Lodestone

SERVICE BRIEF FOR
WEB APPLICATION PENETRATION TESTING

Lodestone's Web Application Penetration Testing (WAPT) analyzes the critical components of your company's web applications, examining everything down to open-source components and plugins. While convenient and useful, applications and websites present the danger of having vulnerabilities that your company can inherit and threat actors can exploit.

Our experts test everything from web-based portals, application programming interfaces (APIs), and web services. We thoroughly map business logic and web application data flow to validate your company's web-related resources to ensure that you enjoy these tools' benefits while minimizing their dangers.

Lodestone's WAPT analyzes the critical components of a web-based portal, APIs, and web services. Unlike traditional security assessments that focus only on automated scanners, Lodestone engineers thoroughly map the business logic and web application data flow, including a deep inspection to identify business-critical logic vulnerabilities. This combination of automated and manual testing ensures a thorough validation of your web applications. Our assessments integrate detailed vulnerability and countermeasure information for authentication, authorization, session management, data integrity, confidentiality, and privacy concerns. Our experts identify potential security weaknesses in your environment and report our findings and recommendations to strengthen your company against would-be attackers.

BENEFITS

- Identifying and mitigating known security exposures and web application flaws before threat actors can find them to ensure that your web applications are more protected. Reduce your chances of becoming a victim of a cyberattack while satisfying compliance requirements from industry standards like the Health Information Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS).
- Identifying vulnerable routes through your infrastructure to pinpoint loopholes in your web applications that may leave sensitive data open to attack. Gain an understanding of web-related resources that strengthens your security policies by highlighting areas that need improvement.
- Keeping untrusted data separate from commands and queries and support in the development of strong authentication and session management controls.
- Improving access control and preventing threat actors from infiltrating systems, hence avoiding costly Data Breaches and Loss of Business Operability.

METHODOLOGY

Lodestone WAPT identifies weaknesses and flaws that may be present in your websites and web application. It provides direction for reducing associated risk to better understand assets, vulnerabilities, severity, and overall risk.

WAPT is comprised of these primary phases:

- Initial Assessment - We work with you to understand your organization's unique blend of web applications and the number of API endpoints that need testing. This collaborative enables us to map out your web applications and their purposes to prepare for and prioritize testing and optimize the order in which we test.

- Open-Source Intelligence - Lodestone will gather open-source intelligence (OSINT) about web applications using automated tools and manual research. Reconnaissance is the first step in any assessment that is also taken by threat actors seeking to exploit the security of a network or application.

- Manual Enumeration of Files and Directories - Lodestone engineers will test common threat actor strategies such as the directory enumeration attack, in which each directory name from a dictionary file of a popular directory name is requested. For each request, threat actors note the HTTP response code, checking for a status of 200, and apply the same technique to enumerate the files in your environment. We use a similar methodology without the risk to your environment and critical data to help you defend your company against these attacker strategies.

- Vulnerability Scanning - We deploy automated vulnerability scanning tools and manual testing to discover any vulnerabilities in your web applications. Lodestone web application vulnerability scans use blackbox testing, which does not require access to the source code to test for security vulnerabilities. These scans can also satisfy certain maintenance requirements for your organization if it is subject to regulations like HIPAA or the General Data Protection Regulation (GDPR).

- OWASP Top 10 Testing - The Open Web Application Security Project (OWASP) Top 10 list details the most common web application security risks. We assess each flaw class using the OWASP Risk Rating methodology and provide guidelines, examples, best practices for preventing attacks, and references for each risk. Our engineers perform this critical step to support your organization's efforts toward changing the software development culture within your organization into one that produces more secure code. *

- Reporting - Reports are a crucial step in any penetration testing engagement as the cornerstone deliverable that provides meaningful insights regarding your organization's security posture, along with recommendations to remediate each detected risk. Our experts share their approach to protecting web applications from advanced cyber-attacks. **

- Report Review - We provide our clients at least two weeks to review the reports and formulate any questions or requests for clarification. At the end of every engagement, a report review call is scheduled to ensure that all of your concerns are addressed.

*** THE FOLLOWING CATEGORIES ARE TESTED:**

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

**** OUR REPORTS INCLUDE PERTINENT DETAILS THAT CAN BE USED TO RESPOND TO IDENTIFIED WEB APPLICATION FLAWS AND VULNERABILITIES, INCLUDING:**

- Vulnerability discovered
- Executive summary for the management board
- Detailed Technical report regarding the findings
- Prioritized risk-based reporting
- Common Vulnerabilities and Exposures (CVE) database reference and score
- Detailed steps to correct the vulnerability

INFORMATION GATHERED:

The following information may be gathered by our team as part of the WAPT:

- Web applications and URLs tested
- Web application login credentials

DURATION AND DELIVERABLES

The WAPT varies in duration based on the size of your environment, the number of systems, and findings, but typically takes two to three weeks. It can be delivered on-premises or remotely.

Lodestone will provide the following deliverables to you as part of the engagement:

- Weekly Status Reporting – Lodestone will provide a weekly or bi-weekly status report to the project sponsor once the kickoff call is complete. Lodestone can accommodate your preferred communications, including via phone call or email.
- Executive Summary Report – Lodestone will provide a high-level report on the engagement, findings, and any applicable recommendations.
- Final Report – After the engagement completion, Lodestone will provide a final report detailing the engagement, findings, and recommendations for mitigating the findings.

Connect with us:
www.lodestone.com
320 East Main Street, Lewisville, TX 75057, USA
Tel: +1-203-307-4984
info@lodestone.com

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection.