ICS 91.120.25
CCS L70

DB21

辽 宁 省 地 方 标 准

DB21/T XXXX—XXXX

信息系统渗透测试技术规范

Technical specification for information system penetration test

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：北方实验室（沈阳）股份有限公司、辽宁省标准化研究院。

本文件主要起草人：张健楠、李海涛、袁洪朋、刘文志、鲁宁、段晓祥、曹明、石绍群、王明俊、王海涛、何永建、王启光、孙辉航、张建宇、李开、邱学思、叶松 、韩燕妮。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通讯地址：辽宁省工业和信息化厅（沈阳市皇姑区北陵大街45-2号），联系电话：024-86893258。

标准起草单位通讯地址：北方实验室（沈阳）股份有限公司（沈阳市浑南新区三义街6-1号21层），联系电话：024-83785841 / 83785849。

信息系统渗透测试技术规范

1 范围

本文件规定了信息系统渗透测试技术规范的术语和定义、原则、渗透测试技术和管理的要求。

本文件适用于辽宁省内信息系统渗透测试的实施。

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—2007 信息安全技术 信息安全风险评估规范

GB/T 25069 信息安全技术 术语

GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

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

3 术语和定义

GB/T 20984—2007、 GB/T 25069、GB/T31509—2015、GB/T 22239—2019、GB/T 28448—2019、GB/T 36627—20181界定的以及下列术语和定义适用于本文件。

3.1

网络安全 CyberSecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2

渗透测试 penetration test

通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

3.3

漏洞扫描 Vulnerability scanning

基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。

3.4

弱口令 weak password

容易被他人猜测到或被破解工具破解的口令。

3.5

测试方 Testing party

为信息系统提供测试服务的机构或人员。

3.6

SQL 注入 SQL injection

web 应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在 web 应用程序中事先定义好的查询语句的结尾上添加额外的 SQL 语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

3.7

跨站脚本攻击 cross-site scripting attack，XSS

一种安全攻击，攻击者在看上去来源可靠的链接中恶意嵌入译码。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。

注：这类攻击通常包含了HTML以及用户端脚本语言。

3.8

安全配置错误 Security configuration error

由不安全的默认配置、不完整的临时配置、开源云存储、错误的 HTTP 标头配置以及包含敏感信息的详细错误信息所造成的配置错误。安全配置错误可以发生在一个应用程序堆栈的任何层面。

注：包括网络服务、平台、web服务器、应用服务器、数据库、框架、自定义的代码、预安装的虚拟机、容器、存储等。

4 原则

4.1 测试目的

利用各种安全测试工具对网站及相关服务器等设备进行非破坏性质的模拟入侵者攻击，侵入系统并获取系统信息并将入侵的过程和细节总结编写成测试报告，由此确定存在的安全威胁，并能及时提醒安全管理员完善安全策略，降低安全风险。

4.2 测试原则

4.2.1 标准性原则

应按照GB/T 31509—2015和GB/T 36627—2018的流程进行实施，包括实施阶段和运维阶段的测试工作。

4.2.2 全面性原则

在规定的测试范围内，应覆盖指定目标信息系统中的全部服务及每个服务中的全部功能。

4.2.3 分级原则

测试过程应对信息系统各项服务及漏洞进行分级管理，以保证信息系统重要应用服务的资源投入。

4.2.4 可控性原则

测试过程应按照GB/T 31509—2015中的项目管理办法对过程、人员、工具等进行控制，以保证渗透测试安全可控。

4.2.5 最小影响原则

针对处于运维阶段的信息系统，应提前确定合适的测试时间窗口，避开业务高峰期，同时做好被测目标系统的应急预案。

4.2.6 保密性原则

未经委托方允许，测试方不应向第三方及社会公众泄露与被测信息系统相关的一切信息，包括但不限于开发及运维人员个人信息以及因测试活动所获取的敏感信息，如网络架构、业务数据、安全漏洞等。

4.2.7 及时性原则

测试方应保证漏洞提交的及时性，检测出漏洞与提交漏洞的时间间隔不应超出规定时间，不应出现漏洞积压的情况。

4.3 测试形式

渗透测试应按照GB/T 28448—2019、GB/T 36627—2018以及GB/T 20984—2007，以人工渗透测试为主，工具漏洞扫描和自评估测试为辅，互为补充。渗透测试实施的组织形式包括但不限于个人测试、团队测试、众测等。

5 技术要求

5.1 测试环境及准备要求

测试环境及准备要求包括以下内容：

a) 渗透测试应提供与生产环境相似的仿真环境，以便进行部分可能影响数据完整性及稳定性的侵入式测试。测试方在生产环境中应避免使用可能导致数据完整性及业务稳定性遭受破坏的测试手段；
b) 委托方应预先准备功能与数据均完备的账号以保证测试的有效性，若完成测试涉及必要的专有设备，如控件、证书等软硬件设备，委托方应给予必要的配合或协助；
c) 如测试过程中发现功能损坏及数据缺失，测试方应对缺失的数据及损坏的功能进行详细记录，并及时反馈给系统开发人员进行功能及数据补足；
d) 通过仿真环境测试时，委托方应提供安全的测试接入方式（如现场接入、VPN 远程接入及 IP 白名单等方式），防止非授权人员对仿真环境进行违规访问或违规测试；
e) 禁止测试方向任何未经授权的第三方泄露任何与测试环境相关的信息；
f) 测试环境提供方应及时与测试方同步系统更新、维护及测试计划等信息，以保证测试环境稳定可用；
g) 如测试对象为应用接口，测试环境提供方应向测试方提供足以用来构造并完成接口请求的说明文档或脚本。

5.2 测试工具及准备要求

测试工具及准备要求包括以下内容：

a) 测试方应使用不存在法律风险的或合规风险的工具进行测试；
b) 测试方应使用获得网络安全主管部门或行业主管部门认可的漏洞扫描工具进行测试，同时提供测试工具清单，并制定明确的扫描策略和扫描计划以规避风险；
c) 委托方应建立运行类测试工具审核机制，对测试方所提供的运行类测试工具的运行安全、版本、组成以及来源渠道进行严格审核；
d) 对于新引入的测试工具，应建立严格的审批及测试机制，确保不存在木马后门程序或严重的软件缺陷。对于已引入的渗透测试工具，应重点关注测试工具本身的安全性，及时针对测试工具进行补丁修复和版本升级；
e) 对于完成当次渗透测试后不再使用的运行类测试工具应在测试完成前彻底删除，防止运行类工具本身引入安全隐患；
f) 测试方应从在信息系统中上传或部署运行类测试工具开始，到通知测试环境提供方并彻底删除运行类测试工具为止的期间内，通过书面记录或全程录屏的方式严格记录每一步操作步骤。针对测试过程的具体记录方式应以测试相关方的协商意愿为准；
g) 在未经授权的情况下，严禁使用公开的平台进行存在数据外发的漏洞利用测试，如采用公开的平台测试远程命令执行、XXS 和 SQL 注入等漏洞。

5.3 测试方法

5.3.1 测试方法分类

根据渗透目标分类：

a) 主机操作系统渗透：对 Windows、Solaris、AIX、Linux、SCO、SGI、Kylin 等操作系统进行渗透测试；
b) 数据库系统渗透：对 MS-SQL、Oracle、MySQL、Informix、Sybase、DB2、达梦等数据库应用系统进行渗透测试；
c) 应用系统渗透：对渗透目标提供的各种应用，如 ASP、CGI、JSP、PHP 等组成的 WWW 应用进行渗透测试；
d) 网络设备渗透：对各种防火墙、入侵检测系统、网络设备进行渗透测试；
e) 内网渗透：内网渗透测试指测试人员从内部网络发起测试，内部主要可能采用的渗透方式：远程缓冲区溢出，口令猜测，以及 B/S 或 C/S 应用程序测试（如果涉及 C/S 程序测试，需要提前准备相关客户端软件供测试使用）；
f) 外网渗透：外网渗透测试指测试人员完全处于外部网络（例如拨号、ADSL 或外部光纤），模拟对内部状态一无所知的外部攻击者的行为。包括对网络设备的远程攻击，口令管理安全性测试，防火墙规则试探、规避，Web 及其它开放应用服务的安全性测试。

5.3.2 渗透测试常用方法

5.3.2.1 指纹识别

指纹识别测试包括以下内容：

a) 对操作系统进行指纹识别测试，方法包括 Banner 抓取、TCP 和 ICMP 常规指纹识别技术、数据包重传延时技术、使用渗透测试工具进行操作系统探测等；

b) 对 CMS 进行指纹识别测试，方法包括基于特殊文件的 md5 值匹配、请求响应主体内容或头信息的关键字匹配、基于 Url 关键字识别、基于 TCP/IP 请求协议识别服务指纹、在 owasp 中识别 Web 应用框架测试方法；
c) 对数据库进行指纹识别测试，方法包括常规判断（如 asp->sql server、php->mysql、jsp-oracle 等）、网站错误信息识别、端口服务识别（如 443->sql server，3306->mysql，1521->oracal）；
d) 对中间件进行指纹识别测试，方法包括通过 http 返回消息中提取 server 字段、通过端口服务探测中间件、通过构造错误界面返回信息查看中间件（例如通过 nginx 和 Tomcat 爆出中间件的版本信息）。

5.3.2.2 漏洞扫描

漏洞扫描测试包括以下内容：
a) 进行网络安全漏洞扫描测试，发现目标主机或网络，搜集目标信息，根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞；
b) 进行主机漏洞扫描测试，从系统用户的角度检测计算机系统的漏洞，包括应用软件、运行的进程、注册表或用户配置等存在的漏洞；
c) 进行数据库漏洞扫描测试，通过自动扫描和手动输入发现数据库，经授权扫描、非授权扫描、弱口令、渗透攻击等检测方式发现数据库安全隐患，形成修复建议报告提供给用户。

5.3.2.3 弱口令破解

弱口令测试包括以下内容：
a) 建立并维护常用的弱口令字典，并保证字典具备较高的命中率；
b) 通过访谈及调研的形式确认目标系统不存在统一分发的弱口令，或确认每个账户的默认口令各不相同且无法基于自身分配的口令对其他账户的口令进行预测；
c) 通过测试确认不能够使用空口令登录目标系统；
d) 通过测试确认不存在能够使用弱口令登录的高权限账户；
e) 对于第三方应用，应通过测试确认第三方应用不存在可预测的默认口令。如出厂口令或可轻易与开发商信息相关联的常见口令。

5.3.2.4 文件下载

文件下载测试内容包括以下内容：
a) 对下载的文件类型、目录做合理严谨的过滤；
b) 利用“../”跳转上级目录，直至跳转到想要下载的目录，测试是否能够查看或下载任意敏感文件；
c) 测试是否能利用漏洞进一步攻入服务器。

5.3.2.5 文件上传

文件上传测试包括以下内容：
a) 通过测试确认系统不存在可以直接部署网页脚本的文件上传功能；
b) 通过测试确认存储上传文件的 Web 应用服务不存在脚本解析漏洞；
c) 通过测试确认上传文档前经过有效的身份验证；
d) 通过测试确认文件上传的校验在服务端进行。

5.3.2.6 命令注入

命令注入测试包括：

a) 用&&、&、|、||判断是否无命令注入；
b) 检查是否有过滤；
c) 检查是否不能绕过。

5.3.2.7 SQL 注入

SQL注入测试包括：

a) 涉及增、删、改的注入测试，应在仿真环境下进行，严禁在生产环境中进行增、删、改相关的各类 SQL 注入测试；
b) 严禁使用第三方运维的域名解析记录平台进行带外注入测试；
c) 在使用了 NoSQL 及 ORM 相关的技术系统中，测试方应根据相关技术特点调整测试手段以便充分发现 SQL 注入风险；
d) 对所有可能存在数据库查询的功能进行 SQL 注入测试。

5.3.2.8 跨站脚本

跨站脚本测试包括：

a) 在进行存储型跨站脚本测试时，应确保写入内容能够通过测试账号进行自行删除，如无法自行删除，应在仿真环境下进行测试；
b) 严禁进行跨站脚本蠕虫测试；
c) 严禁使用第三方运维的跨站脚本反向代理平台进行测试；
d) 通过测试确认输入过滤及输出编码措施的有效性。

5.3.2.9 跨站请求伪造

跨站请求伪造测试包括：

a) 梳理并记录所有与身份强相关的单项操作，包括但不限于不需要原密码的密码修改功能、增加用户功能、删除用户功能、赋予用户权限功能、转账功能、发送公告功能等；
b) 如使用 Referer 校验，则应通过测试确认不存在域内的 CSRF 漏洞；
c) 如使用 Token 校验，则应通过测试确认 Token 验证与会话标识强相关；
d) 如使用双重校验，则应通过测试确认验证码不可预测且不可绕过；
e) 如使用图形验证码，则应通过测试确认图形验证码不可预测且不可绕过；
f) 通过测试确认目标系统无法进行 JSON 和 JSONP 劫持攻击。

5.3.2.10 失效的身份认证

失效的身份认证测试包括：

a) 进行密码破解测试；
b) 进行用户名猜解测试；
c) 进行用户名枚举测试；
d) 进行绕过双因子验证测试；
e) 进行暴力破解 2FA 验证码测试；
f) 进行重置用户密码测试；

g） 进行修改用户密码测试。

5.3.2.11 失效的访问控制

失效的访问控制测试包括：

a） 进行文件包含/目录遍历测试；
b） 进行文件上传、文件包含、任意文件下载、任意文件删除测试；
c） 进行权限绕过（水平越权）测试；
d） 进行权限提升（垂直越权）测试；
e） 对不安全直接对象的引用进行测试。

5.3.2.12 安全配置错误

安全配置错误测试包括：

a） 通过访问默认帐户，测试是否能获得未经授权的访问；
b） 通过访问未使用的页面，测试是否能获得未经授权的访问；
c） 通过访问未修补的漏洞，测试是否能获得未经授权的访问；
d） 通过访问未受保护的文件和目录，测试是否能获得未经授权的访问。

5.3.2.13 已知漏洞组件使用

使用渗透测试扫描工具进行组件漏洞扫描，测试是否存在已知漏洞的库文件、框架和其他软件模块的组件。

5.3.2.14 业务逻辑缺陷

业务逻辑缺陷测试包括：

a） 通过浏览器或渗透测试工具发出对于指定 URL 的请求，检查是否能实现对于特定接口的越权访问；
b） 针对 Cookie 内的参数进行修改，进行提权测试；
c） 通过工具或者脚本直接调用用户名、密码校验接口，检查是否能绕过验证码的校验和刷新逻辑，对登录接口进行暴力破解。

5.3.2.15 信息泄露

信息泄露测试包括：

a） 测试连接数据库的账号密码所在的配置文件，查看配置文件中的账号密码是否被加密；
b） 进入一个有敏感信息的页面(如带有修改口令的页面)，单击右键查看源文件，查看源文件中是否包含明文的口令等敏感信息；
c） 进入一个有敏感信息的页面(如带有修改口令的页面)，单击右键，查看源文件中有关注释信息是否包含明文的口令等敏感信息；
d） 构造一些异常的条件来访问 Web 系统，观察其返回的信息以判断系统是否存在信息泄漏的问题。常见异常处理包括不存在的 URL、非法字符和逻辑错误等；
e） 测试存储在服务器上的配置文件、日志、源代码等是否存在漏洞；
f） 测试 Web 服务器默认提供的服务器状态信息查询功能，是否会泄漏系统信息；
g） 测试 HappyAxis.jsp 页面中是否存在一些服务器的敏感信息。

5.4 测试流程

渗透测试流程见图1。

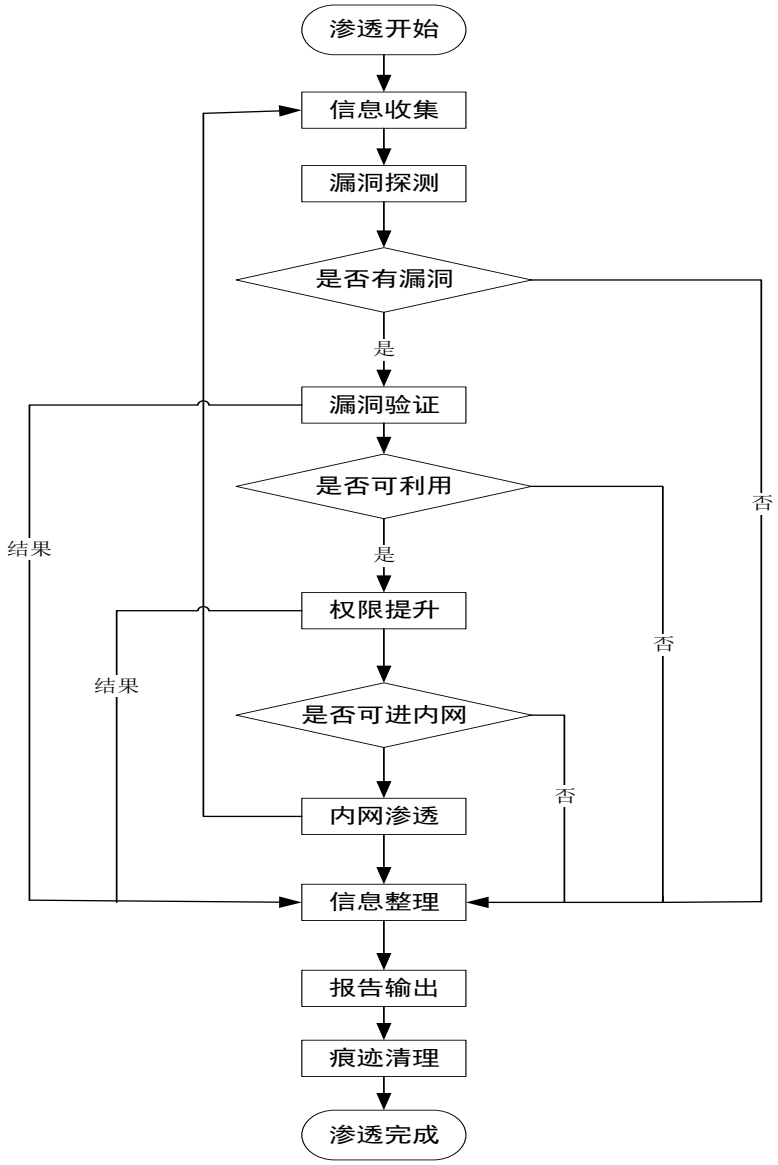

图1 渗透测试流程图

5.4.1 信息收集

信息收集分为主动信息收集和被动信息收集，即：

a) 主动信息收集包括服务器和中间件信息收集、端口信息收集、子域名信息收集、域名目录遍历、目标 IP 收集等，通过直接访问、扫描网站获取目标信息的行为；

b) 被动信息收集包括旁站 C 段查询、CMS 类型、敏感目录/文件收集、whois 信息收集等，对公开渠道可获得的信息，主要对互联网的信息进行收集。

5.4.2 漏洞探测

5.4.2.1 当完成信息收集之后，对网站进行漏洞探测，方法包括：

a) 使用工具进行漏洞扫描：AWVS、AppScan；
b) 结合漏洞去 exploit-db 等平台找漏洞利用程序集；
c) 进行 POC 测试，针对具体应用的验证性测试。

5.4.2.2 漏洞包括以下内容：

a) 系统漏洞：系统没有及时打补丁；
b) Websever 漏洞：Websever 配置问题；
c) Web 应用漏洞：Web 应用开发问题；
d) 其它端口服务漏洞：21/8080(st2)/7001/22/3389 等；
e) 通信安全：明文传输，token 在 cookie 中传送等。

5.4.3 漏洞验证

针对“漏洞探测”中发现的有可能被利用的漏洞进行进一步验证。结合实际情况，搭建模拟环境进行试验，成功后再应用于目标中。以下是几个常见漏洞的验证方法：

a) 自动化验证：结合自动化扫描工具对系统进行扫描，提供的结果；
b) 手工验证：根据公开资源进行手动验证；
c) 试验验证：搭建模拟环境进行验证；
d) 登录猜解：尝试猜解登录口的账号密码等信息，登录系统；
e) 业务漏洞验证：如发现业务漏洞，需要进行验证；
f) 公开资源的利用：exploit-db/wooyun/、渗透代码网站、通用或缺省口令、厂商的漏洞警告等。

5.4.4 权限提升

权限提升包括两种情况：

a) 目标系统存在重大弱点，可以直接控制目标系统；
b) 目标系统没有远程重大弱点，但是可以获得远程普通权限，通过该普通权限进一步收集目标系统信息获取本地权限，收集本地资料信息，提升本地权限。

5.4.5 内网渗透

内网渗透有两种方式：

a) 攻击外网服务器，获取外网服务器的权限，利用外网服务器作为跳板，攻击内网其他服务器，最后获得敏感数据；
b) 攻击内网的系统、内网电脑、内网无线等方式，控制办公电脑，用获得的办公网数据获取内网或者生产网的有用数据。

5.4.6 信息整理

信息整理包括以下三个方面：

a) 整理渗透过程中在渗透工具上用到的代码，如 poc，exp 等；
b) 整理收集信息：整理渗透过程中收集的信息；
c) 整理漏洞信息：整理渗透过程中发现的各种漏洞，各种脆弱位置信息。

5.4.7 报告输出

按照跟客户确定好的范围，需要进行整理资料，并将资料形成报告。要对漏洞成因、验证过程和带来危害进行分析，并提出修补建议，对所有产生的问题提出合理高效安全的解决办法。完成渗透测试报告编写。渗透测试报告包括执行层面的内容、技术层面的内容。

a) 执行层面的内容：业务说明、测试策略方法说明、项目风险评估等；
b) 技术层面的内容：识别系统性问题和技术根源分析、渗透测试评价指标、技术发现、可重现结果、应急响应和监控能力、标准组成部分。

5.4.8 痕迹清理

Windows系统：

a) 可用 MSF 中的 clearev 命令清除痕迹；
b) 如果 3389 远程登录过，需要清除 mstsc 痕迹；
c) 执行命令清除日志：del %WINDR%* .log /a/s/q/f；
d) 如果是 web 应用，找到 web 日志文件，删除。

Linux系统，在获取权限后，执行以下命令，不会记录输入过的命令：

a) 删除 /var/log 目录下的日志文件；
b) 如果是 web 应用，找到 web 日志文件，删除。

6 管理要求

6.1 渗透测试授权

用户应对渗透测试所有细节和风险知晓、所有过程都在用户的控制下进行。

由测试方书写实施方案初稿并提交给客户进行审核。在审核完成后，从客户获取对测试方进行书面委托授权书，授权测试方进行渗透测试，委托授权书格式参照附录A。

6.2 管理基本要求

管理基本要求包括：

a) 应针对渗透测试的原理和特点，建立管理制度，明确对应管理工作的目标、范围、原则及实施框架。渗透测试的原理和特点见附录 B；
b) 应针对渗透测试工作各个相关角色明确定义和职责分工；
c) 应针对渗透测试工作各个相关角色制定明确的操作规程；
d) 应针对渗透测试工作的重要及关键操作建立审批流程；
e) 应对渗透测试方的身份、背景及专业资质进行审查，并签署保密协议；
f) 测试方应在测试前向委托方提供真实准确的测试方案。方案内容包括但不限于测试项清单、测试时间计划和测试人员信息等；
g) 委托方和测试方均应设置紧急联系人,以便必要时进行沟通；
h) 应将测试方案中的测试人员信息进行统一备案，包括但不限于姓名和手机号码等，委托方应仅保留能够通过测试方定位到具体人员的基本信息，由测试方留存与人员身份相关的敏感信息；
i) 应对渗透测试接入的区域、系统、设备和信息等内容应进行书面的规定和记录，并按照规定严格执行；
j) 应对渗透测试制定实施计划，并根据实施计划推进渗透测试工作。实施计划应向所有渗透测试相关方同步；

k） 应指定或授权专门的部门或人员负责渗透测试实施过程的监督和管理；
l） 测试方应对渗透测试实施人员的行为规范进行书面规定，一旦发现违反行为规范的行为应严格按照规定处理。测试方应出具正式的渗透测试报告，其中应至少包含渗透测试目标、人员、时间、测试步骤、测试分析和测试结论以及附录 C 中的渗透测试报告样例所示的其它内容；
m） 委托方可要求测试方在测试实施过程中，参照附录 D 中的漏洞报告样例针对所发现的问题按需逐个提交漏洞报告；
n） 测试方应对渗透测试残留文件进行明确的记录和说明。测试方有义务协助委托方进行残留文件清除及排查工作；
o） 测试方应提供可落地的修复建议；
p） 应针对渗透测试报告进行严格归档和访问授权；
q） 对于网络安全等级保护三级及以上的应用系统及服务，每年应至少进行 1 次渗透测试；
r） 应定期开展互联网和内网资产测绘工作并进行漏洞扫描测试，每年不少于 4 次；
s） 委托方应指定或授权专门的部门负责渗透测试验收的管理，并按照管理规定的要求完成渗透测试验收工作。

附 录 A
（规范性）
渗透测试授权委托书模板

渗透测试授权书

甲方：_____

乙方：_____

甲方委托乙方在20XX年XX月XX日至20XX年XX月XX日对甲方的_____系统进行渗透测试。为确保测试的顺利进行，并保证甲方系统、应用及网络的稳定性和数据的安全性，甲乙双方就下述事宜达成一致，特制定本协议。

一、甲方责任

1、甲方向乙方提供准确的被测系统的IP或域名信息。

2、甲方允许乙方在测试过程中对所获取的信息进行必要的记录。

3、甲方相关技术人员应当全程参与漏洞扫描工作，漏洞扫描所涉及甲方的设备上机操作完全由甲方人员进行，乙方进行结果记录。

4、若甲方要求乙方提供相关测试工具，则甲方不可使用乙方所提供的工具从事危害网络安全的非法行为，否则引起的一切责任由甲方承担。

5、甲方在未经乙方允许的情况下，不得泄露乙方在工作过程中所使用的工具及相关输出。

6、甲方已了解渗透测试被测系统可能带来如下影响：

1）对被测网络设备或主机造成异常运行或停机的可能；

2）对被测主机上的各种系统服务和应用程序造成异常运行或终止运行的可能；

3）漏洞扫描期间，被测主机上的各种服务的运行速度可能会减慢；

4）漏洞扫描期间，网络的处理能力和传输速度可能会减慢。

7、甲方在进行渗透测试之前针对渗透测试可能对系统带来的影响和后果已做好充分应对准备和采取适当措施，如在测试之前做好系统的全面备份。

8、乙方在授权许可范围内开展渗透测试活动而对甲方产生任何不良后果，甲方同意承担相关风险。

二、乙方责任

1、乙方用_____渗透测试工具对_____甲方系统进行渗透测试。

2、对于乙方在测试过程中所获取的任何信息，仅在编写报告时使用。

3、未经甲方授权，乙方不得向任何个人或单位提供测试过程中所获取的信息。

4、乙方在测试过程中应尽量避免影响甲方业务的正常运转，若出现意外操作而导致异常则应立刻通知甲方并积极配合协商解决。

5、乙方承诺不对外泄露甲方测试信息。

6、乙方承诺在取消授权后，销毁所有涉及授权的机密资料。

7、乙方不按规定时间或不使用规定的工具对指定系统进行渗透测试，由此产生的不良后果由乙方承担。

甲方：

甲方代表签字（盖章）

年　　月　　日

乙方：

乙方代表签字（盖章）

年　　月　　日

附 录 B
（资料性）
渗透测试原理和特点

B.1 原理

渗透测试主要依据CVE已经发现的安全漏洞，以及隐患漏洞。模拟入侵者的攻击方法对应用系统、服务器系统和网络设备进行非破坏性质的攻击性测试。

B.2 特点

入侵者的攻击入侵需要利用目标网络的安全弱点，渗透测试也是同样的道理，对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。测试人员模拟真正的入侵者入侵攻击方法，以人工渗透为主，辅助以攻击工具的使用，以保证整个渗透测试过程都在可以控制和调整的范围之内，同时确保对网络没有造成破坏性的损害。

由于采用可控制的、非破坏性质的渗透测试，因此不会对被评估的客户信息系统造成严重的影响。在渗透测试结束后，客户信息系统将基本保持一致。

附 录 C
（资料性）
渗透测试报告样例

渗透测试报告的编制可参考表C.1。

表C.1 渗透测试报告样例

<table>
<tr><td>单位名称</td><td colspan="6"></td></tr>
<tr><td>测试时间</td><td colspan="6">xxxx 年 xx 月 xx 日（生效）至 xxxx 年 xx 月 xx 日（截至）；
测试时间段--：--至--：--</td></tr>
<tr><td>测试类型</td><td colspan="6">☐自评估 ☐检查评估</td></tr>
<tr><td>测试单位</td><td colspan="6">☐内部测试 ☐外部服务机构测试
（外部测试机构名称）</td></tr>
<tr><td rowspan="2">负责人</td><td>姓名</td><td colspan="2"></td><td>单位</td><td colspan="2"></td></tr>
<tr><td>职务</td><td colspan="2"></td><td>联系方式</td><td colspan="2"></td></tr>
<tr><td>测试账号</td><td colspan="6"></td></tr>
<tr><td>测试工具</td><td colspan="6"></td></tr>
<tr><td>测试目标</td><td colspan="6">☐限制目标 ☐不限制目标</td></tr>
<tr><td rowspan="3">测试范围</td><td>站点</td><td colspan="5"></td></tr>
<tr><td>IP</td><td colspan="5"></td></tr>
<tr><td>服务器环境</td><td colspan="5"></td></tr>
<tr><td>漏洞数量</td><td>高危</td><td></td><td>中危</td><td></td><td>低危</td><td></td></tr>
<tr><td>应用分级</td><td colspan="2">重要系统服务</td><td></td><td colspan="2">其他系统服务</td><td></td></tr>
<tr><td>参考标准</td><td></td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
</table>

附 录 D
（资料性）
漏洞报告样例

渗透测试漏洞报告的编制可参考表D.1。

表D.1 渗透测试报告样例

<table>
<tr><td rowspan="2">测试时间</td><td rowspan="2"></td><td>测试人</td><td rowspan="2">漏洞编号</td><td rowspan="2"></td></tr>
<tr><td>联系方式</td></tr>
<tr><td rowspan="2">测试目标</td><td>名称</td><td colspan="3"></td></tr>
<tr><td>信息</td><td colspan="3"></td></tr>
<tr><td>漏洞路径</td><td colspan="4"></td></tr>
<tr><td>漏洞类型</td><td colspan="4"></td></tr>
<tr><td>漏洞等级</td><td colspan="4">□高危 □中危 □低危</td></tr>
<tr><td>漏洞描述</td><td colspan="4"></td></tr>
<tr><td>漏洞危害</td><td colspan="4"></td></tr>
<tr><td>漏洞证明</td><td colspan="4"></td></tr>
<tr><td>修复建议</td><td colspan="4"></td></tr>
</table>