**SECURITY TESTING TOOLS**

The following are some of the Security testing tools:

1. **Zed Attack Proxy (ZAP)**
2. **SonarQube**
3. **Wapiti**
4. **Netsparker**
5. **Arachni**
6. **Iron Wasp**
7. **Grabber**
8. **SQLMap**

**Zed Attack Proxy (ZAP)**

ZAP, or Zed Attack Proxy, is a multi-platform, open-sourceonline application security testing tool developed by OWASP (Open Web Application Security Project).

During the development and testing phases of a web app, ZAP is used to uncover a variety of security flaws.

### **SonarQube**

Sonar Source created this open-source security tool.

It is used to verify the quality of code and run automated reviews on web applications written in various programming languages such as

[Java](https://www.geeksforgeeks.org/java/), [C#](https://www.geeksforgeeks.org/csharp-programming-language/), [JavaScript](https://www.geeksforgeeks.org/introduction-to-javascript/), [PHP](https://www.geeksforgeeks.org/php/), Ruby, Cobol, [C](https://www.geeksforgeeks.org/c-language-set-1-introduction/)/[C++](https://www.geeksforgeeks.org/c-plus-plus/), and so on by discovering bugs, code analysis, and security exposures.

### **Wapiti**

Wapiti is a free, open-source project from SourceForge and develop that is one of the leading web application security testing tools.

Wapiti uses black-box testing to look for security vulnerabilities in online applications.

### **Netsparker**

It is used to detect the web application’s vulnerabilities in a unique way, as well as to verify whether the application’s weaknesses are correct or erroneous.

**Arachni**

Arachni is a web application security scanner that is suitable for both penetration testers and administrators.

This open-sourcesecurity testing program may detect a variety of flaws

**Iron Wasp**

Iron Wasp is a strong open-source scanning tool that can detect over 25 different types of web application flaws.

It can also distinguish between false positives and false negatives.

**Grabber**

The Grabber is a simple web application scanner that can be used to search forums and personal websites.

The Python-based lightweight security testing tool has no graphical user interface.

**SQLmap**

SQLmap is an open-source tool for detecting and exploiting SQL injection problems in penetration testing.

SQLmap is a tool that automates the detection and use of SQL injection. SQL Injection attacks have the ability to gain control of SQL databases.