ACCCF / 应用知识库

09

卷

授权、受控测试与可验证的改进

西班牙语版 · 2026

基于证据的渗透测试手册：企业验证、修复与复测

交战规则、发现、明确界定的影响、修复与验证

将安全测试转化为一个经过授权、可复核的流程：每项发现都有充分证据，每项修复都能在不引发其他事件的情况下得到验证。

面向安全、技术、管理层、合规、保险机构、审计人员和供应商。不包含漏洞利用指导，也不授权在未经明确许可的系统上开展测试。

编辑协调：Jocsan Laguna · 美国网络安全与计算机取证委员会

通用技术指南和开放教育材料。不构成法律意见、专家鉴定意见，也不构成未经授权访问系统的指导。示例和数据均为虚构；插图为编辑重构图。

目录

可见页码对应 PDF 版本。Word 可在打开文档时更新此目录；标题的内部导航保持不变。

前言：扫描并不能证明所有重要事项 3

第1章 授权与规则 3

- **1.1 明确到无需解释即可执行的范围** 3
- **1.2 运营风险与退出计划** 4

第2章 技术准备与验证 5

- **2.1 架构与安全问题** 5
- **2.2 工具与控制数据** 5
- **2.3 记录与同步** 5

第3章 安全执行与日志记录 6

- **3.1 按操作记录日志** 6
- **3.2 停止、升级与沟通** 6
- **3.3 所获信息的处理** 7

第4章 各项发现的证据 7

- **4.1 可复现的记录表** 7
- **4.2 误报与重复项** 7
- **4.3 影响与优先级** 8

第5章 修复与风险管理 8

- **5.1 针对根本原因的修复** 8
- **5.2 按影响与依赖关系制定计划** 9
- **5.3 修复证据** 9

第6章 复测与收尾 9

- **6.1 复现可比条件** 9
- **6.2 关闭状态** 10
- **6.3 最终报告与经验教训** 10

附录A 交战规则与记录表 11

- **A.1 交战规则** 11
- **A.2 发现记录表** 11
- **A.3 复测报告** 12

附录B 法律框架与退出检查 12

前言：扫描并不能证明所有重要事项

一份包含数百条告警的报告，可能仍未回答这些关键问题：哪个风险真实存在、涉及哪项资产、在什么条件下、造成什么影响，以及如何验证修复有效。渗透测试不是一场不惜一切代价获取访问权限的竞赛，而是一项经过授权的评估，旨在形成证据以降低风险，同时不损害人员、数据或业务连续性。

NIST SP 800-115 区分了漏洞审查、识别、分析与验证技术。扫描器可以参与其中，但不能取代规划、分析和后续评估。专业人员的价值不在于运行更多工具，而在于判断需要哪种工具、采用何种范围以及何时停止。[1]

证据应在测试前设计。它必须能够支持复核资产、配置、条件、过程、结果、影响和限制。如果可以使用虚构数据、部分响应或受控环境证明秘密存在，就不应为了证明其存在而捕获真实秘密。修复与复测从一开始就属于委托范围，不应在报告交付后临时补做。

> **指导原则**
> 能够测试某事并不意味着已获授权进行测试。授权应明确资产、技术、时间窗口、数据、联系人和停止条件；测试方法必须守住这一边界。

第1章 授权与规则

1.1 明确到无需解释即可执行的范围

授权文件包括：按域名、地址、应用程序、账户、环境和所有者列明的资产；允许和禁止的技术；日期和时区；测试数据；信息处理；联系人；沟通；停止与交付条件。“你可以审计一切”并未说明是否允许社会工程、拒绝服务、漏洞利用、暴力破解、物理访问或真实数据审查。

应识别第三方及依赖关系：云服务、CDN、邮件服务提供商、支付网关、共享服务、外部 API 和客户网络。获授权的域名可能解析到需要另行授权的第三方基础设施。测试不会因新发现而自动扩大范围：如果出现新资产，应先记录，并在接触前申请扩展授权。

要素	必须书面明确的内容	虚构示例
目标	业务风险与评估问题。	验证客户门户的访问控制。
资产	域名、范围、应用程序、账户和环境。	demo.empresa.invalid 和两个虚构账户。

[1] NIST SP 800-115。《安全测试与评估技术指南》：规划、执行和后续分析。自动化扫描本身并不等同于渗透测试或完整验证。 官方在线来源

要素	必须书面明确的内容	虚构示例
技术	允许、受限和排除的技术。	不开展拒绝服务测试、生产环境暴力破解或垃圾信息发送。
时间窗口	开始、结束、时区和联系时间。	10–12 nov, 22:00–02:00 −06.
数据	虚构数据、脱敏、处理方式与删除。	不得下载真实数据库或导出秘密。
停止	条件、负责人和通知方式。	性能下降、意外访问第三方或范围存疑。
交付	格式、接收人、渠道和删除。	向获授权的负责人交付加密报告。

1.2 运营风险与退出计划

应检查可能发生的阻断、资源消耗、日志、告警、状态变化、残留数据及对用户的影响。计划包括必要时备份、技术联系人、配置回滚、任务暂停和沟通。对于可通过其他方式证明的风险，不得为证明它而启动不可逆操作。

测试应优先使用虚构账户、记录和对象。如果目标是证明未授权访问，应在查看真实内容之前设定停止条件。截图仅保留必要内容：响应、代码、结构和引用，不得传播客户数据。发现证据本身不应构成第二次侵害。

> **启动标准**
> 如果还无法回答由谁授权、包括哪些资产、允许哪些操作、应联系谁以及何时停止，就尚不具备执行测试的条件。



图1。授权是测试方法的一部分。测试前应明确操作范围和退出方式。编辑重构图；不构成真实证据。

第2章 技术准备与验证

2.1 架构与安全问题

应收集架构、资产清单、身份验证流程、角色、日志、依赖关系、近期变更和业务要求。文档审查无需接触服务即可发现弱点。架构为授权、配置、会话管理、数据暴露和集成控制的测试提供指导。并非所有问题都需要漏洞利用。

计划应按影响和概率确定优先级，而不是按漏洞利用的难易程度。无数据服务中的一条告警，其优先级可能低于允许更改收款人的功能。评估应区分技术风险、环境条件和企业后果。如果不了解资产的功能，则只能有限度地评估影响。

2.2 工具与控制数据

应使用已知目标和虚构数据验证工具：识别方式、输出、限制、速率、重试、格式及其对日志的影响。记录名称、版本、配置和结果。扫描器可能产生误报，也可能因把响应当作通用响应而遗漏问题。未经复核，不得将输出直接复制到报告中。

控制数据用于比较预期行为与观察到的行为：无权限用户、具有受限角色的用户、自有资源、虚构的他人资源、有效请求和篡改请求。响应差异无需读取敏感内容即可证明某种情况。如果系统只允许在生产环境中测试，应约定更严格的阈值，并确保有负责人随时可用。

2.3 记录与同步

测试前应检查系统生成哪些日志、谁可以查询以及时间是否同步。记录各数据源的原始值和时区。WAF 告警、应用程序事件和测试人员请求可能使用不同的时钟。关联分析应依据标识符加以说明，而不能仅凭时间接近。

> **质量控制**
> 如果测试未留下可理解的日志，能够据此作出的断言就会受到限制。解决办法不是编造完整的时间序列，而是启用适当的数据源或声明日志缺失。

第3章 安全执行与日志记录

3.1 按操作记录日志

每项操作都记录日期和时区、操作人员、资产、工具及版本、配置、目标、授权请求或程序、响应、产物和影响。日志中不得保存真实凭据或令牌。输出文件应与清单关联，并限制访问。截图仅用于展示必要内容，而不是堆砌图像。

日志还应保留未成功的操作。在有文档记录的条件下得到阴性结果，可以避免错误地断言风险，但并不能证明风险普遍不存在。如果工具失败，应记录版本、错误和范围。重复测试会创建一次关联的新执行，而不是删除此前的尝试。

字段	虚构示例	复核
操作	以受限角色向资源 DEMO-02 发起授权请求。	在范围内，使用虚构数据。
时间与时区	2026-11-10T22:14:03−06:00.	与服务器日志一致。
结果	响应 200，返回他人测试资源的结构。	发生未授权访问，但未读取真实数据。
证据	请求、部分响应、标识符和最小化截图。	不含令牌或个人数据。
影响	无状态变化，服务也无可见影响。	已确认监控和联系人。
决策	停止沿该路径继续测试并记录发现。	不得扩展到其他真实记录。

3.2 停止、升级与沟通

出现性能下降、预期外影响、范围不明、计划外真实数据、需要响应的安全告警或获授权联系人的指示时，应停止测试。通知应包括资产、操作、状态、现有证据和待决定事项。不得为了利用授权未涵盖的机会而继续测试。

真实事件应与测试分开处理。如果团队发现并非由自己产生的活动，应将其记录为独立发现，并通过安全渠道通报。不得自动将其归因于渗透测试，也不得删除其痕迹。时间线必须区分每项操作由谁执行，以及同时发生了哪些事件。

3.3 所获信息的处理

如果测试访问到意外数据，应停止探查，记录该情况而不复制更多内容，并咨询如何处理已获得的数据。交付应通过加密渠道进行，并限制接收人。密钥应通过不同渠道传送。删除测试文件时，应记录范围和限制；未经协商一致，不得删除操作证据。

> **最小证明原则**
> 如果部分响应和一个虚构标识符足以证明问题，就不要下载完整数据库。证据的强弱并不取决于暴露数据量的多少。

第4章 各项发现的证据

4.1 可复现的记录表

记录表包含标识符、标题、资产、版本、条件、来源、过程、结果、影响、范围、限制、约定的严重性、建议和复测标准。测试过程应描述得足够详细，使获授权人员能够复现；但通用报告应避免公开秘密或可能在接收人之外扩大风险的路径。

证据必须将请求和响应与正确的资产关联起来。没有 URL 和日期的截图无法识别对象。错误消息不能证明漏洞已被利用。扫描器标记为“严重”也不能证明业务影响。专业人员必须复核并说明实施了什么操作，以及实际证明了什么影响。

4.2 误报与重复项

误报可能源于推断的版本、自定义响应、代理、配置或错误的扫描器签名。应通过人工复核、日志和预期行为进行交叉验证。如果无法确认，应标记为未确认，且不计入发现总数。同一原因造成的重复项应相互关联，同时不得隐瞒受影响资产。

情形	方法学处理	禁止做法
未确认的告警	复核来源、版本和行为；说明限制。	将其作为已证实的漏洞呈现。
多个资产存在同一原因	按原因归组，并列明各资产覆盖情况。	隐瞒资产或虚增数量。
间歇性结果	记录条件、重试和环境。	只挑选有利的执行结果。
影响未获证实	区分技术条件与潜在后果。	假定已完全控制系统。
超出范围的资产	停止并申请扩大范围。	因其看似相关就进行测试。

4.3 影响与优先级

技术严重性应结合暴露程度、权限、数据、可利用性、补偿控制和对业务的影响进行评估。关键资产中难以利用的漏洞，与隔离环境中容易利用的漏洞，可能需要不同的优先级。既不得因商业关系而淡化风险，也不得为引人注目而夸大风险。

管理层摘要应说明可能发生什么、影响哪些资产、在什么条件下发生，以及需要作出什么决定。不应罗列大量缺乏上下文的术语。技术附录保留证据、日志和限制。管理层获得决策信息；安全团队获得复现路径；合规团队获得跟踪证据。

> **虚构案例**
>
> 某项功能允许通过更改标识符查看另一用户的测试文档。测试在查阅真实文档之前停止。该发现证明了虚构对象上的授权缺陷。不得据此断言所有文档均可访问，也不得声称攻击者已下载数据库：影响范围应通过额外获授权的测试加以界定。

发现记录表支持复核，避免重复造成危害

ACCCF · 编辑重建 · 虚构数据

最小验证、明确影响范围和修复路径

字段	内容	控制
资产和版本	DEMO 服务和观察到的配置。	对象明确且在范围内。
操作过程	受控环境中的步骤和虚构数据。	无需真实凭据即可重复。
结果	技术响应和相关证据。	不要将警告与漏洞利用混为一谈。
影响	资产、条件和已证明的后果。	不得外推至整个企业。
修复	建议的变更和优先级。	负责人、日期和复测标准。

本图说明决策与关系；不代表真实案例的证据。

图2。发现记录表支持复核，无需重复造成损害。最小化证明、明确界定的影响和修复路径。编辑重构图；不构成真实证据。

第5章 修复与风险管理

5.1 针对根本原因的修复

建议应指出需要改变的条件，而不只是笼统地要求更新。如果问题在授权，应检查服务器端验证及其与资源的关系；隐藏链接并不能解决问题。如果问题在配置，应检查对其他环境和组件的影响。修复方案包括负责人、目标日期、依赖关系、测试和可能的回归。

无法立即修复时，应记录已接受的风险、临时缓解措施、负责人和复核日期。风险接受不得被表述为完成修复。WAF 可以限制某条路径，但不能消除根因；应保留两种状态的证据，并验证规则是否影响合法功能。

5.2 按影响与依赖关系制定计划

操作	负责人和日期	验收标准
临时缓解措施	[负责人、实施方式和有效期]	[在不中断运营的情况下降低暴露]
永久修复	[变更、版本和部署]	[范围内的根因已消除]
复核其他资产	[相同模式与覆盖范围]	[无隐藏的重复项]
回归测试	[关键功能与角色]	[不损害合法用户]
文档更新	[图表、配置和程序]	[实际情况与文档一致]
残余风险接受	[接受人、理由和到期日]	[不得与技术关闭混淆]

5.3 修复证据

应保留配置变更、版本、日期、负责人、部署、测试和影响等证据。面板显示“已更新”的截图并不能证明该路径已修复。如果存在多个环境，应记录修复应用的位置。不得通过修改初始报告来删除发现：应添加一份关联的新评估。

> **诚实原则**
> “供应商说已经修复”只是一项声明，不是复测。关闭证据要求完成技术验证，或作出明确的残余风险接受决定并说明其范围。

第6章 复测与收尾

6.1 复现可比条件

复测应尽可能使用相同的对象、角色、条件和程序，并记录新的版本和日期。应与原始发现进行比较，但不得更改此前的证据。如果应用程序或环境发生变化，应予记录，因为这可能解释不同的结果。阴性结果仅适用于本次测试及其覆盖范围。

还应测试回归情况：合法用户可以正常工作，且该功能不会暴露其他数据。如果恶意请求被阻止，但正常访问遭到破坏，状态可能为部分修复。如果修复仅对一条路径有效，且存在等效路径，应在授权范围内检查这些路径。关闭测试不能只截取预期错误的画面。

6.2 关闭状态

状态	标准	证据
已修复	该情况在范围内无法复现，且未观察到回归。	复测、日期、版本和合法功能。
部分修复	部分资产或路径已改善；其他资产或路径仍存在该情况。	按资产列明覆盖范围和待办事项。
已缓解	已有临时控制措施，可降低暴露，但未消除根因。	规则、测试、有效期和限制。
已接受	负责人接受残余风险，并说明理由和到期日。	决定、范围和复核。
未关闭	该情况可以复现，或缺乏充分证据。	原始发现和待完成的操作。

6.3 最终报告与经验教训

最终报告应关联初始发现、变更、复测和状态，不得删除此前记录。报告包括残余风险、限制和下一次复核日期。管理层摘要不得承诺“系统安全”；应说明评估了哪些风险，以及有哪些改进证据。如果某项测试无法执行，应如实声明，而不是标记为通过。

经验教训可能要求采用抗钓鱼身份验证、复核授权、开展回归测试、建立第三方清单或改进日志。NIST SP 800-63B-4 提供身份验证指南和保证级别；但它不能取代对恢复流程的评估，而后者往往是实际的入侵路径。[2]

> **真正关闭**
> 当组织能够展示发现了什么、改变了什么、验证了什么以及仍存哪些风险时，测试才算结束；而不是在 PDF 被命名为“最终版”时结束。

[2]NIST SP 800-63B-4（2025年7月）。身份验证与验证器管理指南，包括保证级别和抗钓鱼身份验证。账户恢复属于风险的一部分，不应将其简化为密码问题。 官方在线来源



图3。复测验证的是风险，而不只是补丁。保留最初的证据并与新证据比较。编辑重构图；不构成真实证据。

附录A 交战规则与记录表

A.1 交战规则

供审批的虚构模板

项目：DEMO-PENTEST-2026-009
目标与企业风险：[具体问题]
纳入的资产：[域名、范围、应用程序、账户]
排除项：[资产、第三方、数据和技术]
时间窗口与时区：[开始、结束、联系人]
允许使用的数据：[虚构数据、脱敏、处理]
允许的操作：[审查、验证、条件]
禁止的操作：[DoS、暴力破解、社会工程、其他]
停止阈值：[性能下降、数据、范围、告警]
紧急联系人及替补：[安全渠道]
证据：[格式、最小化和保管]
交付：[接收人、加密和日期]
删除：[对象、备份和限制]
复测：[日期、范围和验收]
授权：[权利持有人、第三方和版本]

A.2 发现记录表

字段	必填内容	虚构示例
标识符	与日志关联的稳定代码。	DEMO-AUTH-003.
资产与版本	应用程序、环境和配置。	DEMO 门户 v2.4，测试环境。
条件	哪个控制失效，以及在什么角色下失效。	可访问另一虚构用户的资源。

字段	必填内容	虚构示例
过程	授权步骤、请求和参数。	受限角色和对照资源。
结果	响应和不含秘密的产物。	代码 200 和部分结构。
影响	已证明的后果和范围。	仅访问虚构对象；不作外推。
限制	未测试哪些内容，以及原因。	未查阅真实文档。
修复	变更、负责人和优先级。	服务器端授权验证。
复测	条件、日期和结果。	相同路径和角色，并增加回归测试。

A.3 复测报告

对比记录

原始发现：[ID、证据和日期]
已应用的变更：[配置、版本、负责人]
复测日期与时区：[原样记录]
等效条件：[角色、对象、参数]
重复原始测试的结果：[观察结果]
回归测试：[合法功能]
附加覆盖范围：[路径或资产]
状态：[已修复、部分修复、已缓解、已接受、未关闭]
残余风险与限制：[声明]
下次复核：[日期和负责人]
附件：[输出、日志和清单]

附录B 法律框架与退出检查

授权是首要要求；电子证据需要具备规范的方法、可归因性、完整性和可访问性。在墨西哥，适用的 CNBV 规定对信贷机构提出了专门的安全审查和记录要求，包括在其适用范围内至少每年开展一次第 316 Bis 17 条规定的审查。秘鲁和阿根廷设有行业管理与响应要求；西班牙则区分支付与风险。不得将这些义务套用到所有企业。[3][4][5][6][7][8]

[3]《适用于信贷机构的一般规定》，第 316 Bis、316 Bis 1、316 Bis 10 至 17 条：凭证、加密、访问、事件、异常、日志和审查。 官方在线来源

[4]秘鲁。SBS 504-2021，第 12.6.g、15 和 17.3–17.4 条：保存、报告与取证分析、注册记录、身份验证和操作。 官方在线来源

[5]阿根廷。BCRA 通告 A 8280：网络事件响应与恢复；在遏制、恢复和解决之后五个日历日内提交最终报告。 官方在线来源

[6]西班牙。皇家法令 19/2018，第 45、66 和 67 条：未经授权交易的退款、风险管理和重大事件的即时通报。 官方在线来源

[7]墨西哥《商法典》，第 89–94 和 1205 条：数据电文的中立性、归属、书面形式、原件、完整性、可访问性和可采性。官方汇编。 官方在线来源

[8]《国家民事和家庭诉讼法典》，第 348–350 条。包含 15-01-2026 修订的汇编。其应用逐步推进，并取决于相关宣告。 官方在线来源

哥伦比亚、厄瓜多尔、智利和西班牙均有电子文档、签名和保存规则，有助于组织证据；但这些规则本身并不授权入侵测试。即使目标是证明漏洞，数据保护要求仍会限制可捕获和共享的内容。[9][10][11][12][13][14]

控制	验收问题
授权	资产、技术、数据、时间窗口和停止条件是否已获批准？
安全	测试是否避免损害和不必要的暴露？
方法	工具、版本和输出是否经过验证？
发现	资产、过程、结果和影响是否可追溯？
修复	变更和覆盖范围是否有文档记录？
复测	是否验证了相同条件和回归情况？
结论	残余风险和限制是否都没有被隐瞒？

收尾

最佳测试不在于证明获得了多大的访问权限，而在于能够凭借充分证据降低风险，且不引发另一事件。

[9]智利。关于电子文档和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。 官方在线来源

[10]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。 官方在线来源

[11]厄瓜多尔。《电子商务、电子签名和数据电文法》第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。 官方在线来源

[12]欧盟法规 (UE) 910/2014 eIDAS，第 25–26 和 46 条：不得因格式而歧视电子签名和电子文档；高级电子签名；合格电子签名的法律效力。 官方在线来源

[13]墨西哥。《私营主体持有个人数据保护联邦法》，文本公布于 20-03-2025，并于 14-11-2025 修订。第 5–9、18–20 和 31 条：原则、安全、保密、安全违规和权利请求处理。当前联邦主管机构为反腐败与善治部。 官方在线来源

[14]欧盟。欧盟法规 (UE) 2016/679，第 5、25、28 和 32–34 条：原则、设计即保护、受托处理方、安全以及安全违规的通知/通报。西班牙还要求审查适用的国家和行业法律。 官方在线来源