Web Application Penetration Testing

Decoding VAPT

The vulnerability assessment process involves the use of vulnerability assessment tools that identify vulnerabilities in your organization’s IT assets, which have the potential to be exploited by attackers. These are systemic flaws that can leave your organization exposed to both known and unknown threats such as ransomware and more.

What is VAPT?

VAPT stands for Vulnerability Assessment and Penetration Testing (VAPT) and the acronym contains two types of testing approaches, which together offer a comprehensive vulnerability evaluation. The VAPT process includes automated vulnerability assessment, human-centric penetration testing and in certain complex scenarios, also involved red team operations.

Penetration testing is used to identify the extent of weaknesses and their severity. The job of a penetration test is to find flaws and show you how damaging it could be if it is exploited by a real attacker.

Together, both Vulnerability Assessment and Penetration Testing offer a drill down view of the various flaws across different systems and their potential to put your organization’s cybersecurity at risk.

Necessity of VAPT

Cybercriminals are using strategies and tactics that are constantly evolving. In order to ensure your network remains safe at all times, it is imperative that it goes through periodic vulnerability assessment and testing.

Apart from delivering a 360° visibility into organizational security weaknesses and throwing light on the necessary security solution, VAPT also supports your need to meet compliances such as GDPR, PCI DSS and ISO 27001.

Our VAPT Services

VAPT is a collection of services that make your organization more secure by identifying and addressing vulnerabilities before cybercriminals can find them. Before an organization gets started on VAPT, it is imperative they have a better idea of the services that are a part of VAPT.

Vulnerability Assessment

The principal component of vulnerability assessment is vulnerability scanning; as the phrase suggests, it helps in identifying, classifying and addressing security weakness. It can also include offering solutions for risk mitigation.

Penetration Testing

Also called pen testing, this is a comprehensive vulnerability assessment that integrates human-led techniques with an advanced-tech enabled approach to test various layers of an organization’s security for vulnerabilities. This test is conducted across an organization’s infrastructure, systems and applications.

Types of pen testing:

- Network
- Web Application
- Mobile Application
- API
- IoT Device

Diverse VAPT Services

Reliable Security Assessment

Bolster the Security of your IT Assets:

- Web Application VAPT Service
- Mobile App VAPT Service
- Network VAPT Service
- API VAPT Service
- IOT VAPT Service
The use of internal and external web applications is becoming ubiquitous, which is making them a popular attack target. According to Verizon’s 2020 Data Breach Investigation Report, a quarter of breaches were a result of web application attacks. Stop threats at the door with world-class web application security testing services that use the most advanced security testing methods to identify and plug security holes in your web apps and websites.

**Decoding Web Application Security**

**Penetration Expertise that Digs Deep**

With SharkStriker’s web application penetration service, you can identify all kinds of vulnerabilities sitting on your web application. We use a combination of automated vulnerability assessment and advanced manual penetration testing methods to detect even the most well-hidden vulnerabilities in your app.

Our goal is to give you a 360° view of the vulnerabilities not only in the web application also the various elements that make up the app. These elements include backend networks, databases, source code, etc. Our web app VAPT services are not only limited to identifying these weaknesses but also include recognizing the severity of these vulnerabilities and prioritizing threat mitigation.

**Web App Threat Statistics**

**Key takeaways regarding web applications**

- Hackers can attack users in 9 out of 10 web applications. Attacks include redirecting users to a hacker-controlled resource, stealing credentials in phishing attacks and infecting computers with malware.
- Unauthorized access to applications is possible on 39% of sites. In 2019, full control of the system could be obtained on 16% of web applications. On 8% of systems, full control of the web application server allowed attacking the local network.
- Breaches of sensitive data were a threat in 68% of web applications. Most breachable data was of a personal nature (31% of breaches).

**Vulnerability Statistics**

- 82% of vulnerabilities were located in application code.
- The average number of vulnerabilities per web application fell by a third compared to 2018. On average, each system contained 22 vulnerabilities, of which 4 were of high severity.
- One out of five vulnerabilities has high severity.

**Web Application Vulnerability Coverage**

We conduct penetration for both proprietary apps and also those from third-party vendors, and our process is designed to identify the most critical web app security risks as underlined by OWASP and MITRE CVE/SANS.

**PCI DSS (6.5.1-6.5.10)**

The Prioritized Approach provides six security milestones that will help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance.

**The MITRE CVE/SANS Top 10**

MITRE has brought out a list that covers the Top 25 Most Dangerous Software Errors (CWE Top 25) that are extremely common, are widespread, and which if left unaddressed can result in serious vulnerabilities. This list was built keeping in mind the vulnerabilities published in the National Vulnerability Database:
Web Application Penetration Testing

- CWE-79 Cross-site Scripting
- CWE-787 Out-of-bounds Write
- CWE-20 Improper Input Validation
- CWE-125 Out-of-bounds Read
- CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer
- CWE-89 SQL Injection
- CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
- CWE-416 Use After Free
- CWE-352 Cross-Site Request Forgery (CSRF)
- CWE-78 OS Command Injection Your Content Goes Here
- CWE-190 Integer Overflow or Wraparound
- CWE-22 Path Traversal
- CWE-476 NULL Pointer Dereference
- CWE-732 Incorrect Permission Assignment for Critical Resource
- CWE-94 Code Injection
- CWE-522 Insufficiently Protected Credentials
- CWE-611 Improper Restriction of XML External Entity Reference
- CWE-798 Use of Hard-coded Credentials
- CWE-502 Deserialization of Untrusted Data
- CWE-269 Improper Privilege Management
- CWE-400 Uncontrolled Resource Consumption
- CWE-306 Missing Authentication for Critical Function
- CWE-862 Missing Authorization
- CWE-287 Improper Authentication
- CWE-434 Unrestricted Upload of File with Dangerous Type

Testing Methodology
SharkStriker subscribes to a complex, yet highly systematic process that conducts a thorough assessment of your organization’s web application security. We realize there are plenty of tools and products available on the market that can be used to perform quick, assembly-line tests. However, in the evolving threat scenario, organizations need custom VAPT solutions that can conduct penetration tests based on their specific use case to safeguard their web applications from the kind of specific threats they face.

Our focus is on helping you maintain a very high level of operations security (OPSEC) by designing cybersecurity services that offer security based on the kind of threats that your web applications will actually face. We use a blended approach which includes the following testing methodologies:

- OWASP Testing Guide
- NIST Guide to Information Security Testing and Assessment
- PCI-DSS Penetration Testing Guidance
- ISACA’s How to Audit GDPR

Proven Methodology and Global Standards
Testing Methodology
- OWASP Testing Guide
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- PCI DSS Information Supplement: Penetration Testing Guidance
- FedRAMP Penetration Test Guidance
- ISACA’s How to Audit GDPR

Reporting Standards
- Common Vulnerabilities and Exposures (CVE) Compatible
- Common Weakness Enumeration (CWE) Compatible
- Common Vulnerability Scoring System (CVSSv3)
<table>
<thead>
<tr>
<th>SCOPE</th>
<th>Essentials</th>
<th>Professional</th>
<th>Enterprise</th>
<th>Ultimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-credentialed scan</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Credentialed scan</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Automated Penetration Testing</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Manual Penetration Testing by Experts</td>
<td>1 expert</td>
<td>2 expert</td>
<td>2 expert</td>
<td>Custom</td>
</tr>
<tr>
<td>Business Logic Testing</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Zero Flase Positive</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Dark and Deep Web Reconnaissance</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Code Repositories Reconnaissance</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>OSCP Certified Tester</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SLA</td>
<td>3-5 Days</td>
<td>5 - 7 Days</td>
<td>7-9 Days</td>
<td>Custom</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VULNERABILITIES SCAN</th>
<th>Essentials</th>
<th>Professional</th>
<th>Enterprise</th>
<th>Ultimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage of 50K+ Vulnerabilities</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Cross Site Scripting (XSS)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Cross Site Request Forgery (CSRF)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Forms Input Forgery</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Code Injection</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Cookie Positioning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>CWE/SANS TOP 25</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>PCI DSS 6.5.1-6.5.11 FULL COVERAGE</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>OWSAP TOP 10</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REPORTING</th>
<th>Essentials</th>
<th>Professional</th>
<th>Enterprise</th>
<th>Ultimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reproduction Steps</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Web, PDF, JSON, XML and CSV Formats</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Remediation Guidelines</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Compliance Report</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>CVE, CWE and CVSSv3 Scores</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACCESS TO SECURITY CONSULTANT</th>
<th>Essentials</th>
<th>Professional</th>
<th>Enterprise</th>
<th>Ultimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/7 Access to Security Consultant</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>