附件 1
ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0213—2021

金融网络安全 Web 应用服务安全测试通用规范

Financial cyber security General specification for security testing of Web application services

2021－02－10 发布　　2021－02－10 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。

本文件由中国人民银行提出。

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：中国人民银行科技司、公安部第一研究所、中国金融电子化公司、北京长亭未来科技有限公司、中国银联股份有限公司、农信银资金清算中心有限责任公司、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、交通银行股份有限公司、广发银行股份有限公司、招商银行股份有限公司、兴业银行股份有限公司、华夏银行股份有限公司、渤海银行股份有限公司、中国光大银行股份有限公司、中国民生银行股份有限公司、平安银行股份有限公司、中信银行股份有限公司、上海浦东发展银行股份有限公司、晋商银行股份有限公司、四川新网银行股份有限公司、江苏银行股份有限公司、重庆银行股份有限公司、盛京银行股份有限公司、广东华兴银行股份有限公司、广东省农村信用社联合社、长春农村商业银行股份有限公司、中国人民财产保险股份有限公司、中国平安保险（集团）股份有限公司、新华人寿保险股份有限公司、阳光保险集团股份有限公司、幸福人寿保险股份有限公司、华泰人寿保险股份有限公司、天安人寿保险股份有限公司、大童保险销售服务有限公司、国信证券股份有限公司、华泰证券股份有限公司、中国银行保险信息技术管理有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、奇安信科技集团股份有限公司、北京奇虎科技有限公司、深信服科技股份有限公司、北京百度网讯科技有限公司、北京启明星辰信息安全技术有限公司、亚信科技（成都）有限公司、北京中金安服科技有限公司、上海艾芒信息科技有限公司。

本文件主要起草人：李伟、陈立吾、沈筱彦、车珍、咎新、夏磊、王涛、胡光俊、唐辉、马男、王陶然、尹振玺、曹岳、张耀峰、李海威、侯漫丽、曾立环、张晏、陈芳、李强、宋歌、张鹏飞、杨坤、雷涛、李燕、李钢、代留虎、金建新、刘远欢、李吉慧、张念东、赵乔伟、何启翱、郭斌、徐鹏志、肖飞、姚仁毅、冯悦扬、宋克亚、尉洪敏、王福舟、李乐天、金驰、王飞、高滢、刘云、邓振江、姚俊先、边继宗、邵安、崔勤、倪春娟、常明政、于惊涛、丁明明、顾方方、罗英凯、时建军、王心玉、杨韶宁、刘奕明、张建、刘安蒙、李继斌、张庆华、罗逸枫、周扬、白智勇、秦磊、李翌雯、刘占明、龚杰、江超、李一萌、李昱希、张鸿宇、杨国栋、黄剑刚、王晓刚、梁露、侯峻、朱毅、江旺、郭显杰、马东辰、张帆、殷昊南、王勇、张中华、叶猛、毛敏其、邓园园、杜悦艺、马永生、李蕊。

引　言

Web应用服务是金融信息系统的重要组成部分，是金融机构网络安全的重要保护对象。本文件是在收集分析、评估检查所发现的金融信息系统Web应用服务安全问题的基础上，针对性提出的安全测试通用要求，内容涉及金融信息系统Web应用服务安全测试的原则、方法和过程三个方面。

本文件旨在规范和强化现有金融信息系统Web应用服务安全测试内容和方法。本文件既可作为各金融机构进行Web应用服务安全测试的参考标准，也可以作为行业主管部门、专业测试机构进行检查、检测的参考依据，用以指导测试人员对金融信息系统Web应用服务进行安全测试。

金融网络安全 Web应用服务安全测试通用规范

1 范围

本文件规定了金融信息系统Web应用服务安全测试的通用规范。

本文件适用于指导金融机构进行Web应用服务的安全测试与评估工作。

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—2010 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

JR/T 0072—2020 金融行业网络安全等级保护测评指南

JR/T 0168—2020 网上银行系统信息安全通用规范

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010界定的术语和定义以及下列术语和定义适用于本文件。

3.1.1

金融信息系统 financial information system

金融行业相关的应用、服务、信息技术资产或其他信息处理组件。

[来源：GB/T 29246—2017，2.39]

3.1.2

网上银行 internet banking

商业银行等银行业金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供的网上金融服务。

[来源：JR/T 0168—2020，3.1]

3.1.3

Web应用服务 Web application service

基于Web服务器软件，为用户提供应用服务的网站、程序、应用或接口的应用服务部分。

注：Web应用服务包括服务端应用程序及组件、Web服务器、中间件和API接口等。

[来源：GB/T 32917—2016，3.1.3，有修改]

3.1.4

Web 应用服务安全测试 Web application service security testing

通过自动化漏洞扫描和人工测试等手段，对Web服务器及Web应用服务进行安全漏洞发现及安全功能有效性验证的安全性测试。

3.1.5

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，并尝试发现可利用漏洞的一种安全测试行为。

3.1.6

重要 Web 应用 important Web application

包括面向互联网开放服务的Web应用，面向客户涉及账务处理且对实时性要求较高的业务处理类Web应用，渠道类Web应用和涉及客户风险管理等业务的Web应用。

3.1.7

测试方 tester

实施安全测试的团队或个人，由金融机构内部人员及外部测试服务机构人员组成。

3.1.8

热门高危漏洞 popular high-risk vulnerability

在安全测试实施时间点近两年内流行的，针对特定应用及组件的高风险漏洞。

注：包括但不限于CVSS高评分的远程漏洞、CNVD高危漏洞和社区流行的高风险漏洞等。

3.1.9

侵入式测试 invasive testing

基于对数据及程序代码进行侵入性改写的安全测试。

3.1.10

资产测绘 asset mapping

对网络资产相关信息进行持续盘点并具象展示。

3.1.11

线性预测 linear prediction

基于一个线性方程对抽样值序列的预测。

3.1.12

运行类测试工具 run-type testing tool

需要在被测目标中以一定权限运行的测试工具。

注：包括Webshell、反向连接类工具、提权类工具、文件扫描类工具等。

3.2 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

ASP：动态服务器页面（Active Server Pages）

CORS：跨域资源共享（Cross Origin Resource Sharing）

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

CRLF：注入回车换行符（Carriage Return Line Feed）

CSRF：跨站请求伪造（Cross Site Request Forgery）

CSP：内容安全策略（Content Security Policy）

CSS：层叠样式表（Cascading Style Sheets）

CVSS：通用漏洞评分系统（Common Vulnerability Scoring System）

HTML：超文本标记语言（HyperText Markup Language）

HTTP：超文本传输协议（HyperText Transfer Protocol）

HTTPS：超文本传输安全协议（HyperText Transfer Protocol Secure）

IMAP：交互邮件访问协议（Interactive Mail Access Protocol）

JSON：Javascript对象表示法（Javascript Object Notation）

JSONP：JSON跨域访问（JSON with Padding）

LDAP：轻型目录访问协议（Lightweight Directory Access Protocol）

ORM：对象关系映射（Object Relational Mapping）

OWASP：开放式Web应用程序安全项目（Open Web Application Security Project）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）

SQL：结构化查询语言（Structured Query Language）

SSI：服务器包含（Server Side Includes）

SSL：安全套接层（Secure Sockets Layer）

SSRF：服务端请求伪造（Server Side Request Forgery）

TLS：安全传输层协议（Transport Layer Security）

URL：统一资源定位符（Universal Resource Locator）

VPN：虚拟专用网络（Virtual Private Network）

XML：可扩展标记语言（Extensible Markup Language）

XPath：XML路径语言（XML Path Language）

XSS：跨站脚本（Cross Site Scripting）

4 原则

4.1 测试原则

4.1.1 标准性原则

应按照GB/T 31509—2015和JR/T 0072—2020的流程进行实施，包括实施阶段和运维阶段的测试工作。

4.1.2 全面性原则

在规定的测试范围内，应覆盖指定目标中的全部Web应用服务及每个Web应用服务中的全部功能。

4.1.3 分级原则

测试过程应对Web应用服务及漏洞进行分级管理，以保证重要Web应用服务的资源投入。

4.1.4 可控性原则

测试过程应按照GB/T 31509—2015中的项目管理方法对过程、人员、工具等进行控制，以保证安全测试过程的安全可控。

4.1.5 最小影响原则

针对处于运维阶段的Web应用服务，应提前确定合适的测试时间窗口，避开业务高峰期，同时做好被测试目标应用服务的应急预案。

4.1.6 保密性原则

未经金融机构允许，测试方不应向第三方及社会公众泄露与安全测试目标相关的一切信息，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Web应用网络架构、业务数据、安全漏洞等。

4.1.7 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。

4.2 测试形式

Web应用服务安全测试应按照GB/T 20984—2007，以自评估测试为主，自评估测试和检查测试相互结合，互为补充。安全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

测试环境及准备基本要求：

a) 金融机构应针对金融交易类应用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业务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) 金融机构应预先准备功能与数据均完备的账号以保证测试的完备性，若完成测试涉及必要的专有设备，如控件、证书和U盾等软硬件设备，金融机构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，金融机构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与测试环境相关的任何信息。
f) 测试环境提供方应及时与测试方同步测试系统更新、维护及测试计划，以保证测试环境稳定可用。
g) 如测试目标为应用接口，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

测试工具及准备基本要求：

a) 测试方应使用不存在法律风险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) 金融机构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。对于已引入的安全测试工具，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) 对于完成当次安全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，防止运行类测试工具本身引入安全隐患。
f) 测试方应从在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、XSS 和 SQL 注入等漏洞。

5.3 测试技术

5.3.1 通用测试要求

通用测试基本要求：

a) 金融机构应采用技术或管理手段，确保面向安全测试所开放的功能集合完全覆盖生产系统面向最终用户所开放的功能集合。
b) 测试方应参考 CNVD 维护热门高危漏洞所对应的测试方法及工具列表，并每个季度更新测试项列表及对应的测试方法。金融机构应针对测试项列表定期开展评审工作，确认更新内容的覆盖情况满足金融机构的相关要求。
c) 金融机构应进行互联网暴露资产和内网资产测绘，明确安全测试对象清单并进行定期更新。
d) 当出现重大高危漏洞时，测试方应及时跟进漏洞披露进展并向金融机构同步相关信息，同时及时更新测试方法及工具。
e) 测试方应优先保证热门高危漏洞的测试进度及测试效果。
f) 对于面向客户开放且包含支付功能的系统，应保证测试方法覆盖当前热门高危漏洞的全部测试项以及本章测试技术中包含的所有基本要求。这些应用系统包括但不限于网上银行和开放银行等。

通用测试增强要求：

a) 如采用第三方软件或硬件进行热门高危漏洞的防御或修补，需进行安全测试以保证这些防御策略不能被任何已公开手段绕过。
b) 测试方应针对开源的高危系统及高危组件设置单独的测试清单并定期进行更新。
c) 全量内容的安全测试应覆盖热门高危漏洞所对应测试方法以及本章测试技术中包含的所有基本要求。

5.3.2 业务逻辑测试

5.3.2.1 多线程竞争条件测试

多线程竞争条件测试基本要求：

a) 测试方应在仿真环境中进行涉及资金交易的多线程竞争条件测试。金融机构应通过对比分析判断生产环境中是否存在类似问题。
b) 应至少覆盖转账及积分兑换等场景。

多线程竞争条件测试增强要求：

多线程竞争条件测试具备偶发性，对同一个功能应采用至少2种以上工具并分别测试3次以上以确保测试充分。

5.3.2.2 资金查询越权测试

资金查询越权测试基本要求：

a) 应通过测试确认指定账户查询的回显内容中不包含当前用户权限所无法查看的内容。
b) 测试应覆盖到每一个可能对当前用户权限产生影响的参数。

5.3.2.3 资金交易越权测试

资金交易越权测试基本要求：

a) 应通过测试确认不存在同一机构不同账户之间混淆的情况，如将预付账户资金直接汇入应付账户并完成虚假交易。
b) 应通过测试确认不同机构之间不存在平行越权问题，如测试方利用漏洞诱导他人完成自己账户的支付。

5.3.2.4 支付漏洞测试

支付漏洞测试基本要求：

a) 测试方应在仿真环境中进行支付漏洞测试。金融机构应通过对比分析判断生产环境中是否存在类似问题。
b) 支付漏洞是否存在不应通过是否能够结算成功判断，应通过是否能够成功生成订单判断。
c) 应通过测试确认不存在商品属性篡改问题，商品属性包括但不限于商品金额、商品有效期、增值服务有效期、商品分期数和附加优惠等。
d) 应通过测试确认支付功能不存在 0 元支付问题，如删除金额参数或将金额参数置为 0 可以生成合法订单。
e) 应通过测试确认支付功能不存在整数溢出问题。
f) 应通过测试确认支付功能不存在负值反充问题，如通过支付负数成功导致账户余额增加。
g) 应通过测试确认支付功能不存在正负值对冲问题，如在进行多个不同类型商品结算支付时，可以通过正负值对冲构造低价订单。
h) 应通过测试确认支付功能不存在流程异常的问题，如输入非法的金额或数量导致应用出现异常或跳转至预期之外的流程。

5.3.2.5 请求重放测试

请求重放测试基本要求：

应通过测试确认任何涉及资金交易、数据修改、发送短信的操作均无法通过重放数据包的方式被重复执行。

5.3.2.6 用户信息完整性测试

用户信息完整性测试基本要求：

a) 对于应用强制要求用户进行实名认证的场景，应通过测试确认用户在漏填实名认证信息的情况下不能完成注册。实名认证关键信息包括但不限于银行卡四要素、身份证四要素以及生物特征要素等。
b) 应通过测试确认用户在漏填账户关键信息的情况下不能完成注册。账户关键信息包括但不限于用户名、密码、手机号码、电子邮箱、密保问题等信息。
c) 应通过测试确认用户在操作大额交易或找回密码时，无法通过未进行设置的账户关键信息完成客户身份检查。如账户未设置密保问题的情况下，可以通过将密保问题参数置空绕过校验。

5.3.2.7 业务逻辑数据验证测试

业务逻辑数据验证测试基本要求：

应通过测试确认其他不涉及资金支付的业务逻辑功能不存在数据验证缺陷。如将相关业务逻辑功能中的各个关键参数赋值为空值、0 值、负数、超大数、字符串、换行符或制表符，以及将相关参数键值对整体删除之后出现的各类非预期结果。

5.3.2.8 隐藏域测试

隐藏域测试基本要求：

测试方应充分发现并记录隐藏域中的参数，并尝试对这些参数进行直接赋值以模拟非预期的请求。如在隐藏域中发现参数 admin，尝试直接在请求中增加 admin=1 后立即获得管理员权限。

隐藏域测试增强要求：

测试方应结合业务语境充分猜测可能的隐藏参数，并尝试对这些参数进行直接赋值以模拟非预期的请求。如猜测会存在参数 admin，尝试直接在请求中增加 admin=1 后立即获得管理员权限。

5.3.2.9 完整性检查和中间人测试

完整性检查和中间人测试基本要求：

应通过测试确认客户端和服务器在传输交易数据时，服务端采用了有效的完整性检查和防篡改措施。

完整性检查和中间人测试增强要求：

应通过测试确认客户端和服务器之间进行双向认证的有效性，确保无法通过已知手段进行中间人攻击。

5.3.2.10 短信和电子邮箱验证测试

短信和电子邮箱验证测试基本要求：

a) 应通过测试确认短信和电子邮箱验证逻辑不会被整体绕过。
b) 应通过测试确认短信和电子邮箱验证功能不存在短信和电子邮箱验证码前端生成问题。
c) 应通过测试确认短信和电子邮箱验证功能不存在短信和电子邮箱验证码前端验证问题。
d) 对于生产环境，应通过测试确认短信和电子邮箱验证功能不存在特权验证码。
e) 应通过测试确认短信和电子邮箱验证功能存在有效的抗暴力破解措施。
f) 应通过测试确认短信和电子邮箱验证码的随机性，并确认短信和电子邮箱验证码的长度不少于 6 位数。
g) 应通过测试确认短信和电子邮箱验证码的失效时间不长于 6 分钟，并确保验证码到期后立即作废。
h) 应通过测试确认短信验证功能不存在内容定制的问题。如通过参数插入任意文本拼接到短信内容中。

i) 应通过测试确认短信和电子邮箱验证功能不存在定向转发漏洞，如可将当前用户的验证码或身份验证链接通过指定手机号码的方式定向转发至其他手机号码或电子邮箱上。
j) 应通过测试确认短信验证功能不存在短信重放的问题。如可向指定手机号码批量定向发送短信或批量向任意手机号码发送短信 10 次以上。

5.3.2.11 图形验证码测试

图形验证码测试基本要求：
a) 应通过测试确认图形验证码不会被整体绕过。
b) 应通过测试确认图形验证码无法进行低成本的光学字符识别（OCR）。如互联网上可下载的 OCR 验证码识别工具、脚本等。
c) 应通过测试确认图形验证码认证 1 次后即刻失效。

5.3.2.12 滑块验证码测试

滑块验证码测试基本要求：
a) 应通过测试确认滑块验证码不会被整体绕过。
b) 应通过测试确认滑块验证码能够有效防止机器模拟验证。
c) 应通过测试确认滑块验证码认证 1 次后即刻失效。

5.3.2.13 处理用时测试

处理用时测试基本要求：
应通过测试确认所有关键请求不能通过响应时间的变化而进行执行结果预测。如使用通配符导致的响应延迟可能是由于服务端使用了正则表达式，这种情况下攻击者可以通过调整输入以获得预期之外的最佳响应。

5.3.2.14 工作流程绕过测试

工作流程绕过测试基本要求：
a) 应至少在找回密码和重置密码场景处进行业务流程绕过测试。
b) 应通过测试确认当前所在的业务流程阶段不能够通过用户传入的参数直接指定。
c) 对于每一个业务流程阶段，应通过测试确保安全策略与安全原则具备整体一致性。

5.3.2.15 应用程序误用测试

应用程序误用测试基本要求：
应通过测试确认系统存在能够阻止攻击者反复进行攻击尝试的防御机制。如多次输入疑似攻击尝试及攻击利用的内容，系统可以直接阻断请求并进行临时 IP 封禁。该机制可以由第三方设备或软件提供。
应用程序误用测试增强要求：
应通过测试确认系统存在可以自学习的抗攻击尝试机制。

5.3.2.16 文件上传测试

文件上传测试基本要求：
a) 应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) 应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) 应通过测试确认上传文档前应经过有效的身份验证。
d) 应通过测试确认文件上传的校验在服务端进行。

e) 应通过测试确认文件上传功能存在有效的后缀白名单限制，且无法被突破。
f) 应通过测试确认文件上传的位置无法通过参数进行指定或操控。
g) 应通过测试确认文件上传功能不存在竞争上传问题。
h) 对于文件上传后会针对上传文件内容进行展示及重新渲染的功能，应通过测试确认无法利用该功能绕过现有防御机制。

文件上传测试增强要求：

对于文件上传后会针对上传文件内容进行展示及重新渲染的功能，应通过测试确认该功能无法通过内容展示及重新渲染执行外部插入的命令。

5.3.3 身份鉴别测试

5.3.3.1 角色定义测试

角色定义测试基本要求：

a) 测试方应充分了解目标应用中的全部角色并建立权限矩阵。
b) 金融机构应提供所有角色权限的账号及登录方式，并确认测试方建立权限矩阵的准确性。如生产环境中不能提供对应角色权限的账号及登录方式，则需要在仿真环境中进行补充测试。

5.3.3.2 用户注册过程测试

用户注册过程测试基本要求：

a) 应通过测试确认用户主体只能被注册 1 次。
b) 应通过测试确认系统存在能够有效认证用户主体的功能设计。如实名注册中，至少通过查询姓名与身份证号码的匹配度来验证用户主体的真实性。
c) 应通过测试确认不存在可以直接控制注册用户权限的参数。
d) 应通过测试确认注册过程包含有效的人机识别，无法通过自动化批量完成。

5.3.3.3 账户权限变化测试

账户权限变化测试基本要求：

a) 测试方应结合角色权限矩阵，梳理所有涉及权限变化的功能，并确认是否能够最小化满足业务需求。
b) 应通过测试确认任何角色都不能为自身或其他角色赋予超越自身的权限。
c) 应通过测试确认任何角色都不能撤销或转移对等权限以及更高权限。

5.3.3.4 账户枚举和弱用户名测试

账户枚举和弱用户名测试基本要求：

a) 应通过测试确认登录时无法进行账户枚举。
b) 进行账户枚举和弱用户名测试时应尽可能尝试常见用户名与默认用户名。

5.3.3.5 口令信息加密传输测试

口令信息加密传输测试基本要求：

a) 应通过测试确认口令信息传输在当前场景下满足 JR/T 0168—2020 的要求。如网银系统在传输口令时应采用双向校验。
b) 应通过测试确认口令信息传输时至少对口令参数本身使用摘要算法进行加密，或整个请求采用通过国家密码管理部门认可的 HTTPS 协议进行传输。

c) 在使用 HTTPS 协议的情况下，应通过测试确认口令信息传输不能够通过 HTTP 降级请求。如对于一个必须使用 HTTPS 协议进行访问的应用登录界面，可使用 HTTP 协议访问并成功登陆。

5.3.3.6 默认口令与弱口令测试

默认口令与弱口令测试基本要求：

a) 测试方应建立并维护金融机构常用弱口令字典，并保证字典具备较高的命中率。
b) 测试方应通过访谈及调研的形式确认目标系统不存在统一分发的默认口令，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) 应通过测试确认不能够使用空口令登录目标系统。
d) 应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，测试方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关联的常见口令。

默认口令与弱口令测试增强要求：

测试方应针对目标系统及所属金融机构，通过组合关联信息定制弱口令字典的方式提升命中率。

5.3.3.7 账户锁定机制测试

账户锁定机制测试基本要求：

a) 在生产环境中测试时，测试方应只针对授权使用的测试账号进行账户锁定机制测试。
b) 如未设置账户锁定机制，应通过测试确认图片验证码以及其他抗暴力破解措施的有效性。
c) 应通过测试确认账户锁定机制无法被整体绕过。
d) 应结合业务需要，确认每次口令锁定时间不低于该业务要求的基准值。

5.3.3.8 认证绕过测试

认证绕过测试基本要求：

a) 应通过测试确认内部功能均进行了有效的认证保护，无法通过直接请求非授权访问内部功能。
b) 应通过测试确认不存在能够通过参数直接激活登录认证的功能。如参数 login=on 后能够以某一个固定或指定的权限正常使用相应功能。
c) 应通过测试确认会话标识或用来标示身份的其他参数不能进行线性预测。
d) 应通过测试确认无法通过修改响应包的方式简化前端页面分析并获取更多应用入口信息。

5.3.3.9 记住密码功能测试

认证绕过测试基本要求：

应通过测试确认浏览器本地（包括但不限于 Cookie、Local Storage、Session Storage）中没有存储明文密码或哈希。

5.3.3.10 密码策略测试

密码策略测试基本要求：

a) 应通过测试确认目标系统的密码策略满足对应安全级别的要求。如密码长度要求、密码组成要求、密码强制修改周期要求和历史密码策略要求等。
b) 应通过测试确认目标系统无法通过连续多次更改密码的方式绕过历史密码策略。

5.3.3.11 密码修改及重置测试

密码修改及重置测试基本要求：

a) 应通过测试确认密码修改功能验证了原密码，并确保验证的有效性。
b) 如使用了短信及电子邮箱验证码，应通过测试确认密码重置功能的关键步骤中新密码重置与短信及电子邮箱验证码校验同时进行，并确认短信及电子邮箱验证码的设计符合 5.3.2.10 的基本要求。
c) 如使用了电子邮箱找回链接，应通过测试确认找回链接中与身份绑定的标识参数超过 32 位且无法被简单模型预测。
d) 如使用了电子邮箱找回链接，应通过测试确认电子邮箱找回链接的有效时间不超过 12 小时。
e) 如使用了重置令牌，应通过测试确认重置令牌来源的唯一性。即不应在系统的其他位置发现可以生成该令牌的接口与功能。

5.3.4 授权测试

5.3.4.1 目录遍历、文件包含测试

目录遍历、文件包含测试基本要求：

a) 测试方应遍历所有通过用户传入文件名调取文件内容的功能，确保无法基于当前 Web 应用运行权限进行指定操作文件查看及下载的操作。
b) 应通过测试确认传入参数不支持 PHP 封装协议（伪协议）。如 php://input 和 php://filter 等。
c) 应通过测试确认传入参数不支持通过“../”以及对应的各类编码或变体进行父目录穿越。

5.3.4.2 目录浏览测试

目录浏览测试基本要求：

a) 应通过测试确认 Web 应用各级目录均未开启目录浏览功能。
b) 应通过测试确认 Web 应用各级目录不存在通过其他信息间接泄露全部或部分目录名称的问题，如版本控制工具残留文件导致的目录或文件名称泄露。

5.3.4.3 可预测资源定位测试

可预测资源定位测试基本要求：

a) 对于不便进行权限限制的静态资源，应通过测试确认其名称具备不可预测性，包括但不限于图片、文档和附件等静态资源。如图片名称包含 32 位以上哈希且不可线性预测。
b) 应充分尝试请求可能的文件名、后缀及相关变体，确保不存在包含敏感信息的可预测资源。如版本控制文件、备份文件和示例文件等。
c) 应通过测试确认 Web 服务器及中间件的基础配置文件和管理入口，不会因为配置失误导致未授权访问。

5.3.4.4 授权绕过测试

授权绕过测试基本要求：

a) 如具备条件，测试方应使用管理员权限遍历管理页面和功能并进行记录，且通过测试确保普通用户以及其他非授权用户不具备这些页面及功能的使用权限。
b) 应通过测试确认管理功能的权限判断逻辑未仅在前端实现。如在未登录状态下请求某个管理页面，会通过增加 JavaScript 的方式引导用户跳转或关闭窗口，但实际管理功能及数据已经加载并可以正常使用。

5.3.4.5 权限提升测试

权限提升基本要求：

应通过测试确认不存在通过用户输入参数可以直接控制当前账户整体权限的功能实现或接口。如通过增加参数admin=1即可使用管理员功能。

5.3.4.6 不安全的直接对象引用测试

不安全的直接对象引用测试基本要求：

a) 应通过测试确认所有用户输入的与权限相关的线性参数均不存在平行越权的问题。如 ID=150 为当前用户的内容，ID=151 为当前用户所不具备权限的其他用户的内容。
b) 在生产系统中，如涉及写与删除操作的平行越权，应至少在另一个测试账户中进行。如不具备另一个测试账户，则应在仿真环境中进行本项测试。
c) 进行不安全的直接对象引用测试时，应严格禁止批量跑取数据的行为。如需要进行危害验证，应获取不超过 5 条数据用以证明危害即可。

5.3.5 会话管理测试

5.3.5.1 会话管理绕过测试

会话管理绕过测试基本要求：

a) 应通过测试确认 Cookie 中的会话凭证具备不可预测性。
b) 应通过测试确认会话标识符从一个可信系统，如服务器上创建，而不是在客户端创建。
c) 应通过测试确认 Cookie 中的会话凭证不能通过目标系统中的其他功能生成，如存在某个功能实现或接口，在传入用户名后可以得到对应用户的会话凭证。

会话管理绕过测试增强要求：

在验证会话凭证的不可预测性时，宜采用通过工具生成大量会话凭证样本并进行碰撞的方式进行。

5.3.5.2 Cookie 属性测试

Cookie属性测试基本要求：

a) 应通过测试确认 Cookie 中的会话标识设置了 Secure、HttpOnly 和 SameSite 属性。
b) 应通过测试确认对 HttpOnly 不支持的浏览器不能使用站点功能。
c) 应通过测试确认目标系统不存在能够绕过 HttpOnly 机制的漏洞，如特定的中间件漏洞以及利用 CORS 特性导致的 XSS 会话劫持等。

5.3.5.3 会话固定测试

会话固定测试基本要求：

a) 应通过测试确认用户登录成功后目标系统会自动更新会话标识。
b) 应通过测试确认当用户携带一个通过 URL 传递的指定的会话标识进行用户认证后，该会话标识不会生效。

5.3.5.4 会话令牌泄露测试

会话令牌泄露测试基本要求：

应通过测试确认所有涉及身份认证的关键参数均不能通过GET方式传输。如用户名密码对，会话标识以及其他能够独立通过身份校验的各类凭据。

5.3.5.5 CSRF 测试

CSRF测试基本要求：

a) 测试方应梳理并记录所有与身份强相关的单向操作，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。应通过测试确保上述功能不存在 CSRF 问题。
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，则应通过测试确认校验码不可预测及不可绕过。
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及不可绕过。
f) 应通过测试确认目标系统无法进行 JSON 和 JSONP 劫持攻击。

5.3.5.6 登出功能与会话超时测试

登出功能与会话超时测试基本要求：

a) 应通过测试确认用户界面中存在登出功能，并确认登出功能的有效性。
b) 应通过测试确认目标系统存在无动作前提下的自动登出时间设置，且不长于 10 分钟。

5.3.5.7 会话变量重载测试

会话变量重载测试增强要求：

应通过测试确认目标系统的每次会话变量重载都在充分认证的基础之上进行。如任何未登录的用户在访问某个页面后都被动激活了登录会话，那么在该页面之前应存在用户身份认证的逻辑。

5.3.6 输入验证测试

5.3.6.1 XSS 测试

XSS测试基本要求：

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自行删除。如测试账号不具备相关内容自行删除的功能或权限，应在仿真环境下进行存储型跨站脚本测试。严禁在生产系统中进行测试方不可自行删除的存储型跨站脚本测试。
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。如需使用测试方自有平台进行测试，需按照金融机构制定的测试工具管理流程进行报备。
d) 应通过测试确认输入过滤及输出编码措施的有效性。使用的测试手段包括但不限于以下方式：结合上下文环境引入自定义的 HTML、XML、JavaScript、CSS 代码，通过等价替换、变异等方式绕过黑白名单检测，利用上传功能直接上传含有跨站脚本的静态页面等。
e) 应在仿真环境中，通过测试确认当前目标系统中输入的跨站脚本不会作用于其他系统。如 XSS 盲打。
f) 应通过测试确认目标系统不存在可以指定伪协议、JavaScript、Data-ur 和 Blob 等而导致的 XSS 漏洞。

XSS测试增强要求：

a) 测试方应梳理并记录所有能够将用户输入内容存入数据库并回显至页面的功能。包括但不限于用户名、头像、用户信息、转账信息、订单、对账单、论坛、留言板、站内搜索和查询等功能。
b) 如使用了 CSP 技术，应通过测试确认当前 CSP 配置无法被绕过。
c) 应通过测试确保目标应用服务在 Internet Explorer、Chrome、Firefox 和 Safari 等浏览器的主流版本均不存在可利用的跨站脚本漏洞。

5.3.6.2 SSRF 测试

SSRF测试基本要求：

a) 测试方应在所有可能调用内部或外部第三方系统的位置进行充分的 SSRF 测试尝试。包括但不限于直接通过参数传递 IP 地址的功能、传递端口号的功能、传递第三方 URL 的功能以及传递第三方回显数据的功能等。

b) 应通过测试确认传入的 URL 参数仅支持 HTTP(S)协议，不应响应 file://、gopher://、ftp://和 dict://等其他网络协议。

5.3.6.3 HTTP 谓词篡改测试

HTTP谓词篡改测试基本要求：

a) 应通过测试确认目标系统是否开启了 Webdav。

b) 在开启了 Webdav 的前提下，应通过测试确认目标系统无法通过 Webdav 缺陷配置上传 Webshell。

HTTP谓词篡改测试增强要求：

应通过测试确认非标准的HTTP方法不会产生非预期的行为。

5.3.6.4 HTTP 参数污染测试

HTTP参数污染测试基本要求：

a) 应通过测试确认在引入多个同名参数时，安全限制与参数执行始终保持一致。

b) 应通过测试确认在引入多个同名参数时,目标系统在接受了多个参数值组合的前提下无法绕过安全限制。

5.3.6.5 SQL 注入测试

SQL注入测试基本要求：

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。包括但不限于通过堆叠注入引入完整的增删改语句，通过 Outfile 语句向服务器文件写入内容，通过文本输入区域进行二次注入，在增删改语句中拼入恒真表达式或注释后续执行条件等危险操作。

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。如需使用测试方自有平台进行测试，需按照金融机构制定的测试工具管理流程进行报备。

c) 在使用了 NoSQL 及 ORM 相关技术的系统中,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。

SQL注入测试增强要求：

a) 测试方应对所有可能存在数据库查询的功能进行 SQL 注入测试。可通过开发专项工具的方式提升 SQL 注入测试的全面性。

b) 在使用了安全限制的场景下,应通过测试确认负载均衡或代理服务器在向后端服务器做转发的过程中，不存在 HTTP 请求走私（HTTP request smuggling）问题。

5.3.6.6 XML 注入测试

XML注入测试基本要求：

a) 测试方应通过尝试插入 XML 元字符以及节点的方式充分测试当前功能中是否存在 XML 解析的可能。

b) 在目标系统使用了 XML 数据库的前提下，应通过测试确认对应功能不存在 XML 标签注入问题。
c) 应通过测试确认目标系统不存在 XML 外部实体注入问题。

5.3.6.7 其他注入测试

其他注入测试基本要求：

a) 在目标系统使用了 LDAP 服务器的前提下，应通过测试确认对应功能不存在 LDAP 注入问题。
b) 应通过测试确认目标系统不存在系统命令注入问题。
c) 应通过测试确认目标系统是否开启了 SSI 支持，若开启应确认不存在 SSI 注入问题。
d) 在目标系统使用了 XPath 查询方式的前提下，应通过测试确认对应功能不存在 XPath 注入问题。可以尝试使用与 SQL 注入通用的测试方法覆盖部分 XPath 注入测试。
e) 在测试 Web 电子邮箱系统以及具备 Web 电子邮箱功能的其他应用系统时，应通过测试确认目标系统不存在 IMAP/SMTP 注入问题。
f) 应通过测试确认目标系统不存在 HTTP Header 参数注入，如 X-Forwarded-For 注入问题。
g) 应通过测试确认目标系统不存在由于 CRLF 注入所导致的 HTTP 响应分割问题。

其他注入测试增强要求：

a) 应通过模糊测试与域名解析记录相结合的方式，确认目标系统不存在命令注入问题。
b) 应通过测试确认目标系统不存在代码注入问题，包括但不限于应用代码注入、模板注入或表示层语言注入问题。
c) 应通过灰盒或白盒测试的方式，确认目标系统不存在各类注入问题。

5.3.6.8 孵化漏洞测试

孵化漏洞测试增强要求：

在一些复杂的业务逻辑场景下，应通过测试确认目标系统不存在多个条件组合达成时才能成功利用的逻辑漏洞。

5.3.6.9 HTTP 分割/伪造测试

HTTP分割/伪造测试增强要求：

在使用了安全限制的场景下，应通过测试确认安全限制不会通过HTTP分割/伪造的方式绕过。

5.3.7 错误处理测试

错误处理测试基本要求：

a) 测试方应维护一个易于触发服务端错误的模糊测试列表，并在非增删改功能中进行模糊测试以获取充足的错误响应样本。
b) 测试方应充分评估错误响应中暴露的技术细节，并通过这些细节充分测试可能导致风险的各类威胁。

5.3.8 密码学测试

5.3.8.1 传输层防护及敏感数据测试

传输层防护及敏感数据测试基本要求：

a) 测试方应采用专有的线上及线下工具测试 SSL/TLS 的整体安全性。线上及线下工具的选择和使用应遵循金融机构的相关管理制度。
b) 应通过测试确认目标系统的 SSL/TLS 版本及配置不存在已知的高危漏洞。

c) 当目标系统不采用有效的HTTPS配置时，应通过测试确认目标系统无明文传输用户凭据问题。
d) 当目标系统及客户端之间使用双向校验时，应通过测试确认无法实施有效的中间人攻击。

5.3.8.2 填充提示测试

填充提示测试（Padding Oracle）基本要求：
测试方至少应在ASP.NET架构的应用上进行填充提示测试。

5.3.9 客户端测试

5.3.9.1 客户端URL重定向测试

客户端URL重定向测试基本要求：
应通过测试确认目标系统不存在可以指定目标域名进行直接或二次跳转的功能。如用户在访问构造页面后，需经过登录再进行跳转的场景属于二次跳转。

5.3.9.2 跨域资源共享测试

跨域资源共享测试基本要求：
应通过测试确认目标系统是否开启了CORS功能。在开启了CORS功能的前提下，应通过测试确认域限制使用白名单机制。

5.3.9.3 Flash跨站测试

Flash跨站测试增强要求：
应通过对Flash文件进行反编译，测试是否存在能够导致XSS的未初始化全局变量以及不安全方法。

5.4 测试监控

测试监控基本要求：
a) 金融机构应针对测试方所提供的测试方案，结合自身的技术或管理监控手段，细致评估方案的潜在风险。如是否规避了生产系统测试风险、网络拥塞风险、数据失窃风险和用户隐私泄露风险等。
b) 测试方在测试期间如发现正在进行的测试动作可能导致拒绝服务时，应及时停止测试并第一时间上报金融机构。
c) 测试方在测试期间如发现业务中断、数据损坏或其他突发事件时应及时上报金融机构，同时协助金融机构进行恢复、分析及排查工作。
d) 测试方应建立安全测试实施基线及审查机制，保证安全测试开展的有效性。
e) 应通过技术或管理手段保证历史测试过程记录完整，做到可复现、可追溯。

测试监控增强要求：
应通过技术手段保证安全测试实施过程中违规操作风险的监控和审计。操作违规风险包括但不限于使用未授权人员参与测试，使用违规工具进行测试，漏洞利用时进行冗余动作，利用正常功能进行违规数据导出、积压漏洞和藏匿后门等行为。

5.5 测试加固

测试加固基本要求：
a) 金融机构应根据应用重要程度，漏洞危害以及影响范围在机构内部建立统一的漏洞评级标准，并定期维护更新。

b) 漏洞加固应尽可能满足有效性及完备性要求，金融机构应采用现行最佳的方式进行漏洞加固。漏洞加固手段包括但不限于软件补丁、软硬件防护设备、网络控制措施、代码防护和应用升级改造等措施。
c) 金融机构应及时监测漏洞修复情况。如无法进行修复，测试方应配合金融机构补充临时应急方案。对于能直接造成系统被控制、敏感数据泄露或业务中断等严重后果的漏洞，其漏洞修复时间不应超过 72 小时。
d) 对于能直接造成系统被控制、敏感数据泄露、业务中断等严重后果的漏洞，以及金融机构依据漏洞评级标准评价为中危以上评级的漏洞，应经过测试方复测确认修复。

测试加固增强要求：

金融机构可针对加固工作设置变更流程审批，并在加固前验证加固方案有效性，同时进行数据备份，保留回退措施。

6 管理要求

管理要求基本要求：

a) 金融机构应针对安全测试建立管理制度，明确对应管理工作的目标、范围、原则及实施框架。
b) 金融机构应针对安全测试工作各个相关角色明确定义和职责分工。
c) 金融机构应针对安全测试工作各个相关角色制定明确的操作规程。
d) 金融机构应针对安全测试中的重要及关键操作建立审批流程。
e) 金融机构应针对安全测试方的身份、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金融机构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、测试工具清单、测试时间计划和测试人员信息等。
g) 金融机构和测试方均应设置紧急联系人，以便必要时进行沟通。
h) 金融机构应就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。金融机构应仅保留能够通过测试提供商定位到具体人员的基本信息，由测试方或测试组织方留存与人员身份相关的敏感信息。
i) 金融机构应对安全测试接入的区域、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) 测试方应对安全测试制定实施计划，并根据实施计划推进安全测试工作。实施计划应向所有安全测试相关方同步。
k) 金融机构应指定或授权专门的部门或人员负责安全测试实施过程的监督和管理。
l) 测试方应对安全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安全测试报告，其中应至少包含安全测试目标、人员、时间、测试步骤、测试分析和测试结论以及附录 A 中的安全测试报告样例所示的其他内容。
m) 金融机构可要求测试方在测试实施过程中，参照附录 B 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) 测试方应对安全测试残留文件进行明确的记录和说明。测试方有义务协助金融机构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) 金融机构应针对安全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 次安全测试。
r) 金融机构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） 金融机构应指定或授权专门的部门负责安全测试验收的管理，并按照管理规定的要求完成安全测试验收工作。

管理要求增强要求：

测试方应能够提供测试全过程的视频记录，以便在取证时可进行分析回溯。

附 录 A
（资料性）
安全测试报告样例

金融信息系统Web应用服务安全测试报告的编制可参考下表。

表 安全测试报告样例

<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（截止）；
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Web应用服务</td><td></td><td colspan="2">其他Web应用服务</td><td></td></tr>
<tr><td>参考标准</td><td colspan="6"></td></tr>
</table>

附 录 B
（资料性）
漏洞报告样例

金融信息系统Web应用服务安全测试漏洞报告的编制可参考下表。

表 漏洞报告样例

<table>
<tr><td rowspan="2">测试时间</td><td rowspan="2"></td><td>测试人</td><td></td><td rowspan="2">漏洞编号</td><td rowspan="2"></td></tr>
<tr><td>联系方式</td><td></td></tr>
<tr><td rowspan="2">测试目标</td><td>名称</td><td colspan="4"></td></tr>
<tr><td>信息</td><td colspan="4"></td></tr>
<tr><td>漏洞路径</td><td colspan="5"></td></tr>
<tr><td>漏洞类型</td><td colspan="5"></td></tr>
<tr><td>漏洞等级</td><td colspan="5">☐ 高危 ☐ 中危 ☐ 低危</td></tr>
<tr><td>漏洞描述</td><td colspan="5"></td></tr>
<tr><td>漏洞危害</td><td colspan="5"></td></tr>
<tr><td>漏洞证明</td><td colspan="5"></td></tr>
<tr><td>修复建议</td><td colspan="5"></td></tr>
</table>

参 考 文 献

[1] GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇
[2] GB/T 32917—2016 信息安全技术 Web应用防火墙安全技术要求与测试评价方法
[3] JR/T 0071—2020 金融行业网络安全等级保护实施指引
[4] JR/T 0101—2013 银行业软件测试文档规范
[5] 中华人民共和国网络安全法
[6] OWASP TOP 10 2017 OWASP 开放式Web应用程序安全项目