# **Learning ZAP for Beginners**

**By Kazy Hamidur Rahman**

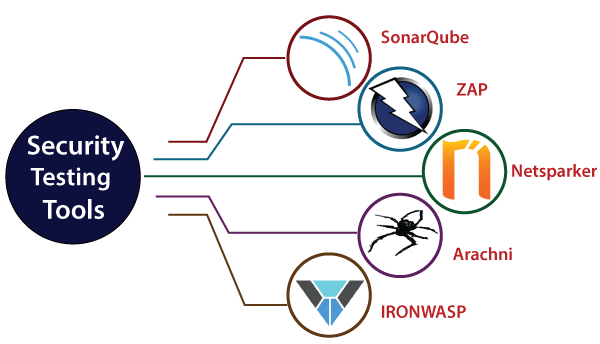
# Security Testing Tools

Security testing tools are used to make sure that the data is saved and not accessible by any unauthorized user. To protect our application data from the threats, we will use these tools. These tools help us to find the flaws and security leakage of the system in the earlier stage and fix it, and test whether the application has encoded security code or not and accessible by the unauthorized users.

These may initially work on authorization, confidentiality, authentication, and availability types of aspects. With the help of these tools, we can avoid the loss of relevant information, the client's trust, sudden breakdown, additional costs required for repairing websites after an attack, and unpredictable website performance.

For this, we have the following tools available in the market:

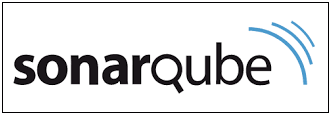
* **SonarQube**
* **ZAP**
* **Netsparker**
* **Arachni**
* **IronWASP**



## SonarQube

It is an open-source security tool which is established by Sonar Source. It is used to test the quality of the code and execute the automatic reviews with the help of identifying the bugs, code analysis and security exposures on various programming languages such as Java, [C#](https://www.javatpoint.com/c-sharp-tutorial), [JavaScript](https://www.javatpoint.com/javascript-tutorial), [PHP](https://www.javatpoint.com/php-tutorial), Ruby, [Cobol](https://www.javatpoint.com/cobol), [C](https://www.javatpoint.com/c-programming-language-tutorial)/[C++](https://www.javatpoint.com/cpp-tutorial) and so on of the web applications. SonarQube tool is written on the [JAVA programming language](https://www.javatpoint.com/java-tutorial).

It will generate the reports of the code coverage, complexity of code, repeated code, security weakness, and bugs. It offers complete analysis with multiple tools like [Ant](https://www.javatpoint.com/apache-ant-tutorial), [Maven](https://www.javatpoint.com/maven-tutorial), [Gradle](https://www.javatpoint.com/gradle), [Jenkins](https://www.javatpoint.com/jenkins), and so on.



### Features of SonarQube

* It will integrate with multiple development environments like Visual Studio, Eclipse, and IntelliJ IDEA over the SonarLint plug-ins.
* It also supports some external tools such as GitHub, LDAP, and Active Directory.
* It can record the metric history and deliver the evolution graphs.
* It will help us to identify the complex issues.
* It will provide application security.

## ZAP [Zed Attack Proxy]

It is another security testing tool, which is established by **OWASP**, where it stands for (Open Web Application Security Project). It is an open-source tool that was written on the Java Programming language. If we use this tool as a proxy server, it offers the user to deploy all the traffic which passes over it. We can run this tool on the daemon mode that is exact through the REST API.

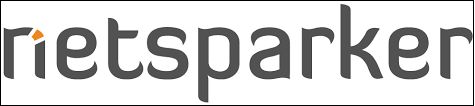


### Features of ZAP

* It will support the command-line access for advance users.
* It can be used as a scanner.
* It will provide the automatic scanning of the web application.
* It supports different operating systems like Windows, OS X, and Linux.
* It uses the powerful and Old AJAX spiders.

## Netsparker

It is used to find the vulnerabilities of the web application uniquely and also validates that the weaknesses of the application are correct or incorrect. It can be easily accessible as Windows software. With the help of this tool, we can do automatic vulnerability assessment and fix the issues and avoid the resources-intensive manual procedures.

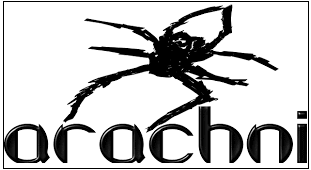


### Features of Netsparker

* It will automatically scan modern web applications like Web 2.0, HTML5, and SPA (single page applications), and all types of legacy.
* For different purposes, it will provide a multitude of out-of-the-box reports for both developers and management.
* We can generate custom reports with the help of our templates.
* We can collaborate this tool with CI/CD platforms such as Bamboo, Jenkins, or TeamCity to protect our application.

## Arachni

It is another open-source security testing tool, which is used to find the security vulnerabilities of the web application. It supports the integrated browser environment, which helps us to identify the security issues of the highly complex web applications.



### Features of Arachni

* It will provide vulnerability exposure, test coverage, and correctness of the web application technologies.
* It supports the various platform and all-important Operating systems like Linus, Mac, OS X, and MS Windows.
* It will support different technologies like HTML5, JavaScript, AJAX, and DOM manipulation.

For more information about Arachni, refers to the below link:

[https://www.arachni-scanner.com/](https://www.arachni-scanner.com/" \t "_blank)

## IronWASP

It is an open-source tool, which is used to identify the vulnerability of the web application. It stands for the **Iron Web Application Advanced Security Testing Platform**. With the help of this tool, a user can make their custom security scanners. It was developed by using [Python](https://www.javatpoint.com/python-tutorial)

and [Ruby programming languages](https://www.javatpoint.com/ruby-tutorial)

.



### Features of IronWASP

* It will support the recording login sequence.
* It will produce the reports for both RTF and HTML formats.
* It is a GUI based tool.
* It will support false Positives and negatives detection.

## Introduction to Postman

* Postman is a standalone software testing API (Application Programming Interface) platform to build, test, design, modify, and document APIs. It is a simple Graphic User Interface for sending and viewing HTTP requests and responses.
* While using Postman, for testing purposes, one doesn't need to write any HTTP client network code. Instead, we build test suites called collections and let Postman interact with the API.
* In this tool, nearly any functionality that any developer may need is embedded. This tool has the ability to make various types of HTTP requests like GET, POST, PUT, PATCH, and convert the API to code for languages like JavaScript and Python.

## Terminologies Related to Postman

### API

Application Programming Interface (API) is software that acts as an intermediary for two apps to communicate with each other. We use APIs whenever we use an application like Twitter, Facebook, sending text messages, or checking the weather over the phone.

### HTTP

HTTP (Hypertext Transfer Protocol) is the collection of rules for the transmission of data on the World Wide Web, like graphic images, text, video, sound, and other multimedia data. The Web users implicitly make use of HTTP as soon as they open their Web browser.

Example: A user or browser enters the HTTP request to the server; the server then returns the user response. This response includes the request status information and may consist of the requested material as well.

The most commonly used HTTP methods are GET, POST, PUT, PATCH, HEAD, DELETE, and OPTIONS.

## Why use Postman?

Postman is based on a wide range of extremely user-friendly power tools. For more than 8 million users, Postman has become a tool of convenience. Following are the reasons why Postman is used:

1. **Accessibility-** One can use it anywhere after installing Postman into the device by simply logging in to the account.
2. **Use Collections**-Postman allows users to build collections for their API-calls. Every set can create multiple requests and subfolders. It will help to organize the test suites.
3. **Test development-** To test checkpoints, verification of successful HTTP response status shall be added to every API- calls.
4. **Automation Testing-**Tests can be performed in several repetitions or iterations by using the Collection Runner or Newman, which saves time for repeated tests.
5. **Creating Environments-** The design of multiple environments results in less replication of tests as one can use the same collection but for a different setting.
6. **Debugging-** To effectively debug the tests, the postman console helps to track what data is being retrieved.
7. **Collaboration-** You can import or export collections and environments to enhance the sharing of files. You may also use a direct connection to share the collections.
8. **Continuous integration-**It can support continuous integration.

## Prerequisites

Before proceeding with this tutorial, you should have a basic knowledge of API, automation, and manual testing.

## Audience

This tutorial is created for those who would like to learn the basics of Postman. As the number of web and mobile applications is increasing, the importance of API testing is also growing. So, this tutorial will help you to learn postman testing for testing APIs.

After completion of this tutorial, you will get a basic level of understanding of Postman and API testing. This tutorial will also give you a good understanding of how to use Postman to execute APIs for any given URL for your daily work.

If you want to **Setup** own **Lab** for security testing, please **Download** & **Install** below things:

1. Virtual Box & its extension

<https://www.virtualbox.org/wiki/Downloads>

2. Kali Linux

<https://www.kali.org/get-kali/#kali-virtual-machines>

|  |  |
| --- | --- |
| ***User: kali*** | ***Password: kali*** |

CommandLine:

**nmap -sP 10.10.1.0/24** – that will start nmap

**arp-scan –** that will show vm ip addresses

3. Metasploitable2-Linux

<https://sourceforge.net/projects/metasploitable/>

|  |  |
| --- | --- |
| ***User: msfadmin*** | ***Password: msfadmin*** |

*Make sure your VM network settings should be set as follows:*

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application

Description automatically generated Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

4. DVWA-1.0.7

<https://www.vulnhub.com/entry/damn-vulnerable-web-application-dvwa-107,43/>

***User: admin Password: password***

Why we need DVWA (Damn Vulnerable Web Application)?

* Practice for beginners
* Hacking a target without permission is illegal
* Organizations don’t allow hacking for practice
* DVWA is used for practicing Ethical Hacking within the boundaries of the law

# Installation and Updates ZAP - Cloud Security

Graphical user interface, text, application

Description automatically generated<https://security.secure.force.com/security/tools/webapp/zapbrowsersetup>

ZAP **Setting up ZAP for Browser**

# **Installation**

* 1. *Download ZAP from*[*here*](https://www.zaproxy.org/download/)
  2. *Install and open ZAP*

# **Installing certificate**

Since all requests and responses are proxied by ZAP, the certificate verification will fail for sites using SSL (HTTPS) and the connection will be terminated. To prevent this from happening, ZAP generates an SSL certificate for each host, signed by its own Certificate Authority (CA) certificate. This CA certificate is generated the first time ZAP is run and is stored locally. To use the ZAP Proxy with these websites, you will need to install ZAP’s CA certificate as a trusted root in your browser.

## *Go to Tools >> Options >> Dynamic SSL Certificate.*

## *Click Generate and then click Save.*

## *Save the certificate in the desired location.*

## *Open your browser and install the Certificate to your browser (*[*Firefox*](https://www.google.com/url?q=https%3A%2F%2Fsupport.mozilla.org%2Fen-US%2Fkb%2Fadvanced-panel-accessibility-browsing-network-upda%3Fredirectlocale%3Den-US%26as%3Du%26redirectslug%3DOptions%2Bwindow%2B-%2BAdvanced%2Bpanel%26utm_source%3Dinproduct%23w_certificates-tab&#38;sa=D&#38;sntz=1&#38;usg=AFQjCNFrkp7G2WQX9KJ-OeEU5EuHmWe3tg)*,*[*Chrome*](https://support.google.com/chrome/answer/95572?hl=en)*,*[*IE*](https://www.google.com/url?q=https%3A%2F%2Fmsdn.microsoft.com%2Fen-us%2Flibrary%2Fcc750534.aspx&#38;sa=D&#38;sntz=1&#38;usg=AFQjCNFBQfl-DQWPTiYcVL8ORA0QHAy5WA)*) accordingly*

# **Configuring Proxy**

* 1. *Open your preferred browser and set up the proxy as shown*[*here*](https://code.google.com/p/zaproxy/wiki/HelpStartProxies)*(You can use port 8080 as the port)*

Graphical user interface, application

Description automatically generated

* 1. *In the ZAP UI, go to Tools>Options>Local Proxy*
  2. *Make sure the port is set to 8080 (or the port you have configured in your browser)*

Graphical user interface, text, application, email

Description automatically generated

* 1. *Open any website using SSL in your browser and make sure the site shows up in the sites list.*

Graphical user interface, application, table

Description automatically generated

[**Next:** *Running the Scan*](https://security.secure.force.com/security/tools/webapp/zaprunningscan)

OWASP **ZAP** – **Zad Attack Proxy and its Features**

<https://digitalvarys.com/owasp-zap-proxy/#Advanced_SQL_Injection_Scanner>

 [Features of OWASP ZAP proxy.](https://digitalvarys.com/owasp-zap-proxy/#Features_of_OWASP_ZAP_proxy)

* [Intercepting Proxy](https://digitalvarys.com/owasp-zap-proxy/#Intercepting_Proxy)
* [Automated Scanner](https://digitalvarys.com/owasp-zap-proxy/#Automated_Scanner)

**Types of Scanning:**

* *Network*
* *Network Devices*
* *Computers*
* *Applications/Services*
* [Brute Force Scanner](https://digitalvarys.com/owasp-zap-proxy/#Brute_Force_Scanner)
* [Fuzzing](https://digitalvarys.com/owasp-zap-proxy/#Fuzzing)
* [Port Scanning](https://digitalvarys.com/owasp-zap-proxy/#Port_Scanning)
* [WebSockets](https://digitalvarys.com/owasp-zap-proxy/#WebSockets)
* [Advanced SQL Injection Scanner](https://digitalvarys.com/owasp-zap-proxy/#Advanced_SQL_Injection_Scanner)
* [Advanced Alerts](https://digitalvarys.com/owasp-zap-proxy/#Advanced_Alerts)
* [Tools Integration](https://digitalvarys.com/owasp-zap-proxy/#Tools_Integration)
* [REST API](https://digitalvarys.com/owasp-zap-proxy/#REST_API)