The Life Cycle of a Crowdsourced Pen Test

Find, Fix, and Prevent AppSec Vulnerabilities

A crowdsourced pen test is a penetration test performed by freelance security researchers via a platform. This approach brings together the methodology, vetting, and structure from traditional pen testing with a global talent pool and modern SaaS platform. A crowdsourced pen test, performed through an integrated platform, allows for communication and teamwork across teams, making the process fast, iterative, and smooth. It also makes application security more data driven; you can easily benchmark results and share your KPIs.

A crowdsourced pen test includes four steps:

Step 1: Match the right skills for a purpose-built team.

□ Your organization provides information about its application's technology stack.

□ The top researchers with matching skill sets are selected to complete your project.

□ The team works together, exploring the complete application over a fixed time period.

□ The team works collaboratively to perform manual security testing related to topics such as input validation, authentication, and access controls identify flaws in the application's implementation.

Step 2: The team submits its findings.

□ As team members discover issues in the application, they submit reports to your organization through the crowdsourced pen test platform.

□ The lead researcher reviews each report before it's submitted to ensure the report is valid.

□ The lead researcher assigns a criticality rating to each report, based on likelihood and business impact.

Step 3: Remediate issues.

□ Your organization receives reports as soon as flaws are discovered and reviewed by the pen test lead. In some cases, receiving the report before the entire pen test is complete gives your organization extra time to get any important vulnerabilities fixed as soon as possible.

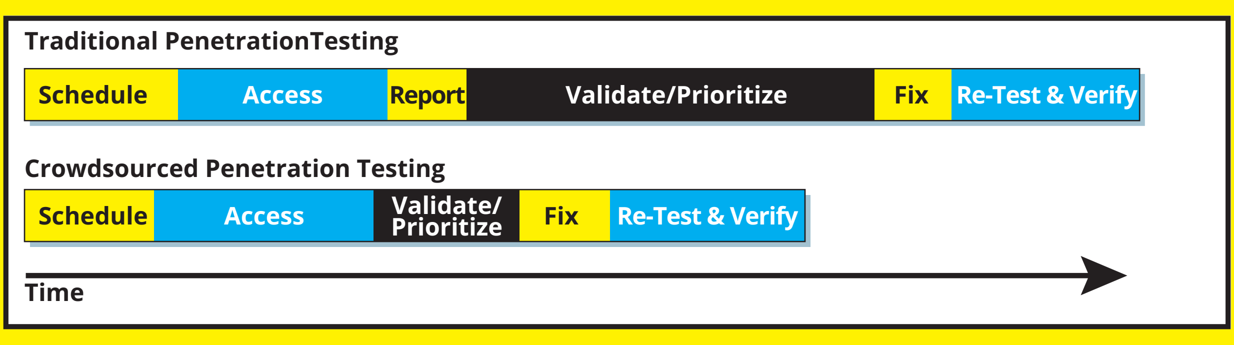
□ Your organization, through the crowdsourced pen test platform, works with the findings and dynamically communicates with the pen testers for months after the initial test is complete.

□ Your platform can even integrate with developer bug tracking systems such as JIRA or GitHub.

Step 4. Share the results.

□ After the fixed time period is complete, your organization can download a PDF summary report to share with internal and external stakeholders, such as development team leads or customers requiring proof of a technical security test.

The timeline for a crowdsourced pen test can differ from a traditional pen test:



Scheduling

□ **Crowdsourced:** On-demand

□ **Traditional:** May require advanced notice

Reporting

□ **Crowdsourced:** Delivered via a platform as issues are discovered

□ **Traditional:** Delivered all at once, after assessment is complete

Validation, prioritization, and communication of results to development

□ **Crowdsourced:** Platform makes it easy to facilitate collaboration between security, pen testers, and development

□ **Traditional:** Manual and takes time

Retesting and verification

□ **Crowdsourced:** Included for up to a year after issues are discovered, performed by the same pen test team

□ **Traditional:** May not be included; may get reviewed in the next pen test by a different pen test team

Communication is also where a crowdsourced pen test differs from a traditional pen test. With a crowdsourced pen test

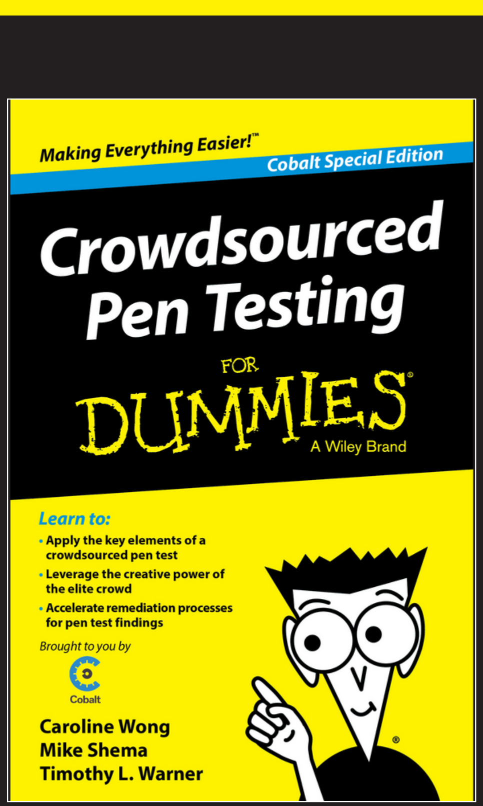
□ Pen testers can ask developers about intended use cases for the application.

□ Developers can ask pen testers questions about security findings.

□ Pen testers can help developers understand exactly how to remediate specific findings.

□ Developers can ask security teams about each finding's criticality and how to prioritize fixes.

□ When a finding is fixed, pen testers can retest the issue and verify that the patch has been effective.



Making Everything Easier!™

Cobalt Special Edition

Crowdsourced Pen Testing

FOR DUMMIES®

A Wiley Brand

Learn to:

- Apply the key elements of a crowdsourced pen test
- Leverage the creative power of the elite crowd
- Accelerate remediation processes for pen test findings

Brought to you by

Cobalt

Caroline Wong
Mike Shema
Timothy L. Warner

To learn more about crowdsourced pen testing, see *Crowdsourced Pen Testing For Dummies* HERE.

for dummies® A Wiley Brand