InfoSight®
www.infosightinc.com

INFOSIGHT'S WEB APPLICATION TESTING

305-828-1003 info@infosightinc.com

Web application server penetration testing reveals vulnerabilities that expose organizations to cyber risks that traditional firewalls and IDS networks aren't designed to protect against.

InfoSight's Web Application Server Penetration Testing provides the most complete and effective suite for web security assessments checks to enhance the overall security of your Web Applications against a wide range of vulnerabilities and sophisticated attack vectors.

InfoSight's suite of services allows for assessment of Web Applications during different phases of the application develop life cycle.

Security Checks Include

- ✓ SQL / Code Injection
- ✓ File & Directory Analysis Web Server Vulnerabilities
- ✓ 3rd Party Package Vulnerabilities
- ✓ Server Side Template Injection Cross-Site Scripting
- ✓ OWASP Top 10
- ✓ Parameter Tampering

After testing is complete, Digital reports are delivered via our proprietary **Mitigator Vulnerability and Threat Management Platform.** Reports can be exported in multiple formats and printed.

MITIGATOR™
VULNERABILITY & THREAT MANAGER

Our Methodology

Design & Develop – plays an important role in building strong applications. We'll assess your run time environment and check for security flaws introduced during coding.

Test & Implement – one of the most important functions in the SDLC. It allows us to verify if security controls and requirements are fulfilled correctly before implementing and promoting applications to production-level. We employ a broad security assessment of your application before hitting production.

Maintain & Check – continuous and periodic security assessments are required in several different industry regulations and is also a key function in your SDLC. Making sure that changes to your web application will not break its security maturity level is important to manage vulnerabilities and security risks.

Bringing the Future into Focus

www.infosightinc.com

InfoSight®
www.infosightinc.com

INFOSIGHT'S WEB APPLICATION TESTING

Other Assessments

Vulnerability & Penetration Testing

Consists of a multi-disciplinary, multi-faceted review of the organization's systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.

Red Team/ Blue Team Testing

Designed to test an organization's readiness to detect, withstand and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches.

Web & Mobile Security & API

Involves the security testing of web, mobile and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

InfoSight's Security Tests Include:

Custom Design Errors

- Cross-site Script Injection Module
- Database Tampering -SQL Injection Module
- Buffer & Integer Overflow Attach Module
- Format String attack Module
- File & Directories Tampering Module
- Parameter Tampering Module

Web Server Exposure

- Web Server Infrastructure Analysis Module
- HTTP Fingerprint Module

File & Directory Exposure Checks

- Search for Backup Files
- Search for Information Leakage Files
- Search for Configuration Files
- Search for Password Files

Web Signature Attacks

- Web Attack Signatures Module including:
- Attack template

Confidentiality Exposure Checks

- Look for Web forms vulnerabilities
- Compliance Analysis

Cookie Exposure Checks

- Find Weakness in Cookie Information
- Find Cookies Sent Without Encryption
- Find Information Leakage in Cookie Information
- Find Cookies Vulnerable to Malicious Client-Side Script