Web Security Testing

Scope of Work

Objectives

ITPSS Penetration Testing team shall assess the Website by conducting a 'Web Security Testing'.

- Discover the security risks within the application and front-end server
- Assess the impact of each vulnerability or weakness
- Prioritize risks and provide recommendations to mitigate risks

Scope

- Conduct Web Security Testing to the Website and provide the findings
- Identify security vulnerabilities on both web application and front-end web server
- Test the application based from two perspective – Non-authenticated and authenticated
- Generate reports based on findings and provide security recommendations. The report will consist of risk values for management section and technical details information for technical section.

Requirements

- Work area for Internal Test (accommodate up to 5 people). If testing needs to be done in the customer's premise. If test can be done externally, we will only need our IP Address to be whitelisted from any Security Devices. The IP Address to be whitelisted will be provided in our Authorised form once the engagement is confirmed via a Purchase Order.
- For Internal Test, ***wired*** network connectivity is generally preferred for laptops to connect onto the target network.
- Test accounts for target web application

Methodology

ITPSS Penetration Testing team utilizes a standards based approach from Open Web Application Security Project Top 10 - 2021 (OWASP Top 10):

- **A1:2021** Broken Access Control
- **A2:2021** Cryptographic Failures
- **A3:2021** Injections
- **A4:2021** Insecure Design
- **A5:2021** Broken Access Control
- **A6:2021** Vulnerable and Outdated Components
- **A7:2021** Identification and Authentication Failures
- **A8:2021** Software and Data Integrity Failures
- **A9:2021** Security Logging and Monitoring Failures
- **A10:2021** Server-Side Request Forgery (SSRF)

Testing timeline

6 Business Days per website (exclude Saturdays, Sundays and Public Holidays). If assessments are done concurrently 2 days per website will be added.

Scanning and Profiling • TCP/UDP Port Scanning • Dynamic Content Scanning • HTTP Fingerprinting • Services Identification • Authentication Method • System Identification • Operating System Identification • Patch or Version level • System Enumeration • Vulnerability Scanning	**2 days**
Automated Testing • Web Spidering • Vulnerability Identification • Hidden content	**1 day**
Security Misconfiguration • Sensitive Data Exposure • Using Known Vulnerable Components • Insecure Direct Object References • Default settings • Out of date applications	**1 day**
Manual Testing (Phase 1) • Database verification (MySQL, MSSQL, Oracle, etc) • Vulnerability Verification • List of vulnerabilities minus false positives • SQL, XPATH, LDAP Injection • Error, Union based and Blind SQL Injection • Cross-site scripting • Cross-site request forgery • SSL Cipher Testing	**1 day**
Manual Testing (Phase 2) • Testing privileges (Write access, Database manipulation) • Command Injection, Local/Remote File include • System Browsing • Password Dump • Broken Authentication and Session Management • Server side security checks	**1 day**

Note: The report will be done by the next following week after the last assessment day.

Checklist

Checklist preparation prior Web Security Testing:

- Systems to be tested must be operational and accessible through TCP/IP network
- New systems are to be fully functional (installed modules, plugins, etc) and recommended to undergo UAT prior to performing security assessment (Web Security Testing)
- Perform and verify system backup
- Provide user test accounts for testing the application.