ICS 35.240
CCS L 67

团　　体　　标　　准

CQAE*****—2025

信息安全渗透测试技术要求

Information security Penetration Test technology specification

报批稿

202X-XX-XX 发布　　202X-XX-XX 实施

中国电子质量管理协会　发布

目　　录

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由北京中电标研技术中心提出。

本文件由中国电子质量管理协会归口。

本文件起草单位：北京中标服检验技术研究院有限公司、内蒙古蒙壹购壹商贸有限公司、招商局检测车辆技术研究院有限公司、上海建工电子商务有限公司、联通（山东）产业互联网有限公司、河南许继仪表有限公司、内蒙古电力（集团）有限责任公司内蒙古电力科学研究院分公司、山西省信息产业技术研究院有限公司、国网思极检测技术（北京）有限公司、中国劳动关系学院、山西省信息化和信息安全评测中心、黑龙江智泽测评科技有限公司、联想（北京）有限公司、北京智芯微电子科技有限公司、中国移动通信集团西藏有限公司、重庆信安网络安全等级测评有限公司、江西师范大学、中移物联网有限公司、济南谷盾信息技术有限公司、SGS通标标准技术服务（上海）有限公司、中科联航（江苏）信息技术有限公司、浙江迈新科技股份有限公司、深圳天致信息工程咨询有限公司、四川省中认信安技术服务有限公司、广西电网有限责任公司信息中心、吉林省赛宝信息服务有限公司、四川九洲电器集团有限责任公司、江苏华检检测科技有限公司、山东胜利职业学院、河北华测信息技术有限公司、湖南省电子信息产业研究院、重庆巽诺科技有限公司、江西省网络安全研究院、鄂尔多斯市政务服务中心、可安评估有限公司、广东电网有限责任公司电力科学研究院、南方电网电力科技股份有限公司、深圳市天龙腾科技有限公司、南京大数据集团有限公司、中国电子信息产业集团有限公司第六研究所、北京技考帮教育科技有限公司、北京数企云服信息技术有限公司、广东优科检测认证有限公司、广州然因普电子科技有限公司、北京北方华测认证服务有限公司、北京中达信成科技有限公司、北京中电标研技术中心。

本文件主要起草人：张伟、侯超、吴超、陈可、陈庆嘉、周鹏、左群业、高子健、杨锦业、周百顺、孔群景、李勇、王蓓、郭亮亮、王倩文、霍海洋、王利斌、潘善民、郑杰、郭丁雷、阮鹏、冯淼、李智杰、郝宇鑫、余俊峰、崔岚、姜帆、付利莉、平措占堆、刘一廷、董文豪、谭龙、郭帆、刘春阳、刘利军、冉毅新、黄小芹、訾强、杨溢、乔轶、朱朝辉、史泰龙、郭峰、童国锋、郑俊昌、万里冰、孟椿智、曾明霏、陈丽娜、李世威、贾智钦、黄伟、陈燕、祁加佳、王月娥、吴上、林峰、滑昭、高红云、李凌志、代松柏、董大庆、樊荣、邓昭晖、许德忠、武玉平、王小龙、代仕勇、曾梦迪、古云峰、林丹生、张羿、陈伟、耿琦、张云、黄文盛、马天飞、刘丹、赵运广、李春阳、杨兆丰、刘畅、石跃超、文煜鑫、陈通、胡蝶、梁峰、温章义、邢献红、马廉杰、谢黑尔扎提·努尔买买提、张玉、张宏波、马啟田、邹金林、吴寒、陈以腊、蒋欣睿、姚固、张百川。

信息安全渗透测试技术要求

1 范围

本文件规定了信息安全渗透测试服务过程中涉及的各项技术要求。

本文件适用于渗透测试服务提供商及其他相关单位开展渗透测试服务。本规范不包含物理环境渗透、社会工程学攻击相关要求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 29246-2023 信息安全技术 信息安全管理体系概述和词汇

GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南

GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南

GB/T 37027-2018 信息安全技术 网络攻击定义及描述规范

GB/T 39412-2020 信息安全技术 代码安全审计规范

3 术语和定义

3.1 网络安全漏洞 cybersecurity vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。

3.2 网络攻击 network attack

通过计算机、路由器等计算资源和网络资源，利用网络中存在的漏洞和安全缺陷实施的一种攻击行为。

3.3 威胁 threat

对系统或组织可能造成意外伤害事件的潜在因素。

[GB/T 29246-2023，定义3.74]。

3.4 攻击面 attack surface

系统可被攻击者利用的潜在入口和漏洞。

3.5 渗透测试 penetration test

渗透测试是在被测试方合法授权的条件下，测试方模拟真实黑客攻击技术和方法，对目标应用程序、信息系统或网络开展的深度安全性测试。

3.6 系统恢复 system recovery

渗透测试实施结束后，将被测目标系统恢复到测试前状态的过程。

3.7 网络杀伤链 cyber kill chain

用于识别网络入侵活动的模型，描述了攻击者实施网络攻击的全过程，帮助安全团队理解攻击者的战术、技术和流程，从而制定针对性防御策略。

4 缩略语

下列缩略语适用于本文件。

API（Application Programming Interface）：应用程序编程接口

CNNVD（China National Vulnerability Database of Information Security）：国家信息安全漏洞库

CNVD（China National Vulnerability Database）：国家信息安全漏洞共享平台

CVE（Common Vulnerabilities and Exposures）：公共漏洞和暴露

CWE（Common Weakness Enumeration）：通用缺陷枚举

DNS（Domain Name System）：域名系统

5 渗透测试技术要求

5.1 概述

渗透测试包含测试准备、信息收集、威胁分析、测试实施、系统恢复和报告编制六个阶段，测试执行中应根据实际需求和目标环境状况开展各阶段工作。

5.2 测试准备

5.2.1 测试准备概述

在开始进行渗透测试前，应与测试委托方或被测试方签订协议。测试方根据协议开展测试需求分析、测试环境确定、明确组织分工、测试方案编制、并通过被测方的评审。

5.2.2 测试需求分析

根据测试需求和相关法律法规要求，分析被测目标主要业务以及支撑业务的资产，结合历史事件和典型威胁来源，提出安全防御需求。结合被测对象的风险承受能力，确定需要完成的渗透测试内容、测试目标和测试边界。

5.2.3 确定测试环境

确定测试环境需求，主要包括被测目标、测试工具、测试数据、陪测环境、测试接入区等，优先搭建与生产环境一致的模拟环境，避免对业务系统造成影响。当采用真实环境作为测试目标时，应综合考虑资源限制以及测试风险，必要时对被测系统的重要数据进行备份，确保业务的连续性和数据完整性。

5.2.4 明确计划安排

依据测试需求，合理安排测试进度，明确测试方和被测试方的责任分工，测试方负责执行渗透测试，被测方负责沟通协调与过程监督，保障渗透测试工作正常开展。

5.2.5 风险分析管控

分析渗透测试活动中可能引发的风险，制定风险应对措施，将渗透测试的潜在风险控制在可接受范围内。

5.2.6 测试方案编制

测试方应当根据渗透测试需求编制测试方案，测试方案作为整个渗透测试过程的指导文件，主要包括文档概述、系统概述、测试环境、测试内容和方法、计划安排和风险应对措施等。

5.2.7 方案评审

渗透测试方案应提交测试委托方或被测试方评审，评审方案中测试方法、测试内容、测试时间、组织分工、风险应对措施是否合理可行。

5.2.8 测试授权

在渗透测试开始之前，测试方应将测试方案提交被测试方审核确认，并获得被测单位出具的安全渗透测试授权书。授权书应由被测单位相关人员签署（相关管理层或相关部门负责人签署）并加盖公章，授权应详细说明测试范围、允许操作的类型及具体限制。

5.3 信息收集

5.3.1 信息收集概述

在获得测试授权后，测试人员应在法律和授权范围内尽可能多地收集目标系统的信息，为后续渗透测试提供基础信息。测试人员应在整个测试过程中持续更新和迭代信息收集，以更好地理解目标系统的环境、结构以及弱点。测试人员应妥善保管所收集的各类信息和数据，严禁向未授权方泄露。信息收集过程中，可采取主动探测、被动收集和其他方式获取被测目标信息。

5.3.2 主动探测

主动信息收集中，使用自动化扫描工具对目标网络进行全面扫描，获取存活的资产列表、开放端口和服务等信息，分析并确认潜在攻击面信息。

a） DNS探测

在被测目标通过公网访问时，利用DNS查询工具获取目标域名的IP地址、子域名、邮件服务器、名称服务器等关键信息。

b） 网络资产探测

使用自动化扫描工具对目标网络进行全面扫描，获取存活的资产列表、开放端口和服务等信息，分析并确认潜在攻击面信息。

c） 网络服务探测

采用标识识别技术或服务指纹识别技术，确定目标系统上运行的服务类型、版本及配置信息，从而发现已知漏洞或弱点。

5.3.3 被动收集

a） 被动通信数据

必要时，可通过部署网络嗅探器，捕获并分析目标系统的网络流量，以识别其通信协议特征、数据传输模式、未加密或弱加密的敏感数据等，并判断是否存在信息泄露的风险。

b） 调试/测试数据

必要时，可通过信息收集工具，查看客户端缓存、临时文件、日志记录等数据，检测是否存在遗留的敏感测试信息，包括但不限于：密钥、会话令牌等。

5.3.4 其他方式

a） 公开信息收集

利用搜索引擎或特定的安全搜索引擎进行查询。查找与目标组织相关的新闻报道、公告、技术文档等内容。获取曾经发生过的信息安全事件或历史存在的安全漏洞信息。

b） 渠道信息收集

通过客户、供应商等渠道，尝试获取部分非公开信息，如被测目标相关的业务流程、通信接口、终端设备等。

5.4 威胁分析

5.4.1 威胁分析概述

在信息收集基础上，测试人员应分析威胁来源和威胁能力，找出主要的攻击面。威胁分析对象应覆盖准备阶段中所有的测试目标，分析能够影响资产的威胁来源和威胁能力，全面识别攻击面，为后续渗透测试提供测试策略。

5.4.2 威胁来源分析

在获取渗透目标重要资产的基础上，分析潜在威胁来源，应根据威胁动机将威胁分为恶意网络安全威胁和非恶意网络安全威胁。非恶意网络安全威胁宜考虑误操作、管理疏忽、数据泄露、物理损害等方面，恶意网络安全威胁宜考虑操作失误、滥用权限、行为抵赖、信息泄露、社会工程、漏洞利用、行为探测、身份假冒、获取权限、密码攻击、拒绝服务、恶意代码、窃取数据、篡改数据、物理破坏、网络欺骗、电磁泄漏截取、管理不到位等。

5.4.3 威胁能力分析

根据威胁来源分析结果，分析此类威胁来源对系统造成危害的可能性。威胁能力分析可根据历史安全事件、接触权限范围、社会公开发布的态势预警等方面评估威胁能力。

5.4.4 攻击面分析

根据威胁动机和威胁能力分析结果，明确渗透测试所需要模拟的主要攻击场景，并结合所需保护的资产信息，构建威胁模型，发现攻击者能够利用的攻击面。攻击面分析可包括网络攻击入口、潜在攻击途径，以及各个攻击面的攻击可能性及影响程度等信息。在渗透测试过程中，随着信息收集的深入，攻击面可能会不断更新和扩展。

5.5 测试实施

5.5.1 测试实施概述

测试人员应基于信息收集中获取的信息，结合威胁分析中发现的攻击面，对被测目标开展渗透测试，测试内容通常包括漏洞扫描、漏洞挖掘、典型漏洞测试、渗透攻击测试和防御能力评估，实施过程中可根据项目需求进行拓展和裁剪。

5.5.2 漏洞扫描

测试人员应基于漏洞扫描工具与CVE、CNVD、CNNVD等漏洞数据库开展漏洞扫描，以发现被测目标中存在的网络安全漏洞。扫描工具应根据被测目标与测试策略选取测试工具，针对不同扫描对象可以采用网络扫描、系统扫描、代码扫描、应用扫描、无线扫描等。在进行漏洞扫描前应对已知漏洞库进行更新。

5.5.3 漏洞挖掘

测试人员应采用多种技术手段，结合人工分析和工具测试的方法，通过静态分析、动态调试、逻辑测试和模糊测试中一种或多种方法，对被测目标的二进制文件、网络数据、硬件电路等进行分析，挖掘未知漏洞。

a） 静态分析

测试人员在被测目标不运行的情况下，通过收集到的各类数据，挖掘漏洞，如采用反汇编方法分析二进制文件的指令使用，适用时结合代码审计方法挖掘漏洞。

b） 动态调试

测试人员应在被测目标运行的情况下，使用动态渗透测试工具，结合CWE分类对目标发起攻击，收集目标在遭受攻击时程序运行状态、系统响应结果等数据，挖掘并分析所发现漏洞，如应用服务漏洞、权限旁路漏洞、信息泄露漏洞等。

c） 逻辑测试

测试人员应分析被测目标业务逻辑，在不同业务场景下，针对业务输入构造有效值或无效值，审查目标是否存在非正常输出或异常状态，从而发现漏洞，如口令找回机制、业务非授权访问、业务流乱序等。

d） 模糊测试

测试人员应通过向系统提供异常、非预期或随机的输入数据，监控系统反应，发现可能导致系统崩溃、内存泄漏或异常状态的漏洞，如边界条件错误、输入验证不足等。

5.5.4 典型漏洞测试

在漏洞扫描和漏洞挖掘基础上，测试人员可采取典型漏洞攻击方法对被测目标实施漏洞攻击，进一步验证被测目标中存在的网络安全风险，测试过程根据被测目标的风险承受能力，在真实环境或实验室环境中执行，典型漏洞测试方法通常包括但不限于：嗅探攻击、身份认证攻击、权限校验攻击、注入攻击、跨站脚本攻击、协议欺骗攻击、敏感信息泄露、路径劫持攻击、信道攻击、无线信号攻击等，具体技术方法详情见附录A。

5.5.5 渗透攻击测试

测试人员应基于信息收集阶段获取的数据信息，结合已确认的漏洞，验证单个或多个漏洞关联利用可能造成的影响，验证过程可结合网络杀伤链模型，通过目标侦察、武器构建、载荷投递、漏洞利用、安装植入、命令控制和目标达成七个步骤逐个验证，具体实施过程宜按照以下内容开展：

a） 目标侦查

在该阶段中，测试人员从收集的信息中筛选出与本次攻击相关的数据，记录这些数据的获取途径、获取方法，以及重点内容。如向应用系统服务，发送异常请求，从系统返回的错误信息中，获取组件版本信息。

b） 工具构建

在该阶段中，测试人员根据攻击意图，选择或开发漏洞验证工具和漏洞利用工具，并配置攻击参数，形成可以实施攻击的测试工具。此过程中使用的工具需满足以下要求：

1）工具应受控并能够被清除。

2）工具宜能够进行特征隐藏，在一定程度上减少被现有的安全设备检测发现的概率。

c） 载荷投递

在该阶段中，测试人员模拟攻击者将攻击载荷发送到被测目标的过程，投递方式应考虑不同类型用户和权限，详细记录投递的方法。如普通用户上传头像，管理员进行系统升级等。

d） 漏洞利用

在该阶段中，测试人员根据攻击目的，利用单个或组合多个漏洞开展攻击的过程，并详细记录漏洞利用的效果，如信息泄露、提权、代码执行等，如果在生产环境中实施漏洞利用，应提前通知被测单位，当发生不控情况时，应能及时停止。

e） 安装植入

在该阶段中，测试人员尝试利用漏洞在系统中植入远程控制程序或后门指令，模拟攻击者尝试持续控制目标系统。

f） 命令控制

在该阶段中，测试人员尝试建立目标系统的控制路径，模拟攻击者自由接触操作系统和网络，实现对整个系统的接管控制。

g） 目标达成

在该阶段中，测试人员验证渗透攻击能够造成的破坏程度。此阶段应记录测试效果，如获取重要数据、破坏系统执行、实现远程控制等。

5.5.6 防御能力评估

在渗透攻击的同时，测试人员应评估被测目标的防护、感知、阻断、恢复能力，全面分析目标系统的防御能力。包括：

a） 防护测试

测试人员应评估系统能够拦截攻击的次数、查杀恶意代码种类等防护能力。

b） 感知测试

测试人员应评估系统是否能够通过异常监控、审计日志、威胁信息等手段发现渗透攻击事件。如异常监控能否发现系统运行状态、网络流量变化；审计日志记录的完整性、真实性；威胁信息能否整合内外部信息数据，实现实时匹配与预警。

c） 阻断测试

测试人员应评估系统能否在感知攻击的基础上，阻断攻击行为、减少损失。当发现用户频繁登录、异常提交、大规模下载、病毒扩散等操作时，能否及时阻断用户操作或网络通信。

d） 恢复测试

测试人员应评估系统在攻击结束后，系统能够恢复到攻击前的程度以及恢复所需的时间。

5.6 系统恢复

在渗透测试结束后，测试人员应协助清除渗透测试痕迹和数据，并配合验证清理效果。完成痕迹清除后，测试人员应对系统清除状态进行恢复验证，验证测试账户是否删除，系统权限是否重置，是否存在未清理的后门等。渗透测试结束后，系统中不应保留任何可被利用的后门。清除对象包括渗透测试过程中安装的各类渗透测试工具、攻击代码、配置变更、临时账户以及其他由渗透测试造成的痕迹。

a） 测试工具清除

测试人员应彻底清除渗透测试过程中使用的所有临时文件、工具和脚本、上传文件、配置文件和测试时产生的日志文件。

b） 攻击代码删除

测试人员应彻底清除渗透测试过程中植入恶意代码或后门，确保未遗留任何能够被攻击者利用的漏洞或后门。

c） 配置变更恢复

所有因渗透测试所做的系统配置变更（如防火墙规则、用户权限、文件访问控制等）应恢复为原先的安全状态，确保系统配置的安全性和完整性。

d） 临时账户删除

测试人员应彻底清除测试过程中创建的账户，并核实剩余账户的权限设置，避免出现未经授权的访问。

e） 其他痕迹清除

测试人员应协助系统管理员彻底清除其他由渗透测试导致改变或取得的数据。

5.7 报告编制

5.7.1 测试报告概述

根据测试过程中的测试结果，测试人员应编制测试报告。测试报告内容宜包括以下几个方面：测试时间、测试环境、测试人员、测试记录、测试结论、改进建议以及其他相关内容和附件。针对报告中敏感内容应当进行脱敏处理。

5.7.2 测试结果分析

分析测试结果确认存在的漏洞，并对漏洞进行分级分类，找出能够影响系统运行的严重漏洞和攻击途径，且应当符合GB/T 30279-2020中对于漏洞分级分类相关的要求。问题报告单示例见附录B。

5.7.3 报告评审

测试报告应通过测试委托方和被测试方组织的评审，评审主要针对测试活动是否达到测试目的、测试执行过程中的各阶段是否覆盖充分、报告内容是否真实准确，以及被测试方对于发现问题的处理是否能规避风险等。

6 其他要求

6.1 合规性要求

渗透测试应在法律和授权允许的范围内开展。包括以下要求：

a) 授权要求

1) 测试方须与被测方签署正式授权文件，明确测试目标、测试范围、测试时间、测试方法及禁止事项等。

2) 若目标系统涉及云服务等第三方平台，应妥善处理，如环境替代、接口模拟、范围控制等。

b) 数据保护要求

测试中获取的数据，需按照委托方要求进行保密，未经被测方授权，禁止传播。

c) 其他要求

1) 不得利用渗透测试期间发现的漏洞从事危害网络安全的活动。

2) 未经委托方同意，不得发布安全测试期间发现的漏洞。

3) 遵守目标系统所属行业的法律法规。

6.2 渗透测试工具要求

为确保渗透测试能够高效合规，渗透测试过程中使用的工具应符合以下要求：

a) 合法性要求

1) 测试中使用的商业工具应通过合法渠道获取，测试中使用的开源工具符合开源协议。

2) 工具不应包含后门、间谍软件或未声明的数据外传功能。

b) 适用性要求

1) 所选取的测试工具应该能够覆盖测试需求，支持渗透测试全生命周期，包括：信息收集、威胁分析、渗透性测试等。

2) 工具应支持自定义扫描策略，降低误报率和漏报率。

c) 更新与维护要求

1) 测试工具定期更新，确保漏洞库和攻击模拟方法同步更新。

2) 工具需支持检测最新公开漏洞，并具备相应的检测规则。

d) 兼容性要求

1) 工具应能够适配目标系统的运行环境，包括：操作系统、中间件及协议等。

2) 工具应能解析目标系统的各类特征，从而准确发现漏洞。

6.3 渗透测试文档要求

a) 渗透测试过程需形成完整的文档体系，包括：方案性文件、记录性文件、报告性文件等。

b) 测试文档应包含完整的测试上下文信息，并保证文档内部及文档间数据内容的一致性。

附 录 A

（资料性）

渗透性测试技术方法

A.1 嗅探攻击技术

使用嗅探工具，根据不同攻击面，接入渗透测试目标系统，尝试通过网络数据包捕获与协议分析技术，对目标系统进行通信监听与分析。具体要求如下：

a） 应使用专业的网络协议分析工具，对目标系统所在网络环境进行数据包捕获。

b） 应对捕获的数据包进行深度协议分析，重点关注：明文传输的用户名、口令等敏感信息；应用层协议实现中的安全缺陷；网络层与传输层协议的安全配置；加密通信过程中的协议实现缺陷。

A.2 身份认证攻击测试

攻击者可以绕过认证机制或以其他用户身份执行操作。常见漏洞包括暴力破解、会话劫持、域认证攻击等。

a） 暴力破解

暴力破解通过穷举所有可能的组合来破解口令或密钥。

b） 会话劫持

会话劫持是指黑客通过某种手段获取合法用户的身份标识，并以此来访问系统受保护的资源。黑客可以通过窃取会话令牌、使用会话固定攻击等方式实施会话劫持攻击。

c） 域认证攻击

指针对域环境中的身份验证机制发起的各类攻击手段。这些攻击主要利用域认证协议中的漏洞或弱点来获取未授权访问权限。

A.3 权限校验攻击测试

测试人员应对被测目标权限分配、提升或验证过程进行测试，若权限认证存在缺陷，可导致攻击者可越权访问资源或执行操作。

a） 未授权访问

未授权访问常见于API、数据库等资产，通常使用工具尝试与对应资产建立连接，若无需输入认证信息即可登录则该资产存在未授权访问漏洞。

b） 垂直越权

垂直越权主要检测权限提升风险，通常修改请求中的角色字段，测试低权限用户是否可执行高权限功能。

c） 水平越权

水平越权主要检测同权限用户间的数据隔离性，通常修改请求中的标识字段，测试同权限用户是否可操作或获取其他用户非授权数据。

d） 权限提升缺陷

测试系统是否存在其他不合理的权限设置。

A.4 注入攻击技术

通过人工与工具结合方式，尝试对系统各类数据交互点进行输入恶意数据，执行数据窃取、非法篡改等非预期操作。具体要求如下：

a） SQL注入测试应包括

验证API接口的参数过滤机制；检查SQL语句的特殊字符处理；测试存储过程的安全实现；验证数据库权限配置的合理性。

b） LDAP注入测试应包括

验证目录服务查询接口的输入验证；检查特殊字符的转义处理；测试目录访问权限控制。

c） XML注入测试应包括

验证XML解析器的安全配置；检查外部实体引用的限制措施；测试XML过滤器的有效性。

d） 命令注入测试应包括

验证命令参数的过滤机制；检查特殊字符的转义处理；测试命令执行权限控制；评估系统命令的访问限制。

e） 代码注入测试包括

当产品允许用户输入包含代码语法时，攻击者可能会以某种方式编写代码，从而改变产品的实际功能，达到攻击的目的。

f） 反序列化攻击测试包括

根据被测目标的序列化传输方式，构建反序列化数据或代码，尝试使用高危函数调用恶意指令。

A.5 跨站脚本测试

测试人员应对Web应用进行全面的XSS漏洞测试。具体要求如下：

a） 反射型XSS测试

验证输入数据的过滤规则；检查HTML编码处理；测试脚本代码注入点；评估响应头的安全配置。

b） 存储型XSS测试

验证数据存储的过滤机制；检查数据读取时的编码处理；测试持久化数据的渲染过程；评估内容安全策略(CSP)的有效性。

c） DOM型XSS测试

验证客户端脚本的输入处理；检查DOM操作的安全实现；测试JavaScript代码的过滤机制；评估浏览器XSS防护措施。

A.6 协议欺骗测试

测试人员应对系统的协议实现安全性，进行欺骗测试。具体要求如下：

a） ARP欺骗测试

验证ARP表项更新机制；检查静态ARP绑定配置；测试ARP防欺骗措施的有效性；评估网络设备的ARP安全策略。

b） DNS欺骗测试

验证DNS查询响应机制；检查DNS缓存管理；测试DNS安全扩展(DNSSEC)配置；评估DNS服务器安全策略。

A.7 敏感信息泄露测试

测试人员根据系统处理和存储的数据重要程度，尝试模拟攻击者获取敏感数据。具体要求如下：

a） 通信泄露

使用抓包工具截取客户端与服务端之间的通信数据，分析数据是否包含明文传输的敏感数据。

b） 存储泄露

使用数据访问工具，对服务端数据库、生成文件进行检查，分析重要数据是否加密存储。

c） 调试信息泄露

构造异常数据并发送给被测目标，触发被测目标运行错误，尝试收集被测目标泄露的调试数据，从而获取目录结构、执行代码等信息。

d） 日志泄露信息

检查日志系统，尝试获取敏感信息如凭证、会话令牌或个人敏感数据。

A.8 路径劫持攻击测试

攻击者可以绕过受限位置，访问系统其他位置的文件或目录。

a） 路径遍历

输入绝对路径参数或路径操作符号，控制文件访问，解析到该目录之外位置。

b） 文件索引越权访问

系统若未对文件索引（如随机生成的下载链接、文件标识）进行权限校验，攻击者可通过遍历ID或构造参数获取敏感文件。例如，通过猜测或爆破文件标识下载未授权文件。

c） 错误的编码格式

通过构造非常规编码格式的请求路径，测试系统对非标准输入的处理能力，尝试绕过防火墙等安全设备，越权下载敏感文件。如多重编码转换、非标准分隔符、编码截断等。

d） 资源列表暴露

尝试通过构建访问路径，获取文件和目录等资源列表，如中间件目录列表、对象存储文件列表等。

A.9 信道攻击测试

测试人员应对系统的信道安全性进行全面测试。具体要求如下：

a） 边信道攻击测试

验证密码系统的时间特征；检查功耗特征分析；测试电磁辐射泄漏；评估缓存访问模式。

b） 隐蔽信道测试

验证协议字段的异常使用；检查网络流量的统计特征；测试存储资源的共享机制；评估时间特征的异常模式。

c） 时序攻击测试

验证操作响应时间特征；检查并发处理机制；测试定时器实现机制；评估时间同步策略。

A.10 无线信号攻击测试

使用无线侦听重放工具，测试人员应对无线通信系统进行安全性测试。具体要求如下：

a） 无线数据采集

验证无线信号的调制方式； 检查信号的频率特征；测试通信协议格式；评估信号强度分布。

b） 协议分析测试

验证握手过程的安全性；检查认证机制的实现；测试加密算法的应用；评估密钥交换过程。

c） 重放攻击测试

验证时间戳机制；检查序列号管理；测试会话标识唯一性；评估重放防护措施。

附 录 B

（资料性）

问题报告单示例

问题标识	xxx-xxx-xx-001	报告人	xxx	报告日期	2025-xx-xx
问题位置	xxx-xxx-AQX-002-001				
问题类别	■代码问题	□配置错误	□环境问题	□其他	
问题级别	□超危	■高危	□中危	□低危	
问题描述	问题： 系统 xx 应用软件存在 CVE-2021-44228 漏洞，攻击者通过构造包含恶意 JNDI 的字符串，能够执行任意代码控制系统。 问题详细描述： Log4j 漏洞是由于 Log4j 2 在处理日志消息中的 JNDI（Java Naming and Directory Interface）查找时存在的不安全实现而引发的。攻击者可以通过特制的日志消息利用此漏洞，从而使 Log4j 在处理日志消息时，连接到恶意的 LDAP 服务器并执行任意代码。 修复建议： 升级 log4j2 到最新版本，修复后的 log4j2 在 Jndi Lookup 中增加了一些限制。				
研发方处理意见	修复措施： 升级 Log4j 依赖库到 2.16.0 版本。				
整改情况	经验证： 已完成 Log4j 依赖库升级，未发现安全隐患。				