In today’s ever changing world, it is quite a challenge to keep business applications, mobile, IT infrastructure etc. free of vulnerabilities. The Vulnerability and Penetration Testing Services (VAPT) from Indium Software helps mitigate risks thereby minimizing any disruption to business delivery. The team at Indium Software works with its customers, understanding the business risks with respect to security and conducts customized assessment recommend customized solutions that suit their business needs.
Indium’s Security Testing Framework


**Input**
- Security requirements and acceptability criteria
- Security test plan
- Security test scenarios and test cases
- Stable application
- Security test infrastructure
- Security test data
- Security Test Strategy

**Process**
- Perform security test execution
- Manual penetration testing
- Automated application scanning
- Perform code review and analysis
- Log defects
- Initiate remediation of defects and complete retesting

**Output**
- Acceptability criteria accomplished
- Relevant OWASP vulnerabilities scanned and analyzed
- All high priority / severity defects fixed, retested and closed
- Test summary report published
- Defect analysis and root cause analysis completed
- Remedial recommendations

**Services we offer**
- Web Application Security Testing (DAST)
- Mobile Application Security Testing
- API Security Testing
- Source Code Review (SAST)
- Game Security Testing
- Network Vulnerable Assessment
- Threat Modeling
Benefits of Our Approach

- Provides a detailed security assessment report which covers the vulnerabilities and remediation plan
- Minimizing the false positives and providing a quality output
- VAPT executed according to various industry compliances

The Indium Advantage

- Certified and highly skilled experts are involved in the testing process
- Automated tools and manual processes are used to find the loopholes and minimize business

Tool Expertise

<table>
<thead>
<tr>
<th>Open Source</th>
<th>Mobile Security</th>
<th>Commercial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireshark</td>
<td>Android Bug Framework</td>
<td>AppScan IBM Xforce</td>
</tr>
<tr>
<td>w3af</td>
<td>APK Inspector</td>
<td>Acunetix</td>
</tr>
<tr>
<td>IronWASP</td>
<td>Frida</td>
<td>Nessus</td>
</tr>
<tr>
<td>Burp Suite</td>
<td>OpenVAS</td>
<td>Fortify</td>
</tr>
<tr>
<td>OpenVas</td>
<td></td>
<td>Rapid7</td>
</tr>
</tbody>
</table>

Use Cases

- Conducted vulnerability assessment on Network Load Balancing Servers and identified various critical vulnerabilities based on CVSS standard.
- Performed OWASP based VAPT on E-commerce application and found domain-based security vulnerabilities.
- Performed Penetration Testing on Data science application and found phishing attack which could have lead to major impact of the user data.
- Performed Reverse Engineering Techniques on mobile application and found major vulnerabilities related to code quality, data storage and security.

Visit our website: www.indiumsoftware.com
Write to us: sales@indiumsoftware.com
© Indium Software