Top 10 Open Source Security Testing Tools

Uendi Hoxha

What is Security Testing?

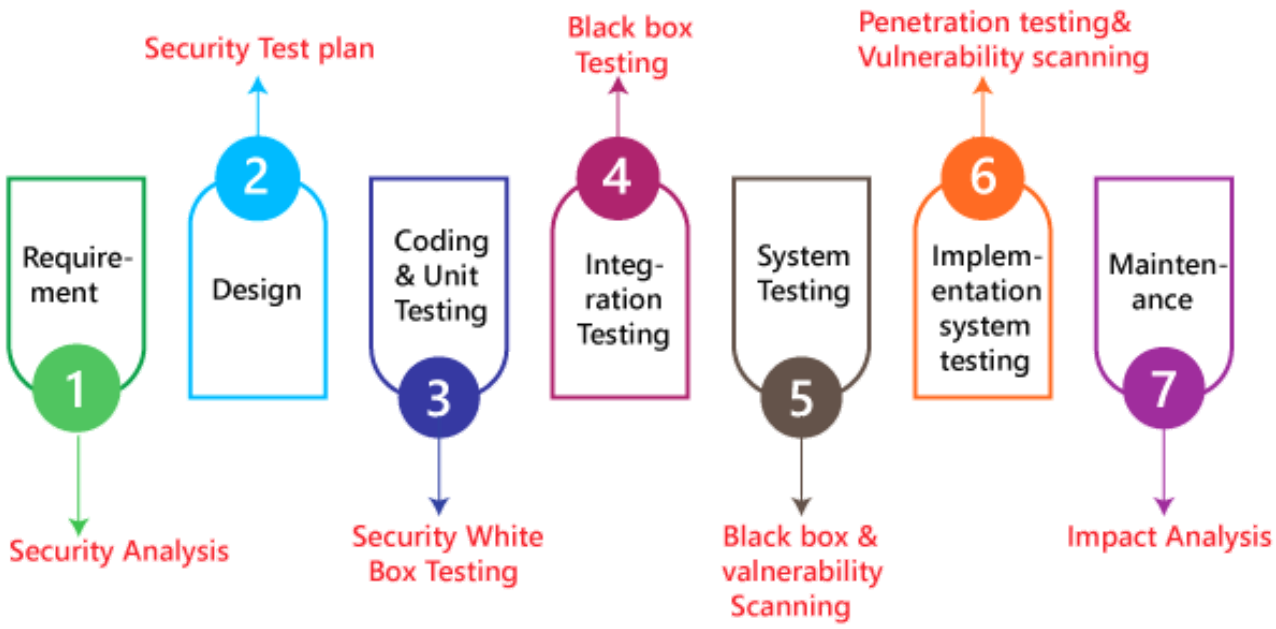
Security testing is performed to ensure that the data within an information system is protected and is not accessible by unauthorized users. It protects the applications against serious malware and other unanticipated threats that may crash it.

Security testing helps to figure out all the loopholes and weaknesses of the system in the initial stage itself. It is done to test whether the application has encoded security code or not and is not accessible by unauthorized users.
Mainly covered critical areas are as below:

- Authentication
- Authorization
- Availability
- Confidentiality
- Integrity
- Non-repudiation

Purpose of security testing

- The primary purpose of security testing is to identify the security leakage and fix it in the initial stage itself.
- Security testing helps to rate the stability of the current system and also helps to stand in the market for a longer time.



Open Source Security Testing Tools

1. Zed Attack Proxy (ZAP)

HIGHLIGHTS: Intercepting Proxy, Automated Scanner, Passive Scanner, Brute Force Scanner, Fuzzer, Port Scanner, Spider, Web Sockets, REST API

ZAP or Zed Attack Proxy is a multi-platform, open-source web application security testing tool. ZAP is used for finding a number of security vulnerabilities in a web app during the development as well as the testing phase. Thanks to its intuitive GUI, Zed Attach Proxy can be used with equal ease by newbies as that by experts. The security testing tool supports command-line access for advanced users. In addition to being one of the most famous OWASP projects, it is awarded the flagship status. ZAP exploses:

- Application error disclosure
- Cookie not HttpOnly flag
- Missing anti-CSRF tokens and security headers
- Private IP disclosure
- Session ID in URL rewrite
- SQL injection
- XSS injection

2. Wfuzz

HIGHLIGHTS: Multiple injection points with multiple dictionaries, Post, headers and authentication data brute forcing, Output to HTML, Cookies fuzzing, Multithreading, Proxy Support, SOCK Support, Authentication Support (NTLM, Basic, Multiple encoders per payload, HEAD scan

Wfuzz is popularly used for brute-forcing web applications. The open-source security testing tool has no GUI interface and is usable only via command line. Vulnerabilities exposed by Wfuzz are:

- LDAP injection
- SQL injection
- XSS injection

3. Wapiti

HIGHLIGHTS: Support HTTP, HTTPS and SOCKS5 proxies, Basic, Digest, NTLM or GET/POST authentication, acts like a fuzzer

Wapiti is a web application vulnerability scanner. It allows us to audit the security of websites or web applications. It performs black box scans of the web application by crawling the web pages of the deployed webapp, looking for scripts and forms where it can inject data.

Once it gets the list of URLs, forms and their inputs, Wapiti acts like fuzzer, injecting payloads to see if a script is vulnerable.Vulnerabilities exposed by Wapiti are:

- Command Execution detection
- CRLF injection
- Database injection
- File disclosure
- Shellshock or Bash bug
- SSRF (Server Side Request Forgery)
- Weak .htaccess configurations that can be bypassed
- XSS injection
- XXE injection

4. W3af

HIGHLIGHTS: Proxy support, HTTP Basic and Digest authentication, UserAgent faking, Add custom headers to requests, Cookie handling, HTTP response cache, DNS cache, File upload using multipart, fuzzing engine.

W3af is a web application attack and audit framework. It comes with both GUI and console interface. It helps developers and penetration testers identify and exploit vulnerabilities in web applications. It is able to identify more than 200 types of security issues in web applications, including:

- Cross-Site Scripting
- SQL Injection
- Guessable credentials
- Unhandled application errors
- PHP misconfigurations
- Blind SQL injections
- Buffer overflow vulnerability
- CORS (Cross-Origin Resource Sharing)
- CSRF (Cross Site Request Forgeries) vulnerabilities
- OS Commanding
- Authentication support

5. SQLMap

HIGHLIGHTS: support a wide range of database services (including MySQL, Oracle & PostgreSQL), operating systems, SQL injection techniques.

SQLMap is a penetration testing tool which allows users to automate the process of detecting and exploiting SQL injection vulnerabilities in a website's database. It comes with a powerful detection engine and many features to detect vulnerabilities. The security testing tool comes with a powerful testing engine, capable of supporting 6 types of SQL injection techniques:

- Boolean-based blind
- Error-based
- Out-of-band
- Stacked queries
- Time-based blind
- UNION query

6. SonarQube

HIGHLIGHTS: Continuous inspection, Multi-Language support, DevOps Integration, Centralize Quality.

In addition to exposing vulnerabilities, SonarQube is used to measure the source code quality of a web application. It is able to carry out analysis of over 20 programming languages. Furthermore, it gets easily integrated with continuous integration tools to the likes of Jenkins. Some of the vulnerabilities exposed by SonarQube include:

- Cross-site scripting
- Denial of Service (DoS) attacks
- HTTP response splitting
- Memory corruption
- SQL injection

7. Wireshark

HIGHLIGHTS: rich VoIP analysis, decryption support, packet browser, deep protocol inspection, live capturing and offline analysis, standard three-pane packet browser.

Wireshark is a security tool that captures and analyzes network packets in real-time and outputs them in readable formats. It comes with an integration for GUI or TTY mode TShark Utility for a graphical presentation of the collected data. Wireshark exploits the following:

- ARP scanning
- IP Protocol scanning
- ICMP, TCP, UDP ping sweeps
- TCP stealth/ Null/ FIN/ Xmass scan
- ARP Poisoning
- ICMP flooding
- VLAN hoping
- Unexplained packet loss
- Client deauthenticaion/disassociation
- Fake AP beacon flood
- Authentication DoS

8. Nogotofail

HIGHLIGHTS: support setting up as a router, proxy or VPN server, SSL certificate verification, HTTPS and TLS/SSL library bugs, SSL and STARTTLS stripping issues, cleartext issues.

Nogotofail is a network security testing tool (network vulnerability scanner tool) designed to help developers and penetration testers. Vulnerabilities exposed by Nogotofail are:

- MiTM attacks
- SSL certificate verification issues
- SSL injection
- TLS injection

9. Vega

HIGHLIGHTS: TLS / SSL security settings, identifying improvements of TLS servers.

Vega is an open-source web application security testing tool with three testing modes: automated, manual, and hybrid. When supplied with a user credential, it can automatically log into a website and scan the web pages for vulnerabilities. It identifies vulnerabilities as:

- Find and validate SQL injection
- Cross-Site Scripting (XSS) injection
- Blind SQL injection
- Header injection
- Remote file include
- Shell injection

10. Arachni

HIGHLIGHTS: Tracing of data & execution flows of DOM and JavaScript environments.

Arachni is an open source security testing tool aimed towards helping penetration testers and administrators evaluate the security of web applications. It is a feature-full, modular, high-performance Ruby framework. It captures the following vulnerabilities:

- Local file inclusion
- Remote file inclusion
- Invalidated redirects
- Invalidated DOM redirects
- XPath injection
- SQL injection
- XSS injection