RAPID7
PROFESSIONAL SERVICES

# Web Application Penetration Testing

## What is it?

In addition to the Open Source Security Testing Methodology Manual (OSSTMM) and the Penetration Testing Execution Standard (PTES) Rapid7's application penetration testing leverages the Open Web Application Security Project (OWASP), a comprehensive framework for assessing the security of web-based applications, as a foundation for our web application assessment methodology. Our web application pen tests simulate real-world attacks to provide a point-in-time assessment of vulnerabilities and threats to the customer's application environment.

The post-assessment analysis presents logical groupings of one or more security issues with common causes and resolutions as a finding, which allows Rapid7 to quantify and prioritize the business risk to an organization. An actionable findings matrix can be used as an overarching workflow plan that can be tracked within the security organization. This plan is intended to assist the remediation team in prioritizing and tracking the remediation effort; consequently, each finding has been categorized according to its relative risk level and also contains a rating as to the amount of work and resources required in order to address the finding. Each finding also contains hyperlinked references to resources and provides detailed remediation information.

## What is the value proposition?

- An understanding of real-world risks posed to an organization from the perspective of an attacker, going beyond the limitations of automated scanning.
- A prioritized risk rating (DREAD framework) that takes multiple business-driven criteria into account.
- Direct communication with an offensive security expert with years of industry experience and with direct access to the product team of the most widely used penetration testing framework.

## What are the drivers?

- Breadth and Depth: Customers that require a comprehensive security assessment, with deeper testing and more detailed results.
- Compliance: Payment Card Industry's Data Security Standard (PCI-DSS) requires annual network penetration testing.
- Best Practices: Beyond compliance, many best practices frameworks recommend completing penetration testing.
- Contractual Obligations: Some larger enterprise organizations require a penetration test as part of doing business.
- Hosted Environments: With a growing reliance on the cloud, an emerging threat comes in the form of a malicious user or customer accessing other silo's data, only manual pen testing can accurately define these risks

## What is the methodology used?

Our penetration testing methodology is as follows:

- Reconnaissance – Checking the Internet for the customer's public-facing presence and information
- Network Surveying and Services Identification – Painting a picture of what the customer's perimeter looks like to the outside world
- Manual Environmental Testing – Analyzing gathered data to build and execute an attack plan
- Password Cracking – Attempting to crack any password hashes or brute force any authenticated mechanisms
- Manual Application Testing / OWASP Testing Methodology including: Access Control / Authorization, Authentication, Session Management, Configuration Management / Web Application Architecture Review, Error Handling, Data Protection, Input Validation
- Root Cause Analysis and DREAD Reporting – Pinpointing the root causes of identified issues to be classified and compiled into a final deliverable

## Want to get started?

**Call:** 866.7.RAPID7 **Email:** sales@rapid7.com **Schedule:** http://www.rapid7.com/services