InfoSight®
Bringing the Future into Focus®

305-828-1003
info@infosightinc.com
www.infosightinc.com

InfoSight's Web Application Testing

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 hacker attacks.

InfoSight's suite of services allows for assessment of Web Applications under different perspectives of system develop life cycle phases including:

1. **Development Phase**
2. **Deployment Phase**
3. **Production Phase**

Our Methodology

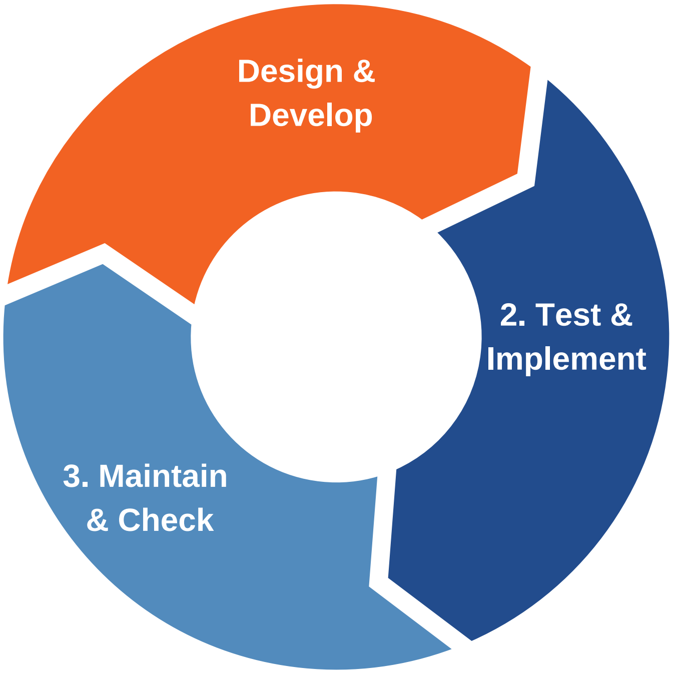
1.Design & Develop – plays an important role in building strong applications. We'll assess your run time environment and check for security flaws introduced during coding.

2. 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.

3. 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.

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



Following all assessments and checks your team will receive 2 reports: an Executive Report and a Technical Report.

InfoSight's Web Application Testing

InfoSight's Security Tests Include:

Custom Design Errors

- Cross-site Script Injection Module
- Database Tampering -SQL Injection Module including:
  - o Direct mode
  - o Blind mode
- Buffer & Integer Overflow Attach Module
- Format String attack Module
- File & Directories Tampering Module including:
  - o Backup Files Discovery
  - o Configuration Files Discovery
  - o Password Files Discovery
  - o Information Leakage Discovery
- Parameter Tampering Module including:
  - o Special Parameter Addition attacks
  - o Boolean Parameter Tampering attacks
  - o Hidden Parameter Discovery
  - o Parameter Deletion attacks
  - o Remote Execution attacks
  - o File & Directory traversal attacks
  - o Header Splitting & CRLF Injection attacks
  - o Remote File Include PHP-based attacks

Web Server Exposure

- Web Server Infrastructure Analysis Module including:
  - o Web Server & Platform version vulnerabilities
  - o SSL encryption and X.509 certificate vulnerabilities
  - o HTTP Method Discovery Module
- HTTP Fingerprint Module, including:
  - o Web Server Fingerprint Module
  - o Web Server technology Discovery Module
  - o Directory Brute-Force
  - o HTTP Protocol vulnerabilities

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:
  - o IIS CGI Decode Test
  - o IIS Extended Unicode Test
  - o IIS File Parsing Test
  - o FrontPage Security Test
  - o Lotus Domino Security Test
  - o General CGI Security Test
  - o HTTP Devices Security Test (routers, switches)
  - o Windows-based CGI Security Test
  - o PHP Web Application Security Test
  - o AP Web Application Security Test
  - o J2EE Web Application Security Test
  - o ColdFusion Web Application Security Test
- Attack template such as:
  - o Complete
  - o SANS/FBI Top 10
  - o Top20

Confidentiality Exposure Checks

- Look for Web forms vulnerabilities including:
  - o Password Cache Features
  - o Insecure Method of Sending Data
  - o Lack of Encryption for Sensitive Data
  - o Insecure Location to Send Data (Leakage)
  - o Find Directory Listing
  - o Find Available Objects to Download
  - o Find Meta-Tag Leakage
  - o Find Sensitive Keywords in Comments and Scripts
- Compliance Analysis including:
  - o Find Copyright Statements
  - o Find Content Rating Statements
  - o Find Custom Content on Web Pages and Forms

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