TOOLS FOR SECURITY TESTING

1) Acunetix

Acunetix online is a premium security testing tool worth trying. You can get the trial version for Acunetix here.

Acunetix Online includes a fully automated network vulnerability scanner that detects and reports on over 50,000 known network vulnerabilities and misconfigurations.

It discovers open ports and running services; assesses the security of routers, firewalls, switches, and load balancers; tests for weak passwords, DNS zone transfer, badly configured Proxy Servers, weak SNMP community strings, and TLS/SSL ciphers, among others.

It integrates with Acunetix Online to provide a comprehensive perimeter network security audit on top of the Acunetix web application audit.

2) Invicti (formerly Netsparker)

Invicti (formerly Netsparker) is a dead accurate automated scanner that will identify vulnerabilities such as SQL Injection and Cross-site Scripting in web applications and web APIs including ones developed using open source CMS.

Invicti uniquely verifies the identified vulnerabilities proving they are real and not false positives, so you do not need to waste hours manually verifying the identified vulnerabilities once a scan is finished. It is available as Windows software and online service.

3) ZED Attack Proxy (ZAP)

It is an open-source tool that is specifically designed to help security professionals to find out the security vulnerabilities present in web applications. It's developed to run on Windows, Unix/Linux, and Macintosh platforms. It can be used as a scanner/filter of a web page.

Key features:

- Intercepting Proxy
- Passive Scanning
- Automated Scanner
- REST-based API

4) Burp suite

It is a tool that is used for performing security testing of web applications. It has professional as well as community editions. With over 100 predefined vulnerability conditions it ensures the safety of the application, **Burp suite** applies these predefined conditions to find out the vulnerabilities.

5) SonarQube

It is an open-source tool that is used to measure the quality of source code.

Though written in Java, it can analyze over twenty different programming languages. It can easily integrate with continuous integration tools like Jenkins server, etc. The results will be populated to the SonarQube server with 'green' and 'red lights'.

Nice charts and project level issue lists can be viewed. We can invoke it from the GUI as well as the command prompt.

6) Klocwork

It is a code analysis tool that is used to identify security, safety and reliability issues of the programming languages like C, C++, Java, and C#. We can easily integrate it with continuous integration tools like Jenkins and can also raise bugs in Jira upon encountering new issues.

Project wise Scanned Result:

Printout of the result can be taken using the tool. On the home page, we can view all the scanned projects with their 'new' and 'existing' issue count. The range and ratio of the issue can be viewed by clicking on the 'Report' icon.