

Project Report on Cyber Security Scanning Using OWASP ZAP

Submitted by
Vishnu Tirth Bysani
2nd Year IITBBS

Contents

1. Abstract.....	3
2. Introduction.....	3
3. What is OWASP ZAP ?	4
4. Main Tools in OWASP ZAP	4
5. Scanning using OWASP ZAP	5
6. Conclusion	10

1. Abstract

Our goal is to demonstrate the use of a open-source web application security scanner called OWASP ZAP by using its various tools for penetration testing.

2. Introduction

A cyber-attack is an assault launched by cybercriminals using one or more computers against single or multiple computers or networks. A cyber-attack can steal data, disable computers, or use a compromised computer (or other devices) as a launchpad for other attacks maliciously.

Today, these attacks not only remain focused on attacking computers. Rather the attackers also target any other device connected to the internet. That includes everything from your smartphones to WIFI routers to internet-connected home appliances like Smart TVs and home security solutions.

Usually, most cyber-attacks that pose a threat to your online security fall into one of these categories:

- ❖ Malware attacks – hackers infect your device/system with a malicious tool.
- ❖ Phishing attacks – hackers trick you via tempting yet malicious text messages or emails.
- ❖ Ransomware attacks – criminals infect your device/network with malware that encrypts all your data and makes your system inaccessible. They then ask you to pay the 'ransom' to free your computer.
- ❖ Denial of Service (DoS) attacks – these attacks render your device or the entire IT structure out of service.
- ❖ Man In The Middle (MiTM) attacks – hackers intercept your network to snoop on your online activities and steal your data.
- ❖ Crypto-jacking – hackers hack your device to mine cryptocurrency for them.
- ❖ SQL Injection attacks – the attackers exploit a security vulnerability to hack your database.
- ❖ Zero-Day exploits – hackers exploit unpatched bugs in the apps or the operating system of your device to target users.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

3. What is OWASP ZAP ?

OWASP ZAP (Zed Attack Proxy) is an open-source web application security tool that helps to identify vulnerabilities in web applications. It is a project initiated by the OWASP (Open Web Application Security Project) Foundation, a non-profit organization dedicated to improving the security of software. The tool is designed for both security professionals and novice users and provides a user-friendly interface that makes it easy to use.

One of the primary features of OWASP ZAP is its ability to detect common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). It does this by intercepting the requests and responses between the web application and the client.

OWASP ZAP also provides a range of automated testing tools that can be used to identify vulnerabilities in web applications. These tools include the spider, which automatically crawls a website to identify all the pages and links, and the active scanner, which actively probes the application to identify any potential security weaknesses. In addition, OWASP ZAP also includes a manual testing mode, which allows security professionals to manually explore the application and identify any vulnerabilities.

4. Main Tools in OWASP ZAP

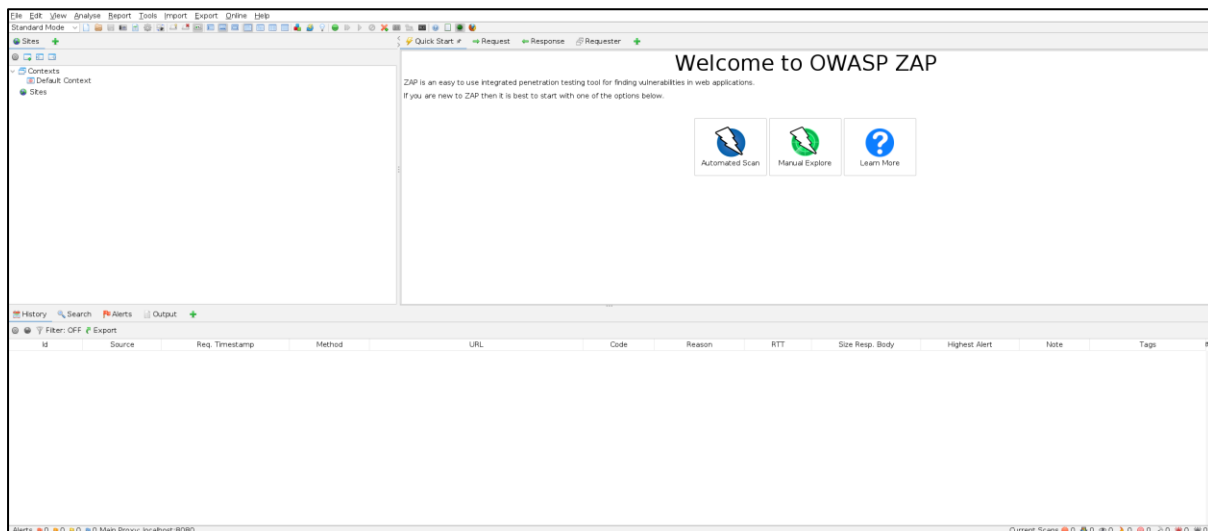
- ❖ Spider: The Spider tool is used to automatically crawl a website and identify all the reachable pages. It helps to discover all the pages and forms on a website, and is used to create a baseline for further testing.
- ❖ Active Scanner: The Active Scanner is used to proactively scan for vulnerabilities and security issues in a website. It works by sending various requests to the website and analyzing the responses to identify potential security risks. The Active Scanner can be configured to run a set of automated security tests, including SQL injection, cross-site scripting, and others.
- ❖ Passive Scanner: The Passive Scanner analyzes traffic and looks for security issues without actively sending requests to the website. It analyzes the traffic that is generated by the user's browsing, including requests and responses, and flags potential security issues.
- ❖ Break / Fuzzer: The Break / Fuzzer tool is used to test a website's input validation and handling by sending malformed and unexpected data. This helps to identify any security issues related to how a website processes and handles user input.

- ❖ **WebSockets:** The WebSockets tool is used to monitor and analyze WebSocket communication. This tool is useful for testing web applications that use WebSockets for real-time communication.
- ❖ **Authorization and Authentication Testing:** The Authorization and Authentication Testing tool is used to test the security of a website's authorization and authentication mechanisms. It checks for common vulnerabilities, such as weak passwords, and can also be used to test for other security issues related to authorization and authentication.
- ❖ **Alerts:** The Alerts tool displays and summarizes security alerts generated by the other tools. This tool provides a consolidated view of all the security issues that have been identified during a scan, making it easier to prioritize and address them.

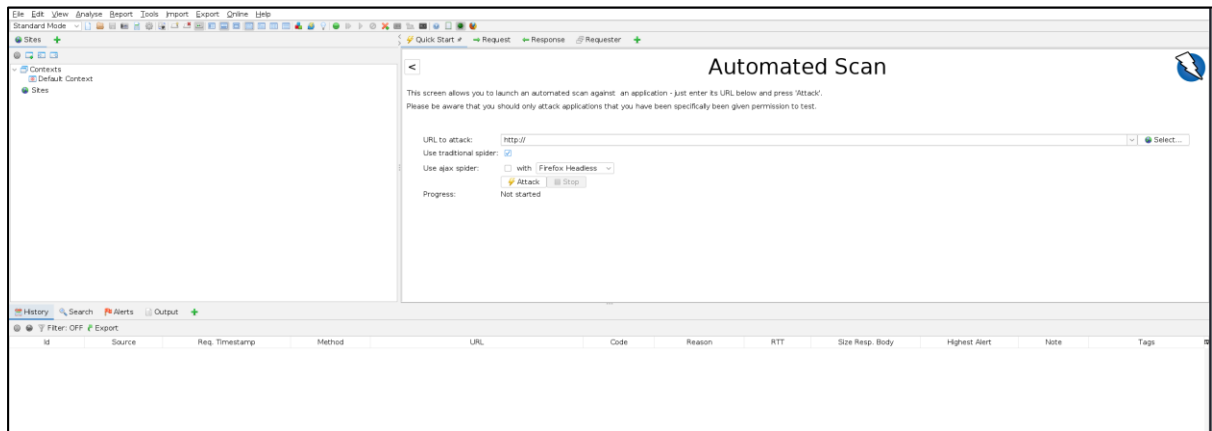
5. Scanning using OWASP ZAP

We will be performing scanning on DVWA which is generally used for penetration testing.

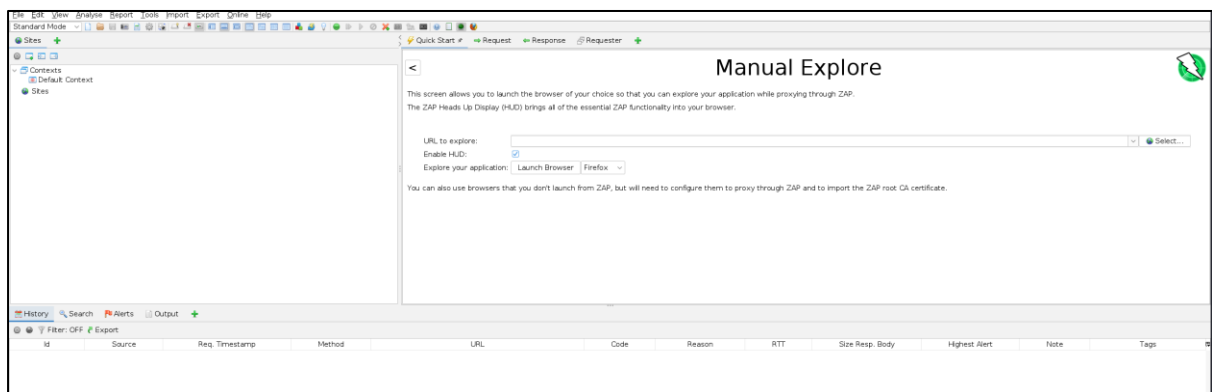
- This is the basic layout of OWASP ZAP. There are two types of scans: automated and manual. Manual Scan requires you to setup a proxy server.



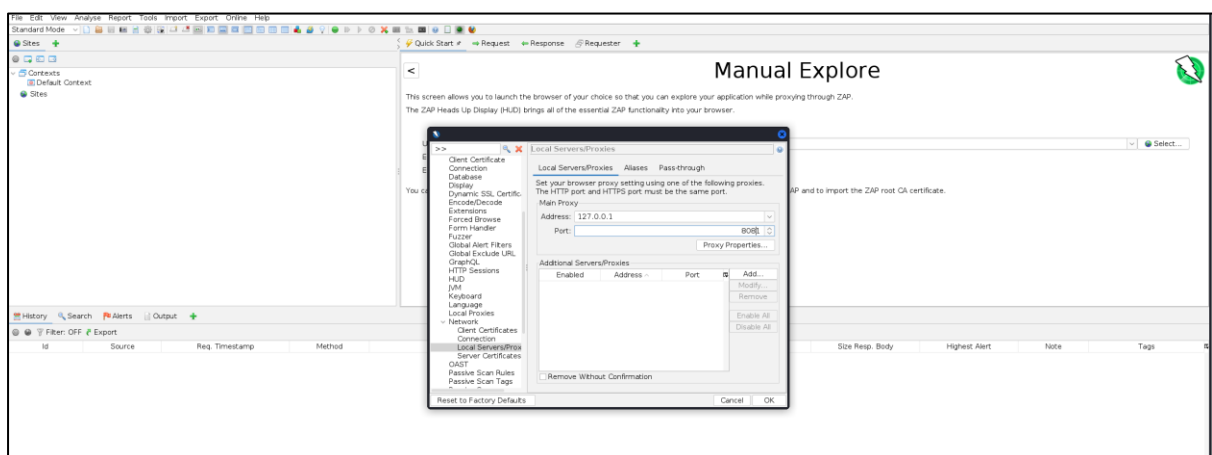
- ii. On selecting Automated Scan, we get the option for typing In the URL and if we want to use a spider or not. The spider will create a sitemap of the URLs.



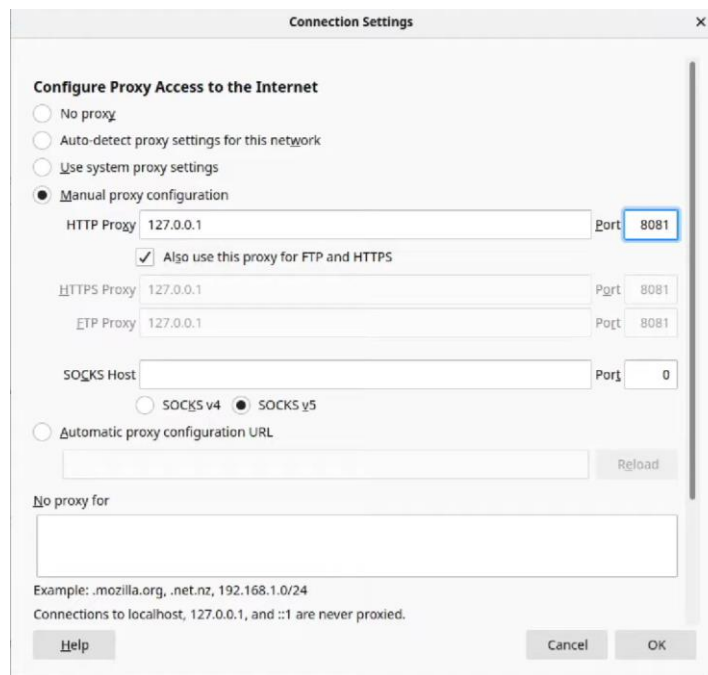
- iii. On selecting Manual Scan, we need to enter the url that we want to attack. Manual Scan requires you to setup a proxy server.



- iv. We can setup a proxy by going to the Tools bar and select Networks->Local Proxies. Enter the address as 127.0.0.1 and the port as 8081.

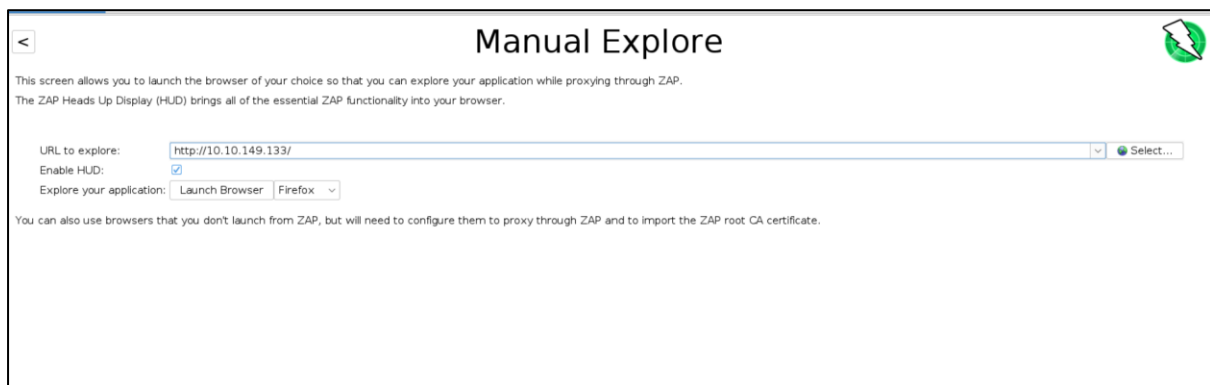


- v. Go DVWA and under Preferences select the proxy connection.



The image shows the 'Connection Settings' dialog box in OWASP ZAP. It has a title bar with 'Connection Settings' and a close button. The main section is 'Configure Proxy Access to the Internet' with four radio buttons: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration'. The 'Manual proxy configuration' option is selected. Below it are fields for 'HTTP Proxy' (127.0.0.1), 'Port' (8081), a checked checkbox 'Also use this proxy for FTP and HTTPS', 'HTTPS Proxy' (127.0.0.1), 'Port' (8081), 'FTP Proxy' (127.0.0.1), 'Port' (8081), 'SOCKS Host' (empty), 'Port' (0), and radio buttons for 'SOCKS v4' and 'SOCKS v5' (selected). There is also an 'Automatic proxy configuration URL' section with a text field and a 'Reload' button. At the bottom, there is a 'No proxy for' text field, an example '.mozilla.org, .net.nz, 192.168.1.0/24', and a note 'Connections to localhost, 127.0.0.1, and ::1 are never proxied.' Buttons for 'Help', 'Cancel', and 'OK' are at the bottom right.

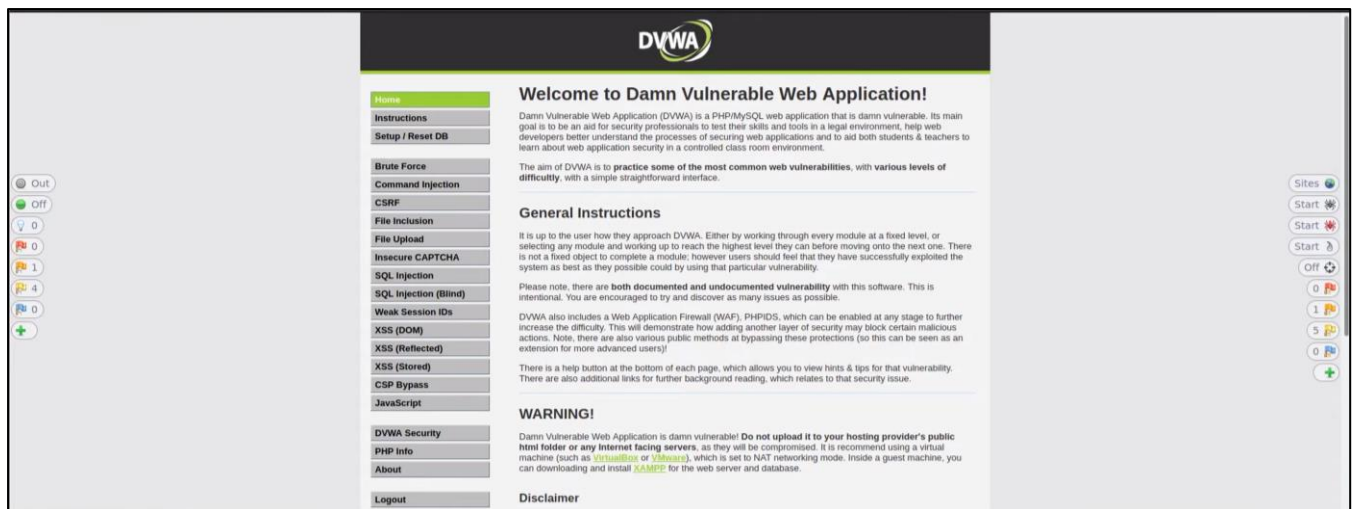
- vi. For proper working of the proxy, import the Dynamic SSL certificates into the browser from the Dynamic SSL Certificates option under Tools in OWASP ZAP.
- vii. Enter the URL of DVWA : `http://10.10.149.133/` in the Manual Explore section and click Launch Browser.



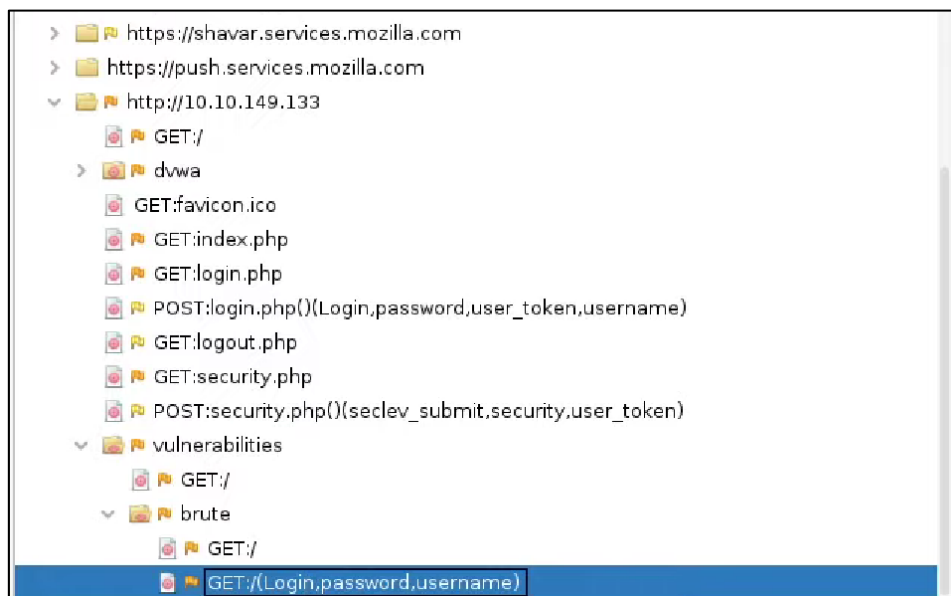
The image shows the 'Manual Explore' dialog box in OWASP ZAP. It has a title bar with 'Manual Explore' and a close button. The main text says 'This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP. The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.' Below this are fields for 'URL to explore:' (http://10.10.149.133/), 'Enable HUD:' (checked), and 'Explore your application:' (Launch Browser, Firefox). There is a 'Select...' button next to the URL field. At the bottom, there is a note: 'You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.'

- viii. Now the browser will be used by OWASP ZAP. In the login page, enter admin as username and password as password.

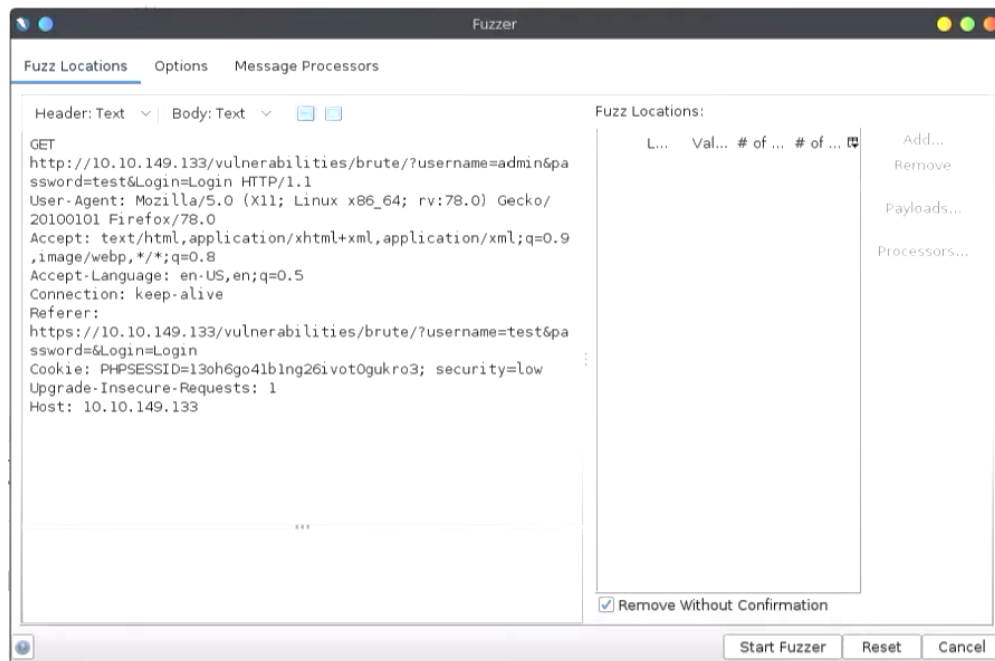
ix. After Login, we have multiple buttons to start different type of scans.



- x. To find the correct Session ID among the HTTP Sessions, go to Cookie Editor in your browser to find the current session and set it as Active Session in OWASP to start the scan. Then select the Active Scan option. After the scan is completed, we can use brute force to retrieve credentials.
- xi. Select Brute Force in DVWA, and then enter username and password as admin and test respectively, because we want to only brute force the password.
- xii. After that right click GET:/(Login.password.username) in OWASP and select the Fuzz option under Attack.



xiii. You will get a layout similar to Burpsuite.



xiv. After that select test and click Add. Then under Type, select File and upload a wordlist like rockyou.txt or fastrack.txt. Then select Start Fuzzer.

xv. OWASP will start the fuzzing, and we will get a set of results under Fuzzer. Sort the results by size. We then notice that one particular payload had taken lesser size that the others which in this case is the keyword 'password'.

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	200 OK	154 ms	364 bytes	4.375 bytes	4.375 bytes	Medium	Reflected	password
1	Fuzzed	200 OK	170 ms	364 bytes	4.375 bytes	4.375 bytes			Spring2017
2	Fuzzed	200 OK	158 ms	364 bytes	4.375 bytes	4.375 bytes			Spring2016
3	Fuzzed	200 OK	157 ms	364 bytes	4.375 bytes	4.375 bytes			Spring2015
4	Fuzzed	200 OK	155 ms	364 bytes	4.375 bytes	4.375 bytes			Spring2014
5	Fuzzed	200 OK	153 ms	364 bytes	4.375 bytes	4.375 bytes			Spring2013
6	Fuzzed	200 OK	90 ms	363 bytes	4.375 bytes	4.375 bytes			spring2017
7	Fuzzed	200 OK	95 ms	363 bytes	4.375 bytes	4.375 bytes			spring2016
8	Fuzzed	200 OK	91 ms	363 bytes	4.375 bytes	4.375 bytes			spring2015
9	Fuzzed	200 OK	93 ms	363 bytes	4.375 bytes	4.375 bytes			spring2014
10	Fuzzed	200 OK	91 ms	363 bytes	4.375 bytes	4.375 bytes			spring2013
11	Fuzzed	200 OK	78 ms	363 bytes	4.375 bytes	4.375 bytes			Summer2017
12	Fuzzed	200 OK	82 ms	363 bytes	4.375 bytes	4.375 bytes			Summer2016
13	Fuzzed	200 OK	85 ms	363 bytes	4.375 bytes	4.375 bytes			Summer2015
14	Fuzzed	200 OK	87 ms	363 bytes	4.375 bytes	4.375 bytes			Summer2014
15	Fuzzed	200 OK	86 ms	363 bytes	4.375 bytes	4.375 bytes			Summer2013
16	Fuzzed	200 OK	77 ms	363 bytes	4.375 bytes	4.375 bytes			summer2017
17	Fuzzed	200 OK	83 ms	363 bytes	4.375 bytes	4.375 bytes			summer2016
18	Fuzzed	200 OK	81 ms	363 bytes	4.375 bytes	4.375 bytes			summer2015
19	Fuzzed	200 OK	81 ms	363 bytes	4.375 bytes	4.375 bytes			summer2014
20	Fuzzed	200 OK	80 ms	363 bytes	4.375 bytes	4.375 bytes			summer2013
21	Fuzzed	200 OK	79 ms	363 bytes	4.375 bytes	4.375 bytes			Autumn2017
22	Fuzzed	200 OK	80 ms	363 bytes	4.375 bytes	4.375 bytes			Autumn2016
23	Fuzzed	200 OK	80 ms	363 bytes	4.375 bytes	4.375 bytes			Autumn2015
24	Fuzzed	200 OK	79 ms	363 bytes	4.375 bytes	4.375 bytes			Autumn2014
25	Fuzzed	200 OK	81 ms	363 bytes	4.375 bytes	4.375 bytes			Autumn2013
26	Fuzzed	200 OK	78 ms	363 bytes	4.375 bytes	4.375 bytes			autumn2017
27	Fuzzed	200 OK	80 ms	363 bytes	4.375 bytes	4.375 bytes			autumn2016

- xvi. Now we can enter the username as admin and password as password as the credentials in DVWA and we are able to login. So in this way we are able to brute force login credentials using OWASP ZAP.


Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin



6. Conclusion

In conclusion, OWASP ZAP is a powerful and user-friendly web application security tool that provides security professionals with a range of tools to identify and address vulnerabilities in their web applications. Its open-source nature and ease of use make it an ideal choice for organizations of all sizes. Whether you are a security professional or a novice user, OWASP ZAP is a tool that is worth considering for your web application security needs.