ICS 03.060
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

XX/T XXXXX—XXXX

证券期货业信息系统渗透测试指南

Guidelines for penetration testing of information systems in the securities and futures industry

（送审稿）

2021 年 12 月 6 日

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国证券监督管理委员会　　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范》的规定起草。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC180）归口。

本文件起草单位：中国证券监督管理委员会科技监管局、上交所技术有限责任公司、深圳证券交易所、上海金融期货信息技术有限公司、中证信息技术服务有限责任公司、国泰君安证券股份公司、华泰证券股份有限公司、光大证券股份有限公司、华福证券有限责任公司、华安基金管理有限公司、杭州安恒信息技术股份有限公司、上海安恒智慧城市安全技术有限公司、天津三六零鸿腾科技有限公司、北京鸿腾智能科技有限公司。

本文件主要起草人：姚前、蒋东兴、周云晖、沙明、张天意、樊芳、房慧丽、李佶、张旭、黄清华、于钊、冯小根、苑立斌、陈凯晖、江旺、刘嵩、甘张生、徐正伟、袁明坤、周亚超、李磊、杨志。

引　言

近年来，证券期货业面向互联网的业务趋于多样化，随之而来承载各业务的信息系统所面临的网络攻击也愈发严峻，并且证券期货业信息系统直接涉及证券账户、资金账户、资金、交易记录等敏感信息，证券期货业信息系统已然成为国家经济建设的重要基础设施。因此，保障证券期货业信息系统安全已成为当前行业内紧迫的需求。

本文件旨在为证券期货业提供一套通用的信息系统渗透测试框架，深化渗透测试对于行业信息系统的作用，提升证券期货行业信息系统的渗透测试能力，以保障渗透测试质量，控制渗透测试实施风险。确保行业内能更加规范、安全稳定地开展渗透测试工作，进一步保障行业信息系统的安全性。

证券期货业信息系统渗透测试是指渗透测试人员从内网侧、互联网侧等通过模拟黑客的恶意攻击方法，对信息系统的任何弱点、技术缺陷或漏洞加以分析和主动利用，以期发现和挖掘信息系统中存在的漏洞，从而评估证券期货业信息系统安全的一种评估方法。本文件可供寻求以通用方法开展证券期货业信息系统渗透测试的各机构使用，确保行业内能更加规范、安全稳定地开展信息系统渗透测试，从而规范证券期货业信息系统的渗透测试工作。

依照本文件开展渗透测试时，应首先遵循国家的法律法规、监管要求及强制性标准的最新要求，如本文件与前述各项要求矛盾，应遵循前述各项要求。

证券期货业信息系统渗透测试指南

1 范围

本文件给出了在证券期货业信息系统建设过程中开展渗透测试的整体流程，同时给出了在确定渗透测试需求、制定渗透测试方案、执行渗透测试、交付渗透测试结果、管理渗透测试风险等环节如何保障测试质量、控制安全风险的操作指南。

本文件适用于证券期货业各机构开展信息系统渗透测试过程中的需求分析、方案制定、测试、总结以及风险管理等工作，可供其他金融机构参考。

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 30279-2020 信息安全技术 网络安全漏洞分类分级指南

JR/T 0158-2018 证券期货业数据分类分级指引

JR/T 0175-2019 证券期货业软件测试规范

3 术语和定义

GB/T 25069-2010 界定的术语和定义适用于本文件。

4 概述

相较于传统的应用安全测试以防护者角度按照测试清单逐项分析不同，证券期货业信息系统渗透测试以攻击者角度不限攻击手段成功入侵信息系统，证明系统存在安全问题为目标。宜根据GB/T 15532-2008和JR/T 0175—2019，结合行业特点，将证券期货业信息系统渗透测试指南流程划分为以下四个阶段：明确渗透测试需求、制定渗透测试方案、执行渗透测试、交付渗透测试结果。

5 明确渗透测试需求

5.1 概述

明确渗透测试需求旨在根据被测信息系统的安全目标定义渗透测试的深度与广度，包括但不限于明确渗透测试范围、渗透测试对象、渗透测试时间等。

执行渗透测试前，既定的渗透测试需求如存在变化，亦需及时二次明确。

5.2 渗透测试范围

渗透测试范围即信息系统渗透测试的广度，包括被测信息系统的IP地址、端口、域名、所属网络环境、业务功能等可能涉及到的关联资产或网络区域。

5.3 渗透测试对象

渗透测试对象即信息系统渗透测试的深度，可从多个维度确定被测信息系统的渗透测试对象，具体如下：

a) 组件作用维度，可分为通信网络、操作系统、中间件、数据库、安全防护设施、应用平台（包含客户端、H5 页面、小程序等）、应用系统；
b) 组件层级维度，可分为前台、中台、后台；
c) 业务功能维度，可分为涉及投资者撮合交易的交易系统、涉及上市公司业务管理的业务系统、存储大量敏感数据的大数据系统、面向投资者服务的互联网信息系统（如上市服务系统）。

5.4 渗透测试时间

渗透测试时间即证券期货业信息系统的渗透时间窗口，包括被测信息系统的授权渗透时间段以及渗透测试开始、截止时间等。

6 制定渗透测试方案

6.1 概述

制定渗透测试方案旨在基于已明确的渗透测试需求，根据证券期货业被测信息系统的特征，开展被测信息系统的信息收集和渗透测试方案制定工作。

根据信息收集结果，分析被测信息系统功能，对信息系统的技术弱点与价值进行评估，判断开展渗透测试的攻击手法，制定渗透测试方案。

6.2 信息收集

被测信息系统的信息收集可根据已明确的渗透测试需求，在需求方知晓并认同的情况下，尽可能收集被测信息系统的各种信息，包括但不限于：

a) IP地址、域名、接口、Web页面框架等Web应用信息；
b) 操作系统、系统组件、开放端口等服务器信息；
c) 已知漏洞、人员社交网络等社会工程信息；
d) 入侵检测设备、访问控制策略等网络安全防御措施。

6.3 信息系统功能及技术弱点研判

研判信息系统功能是指研究信息系统承载的业务功能与流程，并以此分析被测信息系统的功能框架与潜在的技术弱点，包括但不限于：

a) 信息系统功能，例如：身份认证、提供服务、信息展示等；
b) 攻击动机，例如：获取敏感信息、获取系统权限、篡改重要数据等；
c) 可尝试攻击手法，例如：Web 应用入侵、已知漏洞利用、认证绕过等。

6.4 确定渗透测试方案

通过对被测信息系统技术弱点的判断，确定信息系统渗透测试方案，协调渗透测试资源，以进一步挖掘被测信息系统的弱点、技术缺陷或漏洞等。渗透测试方案协调事宜包括如下：

a) 渗透测试团队：根据渗透测试需求与对被测信息系统潜在弱点的分析，针对性地配置具有相关渗透测试经验的人员组成渗透测试团队，例如：Web 安全人员、漏洞挖掘人员、二进制逆向分析人员、系统内核研究人员等；
b) 渗透测试工具：针对被测信息系统的技术弱点准备相应渗透测试工具，并按需求调整配置文件，例如：口令字典、自动化脚本、漏洞特征库等；
c) 访问控制：按照渗透测试需求验证渗透测试工具与被测信息系统间的网络连通性；
d) 授权与保密：根据渗透测试需求方之规定，渗透测试团队签订渗透测试委托书、保密协议等书面文件，确保行业信息系统在执行渗透测试时的合规与保密。

7 执行渗透测试

7.1 概述

证券期货业信息系统渗透测试主要以漏洞扫描、人工探测等方式发现安全漏洞，再通过人工验证对发现的安全漏洞进行主动利用，并通过多漏洞联动对被测信息系统实施深度渗透。

7.2 漏洞扫描

根据前期研判的被测信息系统的弱点、技术缺陷或漏洞，利用渗透测试工具，对被测信息系统发起基于应用层、网络层、系统层等多维度的漏洞扫描，旨在快速探测被测信息系统的漏洞、组件、服务等相关弱点。

7.3 漏洞利用

基于漏洞扫描的结果，结合前期对信息系统功能与弱点分析，尝试通过部分重点漏洞对系统的危害，突破信息系统，从而达到渗透被测信息系统的目的，对信息系统的危害包括但不限于：

a) 危害 Web 应用程序提供服务；
b) 危害移动 APP 提供服务；
c) 危害 PC 端应用程序提供服务；
d) 危害访问信息系统的用户主机运行；
e) 危害微信公众号、小程序运行；
f) 泄露涉及证券期货市场稳定的业务数据；
g) 泄露投资者个人隐私信息。

7.4 深度渗透

利用已知漏洞对被测信息系统的危害，通过多漏洞联动对信息系统进行深度突破，多级联动扩大单一漏洞对系统的危害，进一步渗透被测信息系统，并尝试手工挖掘业务逻辑漏洞，获取信息系统关键敏感信息或业务数据，包括但不限于：

a) 获取证券期货业内未披露信息；
b) 获取投资者个人隐私信息；
c) 获取信息系统管理权限；
d) 获取信息系统服务器用户权限；
e) 获取信息系统服务器管理员权限；

f） 获取信息系统数据库管理员权限。

7.5 成果记录

根据渗透进展，及时对取得的渗透成果进行记录或截图，渗透成果包括但不限于：

a） 利用漏洞成功突破信息系统；
b） 利用不当配置成功突破信息系统；
c） 成功获取信息系统权限；
d） 成功获取信息系统服务器权限；
e） 成功植入后门或木马等恶意应用程序；
f） 成功获取敏感信息。

7.6 恢复环境

将被测信息系统环境恢复至渗透测试前的初始环境，清理渗透测试过程中生成的文件，还原渗透测试过程中变更的配置等，包括但不限于：

a） 后门或木马等恶意应用程序；
b） 各类渗透测试工具及配置文件；
c） 账户、权限等访问控制配置；
d） 系统文件、数据库等核心节点操作。

8 交付渗透测试结果

8.1 概述

整理渗透测试过程，对渗透测试全程进行书面记录，对渗透测试成果进行风险定级并给出修复方案，形成证券期货业信息系统渗透测试结果文档进行交付。

8.2 渗透测试过程整理

基于渗透测试的进展，整理证券期货业信息系统渗透测试的实施全过程，包括渗透测试需求、渗透测试方案、渗透测试实施等阶段涉及的各类操作及使用的技术工具，均需整理汇总并在渗透测试结果文档中予以体现。

8.3 渗透测试成果风险定级

根据本文件附录A（资料性）《证券期货业信息系统渗透测试漏洞风险定级参考》评估渗透测试成果的风险危害程度，风险等级划分为超危、高危、中危、低危四个级别，定级描述如表1所示：

表1 风险等级描述

风险等级	危害程度
超危	对信息系统的正常运行造成严重影响，并可获取敏感信息，影响我国金融市场稳定，造成投资者隐私信息泄露等，且风险可被单一利用，易利用。
高危	对信息系统的正常运行造成较严重影响，获取信息系统敏感信息，且风险可通过多种手段被联合利用，易利用。

表1 风险等级描述（续）

风险等级	危害程度
中危	对信息系统的正常运行造成中等影响，获取信息系统敏感信息，风险可通过多种手段被联合利用，但难以利用。
低危	对信息系统的正常运行影响轻微，仅获取信息系统信息，且无进一步利用价值。

8.4 渗透测试结果文档撰写

完整记录证券期货业信息系统渗透测试的全过程，形成渗透测试结果文档。文档记录内容包括渗透测试需求、渗透测试方案、渗透测试实施、渗透测试成果等各阶段涉及的各类操作及使用的技术工具等。其中渗透测试成果作为渗透测试结果文档的主体部分应予以重点详细描述，主要包括如下内容：

a) 渗透测试成果涉及的风险信息描述及利用截图；
b) 渗透测试成果涉及的风险对信息系统的危害描述及针对性有效修复方案；
c) 渗透测试成果涉及的风险总体分析及分类统计；
d) 被测信息系统渗透测试情况总体摘要及信息系统加固建议。

8.5 渗透测试结果交付

渗透测试结果文档为开展渗透测试活动后的关键交付物，记录着证券期货业信息系统渗透测试的敏感数据。因此存储、交付过程中必须确保渗透测试结果的机密性，包括：

a) 通过加密存储介质储存渗透测试结果；
b) 条件允许时尽可能当面交付渗透测试结果；
c) 通过互联网交付时，压缩并加密渗透测试结果；
d) 明确交付人员，不随意群发、转发渗透测试结果。

9 管理渗透测试风险

9.1 风险分析

鉴于证券期货业信息系统渗透测试的特殊性与专业性，实施过程中会不可避免地引入可预见或不可预见的技术风险，技术风险包括但不限于：

a) 被测信息系统逃逸，渗透测试活动超出授权范围；
b) 渗透测试活动导致被测信息系统运行异常或宕机；
c) 渗透测试工具导致被测信息系统所处的网络环境异常；
d) 渗透测试人员管理不当，渗透测试成果外泄。

9.2 风险管理

为缓释证券期货业信息系统渗透测试过程中的风险，可在确定渗透测试方案后通过人员管理、环境管理、工具管理等管控措施，最大化可控、安全地开展信息系统渗透测试。

9.2.1 渗透测试人员管理

对参与被测信息系统渗透测试的个人及团队行为予以约束，包括但不限于：

a） 团队全员个人信息备案及职业背景调查；
b） 渗透测试执行前宣贯职业操守，严禁利用职务之便泄露敏感信息；
c） 团队全员及所属机构签署承诺书、保密协议等；
d） 明确团队全员应协助配合渗透测试期间的应急处置等；
e） 渗透测试活动结束后销毁生成的过程性文件和资料。

9.2.2 渗透测试环境管理

为防止渗透测试执行过程中，因被测信息系统逃逸而引发渗透测试脱离授权范围，可通过限制访问网络区域等访问控制措施，界定可渗透测试区域，包括：

a） 设定参与渗透测试的专用 IP 地址；
b） 限制渗透测试专用 IP 地址访问被测信息系统边界以外的网络区域；
c） 针对渗透测试专用 IP 地址部署专用数据防泄漏措施；
d） 对渗透测试专用 IP 地址的网络访问行为实施全程监控与审计。

9.2.3 渗透测试工具管理

渗透测试即意味着各类渗透测试工具的使用，但渗透测试工具因其特殊性，自身可能捆绑有其他恶意程序，随意被使用可能对被测信息系统造成间接不可控的风险。

因此在执行信息系统渗透测试时，有必要在确定渗透测试方案后，对拟使用的各类渗透测试工具开展合规性检查及使用报备，包括但不限于：

a）渗透测试工具的用途说明；
b）渗透测试工具的获取途径；
c）渗透测试工具文件校验比对；
d）渗透测试工具使用报备。

9.2.4 被测信息系统数据备份

渗透测试执行过程中可能引起信息系统不可预知的运行异常，为确保被测信息系统的完整性与可用性，开展渗透测试前有必要对被测信息系统的重要数据进行备份，备份内容包括但不限于：

a） 操作系统；
b） 数据库；
c） 信息系统配置文件；
d） 信息系统数据文件。

附 录 A
（资料性）
证券期货业信息系统渗透测试漏洞风险定级参考

A.1 概述

为体现证券期货业交易、监管、披露、其他业务特色，证券期货业信息系统渗透测试漏洞风险定级将在国家指导标准GB/T 30279-2020的基础上，结合证券期货业数据分类分级指引标准JR/T 0158-2018，提出通过被利用性、影响程度、环境因素、业务重要性四个指标类来定性评估漏洞风险综等级。

证券期货业信息系统渗透测试漏洞风险综合分级分为：超危、高危、中危、低危四个级别。漏洞风险综合定级由被利用性、影响程度、环境因素、业务重要性四个指标类决定，漏洞被利用可能性越高（被利用性分级越高），影响程度越严重（影响程度分级越高），环境对漏洞影响越敏感（环境因素分级越高），业务数据重要程度越高（业务数据级别标识越高），漏洞风险综合定级的级别越高（漏洞的危害程度越大）。漏洞风险综合定级方法如下：

a) 对被利用性指标进行赋值，根据赋值结果，按照GB/T 30279-2020附录A计算得到漏洞被利用性分级；
b) 对影响程度指标进行赋值，根据赋值结果，按照GB/T 30279-2020附录B计算得到漏洞影响程度分级；
c) 对环境因素指标进行赋值，根据赋值结果，按照GB/T 30279-2020附录C计算得到漏洞环境因素分级；
d) 对业务重要性指标进行赋值，根据行业机构单位性质，按照JR/T 0158-2018证券期货业数据分类分级方法和附录A，计算得到业务重要性级别标识；
e) 根据被利用性、影响程度和环境因素分级结果，按照GB/T 30279-2020附录D和E，计算得到漏洞技术分级；
f) 根据漏洞技术分级和业务重要性级别，计算得到证券期货业信息系统渗透测试漏洞风险综合定级。

A.2 被利用性

漏洞被利用性指标类反映信息系统漏洞触发的技术可能性。被利用性指标类的组成项包括但不限于：访问路径、触发要求、权限需求、交互条件，各项指标项的赋值说明见GB/T 30279-2020 6.2.1章节。被利用性级别用1-9的数字表示，数字越大表示被利用的可能性越高。被利用性分级见GB/T 30279-2020附录A。

A.3 影响程度

影响程度指标类反映触发漏洞对信息系统造成的损害程度。影响程度根据受漏洞影响的信息系统所承载信息的保密性、完整性、可用性等三个指标决定。各项指标项的赋值说明见GB/T 30279-2020 6.2.2

章节。不同的影响程度级别用1-9的数字表示，数字越大导致的危害程度越高。影响程度分级见GB/T 30279-2020附录B。

A.4 环境因素

环境因素指标类是综合考虑信息系统所处的网络环境、当前漏洞被利用的技术程度等外部环境。环境因素根据漏洞被利用成本、修复难度、影响范围等三个指标决定。各项指标项的赋值说明见GB/T 30279-2020 6.2.3章节。不同的环境因素级别用1-9的数字表示，数字越大环境因素导致的漏洞危害程度越高。环境因素分级见GB/T 30279-2020附录C。

A.5 业务重要性

根据行业机构信息系统运营或管理活动中产生的数据类型，按照JR/T 0158-2018指引推荐的分类分级方法，从信息系统业务条线出发，首先对业务划分，再对数据细分，最后对分类后的数据确定级别，同时，推荐考虑明确数据的具体“数据形态”，即所处的信息系统、存储的媒介等。业务数据级别标识从高到低划分为：4、3、2、1，与数据重要程度标识相对应，从高到低划分为：极高、高、中、低。根据行业机构单位性质，按照JR/T 0158-2018附录A，计算得到漏洞所处信息系统业务数据的重要级别。

A.6 漏洞技术分级

按照国家指导标准GB/T 30279-2020漏洞分级方法，根据被利用性、影响程度、环境因素赋值结果，按照GB/T 30279-2020附录D和E，计算得到漏洞在技术层面的分级结果，漏洞技术分级见GB/T 30279-2020附录E。

A.7 漏洞风险综合定级

证券期货业信息系统漏洞风险综合定级在GB/T 30279-2020基础上，综合考虑信息系统所属行业和业务特色。依据JR/T 0158-2018业务条线和数据分类分级方法，分析得到漏洞所在的信息系统业务数据重要程度，再根据漏洞技术分级和业务重要程度，计算得到证券期货业信息系统渗透测试漏洞风险综合定级表，见表A1。

表 A.1 漏洞风险综合定级表

序号	漏洞技术分级	业务重要性	综合定级
1	超危	极高	超危
2	超危	高	超危
3	超危	中	高危
4	超危	低	中危
5	高危	极高	超危
6	高危	高	高危
7	高危	中	中危
8	高危	低	中危
9	中危	极高	高危
10	中危	高	中危

表 A.1 漏洞风险综合定级表（续）

序号	漏洞技术分级	业务重要性	综合定级
11	中危	中	中危
12	中危	低	低危
13	低危	极高	中危
14	低危	高	中危
15	低危	中	低危
16	低危	低	低危

参 考 文 献

[1] GB/T 20984-2007 信息技术安全 信息安全风险评估规范

[2] 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

[3] GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

[4] JR/T 0158-2018 证券期货业数据分类分级指引

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

[6] GB/T 25069-2010 信息安全技术

[7] GB/T 15532-2008 计算机软件测试规范

[8] JR/T 0175—2019 证券期货业软件测试规范

[9] JR/T 0191—2020 证券期货业软件测试指南 软件安全测试

[10] JR/T 0192—2020 证券期货业移动互联网应用程序安全规范

[11] JR/T 0199-2020 金融科技创新安全通用规范

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

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

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

[15] PCI_DSS_v3.2.1 Payment Card Industry (PCI) Data Security Standard

[16] PTES Penetration Testing Execution Standard

[17] OWASP Open Web Application Security Project

[18] OSSTMM 3 Open Source Security Testing Methodology Manual