

## Veracode Manual Penetration Testing

### DID YOU KNOW?

- ✓ In manual penetration tests, 74% of applications had at least one vulnerability violating the OWASP Top 10.

#### Veracode

- ✓ Every application has a different business process, application-specific logic and can be manipulated in an infinite number of combinations. Not all issues can be found through automation.

#### OWASP



*“A penetration test can determine how a system reacts to an attack, whether or not a system’s defenses can be breached, and what information can be acquired from the system.”*

**CISSP and CAPCM  
Prep Guide**

# Test manually after automation to find more vulnerabilities at lower cost

## Conduct manual penetration tests on applications to achieve compliance

No automated technique can find every vulnerability type. Some categories of vulnerabilities, such as authorization issues and business logic flaws, will always require a skilled penetration tester. Yet penetration testers have become difficult to hire as demand for their skills has increased. In addition, using penetration testing as the only way to assess an application is expensive and time consuming. It can take weeks to perform a full penetration test on an application, with results that vary depending on the tester. As a result, most organizations only use this method where they need it to comply with regulations, or on an infrequent basis.

Veracode Manual Penetration Testing (MPT) complements Veracode’s automated scanning technologies with best-in-class penetration testing services to find business logic and other complex vulnerabilities in web, mobile, desktop, back-end and IoT applications. Using a proven process to ensure high customer satisfaction, Veracode MPT provides detailed results, including attack simulations, through the Veracode Application Security Platform, where both manual and automated testing results are assessed against your corporate policy. Developers can consult Veracode application security consultants on the findings and retest uncovered vulnerabilities to verify successful remediation.

### Get accurate results while reducing cost with a proven process

The strength and weakness of manual application security testing is the people. Missed findings due to lack of process or an unskilled tester are real issues. Veracode uses standardized testing processes that ensure consistency while enabling consultants to apply their individual expertise. We scan your application with automated testing technologies first to ensure consistent results and then use manual penetration testing to test for flaws that can’t be found in an automated way. This improves accuracy of results while reducing cost.

### Comply with PCI DSS, HIPAA and other regulations

Regulations including PCI DSS, HIPAA, GLBA, FISMA and NERC CIP require penetration testing, and security frameworks such as OWASP Top 10 and SANS Top 25 require penetration tests. PCI DSS even specifies that scans without a manual process are not permitted. Veracode MPT focuses on identifying issues that require a manual tester’s insight, and delivers results that are easily consumed by both development teams and auditors, including attack simulations showing how an attacker would exploit a vulnerability.



## Add over 10 years of application security expertise to your team

Veracode has helped thousands of companies run their application security programs. With Veracode, you get over a decade's worth of experience in your corner. In addition to web applications, Veracode can also test mobile, desktop, back-end and IoT applications. Then Veracode penetration testers can review findings with developers and security team members to help them understand the nature and full impact of the findings and how they can address them. In addition, you can retest prior findings to verify that they have been successfully addressed by the development team.

## Integrate manual findings with the rest of your program

Manual test results can be challenging to manage as they're usually delivered via PDF or spreadsheet, and don't integrate with the rest of the data from your application security program. We securely deliver Veracode MPT results through the Veracode Application Security Platform, and integrate them into the Policy Manager and Analytics for comprehensive pass/fail reporting across all your test results. They are also available via Veracode APIs for integration into Jira, Microsoft Team Foundation Server, Archer or other external systems.

**Contact Veracode for more information about how we can help find even the most complex vulnerabilities in your applications.**

## The Veracode Application Security Platform

*The Veracode Application Security Platform offers a holistic, scalable way to manage security risk across your entire application portfolio. We offer a wide range of security testing and threat mitigation techniques, all hosted on a central platform, so you don't need to juggle multiple vendors or deploy tools. Application security cannot be solved with technology alone, so our security program managers will work with you to define policies and success criteria and create a strategic, repeatable way to tackle your application security risk. Veracode educates developers with actionable results, one-on-one coaching, and a variety of training, so they can effectively fix existing flaws and code securely moving forward.*

[www.veracode.com](http://www.veracode.com)