-Policy（跨域资源策略）可能会使文件下载失败：当从设置了 CORP 请求头的资源服务器下载资源时，浏览器会阻止用户使用"保存"或"另存为"按钮将文件保存到本地。在决定生产环境中是否使用这一特性（CORP）之前需要慎重考虑。

解决方案：

支持语法：Cross-Origin-Resource-Policy: same-site | same-origin

漏洞链接：

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	

3.2.5 检测到目标 Permissions-Policy 响应头缺失

漏洞详情：

HTTP Permissions Policy 标头提供了一种机制，在文档中或文档中的任何<iframe>元素中可以允许或拒绝使用浏览器功能。

解决方案：

支持语法：Cross-Origin-Resource-Policy: same-site | same-origin | cross-origin

漏洞链接：

序号	漏洞 URL	参数

1	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	

3.2.6 检测到目标 Referrer-Policy 响应头缺失

漏洞详情:

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。

解决方案:

1）修改服务端程序，给 HTTP 响应头加上 Referrer-Policy 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(Referrer-Policy, value) 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(Referrer-Policy: value) 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader Referrer-Policy, value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response[Referrer-Policy] = value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make_response() response.headers[Referrer-Policy] = value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 Referrer-Policy 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add_header Referrer-Policy value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add Referrer-Policy value。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/amOnline/zdjk-company-base/login	

3.2.7 检测到目标 Strict-Transport-Security 响应头缺失

漏洞详情:

Web 服务器对于 HTTP 请求的响应头中缺少 Strict-Transport-Security，这将导致浏览器提供的安全特性失效。 当 Web 服务器的 HTTP 头中包含 Strict-Transport-Security 头时，浏览器将持续使用 HTTPS 来访问 Web 站点，可以用来对抗协议降级攻击和 Cookie 劫持攻击。其可选的值有： max-age=SECONDS，表示本次命令在未来的生效时间 includeSubDomains，可以用来指定是否对子域名生效 漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 Strict-Transport-Security，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。

解决方案:

1）修改服务端程序，给 HTTP 响应头加上 Strict-Transport-Security 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(Strict-Transport-Security, value) 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(Strict-Transport-Security: value) 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader Strict-Transport-Security, value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response[Strict-Transport-Security] = value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make_response() response.headers[Strict-Transport-Security] = value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 Strict-Transport-Security 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add_header Strict-Transport-Security value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add Strict-Transport-Security value。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/anOnline/zdjk-company-base/login	

3.2.8 检测到目标 X-Download-Options 响应头缺失

漏洞详情:

Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，这将导致浏览器提供的安全特性失效。 漏洞危害: Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，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。

解决方案:

1）修改服务端程序，给 HTTP 响应头加上 X-Download-Options 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(X-Download-Options, value) 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(X-Download-Options: value) 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader X-Download-Options, value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response[X-Download-Options] = value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make_response() response.headers[X-Download-Options] = value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 X-Download-Options 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add_header X-Download-Options value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add X-Download-Options value。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/am0nline/zdjk-company-base/login	

3.2.9 检测到目标 X-Permitted-Cross-Domain-Policies 响应头缺失

漏洞详情:

Web 服务器对于 HTTP 请求的响应头中缺少 X-Permitted-Cross-Domain-Policies，这将导致浏览器提供的安全特性失效。 当一些在线的 Web Flash 需要加载其他域的内容时，很多 Web 会通过设置一个 crossdomain.xml 文件的方式来控制其跨域方式。很有可能有些开发者并没有修改 crossdomain.xml 文件的权限，但是又有和跨域的 Flash 共享数据的需求，这时候可以通过设置 X-Permitted-Cross-Domain-Policies 头的方式来替代 crossdomain.xml 文件，其可选的值有：none master-only by-content-type by-ftp-filename all

漏洞危害： Web 服务器对于 HTTP 请求的响应头中缺少 X-Permitted-Cross-Domain-Policies，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。

解决方案:

1）修改服务端程序，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader(X-Permitted-Cross-Domain-Policies, value) 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header(X-Permitted-Cross-Domain-Policies: value) 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader X-Permitted-Cross-Domain-Policies, value 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response[X-Permitted-Cross-Domain-Policies] = value 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make_response() response.headers[X-Permitted-Cross-Domain-Policies] = value；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 X-Permitted-Cross-Domain-Policies 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add_header X-Permitted-Cross-Domain-Policies value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add X-Permitted-Cross-Domain-Policies value。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/anOnline/zdjk-company-base/login	

3.2.10 点击劫持：CSP frame-ancestors 缺失

漏洞详情:

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

服务器在 Content-Security-Policy 报头中未返回 frame-ancestors 指令，这意味着此网站存在遭受点击劫持攻击的风险。frame-ancestors 指令可被用于指示是否应允许浏览器在框架内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。

解决方案:

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

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/an0nline/zdjk-company-base/login	

3.3 信息风险

3.3.1 可能存在内部 IP 地址泄漏

漏洞详情:

在此页面上找到了一个匹配内部 IPv4 地址的字符串。这可能会披露有关内部网络的 IP 寻址方案的信息。此信息可用于进一步攻击。

解决方案:

防止此信息公开显示。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/	

3.3.2 已过时的 JavaScript 库

漏洞详情:

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

解决方案:

升级至最新版本。

漏洞链接:

序号	漏洞 URL	参数
1	https://124.163.201.106:9999/	

	anOnline/zdjk-company-base/login	

附录 A 附录

A.1 漏洞等级风险说明

漏洞是与信息资产有关的弱点或安全隐患，漏洞本身并不对资产构成危害，但是在一定条件得到满足时，漏洞会被威胁加以利用来对信息资产造成危险！本报告的漏洞共分了以下 4 种漏洞风险等级。

危险程度	危险程度说明
高	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	攻击者可以利用 Web 网站攻击其他用户，读取系统文件或后台数据库。
低	攻击者可以获取某些系统、网站、文件的信息或冒用身份。
信息风险	攻击者可以获取网站相关信息，可能是非敏感信息。

A.2 日常安全建议

随着越来越多的网络访问通过 Web 界面进行操作，Web 安全已经成为互联网安全的一个热点，基于 Web 的攻击广为流行，SQL 注入、跨站脚本等 Web 应用层漏洞的存在使得网站沦陷、页面篡改、插入黑链等攻击行为困扰着网站管理者并威胁着网站以及直接用户的安全。基于此，我们可从如下几个方面来消除这些风险，做到防患于未然：

1、对网站的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

2、请专业的安全研究人员或安全公司对架构网站的程序和代码做全面的源码审计，修补所有发现的安全漏洞，这种白盒安全测试比较全面、深入，能发现绝大部分的安全问题。

3、在网站上线前，使用 Web 应用漏洞扫描系统进行安全评估，并修补发现的问题；在网站上线后，坚持更新并使用网站安全监测系统，对整站以及关键页面进行周期和实时监测，及时消除发现的隐患。

4、建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，特别是影响到 Web 站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

附件 3 基线配置检查报告

一. 配置核查概述

本次评估范围内 6 台主机进行配置核查，其中 6 台主机的安全等级为高风险。

1.1 任务信息

任务名称	生态、生态 1、生态 2、生态 3、生态 5、生态 6
存活主机	6
开始时间	2024-11-19 17:33:24
结束时间	2024-11-19 17:34:49
系统版本信息	2.0.270

1.2 配置核查范围

本次配置核查范围如下：

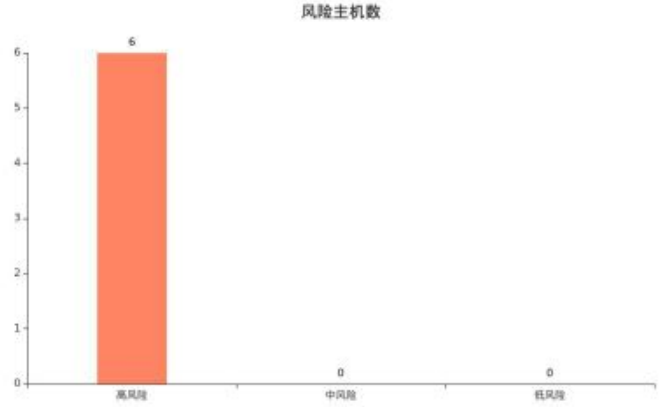
10.0.248.198、10.0.248.199、10.0.248.200、10.0.248.201、10.0.248.202、10.0.248.203。

二. 配置核查结果

本次配置核查针对重要资产的身份鉴别、安全审计、访问控制及入侵防范进行分析。

2.1 风险概况

本次扫描共扫描服务器 6 个，高风险主机 6 个，中风险主机 0 个，低风险主机 0 个。



存在 156 项高风险不合规检查项、80 项中风险不合规检查项、0 项低风险不符合项，详细风险分布如下图：

风险配置比例

2.2 主机风险情况

序号	IP	操作系统	高风险项	中风险项	低风险项	合规项
1	10.0.248.202	linux	26	14	0	53
2	10.0.248.199	linux	26	14	0	53
3	10.0.248.201	linux	26	14	0	53
4	10.0.248.198	linux	26	13	0	54
5	10.0.248.203	linux	26	13	0	54
6	10.0.248.200	linux	26	12	0	55

2.3 详细情况

不合规情况及具体加固建议如下：

2.3.1 Linux 系统_配置规范_等保二级

序号	脆弱点	加固建议	IP 地址	威胁级别
1	检查密码复杂度策略中设置的小写字	Redhat, CentOS, Fedora 系统：修改 /etc/pam.d/system-auth 文件，	10.0.248.198 10.0.248.199	高

	母个数	Suse9：修改/etc/pam.d/passwd 文件， Ubuntu,Suse10,Susel1,Susel2：修改 /etc/pam.d/common-password 文件， 在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加 到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit： 小写字母个数；dcredit：数字个数； ocredit：特殊字符个数	10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	
2	syslog 是否启用记录 cron 行为日志功能	配置： cron.* /var/log/cron ， 其中/var/log/cron 为日志文件。 如果该文件不存在，则创建该文件，命令为： touch /var/log/cron，并修改权限为 775.命令为：chmod 775 /var/log/cron.	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
3	rsyslog 是否配置远程日志功能	在/etc/syslog-ng/syslog-ng.conf 中配 置 destination logserver { udp("10.10.10.10" port(514)); }; log { source(src); destination(logserver); }; 可以将此处 10.10.10.10 替换为实际的 IP	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
4	syslog-ng 是否配置远程日志功能	修改配置文件 vi /etc/syslog.conf， 加上这一行： *.* @192.168.0.1 可以将"*.*"替换为你实际需要的日志信 息。比如：kern.* ; mail.* 等等。 可以将此处 192.168.0.1 替换为实际的 IP 或域名(域名格式形如：	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高

		www.oksec.com,根据具体情况填写)。"		
5	syslog 是否配置远程日志功能	修改配置文件 vi /etc/syslog.conf， 加上这一行： *.* @192.168.0.1 可以将"*.*"替换为你实际需要的日志信息。比如：kern.* ; mail.* 等等。 可以将此处 192.168.0.1 替换为实际的 IP 或域名(域名格式形如： www.oksec.com,根据具体情况填写)。	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
6	检查 syslog 是否配置安全事件日志	编辑/etc/syslog.conf 配置： *.err;kern.debug;daemon.notice /var/adm/messages 其中/var/adm/messages 为日志文件， 如果该文件不存在，则创建该文件，命令为： touch /var/adm/messages，并修改权限为 666.命令为：chmod 666 /var/adm/messages. 重启日志服务： #/etc/init.d/syslog restart 或者 service syslog restart	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
7	检查 syslog-ng 是否配置安全事件日志	编辑/etc/syslog-ng/syslog-ng.conf 配置： filter f_msgs { level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice); }; destination msgs { file("/var/adm/msgs"); }; log { source(src); filter(f_msgs); destination(msgs); }; 其中/var/adm/msgs 为日志文件， 如果该文件不存在，则创建该文件，命令	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高

		为： touch /var/adm/msgs，并修改权限为666.命令为：chmod 666 /var/adm/msgs. 重启日志服务： #/etc/init.d/syslog restart 或者 service syslog restart		
8	检查rsyslog是否配置安全事件日志	编辑/etc/rsyslog.conf 配置： *.err;kern.debug;daemon.notice /var/adm/messages 其中/var/adm/messages为日志文件。 如果该文件不存在，则创建该文件，命令为： touch /var/adm/messages，并修改权限为666.命令为：chmod 666 /var/adm/messages. 重启日志服务： #/etc/init.d/rsyslog restart 或者 service rsyslog restart	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
9	检查系统openssh安全配置	1.确保/etc/ssh/sshd_config或/etc/ssh2/sshd2_config文件存在。如果不存在，则忽略下面配置步骤。 2.在sshd_config或sshd2_config中配置：Protocol 2 3.在sshd_config或sshd2_config中配置：PermitRootLogin no或PermitRootLogin NO	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
10	检查配置文件/etc/snmp/snmpd.conf是否存在	如果系统安装了snmp服务，请确保该文件存在。如果不存在，则在/etc/snmp/目录下创建该文件。	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
11	对于使用IP协议进	利用命令rpm -qa |grep telnet查看是	10.0.248.198	高

	行远程维护的设备,应禁止使用telnet协议	否安装 telnet 和 telnet server 如果安装的话 1、编辑/etc/xinetd.d/telnet, 修改 disable = yes。 2.激活 xinetd 服务。命令如下: # service xinetd restart 如果没安装则说明禁用 telnet 服务	10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	
12	检查是否配置账户认证失败次数限制	Redhat,CentOS,Fedora: 编辑/etc/pam.d/system-auth 文件 配置: auth required pam_tally.so deny=5 unlock_time=600 account required pam_tally.so Suse9: 编辑/etc/pam.d/passwd 文件 配置: auth required pam_tally.so deny=5 unlock_time=600 account required pam_tally.so Ubuntu,Suse10,Suse11,Suse12: 编辑/etc/pam.d/common-auth 文件 配置:auth required pam_tally.so deny=5 unlock_time=600 编辑/etc/pam.d/common-account 文件 配置:account required pam_tally.so 参数说明: deny #连续认证失败次数超过的次数 unlock_time #锁定的时间,单位为秒	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
13	检查是否配置关闭	编辑/etc/host.conf 文件:	10.0.248.198	高

	IP 伪装	nospoof on #关闭 IP 伪装 补充操作说明 Redhat 默认没有/etc/host.conf 文件， 要先新建一个 host.conf 文件	10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	
14	检查是否配置关闭多 IP 绑定	编辑/etc/host.conf 文件： multi off #关闭多 IP 绑定 补充操作说明 Redhat 默认没有/etc/host.conf 文件， 要先新建一个 host.conf 文件	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
15	检查 /etc/hosts.allow 配置	编辑/etc/hosts.allow 增加一行 <service>: 允许访问的 IP； 举例如下： all:192.168.4.44:allow #允许单个 IP； sshd:192.168.1.:allow #允许 192.168.1 的整个网段的 PC 通过 SSH 来访问本机 重启进程： #/etc/init.d/xinetd restart 或者 service xinetd restart	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
16	检查 /etc/hosts.deny 配置	编辑/etc/hosts.deny 增加一行 all:all	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高

17	检查
	send_redirects 配置
		执行命令
		#sysctl -w
		net.ipv4.conf.all.send_redirects="0"
		修改后可查看文件
		cat
		/proc/sys/net/ipv4/conf/all/send_re
			10.0.248.198
			10.0.248.199
			10.0.248.200
			10.0.248.201
			10.0.248.202
			10.0.248.203
				高

		directs 的值为 0 注：修改只能当次生效，重启系统需重新修改		

18	是否禁止 icmp 重定向报文	执行命令
		#sysctl -w
		net.ipv4.conf.all.accept_redirects="0"
		修改后可查看文件
		cat /proc/sys/net/ipv4/conf/all/accept_redirects 的值为 0
		注：修改只能当次生效，重启系统需重新修改
			10.0.248.198
			10.0.248.199
			10.0.248.200
			10.0.248.201
			10.0.248.202
			10.0.248.203
				高

19	启用屏幕锁定	在屏幕上面的面板中，打开“系统”-->“首选项”-->“屏幕保护程序”； 或使用命令： gconftool-2 --direct \ 此处为回车换行 --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \ 此处为回车换行 --type bool \ 此处为回车换行 --set /apps/gnome-screensaver/lock_enabled true	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
20	检查密码复杂度策略中设置的数字个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件， Suse9：修改/etc/pam.d/passwd 文件， Ubuntu,Susel0,Susel1,Susel2：修改 /etc/pam.d/common-password 文件， 在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高

		到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数		
21	检查密码复杂度策略中设置的特殊字符个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件，Suse9：修改/etc/pam.d/passwd 文件，Ubuntu,Suse10,Suse11,Suse12：修改 /etc/pam.d/common-password 文件，在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1 注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
22	检查密码复杂度策略中设置的大写字母个数	Redhat,CentOS,Fedora 系统：修改 /etc/pam.d/system-auth 文件，Suse9：修改/etc/pam.d/passwd 文件，Ubuntu,Suse10,Suse11,Suse12：修改 /etc/pam.d/common-password 文件，在 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 选 3 种，追加到 password requisite pam_cracklib.so 后面，添加到配置文件中。 例如：password requisite pam_cracklib.so ucredit=-1 lcredit=-1 dcredit=-1	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高

		注：ucredit：大写字母个数；lcredit：小写字母个数；dcredit：数字个数；ocredit：特殊字符个数		
23	在/etc/login.defs中设置口令最小长度	在文件/etc/login.defs中设置PASS_MIN_LEN 不小于标准值	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
24	检查口令更改最小间隔天数	在文件/etc/login.defs中设置PASS_MIN_DAYS 不小于标准值	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
25	检查口令过期前警告天数	在文件/etc/login.defs中设置PASS_WARN_AGE 不小于标准值	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
26	检查口令生存周期	在文件/etc/login.defs中设置PASS_MAX_DAYS 不大于标准值,PASS_MAX_DAYS 90，如果该文件不存在，则创建并按照要求进行编辑	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	高
27	检查是否按用户分配账号	为用户创建账号：#useradd username #创建账号#passwd username#设置密码修改权限#chmod 750 directory #其中755为设置的权限，可根据实际情况设置相应的权限，directory是要更改权限的目录）使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。	10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202	中

28	检查是否限制 FTP 用户登录后能访问的目录	1.vsftp 修改/etc/vsftpd.conf(或者/etc/vsfptd/vsftpd.conf) #vi /etc/vsftpd.conf 确保以下行未被注释掉，如果没有该行，请添加： chroot_local_user=YES 重启网络服务 #/etc/init.d/vsftpd restart 2.pure-ftp 修改/etc/pure-ftpd/pure-ftpd.conf #vi /etc/pure-ftpd/pure-ftpd.conf 确保以下行未被注释掉（并且值为以下值），如果没有该行，请添加： ChrootEveryone yes AllowUserFXP no AllowAnonymousFXP no 重启 ftp 服务 #/etc/init.d/pure-ftpd restart	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
29	检查是否配置 NTP 服务器地址	编辑 ntp 的配置文件： #vi /etc/ntp.conf, 配置：server IP 地址（提供 ntp 服务的机器） 如：server 192.168.1.1 开启 ntp 服务： Redhat 为：/etc/init.d/ntpd start 或者 service ntpd start suse9 为：/etc/init.d/xntpd start suse10,11,12,Ubuntu,Fedora 为：/etc/init.d/ntp start centos 为：systemctl start ntpd	10.0.248.198 10.0.248.199 10.0.248.201 10.0.248.202 10.0.248.203	中
30	检查 ntp 服务是否开启	1.如果未安装 ntp 服务，请先安装 ntp 服务	10.0.248.198 10.0.248.199	中

		2.如果 ntp 服务未开启，开启 ntp 服务： Redhat 为：/etc/init.d/ntpd start 或者 service ntpd start suse9 为：/etc/init.d/xntpd start suse10,11,12,Ubuntu,Fedora 为：/etc/init.d/ntp start centos 为：systemctl start ntpd	10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	
31	检查是否禁止 root 用户远程 ssh 登录	修改/etc/ssh/sshd_config 文件,配置 PermitRootLogin no。重启服务，/etc/init.d/sshd restart 或者 service sshd restart	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
32	检查是否使用 PAM 认证模块禁止 wheel 组之外的用户 su 为 root	编辑 su 文件(vi /etc/pam.d/su)，在开头添加下面两行： auth sufficient pam_rootok.so 和 auth required pam_wheel.so group=wheel 这表明只有 wheel 组的成员可以使用 su 命令成为 root 用户，你可以把用户添加到 wheel 组，以使它可以使用 su 命令成为 root 用户。 添加方法为：usermod -G wheel username	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
33	/etc/rc.d/init.d/文件权限是否符合规范	chmod 750 /etc/rc.d/init.d/	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
34	/etc/xinetd.conf 文件权限是否符合规范	chmod 600 /etc/xinetd.conf 补充说明：低版本的 Linux 系统采用 inetd.conf 配置文件，执行命令:chmod 600 /etc/inetd.conf	10.0.248.198 10.0.248.199 10.0.248.201 10.0.248.202 10.0.248.203	中
35	/etc/security 目	chmod 600 /etc/security	10.0.248.198	中

	录权限是否符合规范		10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	
36	检查/etc/passwd 文件属性	执行 chattr +i /etc/passwd 如果不支持 chattr,编辑/etc/fstab 在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
37	检查/etc/group 文件属性	执行 chattr +i /etc/group 如果不支持 chattr,编辑/etc/fstab 在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
38	检查/etc/gshadow 文件属性	执行 chattr +i /etc/gshadow 如果不支持 chattr,编辑/etc/fstab 在相应的 reiserfs 系统的选项中添加"user_xattr,attrs"这两个选项，然后重启主机。	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
39	检查 /var/log/localmessages 文件是否 other 用户不可写	执行命令：chmod 775 /var/log/localmessages	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202 10.0.248.203	中
40	检查 /var/log/mail 文件是否 other 用户不可写	执行命令：chmod 775 /var/log/mail	10.0.248.198 10.0.248.199 10.0.248.200 10.0.248.201 10.0.248.202	中

			10.0.248.203	