InfoSight®
www.infosightinc.com

WEB APPLICATION TESTING

305-828-1003 info@infosightinc.com

Overview

Web Application 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 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 development life cycle.

The Challenge

Web Applications are very common today, however so are their vulnerabilities. There are many reasons these applications are so insecure. First, many have inadequate Authentication and Authorization which can lead to unauthorized access to sensitive data or functionality. They often have Insecure Dependencies that rely on third-party plugins and open-source code. Additionally, sometimes they lack Encryption so data can be intercepted and stolen. They can also have File Upload Vulnerabilities, allowing users to upload files without proper validation and controls which can lead to malware injection. And of course, there's always the Zero Day, so assessing security routinely is wise.

Our Methodology

We take all these insecurities into consideration and help you to better:

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.

The Outcome

To mitigate these security risks, we assist web developers and organizations to follow security best practices, conduct regular security assessments and audits, stay updated on emerging threats, and implement security measures that make your application more secure. Web Application Security is an ongoing process that requires vigilance and continuous improvement.

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

Other Assesments

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.