

# CORE Impact for Web Application Testing

## Assess Your Web Applications Against Real-World Attacks

CORE Impact<sup>®</sup> Pro offers the most comprehensive web application penetration testing capabilities available in one solution. With Impact, you go beyond scanning to exploit and interact with vulnerable web applications just as an attacker could. Only Impact integrates web application testing with network, endpoint and wireless testing, enabling you to assess your organization's ability to detect, prevent and respond to real-world, multistaged threats.

## The Web Application Rapid Penetration Test

The CORE Impact Web Application Rapid Penetration Test (RPT) automates and speeds the web application testing process for more frequent, repeatable and consistent security assessments.

### Information Gathering and Scan Import

- Crawl web pages and identify URLs to test
- Import results from web application vulnerability scanners including Acunetix<sup>®</sup> Web Security Scanner, HP WebInspect<sup>®</sup>, IBM Rational AppScan<sup>®</sup>, and NTOSpider<sup>®</sup>
- Filter scan results and identify significant points of exposure
- Fingerprint applications to select known exploits for off-the-shelf web applications
- Gather information for dynamically creating exploits for custom applications
- Impersonate authenticated users + several desktop and mobile browsers

### Attack and Penetration: Address All OWASP Top 10 Threats

#### SQL Injection - Traditional and Blind (OWASP A1)

SQL Injection attacks inject SQL commands into web application databases through web forms, page parameters and cookie fields. CORE Impact safely identifies both traditional and blind SQL injection vulnerabilities and then leverages the results to dynamically create and inject SQL queries in an attempt to retrieve output from the SQL database.

#### OS Command Injection (OWASP A1)

If a web application utilizes user-input variables in system-level commands, Impact can attempt to change those variables in a way that causes the system to download an Impact Agent, giving the security tester control over the system.

#### Cross-Site Scripting (OWASP A2)

Cross-Site Scripting (XSS) threats take advantage of vulnerabilities in web applications and allow attackers to interact with end users' browsers. Impact identifies and confirms the exploitability of GET- and POST-based XSS vulnerabilities, including:

- URL-based, reflective XSS vulnerabilities
- Persistent (or stored) XSS vulnerabilities
- XSS vulnerabilities in dynamic Adobe Flash objects

The window for interacting with systems exploited by XSS can be brief, so Impact allows testers to queue information gathering modules to run automatically upon a successful compromise.

### Key Capabilities

- Identify weaknesses in web applications, web servers and associated databases
- Dynamically generate exploits that can compromise security weaknesses
- Demonstrate the potential consequences of a breach
- Gather information necessary for addressing security issues and preventing data incidents

### Web Application Scanner Integration and Validation

CORE Impact integrates with web application scanners including IBM Rational AppScan<sup>®</sup>, HP WebInspect<sup>®</sup>, and NTOSpider<sup>®</sup> to filter scan results and identify significant points of exposure.

- Prove the exploitability of application vulnerabilities to inform remediation efforts and minimize coding expenditures
- Gain administrative access on web servers, leveraging them as beachheads for attacks against backend network systems
- Identify URLs to test by importing scan results or by using Impact's page crawling and profiling capabilities

## Dynamic Exploits for Custom Web Applications

Testing custom applications for security vulnerabilities requires the creation of unique exploits. Impact dynamically creates customized exploits on-the-fly to safely replicate attacks against both proprietary and out-of-the-box web applications.

## Other Web Application Testing Capabilities

In addition to addressing the OWASP Top 10, Impact enables you to:

- Test PHP applications against Remote and Local File Inclusion
- Exploit WebDAV configuration weaknesses
- Evade firewalls
- Reveal weak HTTPS encryption

## Next Steps

CORE Impact Pro also allows you to test the security of your network systems, endpoint systems, mobile devices and wireless networks. Learn more by contacting us today to schedule a demonstration:

Phone: (617) 399-6980

Email: [info@coresecurity.com](mailto:info@coresecurity.com)

## Broken Authentication and Session Management (OWASP A3)

The Impact Authentication Testing Module guesses usernames and passwords for target applications.

## Insecure Direct Object References (OWASP A4)

- Hidden Pages Identification: Check for unlinked administration and configuration pages
- Backup / Old Pages Identification: Identify old versions & backups left on the web server
- Retrieve and Follow Robots.txt Files: Search for admin pages and other sensitive URLs

## Cross-Site Request Forgery (OWASP A5)

Impact can identify CSRF weaknesses and replicate attacks to demonstrate exploitability.

## Security Misconfiguration (OWASP A6)

A truly secure web application depends on secure configuration across the application, framework, web server, application server, and platform layers. Impact's multi-vector testing capabilities test not only the application, but also the underlying server and its environment.

## Insecure Cryptographic Storage (OWASP A7)

Upon accessing a SQL database via SQL Injection, testers can leverage the Impact's Get Sensitive Data module to identify unencrypted data stored in the database. This module can identify credit card and social security numbers, email addresses, and custom data types.

## Failure to Restrict URL Access (OWASP A8)

Impact Pro determines whether attackers can access admin pages, as well as backup and old pages, via both authenticated and unauthenticated sessions.

## Insufficient Transport Layer Protection (OWASP A9)

The Impact SSL Strength Module flags weak levels of encryption in HTTPS-secured sites.

## Unvalidated redirects and forwards (OWASP A10)

Through its web crawling and analysis capabilities, Impact can identify applications that redirect and forward without proper validation. Testers can then use Impact to demonstrate how an attacker could leverage the vulnerability to redirect victims to malicious sites.

## Cleanup and Reporting

Impact Pro is self-contained and safe for production systems, since it does not install or run code on compromised web servers during testing. Impact's reports provide security professionals and developers with critical information for identifying security weaknesses, determining possible fixes, and prioritizing remediation efforts. Impact maintains audit trails of all tests performed, servers and databases accessed, and all actions taken during testing.