

# Web Application Penetration Testing

## Protecting your websites and applications from cyberattacks

### Overview

Ivanti's web application penetration test provides a comprehensive understanding of how user inputs change data inside an application. Our proprietary framework helps to discover multiple attack vectors including thorough and dynamic testing of user, network and API interfaces. Our web application penetration test also enhances visibility, helps to prioritize and provides actionable remediation insights to help shrink your attack surface. We evaluate applications based on OWASP Top 10, OWASP Mobile Top 10 and CWE Top 25 programming errors. Our pentesters also look for open-source vulnerabilities and other security-related weaknesses during the engagement.

### The challenge

As web applications gain precedence, they are required to undergo security posture assessments to ensure vulnerabilities that are most likely to be used by adversaries to exploit and infiltrate your organization are discovered before they can carry out enterprise-wide attacks. A web application penetration test enhances visibility, helps to prioritize and provides actionable remediation insights to help shrink the attack surface.



Detect, prioritize and remediate

100+

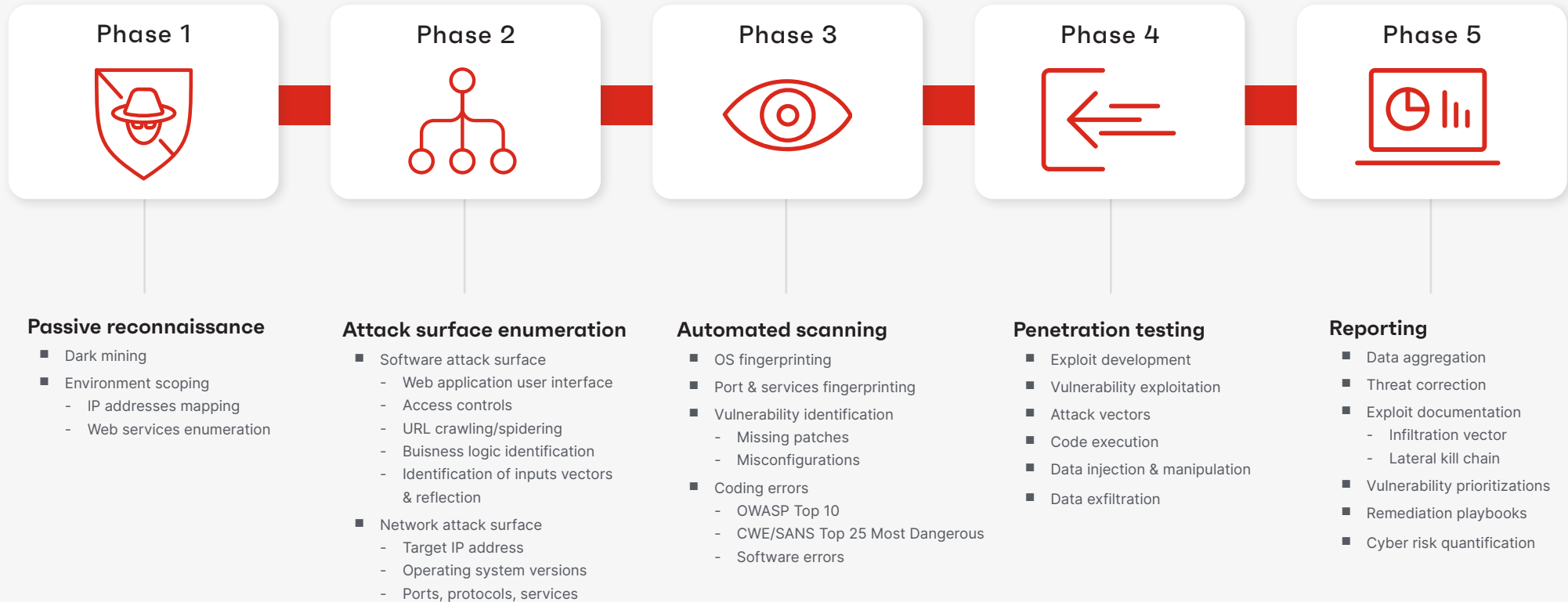
Pentesters & threat hunters

49+

Zero-days discovered

## Our methodology

We perform the test from an attacker's perspective with these five steps:



## Key benefits



### Expert pentesters

Our team comprises skilled pentesters who have reported numerous zero-days.



### Complete coverage

Complete end-to-end coverage is provided to secure your attack surfaces.



### Manual scanning

We do a detailed manual verification of findings while eliminating false positives.



### Prioritize vulnerabilities

We formulate a list of prioritized vulnerabilities, mapped to CWE Top 25 and OWASP Top 10 programming error lists, to help your security team know what to fix first.



### Actionable insights

Know whether your critical data is at risk and how easily a malicious actor may access it.



### Support

Get comprehensive guidance and support towards prioritizing and remediation of vulnerabilities.



### Synchronous reporting

We provide results within hours of initiating the assessment through [Ivanti Neurons for App Security Orchestration & Correlation \(ASOC\)](#).


## What to expect

- Detailed findings of vulnerabilities and weaknesses
- Executive summary
- Attack surface exploitability
- Vulnerability prioritization
- Demonstration of complex attack paths
- Remediation and recommendations



## About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit [ivanti.com](https://www.ivanti.com).

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

[sales@ivanti.com](mailto:sales@ivanti.com)