附件 9

ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0232—2021

银行互联网渗透测试指南

Guidelines for internet penetration test in bank

2021－07－22 发布　　2021－07－22 实施

中国人民银行　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。

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。

本文件由中国银行业协会提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国银行业协会、中国工商银行股份有限公司、中国农业银行股份有限公司、中信银行股份有限公司、兴业银行股份有限公司、北京银联金卡科技有限公司、中金金融认证中心有限公司、北京梆梆安全科技有限公司、北京长亭未来科技有限公司。

本文件主要起草人：潘光伟、张芳、高峰、李宽、王阳、敦宏程、苏建明、刘涌、王贵智、蒋家堂、叶红、戴心齐、孟宪哲、李亚敏、王金希、李沁蕾、赵成刚、陈嘉、江超、李乐天、高强裔、刘淑敏、刘一鸣、马男。

引　言

渗透测试（Penetration Test）也叫穿透测试，是一种通过模拟真实世界中的攻击动作，发现并利用安全漏洞，进而检验、评估信息系统实际安全水平的测试方法。渗透测试具有深入、直接、客观的特点，是主动提升信息系统（尤其是互联网信息系统）安全性的有力手段，已得到了广泛使用。互联网渗透测试主要模拟的是来自互联网的攻击行为，是当前最主要的一种渗透测试形式。银行信息系统是国家的重要基础设施，对互联网的依赖与日俱增，面临的互联网攻击也日趋严峻。因此通过互联网渗透测试这一技术手段主动发现安全漏洞也是当前银行普遍的现实需求。

渗透测试虽然是一项基础的安全技术，但在不同的行业应用场景下又有各自的特殊性。银行信息系统直接涉及资金安全，且需要非常高的稳定性，不规范的渗透测试不仅无法全面覆盖与资金安全密切相关的核心安全风险，还可能给系统的安全稳定带来负面影响。

因此，在国家层面尚未建立成熟的渗透测试实施相关标准的情况下，很有必要从行业安全的角度，结合银行业务的特点，针对性地制定一套规范的银行互联网渗透测试方法，以保障测试质量、控制实施风险，确保银行机构能更加规范、系统、有效、方便地开展互联网渗透测试工作。

基于以上行业需求，制定本文件。依照本文件开展渗透测试时，首先遵循国家的法律法规、监管制度及强制性标准的最新条款，如本文件与前述各项条款矛盾，遵循前述各项条款。

银行互联网渗透测试指南

1 范围

本文件提供了在银行信息系统中开展互联网渗透测试的整体流程以及流程各个环节中保障测试质量、控制测试风险的指南。

本文件适用于银行互联网渗透测试的策划、设计、执行、总结，也供保险、证券等其他金融行业参考。

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 15532—2008 计算机软件测试规范

GB/T 25069—2010 信息安全技术 术语

GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

JR/T 0101—2013 银行业软件测试文档规范

3 术语和定义

GB/T 25069—2010和GB/T 29246—2017界定的以及下列术语和定义适用于本文件。

3.1

渗透测试 penetration test

渗透性测试

穿透性测试

以模拟真实攻击的动作，检测发现信息系统存在的技术漏洞，并利用漏洞突破信息系统的安全控制机制，进而评估信息系统面临的实际安全风险的一种测试手段。

[来源：GB/T 25069—2010, 2.3.87,有修改]

3.2

授权 authorization

通过技术手段界定渗透测试实施范围的过程。

示例：通过防火墙策略仅允许渗透测试实施人员访问测试范围内的信息系统。

[来源：GB/T 25069—2010, 2.1.33,有修改]

3.3

威胁代理 threat agent

有动机和能力破坏信息系统安全性的人或程序。

示例：企图通过攻击信息系统非法获取资金的黑客团伙。

3.4

威胁建模 threat modeling

对信息系统的资产、流程、攻击信息系统的主要动机、潜在威胁代理及其能力等进行分析，对相关的主体和关系进行有效组织。

注：威胁建模的目的是构建信息系统面临的最可能攻击场景。

3.5

敏感信息 sensitive information

由权威机构确定的必须受保护的信息，该信息的泄露、修改、破坏或丢失会对人或事产生可预知的损害。

注：敏感信息的具体分级标准宜参考JR/T 0197—2020。

[来源：GB/T 25069—2010, 2.2.4.7]

3.6

漏洞 vulnerability

脆弱性
弱点
信息系统中可能被攻击者利用的薄弱环节。
[来源：GB/T 25069—2010, 2.3.30,有修改]

3.7

实施风险 implement risk

渗透测试实施过程中可能对目标信息系统的保密性、完整性、可用性带来的影响。

3.8

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。
[来源：GB/T 25069—2010, 2.2.1.42]

3.9

仿真环境 simulation environment

为避免直接在目标信息系统中实施测试所引入的实施风险，仿照目标信息系统搭建且具备测试所需的各项条件的渗透测试实施环境。

示例：业务系统及配置与生产一致的测试环境；生产环境中与生产服务器配置一致但不承载实际业务的模拟服务器；与生产高度一致的网络靶场环境。

3.10

权限提升 privilege escalation

在低权限用户状态下，利用信息系统中存在的漏洞突破权限控制，获得该用户原本不具备的操作权限的过程。

示例：利用操作系统漏洞从普通用户权限提升为超级管理员用户权限。

3.11

现场清理 site clearing

渗透测试实施完毕后，将目标信息系统恢复到测试前状态的过程。

示例：删除上传到目标信息系统中的测试脚本。

3.12

应急预案 contingency plan

一种关于备份、应急响应和灾后恢复的计划。
[来源：GB/T 25069—2010, 2.2.3.4]

3.13

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的特性。
[来源：GB/T 29246—2017, 2.12]

3.14

完整性 integrity

准确和完备的特性。
[来源：GB/T 29246—2017, 2.40]

3.15

可用性 availability

根据授权实体的要求可访问和可使用的特性。
[来源：GB/T 29246—2017, 2.9]

3.16

遵从性 compliance

遵守指导活动的相关条款的程度。

4 概述

银行互联网渗透测试是指从互联网渠道发起的针对银行信息系统的渗透测试，宜按照GB/T 15532—2008中4.3规定的要求，将测试流程划分为策划、设计、执行、总结四个阶段，并根据整体测试情况编制总结文档。渗透测试过程中的相关文档，宜按照JR/T 0101—2013中4.4.3规定的要求，给出的单项测试三级规范编制。

5 渗透测试策划

5.1 概述

渗透测试策划（以下简称测试策划）主要进行渗透测试需求分析，包括确定测试范围，确定测试引用文档，确定测试项以及被测试特性和不被测试特性，确定测试方法与测试通过准则，确定暂停准则和恢复条件，规定测试活动、任务与进度，明确环境需求，分配职责、权限和各部门间的工作衔接，明确人员配备和培训目标，明确风险和应急措施，确定质量保证过程。在测试过程中，如发现在测试规划阶段确定的内容有变化，宜及时变更测试策划，并妥善管理测试策划的版本。

应用程序编程接口（API，Application Programming Interface）方式接入前，需要进行接入方系统改造和接口开发，并与接口平台开展联调测试，其中功能测试和业务场景测试是必做项。

5.2 确定测试范围

概述本渗透测试涉及到的范围及其特征。

示例：本渗透测试在因特网中国境内网段，针对实际生产环境进行。

5.3 确定测试引用文档

确定开展渗透测试所考虑的需求因素，每个文档宜明确具体的标识（包括版本）和条款，典型的引用文档包括：

a) 国家监管制度。

b) 金融行业监管制度。

c) 组织自身安全管理策略规范。

d) 团体组织准入规范。

示例：支付卡行业安全标准委员会（PCI SSC，Payment Card Industry Security Standards Council）、环球银行金融电信协会（SWIFT，Society Worldwide Interbank Financial Telecommunication）等团体组织均有定期对特定信息系统进行渗透测试的相关规范。

e) 业务需求以及非功能需求。

示例：某些重要业务系统需要很高的安全性，上线前和（或）上线后可能会提出专项的渗透测试需求。

5.4 确定测试项

根据界定的测试范围，确定具体的渗透测试对象。测试项宜能够进行明确的标识和界定。

示例：测试项通过具有唯一性的属性予以标识的例子包括互联网协议（IP，Internet Protocol）地址、域名、域名+统一资源定位符（URL，Uniform Resource Locators）、客户端程序版本、客户端程序文件哈希值。当测试范围为因特网中国境内网段实际生产环境时，测试项为银行的整个信息与通信（ICT，Information and Communications Technology）系统。

5.5 确定被测试特性和不被测试特性

确定具体的渗透测试特性，即渗透测试针对测试项的哪些方面和不针对哪些方面。

示例：当测试范围为因特网中国境内网段，测试项为银行的整个 ICT 系统时，被测试特性为针对通用信息技术产品的通过互联网的攻击和利用应用系统业务需求逻辑漏洞进行的攻击。不被测试特性包括高级可持续威胁（APT，Advanced Persistent Threat）攻击和分布式拒绝服务（DDOS，Distributed Deny Of Service）攻击。

5.6 确定测试方法与测试通过准则

根据渗透测试的目的、内容以及实施特性，选定渗透测试方法，明确成功实施该测试的准则。

示例：渗透测试全流程中典型的测试方法包括：

a) 搜索，如基于搜索引擎收集信息。

b) 扫描，如通过自动化扫描工具收集信息或检测漏洞。

c) 监听，如通过网络监听窃取未加密敏感信息。

d) 篡改，如篡改上传服务端的交易数据。

e) 绕过，如绕过登录控制直接访问敏感信息。

f) 滥用，如恶意、频繁地使用正常的业务功能。

g) 破解，如破解相关密码算法还原加密的敏感信息。

h) 逆向，如通过动态调试、反编译等方式掌握程序的运行逻辑。

i) 注入，如输入包含恶意代码的数据。

5.7 确定暂停准则和恢复条件

包括计划内暂停和计划外暂停两种情况。

在暂停后恢复时，宜关注是否需要进行回归测试。

5.8 测试交付项

确定可交付的文档。测试输入数据、测试输出数据以及测试辅助软件（如渗透测试工具的脚本），宜确定为可交付项。

5.9 确定测试活动、任务与进度

明确准备和执行渗透测试的主要活动、任务和所需的时间周期，粒度宜符合实际需要，对不同的活动、任务可按照不同的粒度进行规划。明确各项任务间的所有依赖关系和所需要的任何特殊技能。

示例：在典型情况下，具体的实施计划宜包括测试的起始时间点、测试的结束时间点或结束标志，以及测试周期内的具体实施时间段。

5.10 明确环境需求

典型的测试环境需求包括但不限于：

a) 所需的硬件。

b) 所需的软件，包括基础软件和测试工具软件。

c) 所需的特殊硬件设备。

d) 所需的网络环境，包括网络种类、带宽、账号。

e) 测试所需的基础数据。

f) 测试设计和执行的物理场地与办公设施。

g) 测试所需的银行产品凭据。

5.11 分配职责、权限和各部门间的工作衔接

确定负责管理、设计、准备、执行、监督和解决问题的各个小组，实现所有的工作任务均有任务属主，且明确承担相关属主角色之间的不兼容职责。所有参与者从承担责任上分为任务属主或参与者。从时间投入上分为全职人员或共享人员。宜确定这些个人和小组之间交流的内容和方法，包括阐明信息流和数据流的图表。

按最小权限原则对渗透测试全体人员进行合理授权。对涉及到内部网络的，宜仅开通测试所需的网络访问范围和相关支撑系统、应用系统所必要的用户权限。

对所有渗透测试涉及的文档（包括本计划）、工具、数据的归属、共享做出规定。

5.12 明确人员配备和培训目标

根据任务和设置的小组与职责提出对人员的配备和技能的需求，对不具备相关技能的情况，说明如何进行培训。

示例：指导组、工具组、环境组人员来自专业团队且已经具备了所需的知识与技能。设计组需外部专家指导且已经在相关采购合同中包括了所需的人员，需要由工具组和外部专家进行工具脚本设计和工具使用的专业培训。

5.13 明确风险和应急措施

标识测试策划的风险假设，提出应对各种风险的应急措施。

示例：本渗透测试可预料到的风险和应急措施包括：

a) 对生产环境可能导致的破坏风险，应急措施为提前编制应急预案，提前备份敏感数据及重要系统。

b) 对生产环境的功能产生影响的风险，应急措施为提前编制应急预案，实施过程中暂停测试，并马上启动对该功能涉及到应用系统的修复。

c) 对生产环境的性能产生影响的风险，应急措施为加强对应用系统的监控，实施阶段的渗透攻击环节错开生产业务高峰期，限制自动化工具的并发数。

d) 测试过程中误操作可能导致的风险，应急措施为测试均应采用脚本化方式，操作时双人实施。

e) 渗透测试不充分导致的残留风险，应急措施为对测试结果进行分析，保留测试现场数据和测试用例、规程数据，以便后期通过回归测试复现测试过程。

5.14 确定质量保证过程

明确为保证测试过程和产品质量所用的方法，包含或引用异常的跟踪和解决过程。

示例：所有的渗透测试均经过设计，编制了测试规格说明并经过评审。所有的测试过程均编制了测试日志，经质量控制人员审核，记录内容与测试过程一致。编制了测试总结报告并通过评审。

5.15 测试策划阶段文档

在测试策划阶段，宜按照JR/T 0101—2013中第5章规定的要求，制定测试策划。在本测试复用概率较低、且对后继工作影响较小情况下，可按照JR/T 0101—2013中第10章规定的要求，编制测试预案中与测试策划相关的部分。在应急测试时，宜按照JR/T 0101—2013中第15章规定的要求，编制测试综合报告中涉及到测试策划的相关内容。

在确定质量保证过程中，参考相关文档进行审核时，测试规格说明宜按照JR/T 0101—2013中第9章规定的要求编制；测试日志宜按照JR/T 0101—2013中第11章规定的要求编制，测试总结报告宜按照JR/T 0101—2013中第14章规定的要求编制。

6 渗透测试设计

6.1 概述

渗透测试设计（以下简称测试设计）是按照测试策划，进一步细化针对被测试特征的测试方法和通过准则，选用已有的测试用例或设计新的测试用例；获取并验证测试数据；确定测试用例执行顺序的测试规程；准备测试工具并在必要时开发测试软件；建立并验证测试环境；进行测试就绪评审。

在测试设计过程中，发现测试策划需要变更的，宜在经过评审后及时变更测试策划，使测试策划与测试规格保持一致与协调。

6.2 确定测试范围

说明本渗透测试涉及到的范围及其特征。

若测试策划的范围描述已经能够满足对不同测试方法的设计，则可直接参考该测试策划。在必要时，可针对测试策划中描述的测试范围有选择地进行细化，以说明应用相关测试方法的必要性。

6.3 被测试特征、测试方法与通过准则

在测试策划描述的测试项、测试方法与测试通过准则的基础上，针对每一测试特征，在必要时细化测试方法。描述的粒度宜能按照给定的方法进行测试用例和测试规程的设计。

示例：测试项、测试方法与测试通过准则见测试策划。

6.4 测试用例

6.4.1 测试用例标识规则

明确测试用例描述的方式。不论采用哪种方式，均可唯一定位和检索，并说明使用的规则与注意事项。

6.4.2 测试用例概述

测试用例可根据测试的特征分组，其粒度可根据测试用例是新设计还是选用库中现有测试用例、测试设计，本测试使用是否需要执行回归测试，测试用例是否计划复用，以及实施人员的知识与技能综合确定。宜集中描述测试用例的公共属性，包括但不限于：

a) 对相关测试用例集合中每个输入都有效的约束条件。

b) 任何共享环境的需求。

c) 对共享的特殊规程的规定。

d) 共享的测试用例之间的依赖关系。

6.4.3 测试用例详述

6.4.3.1 概述

每个或每组测试用例均宜遵循的规范，具体如下：

a) 测试用例宜具有可操作性，完整包含测试用例执行所必不可少的各项内容，包括但不限于：

1) 对应的测试要点。

2） 适用测试规程（场景）描述。
3） 测试用例的输入和预期的结果。
4） 测试结果判定方法。
5） 案例实施所需数据，如用户。

b） 测试用例对应的测试要点覆盖整体测试规程，见附录A。
c） 测试用例宜满足的特殊需求。
d） 宜对测试用例潜在的实施风险及应急措施进行说明。
e） 生产环境下的渗透测试所使用的用户宜提前备案并全程监控。

6.4.3.2 测试用例编号

为本测试用例赋予一个唯一标识符，以便将其与其他测试用例区分开，宜通过自动工具生成标识符。

6.4.3.3 输入与输出说明

规定执行测试用例所需的各种输入（或测试方法）与预期的输出（或预期可能接收到的反馈）。宜参考“10项最严重的互联网应用程序安全风险列表”（OWASP Top10，Open Web Application Security Project Top10）等各项行业最佳实践，对本文件漏洞发现（见7.4）和攻击验证内容（见7.5.1）的每一项的用例制定明确的输入和输出说明，规定所有合适的数据库、文件、配置参数、接口报文、输入终端、内存驻留区域及操作系统传送的各个值。对于新技术、新业务场景等原因无法明确测试输入输出的，可采用莽撞测试的方法，宜描述具体数据记录的方法，但相关测试宜由具有三年以上渗透测试工作经验的测试人员完成，并提前获得测试需求方授权。

规定输入之间的所有必要的关系。

示例：输入存在时序，前导交易和后继交易均为输入之间的关系。

6.4.3.4 采用的测试设计方法

描述本测试用例所采用的测试设计方法。对于在6.3中已经详细描述的方法，本节不必重新描述，仅需引用。

注：本节的目的是使得所有测试用例都采用了已经确定的测试设计方法。

6.4.3.5 对其他用例依赖关系

列出本测试用例与其他用例的依赖关系，宜区分以下情况：

a） 其他用例是执行本测试用例的必要条件。
b） 本测试用例是执行其他用例的必要条件。

6.4.3.6 特殊需求说明

描述执行本测试用例时特殊的需求，包括但不限于管理需求、对人员的需求。对环境的需求宜在6.5中描述，本测试用例属于特殊情况的，宜在本节提及。

6.5 测试环境

6.5.1 概述

描述启动渗透测试、执行渗透测试和记录结果所需的测试环境，通常按每个（或每组）场景进行描述，可使用一个（或多个）图形来展示所有的环境组成成分及其间信息交互。渗透测试环境描述策略，具体如下：

a） 当渗透测试环境为生产环境时，可仅描述测试现场所需的环境。
b） 当在测试策划中对环境的描述足够清晰和细致的情况下，以及在单独制定了测试环境需求规格说明和（或）测试数据需求规格说明时，本节可直接引用这些文档。

c) 当测试策划、测试环境需求规格说明、测试数据需求规格说明发生变更时，本节宜对变更情况进行详细描述。

d) 仅为部分特殊的测试用例需求的测试环境，可不在本节描述。

6.5.2 测试执行环境

渗透测试实施前宜完成各项环境准备工作，具体如下：

a) 基础环境准备工作，当在为渗透测试专门搭建的仿真环境进行测试时，需说明与生产环境的差异并评价可比性，主要包括：
   1) 测试所需的系统资源，包括硬件、基础软件和支撑软件等。
   2) 测试所需的网络资源，包括硬件、地址、端口、账号等。
   3) 应用系统。
   4) 测试基础数据。

b) 监控审计环境准备工作，确保测试过程得到有效的监控和记录，该环境宜满足：
   1) 所有网络流量均得以记录，并在所需的时间周期（例如半年）内可用。
   2) 所有终端操作均得以记录，并在所需的时间周期（例如半年）内可用。终端操作记录方式可通过录屏、命令行日志记录等方式实现。
   3) 已采取信息防泄漏措施。

c) 对基础环境及监控审计环境的有效性设立了检查确认准则。

6.5.3 测试工具准备

渗透测试实施前宜完成各项工具准备工作，具体如下：

a) 准备以下常用渗透测试工具：
   1) 信息收集工具，如端口扫描工具、目录枚举工具、网络监听工具等。
   2) 漏洞扫描工具，如网站漏洞扫描工具、系统层漏洞扫描工具等。
   3) 漏洞利用工具，如暴力破解工具、数据包拦截和篡改工具、典型高危漏洞的专用工具等。
   4) 测试文档管理工具。
   5) 缺陷管理工具。

b) 非实施方自主开发测试工具宜具备可跟踪的、合规的获取路径。

c) 实施方自主开发测试工具宜由实施方进行工具安全性审查，重点审核不包含与银行互联网渗透测试实施无关的功能。

d) 对拟采用的工具进行详细记录，包括但不限于：
   1) 工具名称。
   2) 工具用途。
   3) 工具提供方。
   4) 工具获取途径。
   5) 工具版本号。
   6) 工具的散列值。

6.5.4 测试验证授权

对授权策略的执行情况进行验证，具体如下：

a) 测试实施人员宜具有达成测试目标所需的必要权限，包括以下内容：
   1) 测试对象网络可达。
   2) 具有特定权限的测试用户。

b) 根据测试目标配置合理的安全策略，包括以下内容：

1） 单纯以发现应用软件漏洞为目标的测试，宜通过白名单策略，放开对测试源的限制。
2） 以验证目标系统整体安全防护状况为目标的测试，不宜单独为测试源开通特殊安全策略。

c） 采取有效措施来控制测试实施人员行为超越授权范围的风险，包括以下内容：
1） 防火墙隔离。
2） 边界监控。
3） 日志审计。

6.6 测试过程描述

6.6.1 日志

列出记录日志的工具和方法，记录的内容包括测试执行的结果，任何观测到的异常，以及任何其他有关测试的事件。

6.6.2 建立

提供准备执行规程所需的动作序列。典型地，信息收集、威胁建模、漏洞发现都是建立的重要动作。

6.6.3 启动

提供开始执行规程所需的动作。典型地，渗透攻击是启动的重要动作。

6.6.4 处理

提供在规程执行过程中所需的动作。若测试用例按照场景或系列场景设计，即由多组输入、输出的有序排列构成，则不必在此重复描述测试用例的执行序列。

本文件描述的攻击过程（见7.5.2）是典型的处理过程。

6.6.5 度量

描述如何进行测试度量。度量可以是多维度的，例如对进度的度量和对测试结果的度量。

6.6.6 暂停

因计划外事件导致的临时暂停，描述测试所需的动作。对已经在测试策划中描述了暂停的，此处引用即可。

6.6.7 再启动

规定所有再启动点，描述在各再启动点上重新启动规程所必需的动作。对已经在测试策划中描述了再启动的，此处引用即可。

6.6.8 停止

描述正常停止执行时所必需的动作。

6.6.9 结束

描述在运行的规程全部执行完成后（包括终止记录日志），恢复环境所必需的动作。典型地，包括回收用于测试的权限。

6.6.10 应急

描述处理执行过程中可能发生的异常事件所必需的动作。

6.7 测试就绪评审

在测试执行前，宜对测试策划和测试设计进行评审，评审测试策划的合理性、测试环境和测试工具的有效性，以及测试用例的可操作性和覆盖充分性等。评审的主要内容有：

a) 评审测试策划的合理性，包括测试目标、测试项、测试内容、测试方法、时间计划及授权策略等的合理性。
b) 评审测试环境和测试工具的有效性。
c) 评审测试用例的可操作性和充分性。

6.8 测试设计阶段文档

在测试设计过程中，宜按照JR/T 0101—2013中第9章规定的要求，编制测试规格说明。对认为本渗透测试文档具有高度复用价值的，宜按照JR/T 0101—2013中第6、7、8章规定的要求，分别编制测试设计说明、测试用例说明和测试规程说明。在本测试复用概率较低且对后继工作影响较小情况下，可按照JR/T 0101—2013中第10章规定的要求，编制测试预案中与测试设计相关的部分；在应急测试时，宜按照JR/T 0101—2013中第15章规定的要求，编制测试综合报告中涉及到测试设计的相关内容。

如有必要，测试环境需求规格说明宜参照JR/T 0101—2013中附录D.4规定的要求，测试数据需求规格说明宜参照JR/T 0101—2013中附录D.5规定的要求。

7 渗透测试执行

7.1 概述

渗透测试执行（以下简称测试执行）是按照设计的过程执行测试用例，获得渗透测试结果，编制测试日志；分析并判定渗透测试是否达到预期以及是否进行多轮测试；测试结束前，审核测试记录文档是否完整、有效、一致；在测试过程中，如出现异常情况，按照测试设计进行处理并编制测试事件报告；完成全部预定的测试任务后，清理测试现场。

本章描述的是测试过程的典型活动，宜事先在测试设计的建立、启动、处理等活动中有所反映，鉴于渗透测试可能需要根据某个测试的结果动态进行调整，故本文件将有关活动的细节放在本章描述。

在应急测试时，编制测试综合报告中涉及到测试执行的相关内容。

在测试执行过程中，发现测试策划、测试设计需要变更的，宜在评审后及时变更，使测试策划、测试设计与实际执行的渗透测试保持一致与协调。

7.2 信息收集

渗透测试的信息收集宜根据具体的测试范围、测试引用文档和测试项，结合测试需求方提供的信息，在测试需求方认同并知晓的情况下，通过渗透收集或刺探性收集。

7.2.1 基础信息收集

渗透测试宜尝试进行基础信息收集，具体如下：

a) 网络信息，包括但不限于：
   1) 域名解析记录。
   2) IP 地址段。
   3) 开放端口。
b) 系统信息，包括但不限于：
   1) 设备类型。
   2) 操作系统版本，既包括通用操作系统也包括网络设备、专用硬件设备的专用操作系统。
   3) 已安装的软件，如中间件、数据库、虚拟化软件等。
   4) 操作系统和已安装软件的官方补丁列表。
c) 应用信息，包括但不限于：
   1) 开发语言。
   2) 开源框架或插件。

3) 功能接口。
4) URL 路径。
5) 业务功能。
6) 业务面向的用户群体。
7) 应用的官方补丁列表。

d) 安全防护信息，包括但不限于：
1) 已部署的安全防护产品功能。
2) 已部署的安全防护产品的厂商。

7.2.2 其他信息收集

渗透测试可尝试开展信息收集工作，具体如下：

a) 通过互联网等公开合法渠道进一步收集与本渗透测试相关的信息如下：
1) 相关文档资料。
2) 邮件列表。
3) 所处公共托管环境。
4) 已公开历史安全漏洞。
5) 通过公开渠道所收集的信息如为委托方已泄露的内部敏感信息，及时告知委托方。

b) 提升测试效率及质量，经委托方同意，实施方可申请直接从委托方获取部分测试对象相关信息如下：
1) 已使用的各类软、硬件及其版本。
2) 部分源代码。
3) 网络拓扑。

7.3 威胁建模

7.3.1 概述

威胁建模是指在分析业务功能特征基础上分析攻击者动机、判断最主要威胁场景的过程。不是所有渗透测试或黑客攻击都有该流程，在银行互联网渗透测试实施阶段引入该环节的目的是通过分析银行系统的不同业务特性，能更好地判断攻击动机，从而开展更加有针对性的测试。

7.3.2 攻击动机分析

在分析渗透测试对象承载的业务及其流程的基础上，分析评估潜在攻击者的攻击动机，具体如下：

a) 窃取资金。
b) 窃取敏感信息。
c) 作为入侵更重要系统的跳板。
d) 造成不良社会影响。

7.3.3 威胁主体分析

根据攻击动机分析结果，分析评估潜在的威胁主体及其能力，具体如下：

a) 分析潜在外部威胁主体：
1) 逐利的黑产团伙。
2) 追求知名度的非授权安全技术人员。
3) 敌对政治势力。
4) 无政府主义组织。

b) 分析潜在内部威胁主体：

1) 心怀恶意的员工。
2) 外包技术支持人员。

7.3.4 主要攻击场景判断

在攻击动机分析和威胁主体分析基础上，明确本次渗透所需要模拟的最主要攻击场景，并据此调整渗透测试案例及工具方法。

7.4 漏洞发现

7.4.1 基础漏洞发现

渗透测试的基础漏洞发现宜满足如下一般性操作要点：

a) 在使用自动化漏洞扫描工具检测漏洞的同时，根据威胁建模结果，有重点地开展手工漏洞检测工作。
b) 在生产环境中，不直接实施影响系统正常对外提供业务服务的漏洞检测技术。
c) 根据目标系统性能情况控制自动化漏洞扫描工具的并发数。
d) 在生产环境中，不直接对原有数据进行篡改。

7.4.2 应用层漏洞发现

根据信息收集情况，尝试检测发现潜在的应用层漏洞，具体如下：

a) 检测应用在身份鉴别方面的漏洞，包括但不限于：
   1) 弱口令。
   2) 图片验证码绕过。
   3) 认证绕过。
   4) 会话未正常结束。
   5) 登录请求重放。
   6) 短信验证码泄露。
b) 检测应用在访问控制方面的漏洞，包括但不限于：
   1) 越权访问。
   2) 交易步骤绕过。
   3) 内部接口暴露。
   4) 后台安全防控模型绕过。
c) 检测应用在敏感数据保护方面的漏洞，包括但不限于：
   1) 重要业务参数篡改与伪造。
   2) 数据访问频度控制不足。
   3) 数据重放。
   4) 返回非业务所需敏感数据。
d) 检测应用在网站实现层面的漏洞，包括但不限于：
   1) 结构化查询语言（SQL，Structured Query Language）注入。
   2) 操作系统命令注入。
   3) 可扩展标记语言（XML，Extensible Markup Language）注入。
   4) 代码注入。
   5) 跨站脚本（XSS，Cross Site Scripting）。
   6) 跨站请求伪造（CSRF，Cross Site Request Forgery）。
   7) 可执行文件上传。
   8) 任意文件下载。

9） 服务端请求伪造（SSRF，Server Side Request Forgery）。
10） 不正确的目录及页面访问控制。
11） 不正确的错误处理。
12） 存在通用应用层框架已知漏洞。

e） 检测应用在客户端程序实现层面的漏洞，包括但不限于：
1） 缓冲区溢出。
2） 敏感信息截取。
3） 功能接口滥用。
4） 程序逻辑逆向破解。
5） 生物识别突破。
6） 密码密钥硬编码。

7.4.3 网络层漏洞发现

根据信息收集情况，尝试检测发现潜在的网络层漏洞，具体如下：

a） 检测网络传输的敏感信息是否已采取有效的保密性和完整性保护措施，包括但不限于：
1） 机密数据是否加密传输。
2） 所使用密码算法是否安全。

b） 检测相关网络协议的安全性，包括但不限于：
1） 域名解析协议。
2） 路由交换协议。
3） 网络管理协议。
4） 文件传输协议。
5） 无线射频协议。

c） 检测网络安全策略中可能存在的漏洞，包括但不限于：
1） 防火墙策略不严格。
2） 入侵防御系统（IPS，Intrusion Prevention System）策略绕过。
3） 入侵检测系统（IDS，Intrusion Detection System）策略绕过。
4） 网站应用级防火墙（WAF，Web Application Firewall）策略绕过。

d） 检测网络设备中软件版本存在的已知漏洞。

e） 检测网络设备中存在的配置漏洞，包括但不限于：
1） 弱口令。
2） 权限过高。
3） 未限制远程管理地址。

7.4.4 系统层漏洞发现

根据信息收集情况，尝试检测发现潜在的系统层漏洞，具体如下：

a） 检测相关系统存在的已知版本漏洞。

b） 检测相关系统存在的配置漏洞，包括但不限于：
1） 弱口令。
2） 访问控制不严格。
3） 权限过高。

c） 检测相关系统在敏感数据存储方面的漏洞，包括但不限于：
1） 敏感信息明文存储。
2） 测试数据未变形。

7.5 渗透攻击

7.5.1 攻击验证内容

在渗透攻击阶段通过模拟实际攻击，尝试对漏洞的保密性、完整性、可用性及可能造成的实质影响进行验证，具体内容包括但不限于：

a) 通过模拟实际攻击，验证可能对保密性造成的实质影响，包括但不限于：
   1) 获取网络中敏感数据。
   2) 获取服务器中敏感文件。
   3) 获取数据库敏感信息。
   4) 获取应用系统中未授权访问的敏感信息。
b) 通过模拟实际攻击，验证可能对完整性造成的实质影响，包括但不限于：
   1) 获取数据库操作权限。
   2) 获取服务器控制权限。
   3) 获取专用设备控制权限。
   4) 获取应用系统管理权限。
   5) 篡改网站页面、应用逻辑等应用系统的各个组成部分。
   6) 篡改交易金额、账户、时间、重要提示信息等关键交易要素。
   7) 破坏交易的不可否认性。
c) 通过模拟实际攻击，验证可能对可用性造成的实质影响，包括但不限于：
   1) 导致网络不可用。
   2) 导致服务器不可用。
   3) 导致应用程序不可用。
   4) 导致数据库服务不可用。

7.5.2 攻击过程

在渗透攻击阶段宜尝试实施如下攻击过程：

a) 验证单个漏洞的可利用性及可能造成的实质影响。
b) 尝试通过多个漏洞的关联利用验证漏洞的综合可利用性及可能造成的实质影响。
c) 攻击获取权限后，如非系统最高权限，尝试开展权限提升可行性验证。
d) 攻击获取权限后，尝试横向渗透。以已有成果为基础，重复信息收集、威胁建模、漏洞发现、渗透攻击等环节，确定进一步攻击渗透其他目标的可能性。如具有可能性，开展相关验证工作。
e) 攻击实施完成后保存相关证据，包括但不限于截图、录像等。
f) 攻击实施完成并保存相关证据后，开展现场清理工作，确保应用系统得到恢复，包括但不限于删除上传的文件、删除增加的用户、删除安装的工具等。

7.5.3 风险控制

在渗透攻击阶段宜采取如下措施控制实施风险：

a) 攻击实施前在测试用例中说明含详尽步骤的攻击实施方案。
b) 攻击实施过程每个步骤的指令及结果均在测试日志中进行详细记录。
c) 如渗透测试执行过程涉及非法定必要的第三方人员，宜从如下方面做好工作：
   1) 评估第三方人员可执行的测试任务，使第三方人员仅接触必要且可控的信息。
   2) 在相关工作实施前与第三方人员及其派出单位签署保密协议。

3） 在项目实施过程中，第三方人员不能使用未经授权的设备，必要时不能携带电子设备入场。

4） 项目完成后，在做好备份的前提下，监督第三方人员清除测试现场，删除测试相关数据，妥善处置纸质记录文档。

d） 如相关工作的实施风险在生产环境不可接受，则在仿真环境中开展。

示例：对重要业务系统的DDOS攻击测试，在仿真环境中开展。

7.6 测试执行阶段文档

在测试执行阶段，宜按照JR/T 0101—2013中第11章规定的要求，编制测试日志；在测试过程中，如出现异常情况，按照测试设计进行处理并按照JR/T 0101—2013中第12章规定的要求，编制测试事件报告。

在应急测试时，宜按照JR/T 0101—2013中第15章规定的要求，编制测试综合报告中涉及到测试执行的相关内容。

8 渗透测试总结

8.1 概述

渗透测试总结（以下简称测试总结）包括整理和分析测试数据，说明实际测试与测试策划和测试设计的差异，进行测试充分性分析并描述未能解决的测试事件，进行测试结果汇总，给出建议和结论并说明依据，编制测试总结报告，并通过测试评审。

在应急测试时，编制测试综合报告中涉及到测试总结的相关内容并最终完成测试综合报告。

在认为必要时，可编制测试工作总结。

8.2 测试数据分析

对所有的测试日志进行分析。根据是否需要进行回归测试判定测试日志记录（包括采用信息化手段进行的记录）的完整性，确认根据测试日志得出测试结论的充分性和可信性。

8.3 差异分析

分析测试日志和测试事件报告记录的测试过程与测试策划和测试规格说明的一致性，对不一致的内容进行分析以判定是否实现了预定的测试覆盖。

按照基线管理策略，在此时对测试策划和测试规格说明进行变更的，宜进行必要的回归测试以保证最小的测试覆盖。

8.4 风险决策根据分析

8.4.1 分析目的

对安全漏洞的风险定级方法做出统一的原则性规定，同时提供一个参考性的风险定级计算工具，以实现：

a） 漏洞定级既考虑了技术风险，又考虑了银行业务的特性以及监管规定。

b） 本文件的应用者有较为统一的漏洞定级方法，为统一管理评价奠定基础。

8.4.2 分析维度

对风险的分析宜按照如下维度进行：

a） 信息系统重要性考量：

1） 受漏洞影响的信息系统整体重要性。

2） 受漏洞影响的具体功能模块的重要性。

b） 漏洞对信息系统安全属性的影响程度考量：

1） 对保密性的影响程度。

2) 对完整性的影响程度。
3) 对可用性的影响程度。

c) 漏洞本身的利用难度考量：
1) 漏洞被利用的前提条件限制。
2) 针对漏洞的攻击发起路径。
3) 攻击工具的获取难度及操作复杂度。

d) 遵从性主要考量漏洞的存在是否违背国家法律、法规及相关行业监管规定的情况。

根据上述描述可将漏洞带来的风险分为严重、高、中、低、提示五个级别，具体定级方法见附录B。

8.5 报告编写

8.5.1 总体设计

银行互联网渗透测试报告宜按照JR/T 0101—2013中第14章规定的要求编制，其中对引用文献中描述的内容，可根据需要在测试总结报告中做必要的引用，以便于阅读。

8.5.2 范围

概要描述本渗透测试的工作范围，宜特别说明是否对生产环境进行测试。
在认为必要时，可说明哪些内容没有包括在本渗透测试中。

8.5.3 引用文件

引用列出所有适用的引用文件。尤其是外部有关渗透测试的文件，以及内部的测试策划、测试规格说明文档。
为了便于阅读，宜说明对引用文件摘录到本测试总结报告中的情况。

8.5.4 测试概要情况

测试概要情况宜包括以下内容：

a) 规划及准备阶段各个环节的概要描述包括：
1) 委托方、实施方、实施人员。
2) 测试目标。
3) 测试对象。
4) 测试内容。
5) 测试方法。
6) 实施环境。
7) 工具清单。
8) 案例清单。

b) 在测试数据分析（见8.2）的基础上，描述实施阶段各个环节具体开展情况的概要描述包括：
1) 信息收集情况。
2) 威胁建模结论。
3) 漏洞发现情况。
4) 渗透攻击情况。

c) 在差异分析（见8.3）的基础上，说明制定的测试策划、测试规格说明与测试执行的差异以及必要的回归测试情况。

8.5.5 决策根据与结论和建议

决策根据与结论和建议宜包括如下内容：

a) 描述包括风险决策根据分析（见 8.4）的内容。

b) 所发现漏洞的详细技术分析及整改建议包括：

1) 漏洞在信息系统中的具体位置。

2) 漏洞的可利用情况及相关证据。

3) 漏洞的具体利用方式。

4) 漏洞的整改方案建议。

c) 所发现漏洞的整体统计分析及改进建议包括：

1) 不同维度的统计分布图。

2) 统计分析所反映的问题。

3) 针对相关问题的改进建议。

8.6 测试评审

在测试完成后，评审测试执行过程是否达到渗透测试目的。主要对测试执行过程中的信息收集和漏洞发现的覆盖充分性、威胁建模的有效性、渗透攻击的完整性和深入性，以及攻击验证内容的保密性、完整性、可用性进行评审。评审的主要内容有：

a) 评审信息收集和漏洞发现的覆盖充分性。

b) 评审威胁建模的有效性。

c) 评审攻击验证内容的保密性、完整性、可用性，以及攻击过程的深入性。

8.7 测试总结阶段文档

按照JR/T 0101—2013中第14章规定的要求，编制测试总结报告。

在应急测试时，宜按照JR/T 0101—2013中第15章规定的要求，编制测试综合报告中涉及到测试总结的相关内容并最终完成测试综合报告。

在认为必要时，可按照JR/T 0101—2013中附录D.2规定的要求，编制测试工作总结。

附 录 A
（资料性）
银行互联网渗透测试过程要点清单

本附录给出了在进行银行互联网渗透测试设计时需要考虑到的基本测试要点，见表A.1。

表 A.1 银行互联网渗透测试过程要点清单

一级项	二级项	三级项	测试要点
信息收集	基础信息收集	网络信息收集	IP 地址段信息收集
			开放端口信息收集
			域名解析记录收集
		系统信息收集	设备类型信息收集
			操作系统版本信息收集
			已安装软件信息收集
		应用信息收集	开发语言信息收集
			开源框架或插件信息收集
			功能接口信息收集
			URL 路径信息收集
			业务功能信息收集
			业务面向的用户群体信息收集
			应用的官方补丁信息收集
		安全防护	安全防护产品功能信息收集
			安全防护产品厂商信息收集
	拓展信息收集	互联网搜索	相关文档资料信息收集
			相关邮件列表信息收集
			所处公共托管环境信息收集
			已公开历史安全漏洞信息收集
		委托方提供信息	从委托方获取相关信息
威胁建模	目标对象分析	目标对象业务分析	业务流程分析
		目标对象价值分析	可能包含的敏感信息分析
			可能的资金窃取途径分析
			对入侵其他重要系统的帮助分析
			可能造成的社会影响分析
	威胁主体分析	外部威胁主体分析	外部威胁主体的动机及能力分析
		内部威胁主体分析	内部威胁主体的动机及能力分析
	主要威胁判断	明确主要攻击场景	明确主要攻击场景
漏洞发现	应用层漏洞发现	身份鉴别	弱口令检测

表 A.1　银行互联网渗透测试过程要点清单（续）

一级项	二级项	三级项	测试要点
漏洞发现	应用层漏洞发现		图片验证码绕过检测
			认证绕过检测
			会话未正常结束检测
			登录请求重放检测
			短信验证码泄露检测
		访问控制	越权访问检测
			交易步骤绕过检测
			内部接口暴露检测
			后台安全防控模型绕过检测
		功能逻辑	重要业务参数篡改与伪造检测
			频度控制不足检测
			数据重放检测
			返回非业务所需敏感数据检测
		网站程序实现	SQL 注入检测
			操作系统命令注入检测
			XML 注入检测
			代码注入检测
			XSS 检测
			CSRF 检测
			可执行文件上传检测
			任意文件下载检测
			SSRF 检测
			不正确的目录及页面访问控制检测
			不正确的错误处理检测
			存在通用应用层框架已知漏洞检测
		客户端程序实现	缓冲区溢出检测
			敏感信息截取检测
			功能接口滥用检测
			程序逻辑逆向破解检测
			生物识别突破检测
			密码密钥硬编码检测
		网络传输	机密数据是否加密检测
			密码算法是否安全检测
		网络协议	域名解析协议相关漏洞检测
			路由交换协议相关漏洞检测

表 A.1　银行互联网渗透测试过程要点清单（续）

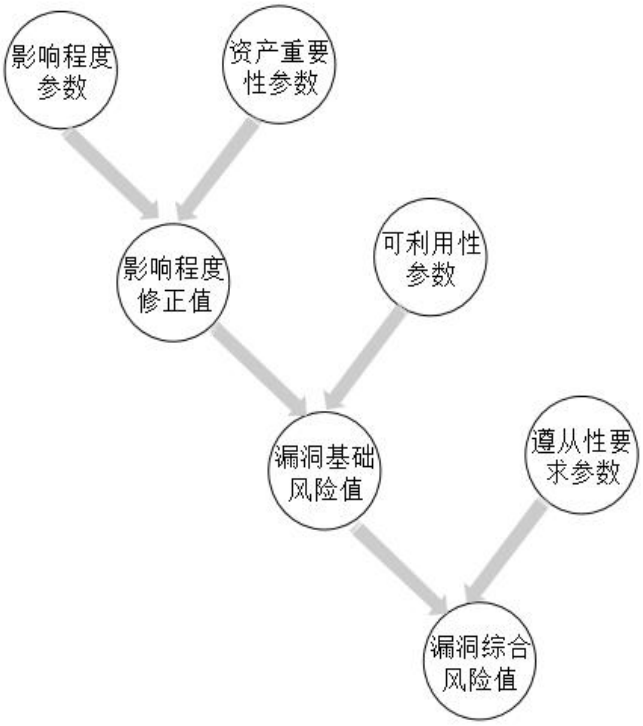
一级项	二级项	三级项	测试要点
漏洞发现	应用层漏洞发现		网络管理协议相关漏洞检测
			文件传输协议相关漏洞检测
			无线射频协议相关漏洞检测
		网络安全策略	防火墙策略不严格检测
			IPS 策略绕过检测
			IDS 策略绕过检测
			WAF 策略绕过检测
		网络设备软件版本	软件版本已知漏洞检测
		网络设备配置	弱口令检测
			权限过高检测
			远程管理地址限制检测
	系统层漏洞发现	系统软件版本	软件版本已知漏洞检测
		系统软件配置	弱口令检测
			访问控制不严格检测
			权限过高检测
		敏感数据存储	敏感信息明文存储检测
			测试数据未变形检测
渗透攻击	攻击过程（如无法在生产环境直接开展，则在仿真环境开展）	单个漏洞验证	尝试验证单个漏洞的可利用性（包括对保密性、完整性、可用性三方面造成的实质影响）
		关联利用	尝试多个漏洞的关联利用
		权限提升	尝试权限提升
		横向渗透	以已有成果为基础，尝试进一步攻击渗透其他目标的可能性
		保存证据	保存证据信息
		现场清理	删除上传的文件
			删除增加的用户
			删除安装的工具
在具体实施阶段，当某一测试用例需以某项特殊条件为前提时，如该前提客观上不存在，则该要点可标注为“不具备前提条件”，并说明具体原因。 **示例：**在设计“权限提升”用例时，宜以能获取某个系统的低级别权限的测试用例为前提。若在漏洞检测及模拟利用过程中并未发现可获取低级别权限的安全漏洞，则“权限提升”要点即为“不具备前提条件”。			

附 录 B
（资料性）
银行互联网渗透测试漏洞风险定级参考

B.1 概述

本附录是在参考通用漏洞评分系统（CVSS，Common Vulnerability Scoring System）、开放式互联网应用程序安全项目（OWASP，Open Web Application Security Project）等漏洞定级相关业界最佳实践方法基础上，结合银行信息系统的特点制定。

本附录提出先通过影响程度、资产重要性、可利用性、遵从性4个参数计算出漏洞综合风险值，再根据风险值给出定性的漏洞风险等级判定，具体见下图，具体测算方法见本附录其余各章。



风险等级	风险值区间	所代表的一般性意义
严重	>=9	漏洞综合危害极大，实际被攻击者利用的可能性也很高。
高	>=8且<9	漏洞综合危害较大，且较容易被攻击者利用。
中	>=5且<8	漏洞综合危害一般，被利用难度较大或利用后不会造成严重影响。
低	>=2且<5	漏洞综合危害较低，在攻击过程中只起到辅助作用。
提示	<2	漏洞综合危害很低，只是理论上有被攻击者用于辅助攻击的可能性。

图 B 弱点综合风险关系图

B.2 影响程度测算

影响程度由漏洞对保密性、完整性、可用性的影响3方面决定，不同的影响级别赋予不同的值，见表B.1。

表 B.1 影响程度测算

影响因子	定性分级	定性描述	赋值
对保密性的影响	无影响	不会导致信息泄露的漏洞。	0
	部分影响	a）可导致少量服务器敏感泄露的漏洞，包括内网 IP 地址、隐藏目录、JAVA 错误信息、服务器物理路径等信息。	0.275

表 B.1　影响程度测算（续）

影响因子	定性分级	定性描述	赋值
对保密性的影响	部分影响	b）可导致个别客户信息被泄露的漏洞。	
	严重影响	a）可导致操作系统、网站后台、数据库等系统的管理员权限被获取的漏洞。 b）可导致客户的账户权限被获取的漏洞。 c）可导致大量客户敏感信息被泄露的漏洞。 d）可导致数据库信息被泄露的漏洞。 e）可导致服务器上大量敏感信息被泄露的漏洞。 f）可导致机密程度非常高的信息被泄露的漏洞，即使量少，也描述为严重影响。 **示例：**漏洞泄露了账户密码或其他公司秘密信息。	0.66
对完整性的影响	无影响	攻击者无法利用漏洞非法篡改（新增、删除或修改）目标系统上的任何数据。	0
	部分影响	a）攻击者可非法篡改的数据范围非常有限。 b）攻击者不能非法篡改指定的数据，即攻击者无法控制和使用篡改的数据。	0.275
	严重影响	a）可导致操作系统、网站后台、数据库等系统的管理员权限被获取的漏洞。 b）可导致任意客户的账户权限被获取的漏洞。 c）攻击者可非法篡改目标系统上指定数据内容，即攻击者可控制和使用这些数据。 d）攻击者可非法篡改目标系统的大量数据。 e）攻击者可非法篡改目标系统上的核心数据，比如资金交易数据。	0.66
对可用性的影响	无影响	对目标系统的使用和运行无任何影响的漏洞。	0
	部分影响	a）对目标系统的可用性造成一定影响的漏洞。比如服务器基本可用，但运行效率会明显下降。 b）对网络造成部分影响的漏洞，出现一定程度的网络延迟。 c）对服务器运行没影响，但一定程度上会影响用户正常使用的漏洞，比如未验证的重定向和转发。	0.275
	严重影响	a）可导致操作系统、网站后台、数据库等系统的管理员权限被获取的漏洞。 b）可导致任意客户的账户权限被获取的漏洞。 c）可导致服务器拒绝服务的漏洞，比如导致服务器崩溃、宕机、重启或者其他导致服务器无法正常运行的漏洞。 d）导致网络拥塞、瘫痪或其他影响正常访问的漏洞。 e）虽然对服务器运行没有影响，但可能完全影响用户正常使用该服务器提供的服务，比如服务器内的数据被篡改后，严重影响用户使用。	0.66
影响程度的具体测算公式为： Impact=10.41×(1-(1-ConfImpact)×(1-IntegImpact)×(1-AvailImpact)) 式中： ConfImpact—对保密性的影响。 IntegImpact—对完整性的影响。 AvailImpact—对可用性的影响。			

B.3　资产重要性测算

资产重要性由信息系统类别和业务交易类型2个因素决定。信息系统类别是指存在漏洞的信息系统的整体功能属性，业务交易类型是指漏洞所在功能点所对应的功能属性，具体见表B.2。

表 B.2　资产重要性测算

影响因子	定性分级	定性描述	赋值
信息系统类别	A 类系统	处理 JR/T 0171—2020 的 4.2 规定的 C3 类信息的信息系统。	1
	B 类系统	处理 JR/T 0171—2020 的 4.2 规定的 C2 类信息的信息系统。	2
	C 类系统	处理 JR/T 0171—2020 的 4.2 规定的 C1 类信息的信息系统。	3
	D 类系统	处理不包含在 JR/T 0171—2020 的 4.2 规定信息的信息系统。	4
业务交易类型	资金交易类	指通过银行信息进行资金操作交易，如转账、订单支付、缴费等。本人名下的投资理财、托管账户以及本人签订委托代扣协议的委托代扣等风险可控的资金变动不属于此范畴。	1
	业务变更类	通过银行信息变更客户相关信息或开通、取消业务的交易，如客户修改基本信息、调整交易额度、授权委托交易、修改交易订单、开通（签订）新业务、取消某项业务、电子合同签署、电子保单等。	2
	业务查询类	仅仅是一个查询的平台，不能进行任何资金交易和信息业务变更。	3
	其他类	a）不涉及客户数据及业务办理，比如业务介绍、广告、咨询平台。 b）涉及其他与业务无关的数据，比如与业务无关的论坛。 c）漏洞为一般的技术漏洞，与具体业务功能无关。	4
资产重要性（Req）的具体测算公式为： Req=0.2+(8-AppType-FuncType)×1.31/6 式中： AppType—信息系统类别。 FuncType—业务交易类型。			

B.4　影响程度修正

影响程度修正是指在考虑资产重要性因素后对影响程度进行相应调整后的一个漏洞影响度量值，其计算公式为：

AdjustedImpact=min(10,10.41×(1-(1-ConfImpact×Req)×(1-IntegImpact×Req)×(1-AvailImpact×Req)))

式中：

ConfImpact—对保密性的影响。

Req—资产重要性。

IntegImpact—对完整性的影响。

AvailImpact—对可用性的影响。

B.5　可利用性测算

可利用性通过利用发起路径、利用复杂度、登录认证限制3个维度来测算，具体见表B.3。

表 B.3　可利用性测算

影响因子	定性分级	定性描述	赋值
发起路径	远程	a）直接通过互联网即可远程访问利用的漏洞。 b）在测试环境中发现的，但将来部署在生产环境后可通过互联网远程利用的漏洞。	1
	局域网	在内网环境才能利用的漏洞，通过互联网上无法直接利用该漏洞。	0.646
	本地	a）黑客或黑客制作的木马、病毒等在进入目标设备系统后才能利用的漏洞，通常是本地运行的软件或系统上存在的缺陷，远程无法直接利用，比如本地提权漏洞、本地溢出漏洞。 b）与服务器没有直接关系，并且是在用户机器被黑客或黑客制作的木马、病毒等入侵后才能利用的漏洞。比如密码输入框插件、U 盾等介质上存在的安全漏洞。	0.395
利用复杂度	高	a）攻击者通过复杂的社会工程学的方法才能利用，比如电话、短信或其他方式一对一联系客户，欺骗客户下载运行木马，骗取客户相关信息等。 b）发起路径为本地的漏洞，或者其他需要突破多个安全防线才能利用的漏洞。 c）利用该漏洞达到有价值的目的或破坏性的结果，需要耗费大量的时间、大量的精力或者大量的设备。如暴力破解、DDOS 漏洞。 d）利用该漏洞需要非常强的专业水平，利用过程非常复杂。 e）现有的安全扫描软件均无法直接发现该漏洞。 f）利用该漏洞需要较多的前提，比如必要的数据信息、必要的网络条件、必要的权限、必要的其他漏洞等。	0.35
	中	a）攻击者仅需通过简单的社会工程学方法即可利用，比如通过批量发送邮件和短信一对多地欺骗客户点击指定链接。 b）攻击者利用前需要收集相关数据，但是可以容易地搜集到这些数据，不必与客户取得联系。比如通过谷歌搜索引擎对某些特定的网络主机漏洞进行搜索，找到相关数据、或通过其他漏洞可以方便收集的数据。 c）发起路径为局域网的漏洞，或者其他需要突破一个安全防线才能利用的漏洞。 d）利用该漏洞需要较强的专业知识，普通扫描软件、黑客工具无法发现和利用该漏洞。 e）利用该漏洞只需要少量的前提，比如常见的漏洞、容易获取的信息等。	0.61
	低	a）可直接通过互联网远程利用的漏洞，无需通过任何社会工程学方法，无需联系客户。 b）平均技术水平的黑客无需花费多少时间、精力即可简单利用的漏洞。	0.71
登录认证限制	多次认证	利用前需要非法获取多个口令信息，比如需要用户的网银账号密码的同时还需要用户的手机验证码。	0.45
	一次认证	a）需要非法获取一次口令信息，比如只需要用户的网银账号密码，或只需要用户的电子密码器密码。 b）目标系统的所有认证过程都使用同一密码，算作仅需一次认证。 c）目标系统的所有认证都是使用默认密码，算作仅需一次认证。 d）发起路径为本地漏洞，至少是需要通过一次认证，获取系统用户权限。	0.56

表 B.3　可利用性测算（续）

影响因子	定性分级	定性描述	赋值
登录认证限制	一次认证	e）黑客需要一个实名认证的账户才能利用的漏洞。	
	不必认证	a）黑客直接可以利用的漏洞，不需要输入任何口令信息，不需要任何身份认证证书。 b）口令信息可以通过公开注册获取，注册时不会验证黑客的真实身份。	0.704
可利用性（Exploitability）的具体测算公式为： Exploitability=20×AccessVector×AccessComplexity×Authentication 式中： AccessVector—发起路径。 AccessComplexity—利用复杂度。 Authentication—登录认证限制。			

B.6　漏洞基础风险值

漏洞基础风险值（BaseScore）是指综合考虑影响程度、资产重要程度及可利用性后的漏洞风险度量，其具体测算公式为：

BaseScore=(0.6×AdjustedImpact)+(0.4×Exploitability)-1.5

式中：

AdjustedImpact—影响程度修正。

Exploitability—可利用性。

B.7　遵从性测算

遵从性测算见表B.4。

表 B.4　遵从性测算

影响因子	定性分级	定性描述	赋值
监管及行业标准	无要求	可	0.9
	建议	宜	1
	应	应	1.15
		必须	1.5

B.8　漏洞综合风险值

漏洞综合风险值（FinalScore）是在漏洞基础风险值基础上，在考虑合规遵从性方面的规定后，其具体测算公式为：

FinalScore=BaseScore×Compliance

式中：

BaseScore—漏洞基础风险值。

Compliance—遵从性。

参 考 文 献

[1] GB/T 20984—2007 信息安全风险评估规范

[2] JR/T 0068—2020 网上银行系统信息安全通用规范

[3] JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引

[4] JR/T 0171—2020 个人金融信息保护技术规范

[5] JR/T 0197—2020 金融数据安全 数据安全分级指南

[6] ISO/IEC TR 20004:2015 Information technology — Security techniques Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

[7] ISO/IEC 18045:2008 Information technology—Security techniques—Methodology for IT security evaluation

[8] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

[9] PCI DSS 3.2.1 Payment Card Industry (PCI) Data Security Standard

[10] PTES Penetration Testing Execution Standard