Penetration Testing Methodology for SaaS: OWASP, ASVS, and Beyond

Bev Waller & Erik Jones January 27, 2026

Executive Summary

Penetration testing is required by every meaningful security framework — **SOC 2 CC4.1, PCI DSS Requirement 11, HIPAA Security Rule, ISO 27001 A.8.8**, FedRAMP, and increasingly customer security questionnaires. Done well, a pen test is a structured adversarial assessment that produces actionable findings; done poorly, it is a Nessus scan with a cover page. This guide describes the methodology distinctions that matter, the standards that frame the work, and the deliverables that satisfy auditors and customers.

Why Penetration Testing Matters

Vulnerability scanners find known issues in known places. Penetration testers find unknown issues, exploit chains across multiple systems, and the operational drift that scanners cannot detect — like the staging

environment with production data, the deprecated API still serving traffic, or the IAM role with one too many permissions.

The OWASP Foundation describes the difference plainly in the *"Web Security Testing Guide v4.2"*: *"automated tools detect technical issues; humans uncover business-logic flaws and the exploit chains that combine multiple lower-severity issues into a high-severity outcome."* The methodology gap matters because the most-cited findings in serious breach reports involve chained low-severity issues, not single high-severity vulnerabilities.

The Standards That Frame the Work

Pen testing is not free-form. Established methodologies define scope, technique, and deliverable expectations. Choosing one (or composing from multiple) signals rigor.

OWASP Methodologies

OWASP Web Security Testing Guide v4.2

The most widely-adopted methodology for web application testing. **11 testing categories** covering information gathering, configuration management, identity management, authentication, authorization, session management, input validation, error handling, cryptography, business logic, and client-side. Each category has dozens of specific test cases with reproduction steps.

OWASP Application Security Verification Standard (ASVS)

Three verification levels:

> **Level 1:** opportunistic — defense against common, easily-exploitable issues. Suitable for most internal applications.
>
> **Level 2:** standard — applications handling sensitive business data. Suitable for SaaS handling B2B customer data.
>
> **Level 3:** advanced — applications requiring high-trust assurance. Healthcare, financial services, critical infrastructure.

ASVS pairs well with WSTG: WSTG describes how to test, ASVS describes what good looks like.

OWASP Top 10

The reference list of dominant web application risks. Updated approximately every 4 years; the 2021 list and the 2025 LLM-specific list are current. Top 10 categories anchor pen test scope without being a complete methodology.

NIST and PTES

NIST SP 800-115

"Technical Guide to Information Security Testing and Assessment." Federal-government-grade methodology covering planning, discovery, attack, and reporting phases. Common reference for FedRAMP and federal-adjacent engagements.

Penetration Testing Execution Standard (PTES)

Industry-driven methodology with seven phases: pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, reporting. Less formal than NIST 800-115, broader than OWASP WSTG.

Engagement Models

Two axes define an engagement: scope (what is in/out) and knowledge (what the tester knows going in).

Internal vs External Scope

External: testing from the public internet against internet-facing assets. Required by PCI DSS quarterly via ASV; required annually for most frameworks.

Internal: testing from inside the network perimeter — a compromised laptop, a malicious insider, a successful phishing payload. Captures lateral movement risk that external testing misses entirely.

Cloud: AWS, Azure, GCP-specific testing methodology. Different attack surface — IAM misconfigurations, exposed S3 buckets, IMDS abuse, cross-account roles. Tools include **Pacu, ScoutSuite, CloudSploit, Prowler**.

Application: deep testing of one or more applications, usually combining authenticated and unauthenticated testing. Where business logic flaws emerge.

Black Box, Gray Box, White Box

> **Black box:** tester has no internal knowledge. Simulates an external attacker. Maximum realism, minimum coverage.
>
> **Gray box:** tester has partial knowledge — credentials, architecture diagrams, or both. The most common engagement model. Balances coverage and realism.
>
> **White box:** tester has full source code, architecture, and credentials. Maximum coverage, simulates a determined insider with full visibility.

Most SaaS engagements run gray box: tester gets standard-tier customer credentials and architecture overview, then probes for both standard customer-tier issues and privilege escalation paths.

Practical Methodology

A well-run engagement follows the PTES seven-phase model with OWASP WSTG providing the technical depth.

Phase 1: Pre-Engagement

Scope definition, rules of engagement, communication protocols, emergency contacts. The phase that prevents accidents — the tester does not knock production over because the boundaries are documented in advance.

Phases 2-3: Intelligence and Threat Modeling

OSINT, asset discovery, attack surface enumeration, threat-actor profiling. Maps what is in scope and identifies what is most worth testing.

Phases 4-6: Vulnerability Analysis, Exploitation, Post-Exploitation

The technical work. Vulnerability scanning establishes baseline; manual testing finds the issues scanners miss; exploitation validates that findings are real; post-exploitation maps what an attacker could do after initial compromise. Tools include **Burp Suite Professional, OWASP ZAP, Nuclei, Nmap, Metasploit, BloodHound (for AD), Pacu (for AWS)**.

Phase 7: Reporting

The deliverable. Executive summary, methodology, findings with CVSS scores, reproduction steps, screenshots, and remediation guidance. The report is the audit-grade artifact.

Tester Credentials

Customer security questionnaires increasingly ask for tester certifications. The recognized credentials:

> **OSCP** (Offensive Security Certified Professional) — practical, hands-on certification. The de facto baseline for pen testers.

OSWE (Offensive Security Web Expert) — advanced web application testing certification.

CREST CRT, CCT (Council for Registered Ethical Security Testers) — UK-led, internationally recognized; required for PCI DSS engagements in many regions.

GIAC GPEN, GWAPT, GXPN — SANS-affiliated, well-regarded for enterprise environments.

Common Pitfalls

Scanner-as-pen-test: a Nessus or Burp scan with a cover page is not a pen test. Auditors and serious customers will identify the substitution.

Scope ambiguity: unclear scope produces the worst kind of finding — a critical issue in a system the tester thought was out-of-scope.

No exploitation: a finding without exploitation is a hypothesis. Validating exploitation distinguishes real findings from theoretical ones.

Reports without remediation guidance: a list of findings without clear remediation steps shifts the work to engineering teams who lack security context.

Annual cadence only: annual testing for systems that change daily creates a drift gap of 364 days. Continuous testing (DAST, attack-surface monitoring) closes it.

Measured Outcomes

Testers credentialed with OSCP minimum, often OSWE or CREST

Methodology aligned to OWASP WSTG and ASVS Level 2 minimum

2-4 week engagements for typical SaaS scopes

Findings with CVSS 3.1 scores, reproduction steps, and specific remediation guidance

Retest included after remediation to verify fixes

Audit-grade reports satisfying SOC 2, PCI DSS, HIPAA, and customer questionnaire requirements

How Jacobian Helps

Penetration testing benefits from the same engineering depth that builds the systems being tested. Our team brings both the offensive-security skill (OSCP/OSWE-credentialed testers running OWASP WSTG-aligned engagements) and the audit perspective (Bev's compliance background frames findings against the frameworks that customers and auditors actually care about). We deliver findings that are exploitable, not theoretical; reports that are remediation-actionable, not just documentation; and retest cycles that close the loop. Whether you need annual SOC 2 / PCI testing or a continuous adversarial assessment program, the methodology is the same — only the cadence differs.

Resource Details

Author: Bev Waller & Erik Jones

Published: January 27, 2026

Categories:

Security | Penetration Testing | Compliance

Download

Full Document

About This Resource

A practical guide to penetration testing for SaaS companies. Covers OWASP Testing Guide methodology, ASVS verification levels, scoping decisions, and what separates a real pen test from a vulnerability scan.

Categories:

Security | Penetration Testing | Compliance