

# HackerOne Pentest

Achieve high-impact results with AI-augmented, human-led security testing through Pentest as a Service (PTaaS)

## High-impact, Scalable Pentesting

HackerOne Pentest applies methodology-driven testing aligned to OWASP, PTES, and CREST, enhanced by human expertise and AI-powered platform intelligence. Each engagement is tailored for depth and impact across APIs, applications, cloud infrastructure, and AI models; mapped to your asset complexity, risk profile, and regulatory needs.

Every pentest includes Hai, our AI security agent, which streamlines reporting, accelerates remediation, and produces audit-ready outputs. Unlike legacy firms, we launch tests in days, provide real-time visibility, and integrate directly into developer workflows for continuous security improvement.

“

***“HackerOne’s pentest solution has helped us identify ways to strengthen our products by uncovering inconsistencies we may not have been alerted to previously.”***

Dallan Wagner,  
Senior Product Security Engineer at Adobe

## Adobe by the Numbers: Pentest Outcomes That Matter

**35%**

Increase in total vulnerabilities identified compared to previous vendors

**20–50%**

More vulnerabilities surfaced across engagements

**2 days**

Time to first valid finding, accelerating remediation

**3 hours**

Staff time saved per test through automated workflows

## Use Cases

### Proactive Risk Reduction

Uncover complex vulnerabilities missed by scanners with human-led testing and AI-assisted prioritization.

### Secure Product Development

Embed pentesting into agile workflows for fast, AI-augmented findings and remediation before release.

### Audit-Ready Reporting

Produce consistent, high-quality reports aligned to leading regulatory frameworks, so you're always prepared for audits.

### Code Security Audit (CSA)

Go deeper than SAST with whitebox source code reviews delivered by a community of 600+ vetted software engineers.





## Web

Perform in-depth testing on web apps across OWASP Top 10 risks, including injection, broken access control, and misconfigurations. Uncover vulnerabilities in modern [web applications](#) and frameworks.



## Cloud Configurations

Assess cloud infrastructure for misconfigurations, insecure access controls, improper resource segregation, and exposed storage or policies across platforms like [AWS](#) and [Azure](#).



## AI and LLM Testing

[Test Large Language Models \(LLMs\)](#) for prompt injection, insecure output handling, model denial of service, training data poisoning, and over-reliance or misuse of AI agents in production.



## Mobile App Testing

Conduct mobile security testing across [iOS](#) and [Android](#), including static analysis, injection risk detection, built-in security control review, and identification of outdated or vulnerable app versions.



## API Security Testing

Map and test APIs by analyzing business logic, versioning, and endpoint exposure. Detect injection flaws, misconfigurations, and authorization gaps across REST, GraphQL, and more.



## Network Testing

Evaluate [internal](#) and external network surfaces through TCP/UDP scanning, asset discovery, and service enumeration. Identify misconfigurations, exposed systems, and external-facing assets.



## Desktop App Testing

Review desktop software for embedded secrets, injection vectors, and hardcoded URLs/strings. Test for legacy vulnerabilities and security risks common in native or cross-platform desktop apps.



## AWS Pentesting

Test your AWS applications and environment, identify misconfigs, SSRF risks, and cloud-specific exposures with support from AWS-certified HackerOne pentesters. Available on [AWS Marketplace](#) for streamlined procurement and deployment.



## Code Security Audit

[Conduct source code reviews](#) to identify logic flaws, insecure design patterns, hardcoded secrets, and vulnerabilities such as SSRF, XSS, and improper input validation across repositories and development environments.



## Elite Pentester Expertise

- Pentesters average 3+ years in the field; 75% hold 5+ years of experience
- 16% of findings are high or critical severity, doubling the industry standard
- Our intelligent talent-matching engine ensures each test is staffed with the right expertise to maximize impact



## Fast, Repeatable Test Delivery

- Launch a pentest in 4 to 7 business days, minimize manual scoping steps, and easily repeat the process via a centralized platform
- Real-time collaboration with pentesters enables continuous visibility and immediate response to findings



## Strategic Engagement Support

- Dedicated Engagement Managers (TEMs) provide scoping guidance, coordinate communication, and ensure alignment with your internal workflows
- They act as strategic partners, driving repeatable, quality testing outcomes across engagements



## Advanced Access Control and Tester Verification

- HackerOne Clear allows you to choose the level of researcher identity verification to align with risk and compliance needs
- HackerOne Gateway secures assets with a Cloudflare-powered Zero Trust tunnel when needed, giving you oversight with start/stop controls, traffic logs, and coverage analytics



## Workflow Integration and Automation

- Over 36 native integrations with tools like Jira, Github, Gitlab, ServiceNow, Slack, Splunk, for optimized remediation workflows and developer time savings
- HackerOne API and webhook capabilities enable custom workflows and automated reporting across your enterprise systems



## AI-Augmented Pentest Delivery with Hai

- Hai, our AI-powered security engine, auto-generates clear, consistent reports, remediation guidance, and proof-of-concept examples.
- It supports multilingual communication and policy enforcement, reducing the manual review burden for your team and researchers alike

**“With PTaaS, you have a software-enabled platform that you can use to integrate and directly streamline results to your engineering teams. You can also tap into a huge talent market, so rather than having five pentesters a consultancy has selected, you have the choice of hundreds, all with their own specialties and skills.”**

Robert Kugler,  
Head of Security and Compliance, Cresta AI



**CRESTA**

**Contact** our experts today to explore how the HackerOne Pentest can be adapted to fit your unique compliance and security objectives.

hackerone.com