**SECURITY TESTING**

Nikita Ovhal

Batch No: 2022-7669

**Security Testing**

The main goal of Security Testing is to identify the threats in the system and measure its potential vulnerabilities, so the threats can be encountered and the system does not stop functioning or cannot be exploited. It also helps in detecting all possible security risks in the system and helps developers to fix the problems through coding.

Types of security Testing

Vulnerability Scanning. ...

Security Scanning. ...

Penetration Testing. ...

Security Audit/ Review. ...

Ethical Hacking. ...

Risk Assessment. ...

Posture Assessment. ...

Authentication.

**KeyTerms used in Security Testing**

**URL Manipulation:**

One of the popular ways to hack a website is URL manipulation where in hackers manipulate website URL query strings and get access to confidential information. This usually takes place when the application makes use of HTTP GET to pass information between client & server. Information is passed via query string. The tester alters the query parameters to check if is accepted by the server. An URL Manipulation testing ensures that database records are not accessed neither other vital information of the website by unauthorized users.

**SQL Injection:**

One of the other common ways picked by hackers to steal the vital information from the web, the SQL Injection testing ensures all the databases are safe and protected. It is a type of testing that takes the advantages of the loopholes that make the hackers easily pass into the system by passing all possible SQL queries to hack it. They try to query the database using the SQL Injection statements to pull information and crash the system. Even the errors displayed while crashing the system will provide generous amount of important data to the hackers. So, SQL Injection testing is purposed to take care of the input fields like comments, text boxes etc. Special characters are either handled or skipped from the input.

**Vulnerability:**

This is to identify the weakest attributes in the system which might lend easy paths for the malicious software to be attached by unauthorized users. Vulnerability can occur due to bug in software, inaccurate software testing or presence of malicious code. This phase requires fixes, patches to prevent the compromised integrity by malware or hackers.

**Cross-Site Scripting (XSS)**

Cross-site scripting is a computer security vulnerability found in web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users and trick a user into clicking on that URL. Once executed by the other user’s browser, this code could then perform actions such as completely changing the behavior of the website, stealing personal data, or performing actions on behalf of the user.

Types of XSS

* **Stored XSS** − Stored XSS also known as persistent XSS occurs when user input is stored on the target server such as database/message forum/comment field etc. Then the victim is able to retrieve the stored data from the web application.
* **Reflected XSS** − Reflected XSS also known as non-persistent XSS occurs when user input is immediately returned by a web application in an error message/search result or the input provided by the user as part of the request and without permanently storing the user provided data.
* **DOM Based XSS(**Document Object Model-based) − DOM Based XSS is a form of XSS when the source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser.

**Security Testing Tools**

1. **ACUNETIX**

Acunetix is an end-to-end web application security scanner. This will give you a 360-degree view of the security of your organization. It is capable of detecting 6500 types of vulnerabilities like SQL injections, XSS, and Weak Passwords, etc. It makes use of advanced macro recording technology for scanning complex multi-level forms. The platform is intuitive and easy to use. You can schedule and prioritize full scans as well as incremental scans. It contains a built-in vulnerability management functionality. With the help of CI tools like Jenkins, new builds can be scanned automatically.

1. **INVICTI**

Invicti (formerly Netsparker) is a platform for all web application security testing requirements. This web vulnerability scanning solution has capabilities of vulnerability scanning, vulnerability assessment, and vulnerability management. Invicti is best for scanning precision and unique asset discovery technology. It can be integrated with popular issue management and CI/CD applications. Invicti provides proof of exploit on the identification of vulnerability to confirm that it is not a false positive. It has an advanced scanning engine, advanced crawling authentication features, and WAF integration functionality, etc. With this tool, you will get detailed scanned results with insights on vulnerability.

1. **NetSparker**

NetSparker acts as a one-stop shop for all the web security needs. Available as both hosted as well as self-hosted solution, this platform can be easily integrated completely in any type of test and dev environment. NetSparker has a trade-marked Proof-Based-Scanning technology that uses automation to identify vulnerabilities and verify false positives, thus eliminating the need for unnecessary investment of huge man hours.

1. **ImmuniWeb**

ImmuniWeb is a next-gen platform that employs Artificial Intelligence to enable security testing. This AI-enabled penetration testing platform offers holistic benefits package for security teams, developers, CISOs, as well as CIOs. Having a one-click virtual patching system, this platform assists continuous complaince monitoring. It boasts a proprietary Multilayer Application Security Testing technology and checks a website for compliance, server hardening, and privacy.

1. **SQLMap**

SQLMap is a penetration testing tool, powered by a detection engine for automating identification and exploitation of SQL injection flaws. Encompassing support for a broad spectrum of database management systems and SQL injection techniques, SQLMap automatically recognizes hash-based passwords and supports orchestration of a dictionary-based attack to crack them. With seven levels of verbosity support, it offers ETA support for each query and brings granularity and flexibility for both users’ switches and features. Its fingerprint and enumeration features are valuable in streamlining an effective penetration test run.