Web Application Pentesting

Get your vulnerabilities identified on-demand

OVERVIEW

Web applications are being churned out faster than security teams can test them. CSW gets ahead of the race, protecting not just your websites but all your applications from attack. CSW's Web Application Penetration Testing focuses on evaluating your web applications for OWASP Top 10 and SANS Top 25 programming errors, and any other security related weakness. We also look for open-source vulnerabilities.

Our process comprises four main steps:

- Information gathering
- Research and analysis of findings
- Exploitation
- Reporting with ongoing support

The testing process is comprehensive and enables faster remediation.

THE CHALLENGE

Attackers are targeting critical assets around the world. To stay safe, organizations need to assess their defenses continuously to understand inherent vulnerabilities and weaknesses that could attract attackers. The challenge here is that most organizations fail to understand an attacker's mindset and attack chaining capabilities.

OUR APPROACH

Identify vulnerabilities and misconfigurations

Verify the efficiency of security controls such as web application firewalls (WAF)

Determine the most vulnerable path for an attack

KEY PRODUCT CAPABILITIES

SYNCHRONOUS REPORTING

We provide results within hours of commencing the assessment.

STANDARDS

Findings align to OWASP Mobile Top 10, OWASP Top 10, and SANS Top 25.

EXPERT PENTESTERS

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

TRANSPARENT PROCESS

Our process simulates an adversary's attack.

ON-DEMAND RETESTS

We provide retesting if required.

RBVM PLATFORM

We deliver our results through an award-winning risk-based vulnerability management **(RBVM)** platform.

KEY BENEFITS

COMPLETE COVERAGE

We test using all user roles and back-end APIs. We provide end to end coverage.

FLEXIBILITY

On-demand pentesting based on business requirements.

ASSURANCE

We replicate an adversary's intent in order to identify the maximum impact of vulnerabilities.

ACTIONABLE INSIGHTS

We provide a prioritized list of vulnerabilities on what to fix first.

WE DO MORE THAN SCANNING

We manually test and verify the findings for completeness.

SUPPORT

Comprehensive remediation guide and support.

LUCID PROCESS

Our process is transparent right from kick-off to remediation.

Web Application Pentesting

Get your vulnerabilities identified on-demand

OUR APPROACH

CSW identifies security vulnerabilities in a web application by testing the application from an attacker's perspective.

Reconnaissance	• Fingerprint the web application • Probe web applications using automated web crawling or spidering
Attack Surface Enumeration	• Identify all paths of user-controlled data • Track how the application uses data
Automated Vulnerability Scanning	• Conduct a high-level test for potential vulnerabilities • Scan for OWASP Top 10 vulnerabilities and SANS Top 25 programming errors • Scan single page, multi-page, and AJAX-based applications
Manual Penetration Testing	• Manually detect authorization issues and logical flaws • Eliminate false positives through inherent manual testing
Reporting	• Map vulnerabilities (CVEs) and weaknesses (CWEs) to severity ratings • Prioritize critical issues and recommend order of remediation

WHAT TO EXPECT IN OUR REPORT?

Our reports contain detailed findings of vulnerabilities mapped against OWASP and SANS security standards and use cases.

- Methodology used
- Scope and implemented test plan
- Categorization of vulnerabilities based on severity ratings using VRR and CVSS3
- Mapped findings
- Detailed proof-of-concept
- Remediation guidance

ATTACK SURFACES WE FOCUS ON

Web | Mobile | Applications | Cloud

Reach out to us to reduce risk and exposure.

To schedule a consultation write to info@cybersecurityworks.com

Cyber Security Works | info@cybersecurityworks.com | www.cybersecurityworks.com

Follow us at Linkedin | Twitter | Facebook | Instagram