VAPT Testing of an E-commerce Website

Client Overview

- Leading fashion and lifestyle retailer with a large portfolio of brands

Business Requirements

- Build a secure e-commerce website and drive secure sales online
- Ensure that the web portal is safe for customer interactions and sharing personal information
- Verify website susceptibility to technical / design flaws that may invite hackers or unethical transactions
- Perform static source code review to achieve security standards

Our Solutions

- Performed vulnerability scanning using Open Source Tools across Website pages and across categories based on OWASP standards
- Functional mapping of the website pages with URLs and inclusive parameters
- Special case testing for Tampering Attacks in the payment workflow
- Data Validations for the order fulfillment and payment workflows
- Performed Vulnerability Assessments for all web pages for security misconfigurations
- Domain based testing for Privilege escalations – testing for unauthorized access to premium accounts using session logs and IDs
- Performed search overflow attacks covering the vulnerabilities against server interruptions and app responsiveness
- Verified for Injection attacks – injection of technology based scripts / files in URLs and search fields
- Performed Penetration Tests using proxy techniques to manipulate parameter values / tamper operational data
- Conducted Static source code review to achieve Security Standards

QA Process

- Created Test Cases based on ecommerce workflows such as login, user account management, order management, checkout etc. and mapped functionality / security scope
- Test Deliverables : Test Strategy, Vulnerability Assessment report with observations and detailed remediation
- Reports with identified vulnerability, details and description with reproduced screenshots / video, impact, affected files and web pages, affected code, remediation measures and code replacement / vulnerability fixes

Engagement

- 1 Test Engineer
  1 Test Lead
  4 Weeks for Security Testing and Regression / Retests

Tools

- OWASP ZAP, IronWASP, Burpsuite, Wireshark, Vega, Kali Linux Tools, Tamper Data, SonarQube, PHP RIPS

Business Impact

- Security Testing conforming to OWASP Top 10 and domain based vulnerabilities
- Tested through maximum number of tools to reproduce an issue and avoid false positives in the security bug report
- Minimized security risks with recommended solutions and proven methods to augment security of the application
- 100% Test coverage for all functionality

INDIA
Chennai
+91 44 6606 9100

Bengaluru
+91 80 4645 7777

Mumbai
+91 022 6215 4028

USA
Cupertino | Princeton
Toll-free: 1 888 207 5969

SINGAPORE
+65 9630 7959

UK
London
+44 773 653 9098

General Inquiries: info@indiumsoftware.com | Sales Inquiries: sales@indiumsoftware.com