Web Application Test Results

Kaneshia Lovick

Security Analyst

Overview

Web application testing is a key component to insure the quality of a product and the functionality of a product, prior to it's release.

Our web application assessment of our toll road client demonstrated 5 key risks of vulnerabilities.

Vulnerabilities, their risks and remediation suggestions will be outlined in this presentation as per guideline of the OWASP top ten standards https://owasp.org/Top10/

Results:

The results of the web application scan, found five critical vulnerabilities in which we must remediate to prevent malfunction or attacks of the software.

A. Cross-site scripting(XSS)
B. Cross-site request forgery(CSRF)
C. SQL Injection
D. Sensitive Data Exposure
E. Insufficient Logging and Monitoring.

Cross-Site Scripting (XSS)

Risks Posed-Stealing of credentials,sessions or delivery of malware to customers.

Severity-High. Second most common attack. Can turn application into a malicious one,causing serious harm to customers and reputation of application owner.

Remediation

A. Scan and patch vulnerability.
B. Set up a process of filtering out code input on application
C. Websites and server software.(update PHP, Linux, Apache)

Cross-Site Request Forgery (CSRF)

Risks Posed- A CSRF attack can damage client relationship,data theft and unauthorized funds transfer.

Severity-High due to attack limited to functionality of web application and attacker does not receive HTTP, therefore can not read or access sensitive information.

Remediation

A. Ensure web browsers are updated, that supports same site cookies.
B. Disable access of browsers that do not support, samesite cookies,

SQL Injection

Risks posed-Unauthorized access to user lists and gaining administration rights. Entire system can be compromised,

Severity-High.Can cause a complete system takeover, gaining access to credit card information,customer addresses and other attacks such as ransomware.

Remediation

A. Minimize privileges to all database accounts.
B. Parameterized queries or stored procedures.
C. Check security advisories for updates and update to non vulnerable version.

Sensitive Data Exposure

Risks posed-Application exposes data of customers such as social security numbers. Financial info and login info.

Severity-High. Hackers can easily access data and legal implications of company.

Remediation

A.Encrypt data

B. Implement data loss prevention software.

C. Security awareness training of users.

Insufficient Logging and Monitoring

Risks posed-Attackers are free to access system on several occasions. Attackers can have access to system, without anyone noticing.

Severity-High. Attackers can pivot to more systems. Tamper, attack or destroy data.

Remediation

A. Security awareness and training of staff.
B. Set up logging and monitoring system. Decide what should or should not be recorded in the logs(Access tokens/Authentication passwords.
C. Document failed and success login attempts.