

Get Clear Answers About Your Web Application Security

Identify and prove OWASP Top 10 vulnerabilities in your environment

Web applications are frequent targets for outside threats, so proactive security assessments are crucial. However, traditional assessments such as vulnerability scans can deliver a flood of data without definitive answers about where and how applications can be breached. Reworking code can be expensive and time consuming, so there shouldn't be any room for ambiguity in your application security testing initiatives.

Core WebVerify™ allows you to see your web applications as an attacker would, providing indisputable intelligence on their ability to withstand real-world threats. By safely replicating attacks that target OWASP Top 10 vulnerabilities and other weaknesses, WebVerify pinpoints exposures and provides clear, actionable information for prioritizing and remediating exposures with speed and efficiency.

WebVerify can also validate the security of associated databases, web servers, backend network systems, and end users against subsequent attacks. The result is a more holistic assessment of your web application security as it relates to the rest of your business.

IT Security Professionals and Consultants

Regularly identify, profile and validate the security of live web applications in an automated, repeatable way.

- Crawl sites and applications to find and profile targets
- Import and filter results from web vulnerability scanners
- Determine exploitability with no false positives
- Identify attack paths that could lead to network breaches
- Validate security controls for PCI, FISMA and other regulations
- Schedule tests to run at specific times or planned intervals

Web Developers and QA Professionals

Quickly test applications throughout the development life cycle and gain actionable information for remediating exposures.

- Test customized applications with dynamic, targeted attacks
- Verify security before going live and as updates are applied
- Get remediation information necessary for addressing security issues quickly and efficiently
- Detail exposures and share progress with targeted reports
- Rely on proven testing capabilities developed and honed by Core Security for over a decade

Go Beyond Scanning to Pinpoint and Demonstrate Real Risks

WebVerify enables you to pinpoint, demonstrate and confirm web application exposures with confidence and clarity.

- Identify and prove the exploitability of all OWASP Top 10 web application vulnerabilities (see reverse)
- Eliminate false positives and ensure that development resources are focused on fixing actual exposures
- Reveal the implications of a vulnerability by demonstrating how an attacker could steal and manipulate data
- Validate cross-site scripting (XSS) exposures by crafting and emailing URLs that exploit XSS vulnerabilities
- Detect sensitive data exposed by vulnerabilities, such as email addresses, credit card numbers, and social security numbers
- Gain information about available patches and other necessary security updates for out-of-the-box applications
- Reveal exploitable OS, services and application weaknesses in underlying web servers
- Determine if an attacker could gain administrative privileges on the web server via local privilege escalation techniques
- Conduct application penetration tests as mandated by PCI DSS Requirement 11.3
- Validate that FISMA-mandated security measures are in-place and working effectively

Web Application Vulnerability Coverage

OWASP Top 10 Vulnerabilities	WebVerify Testing Capabilities
A1. SQL Injection	<ul style="list-style-type: none"> • Safely identify both traditional and blind SQL injection vulnerabilities • Dynamically create and inject SQL queries in an attempt to access the database • Interact with the compromised database
A1. OS Command Injection	<ul style="list-style-type: none"> • Detect and exploit OS Command Injection weaknesses in web applications • Reveal the implications of a breach by taking control of the web server
A2. Cross-Site Scripting (XSS)	Identify and exploit GET- and POST-based XSS vulnerabilities, including: <ul style="list-style-type: none"> • URL-based, reflective XSS • Persistent (or stored) XSS • XSS in dynamic Adobe Flash objects
A3. Broken Authentication and Session Mgt.	Guess usernames and passwords.
A4. Insecure Direct Object References	Identify, search and follow hidden pages, backup/old pages, and robots.txt files.
A5. Cross-Site Request Forgery (CSRF)	<ul style="list-style-type: none"> • Identify CSRF weaknesses in web applications • Replicate CSRF attacks to demonstrate exploitability
A6. Security Misconfiguration	Leverage multi-vector testing to identify security misconfiguration issues across: <ul style="list-style-type: none"> • Web applications • Web servers • Backend network environments
A7. Insecure Cryptographic Storage	<ul style="list-style-type: none"> • Identify unencrypted data upon successfully accessing a SQL database • Identify exposed credit card numbers, social security numbers and email addresses • Define custom searches for other types of sensitive data
A8. Failure to Restrict URL Access	Access admin, backup and old pages via authenticated and unauthenticated sessions.
A9. Insufficient Transport Layer Protection	Flag weak encryption in HTTPS-secured sites.
A10. Unvalidated Redirects and Forwards	<ul style="list-style-type: none"> • Identify applications that redirect and forward without proper validation • Demonstrate how an attacker could redirect victims to malicious sites
Other Vulnerabilities	
Remote and Local File Inclusion for PHP	Manipulate PHP templates in an attempt to retrieve commands from the web server.
WebDAV Configuration Weaknesses	Detect and exploit poorly configured WebDAV implementations.

Core Security

+1 (617) 399-6980
 info@coresecurity.com

www.coresecurity.com
 blog.coresecurity.com
 www.twitter.com/coresecurity
 www.facebook.com/coresecurity

Next Steps ...

Contact us at +1 (617) 399-6980 or info@coresecurity.com to see a demonstration of Core WebVerify, and learn how it can help you improve your organization's security posture.