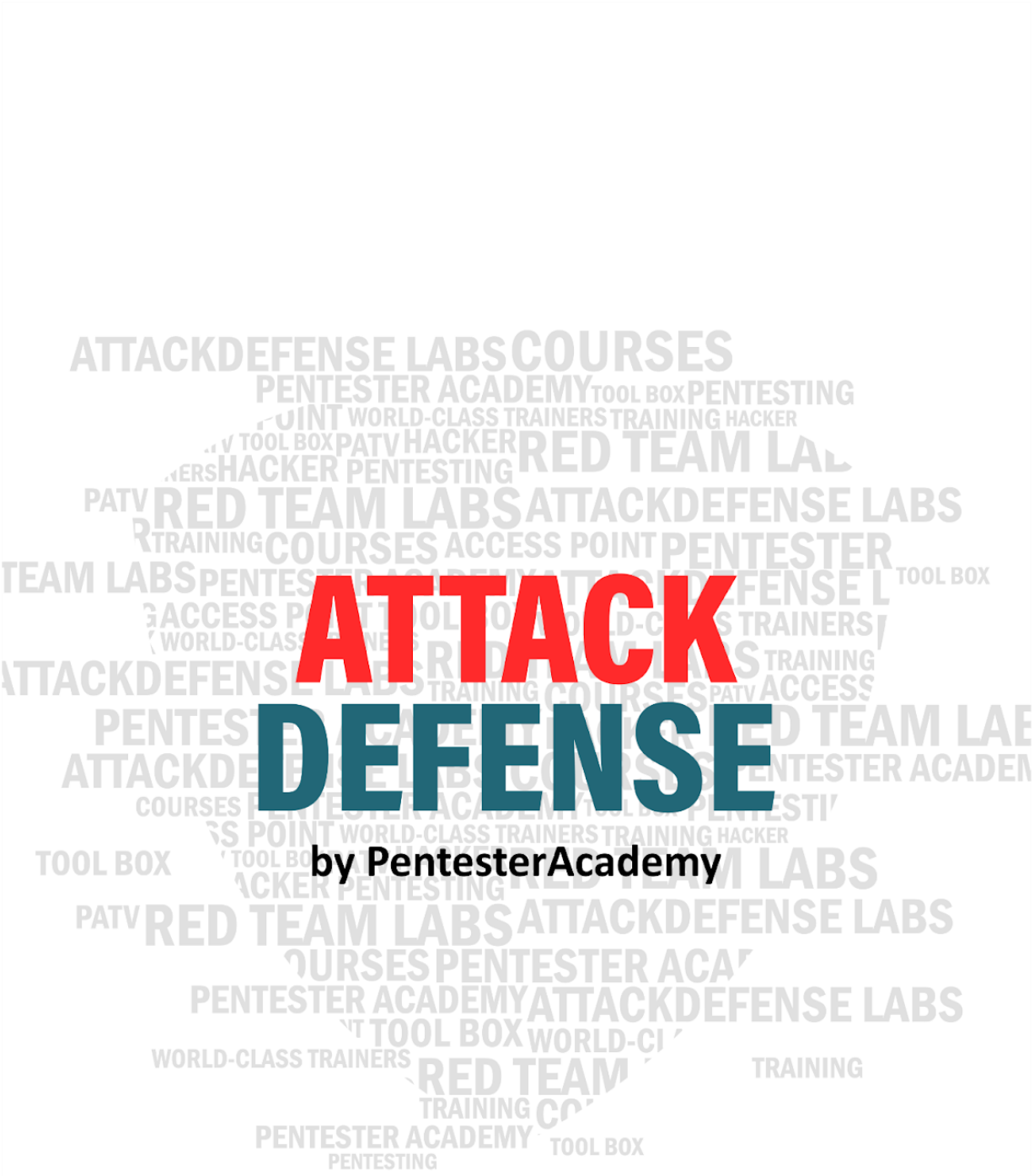

ATTACK
DEFENSE
by PentesterAcademy

Name	Directory Enumeration with ZAProxy
URL	https://attackdefense.com/challengedetails?cid=1885
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Perform directory enumeration with ZAProxy

Step 1: Identifying IP address of the target machine

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
24861: eth0@if24862: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
24864: eth1@if24865: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:9c:cf:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.156.207.2/24 brd 192.156.207.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.156.207.2. The target machine is located at the IP address 192.156.207.3

Step 2: Identifying open ports.

Command: nmap 192.156.207.3

```
root@attackdefense:~# nmap 192.156.207.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-20 18:59 IST
Nmap scan report for target-1 (192.156.207.3)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:9C:CF:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@attackdefense:~#
```

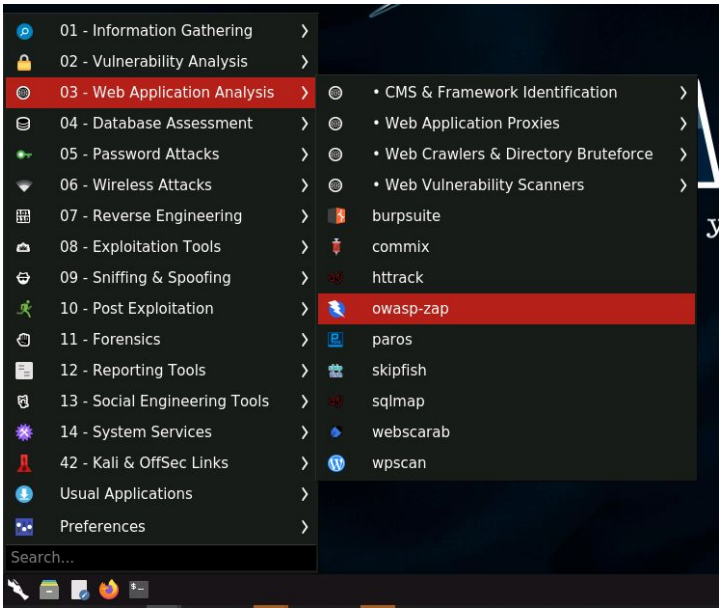
Port 80 and 3306 are open.

Step 3: By default, ZAP only has one wordlist for fuzzing. The wordlists are present in the directory "/root/.ZAP/fuzzers/dirbuster/". Adding dirb common.txt wordlist to the ZAP wordlist directory.

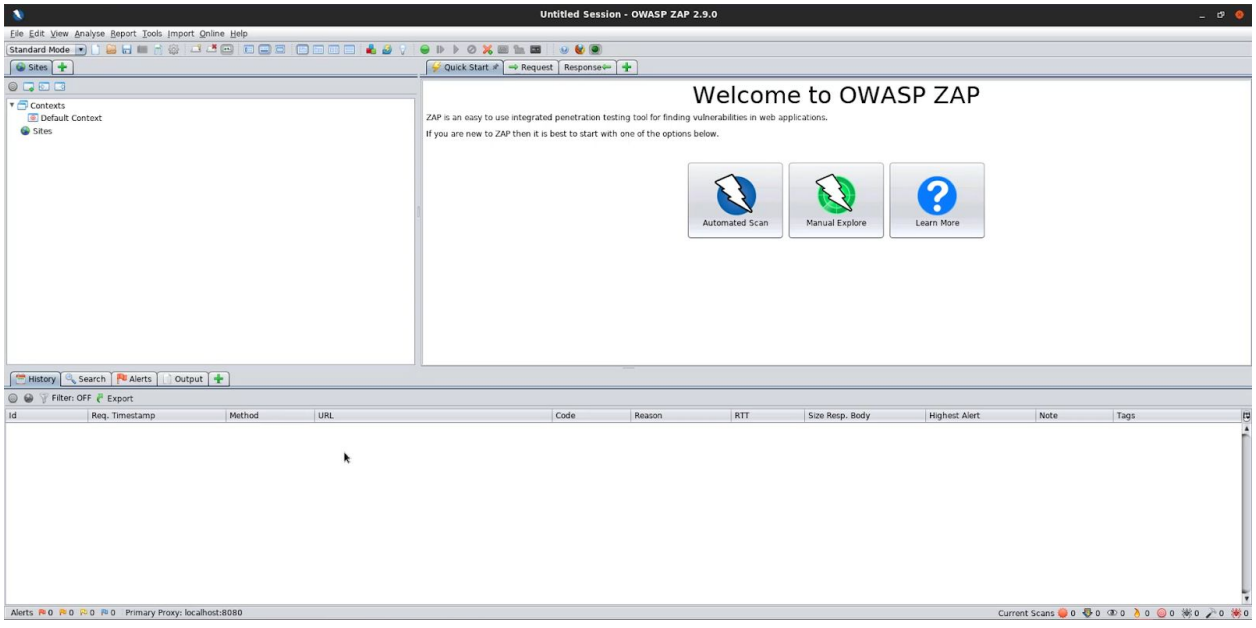
Commands:
ls -l ~/.ZAP/fuzzers/dirbuster
cp /usr/share/wordlists/dirb/common.txt ~/.ZAP/fuzzers/dirbuster/

```
root@attackdefense:~#
root@attackdefense:~# ls -l ~/.ZAP/fuzzers/dirbuster/
total 1764
-rw-r--r-- 1 root root 1802691 Feb 19 12:03 directory-list-1.0.txt
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# cp /usr/share/wordlists/dirb/common.txt ~/.ZAP/fuzzers/dirbuster/
root@attackdefense:~#
root@attackdefense:~#
```

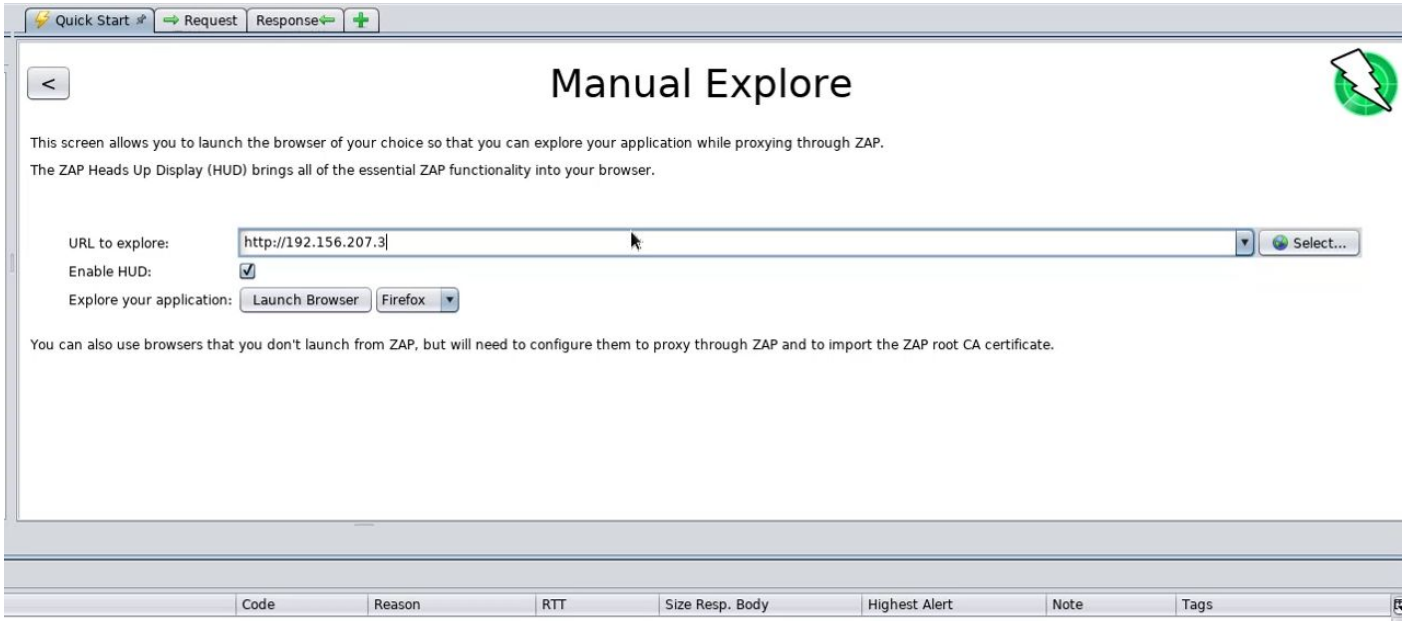
Step 4: Starting ZAProxy. Click on the Menu, Navigate to "Web Application Analysis" and click on "owasp-zap".



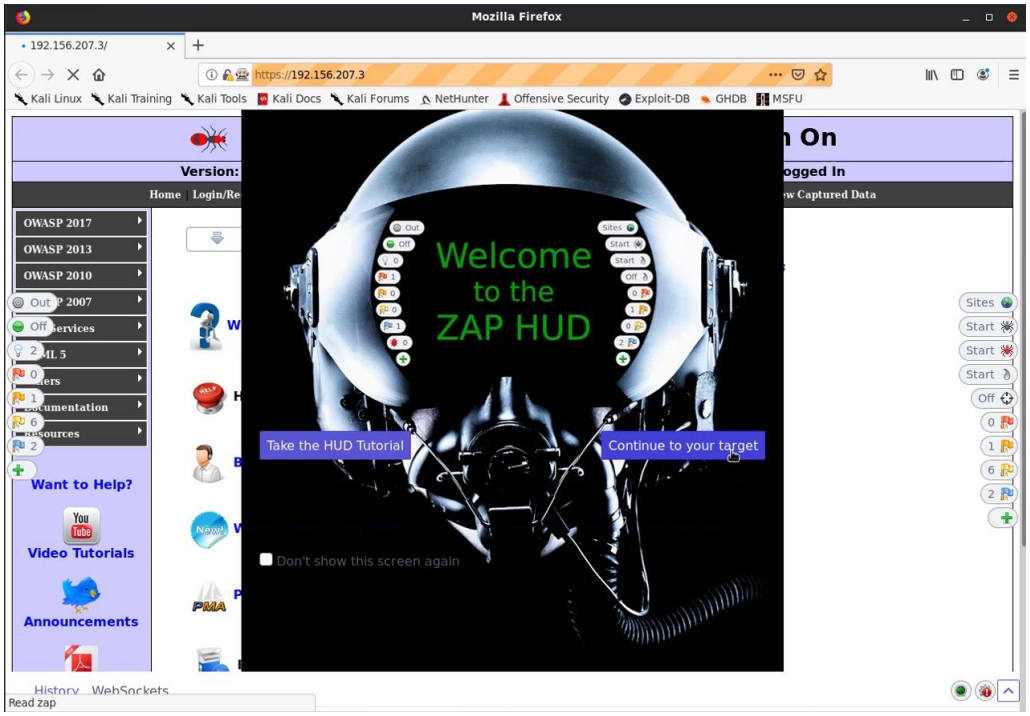
ZAP:



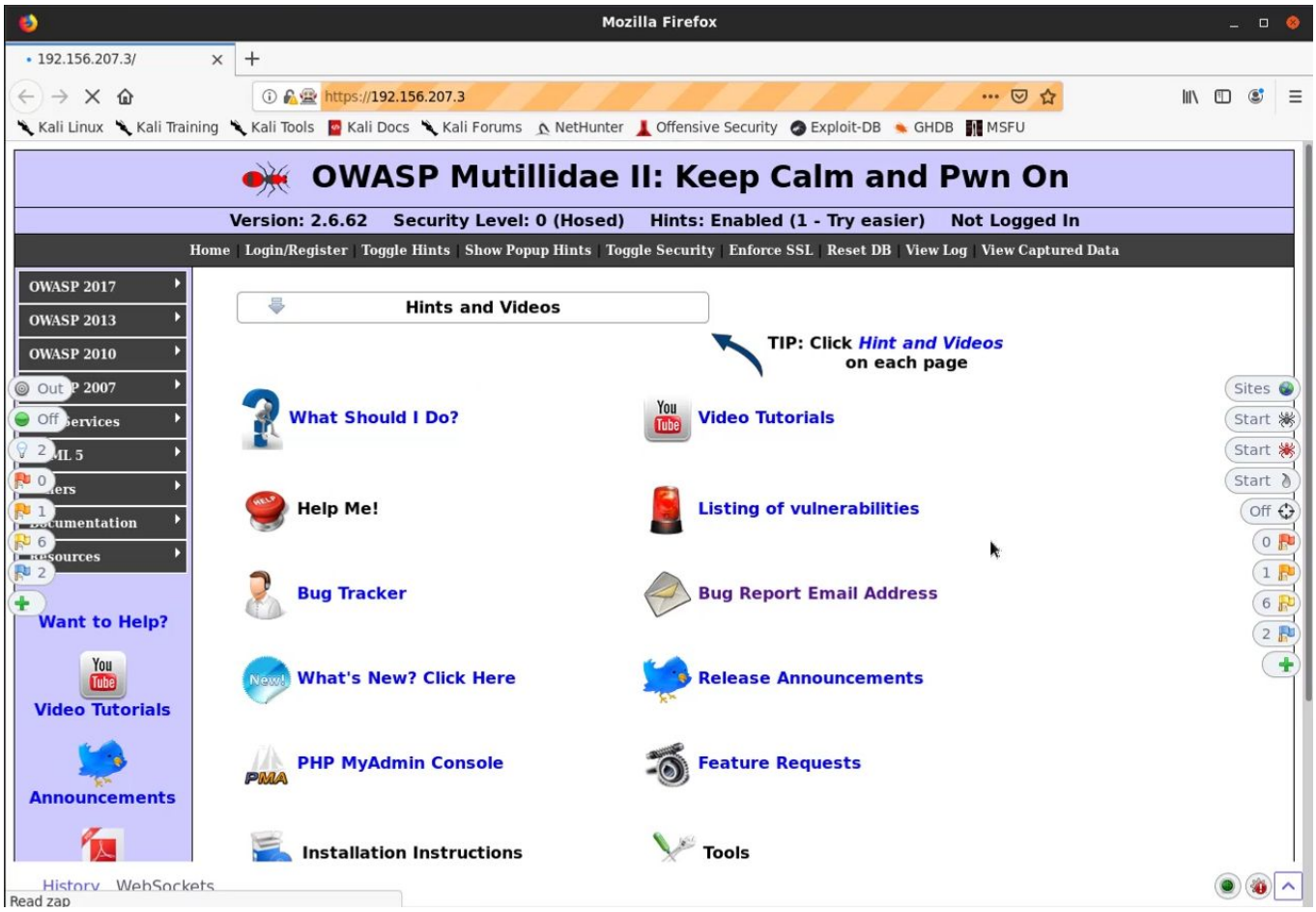
Step 5: Click on "Manual Explore", enter the target IP address in the Input field and click on "Launch Browser".



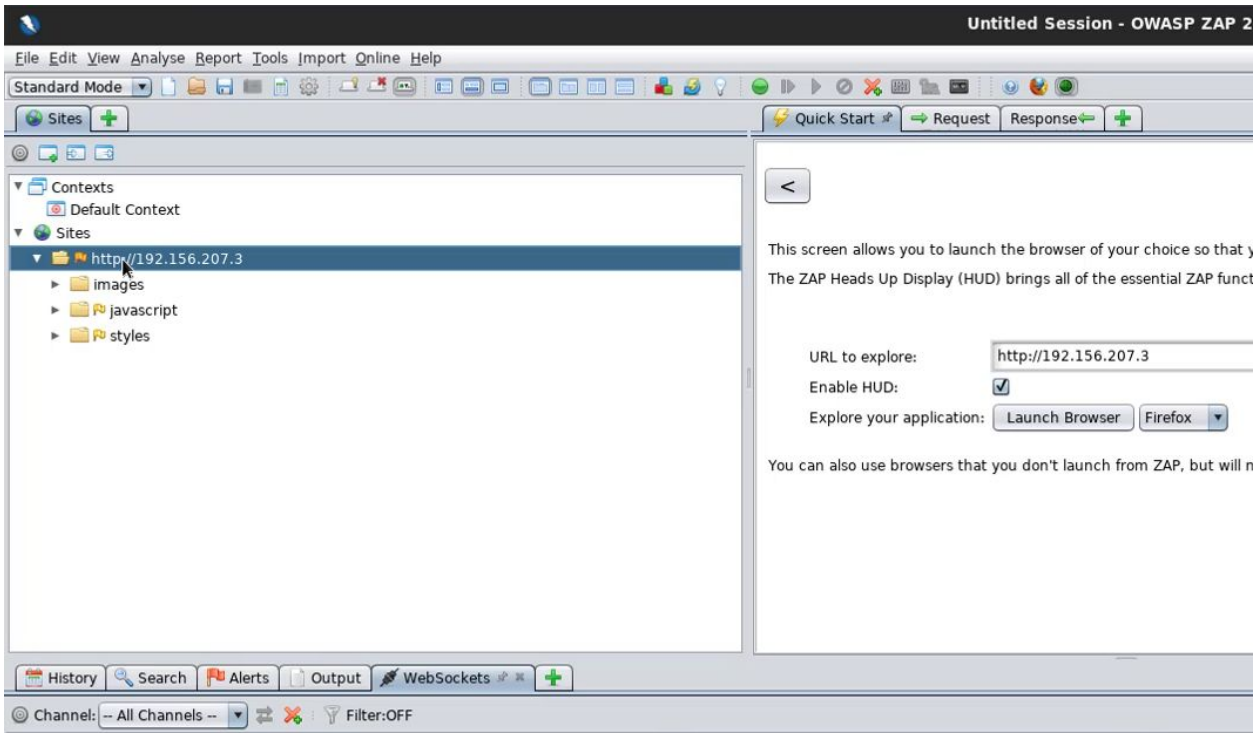
A browser session will be started with ZAP HUD.



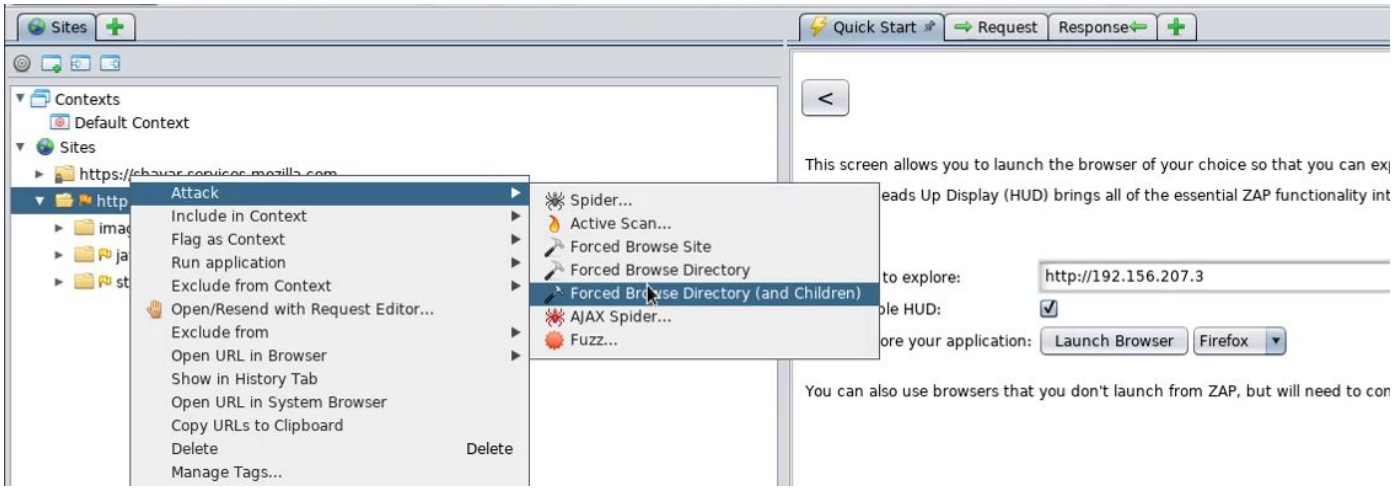
Step 6: Click on "Continue to your target".



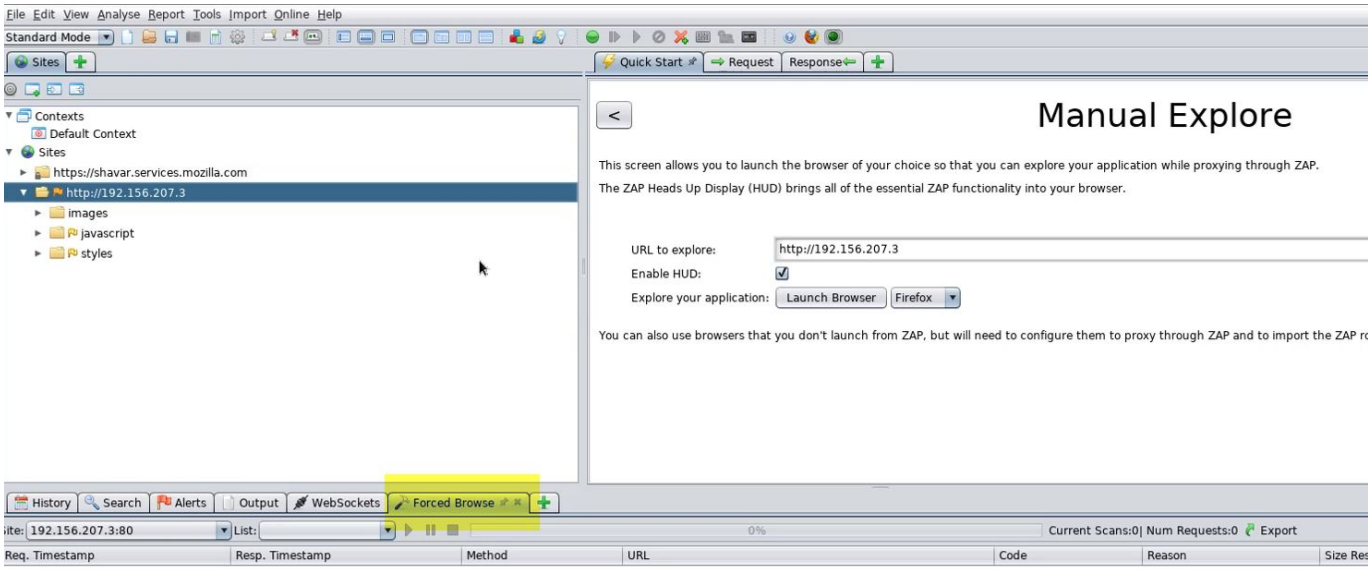
Upon visiting the website, the website will be added to the Site map.



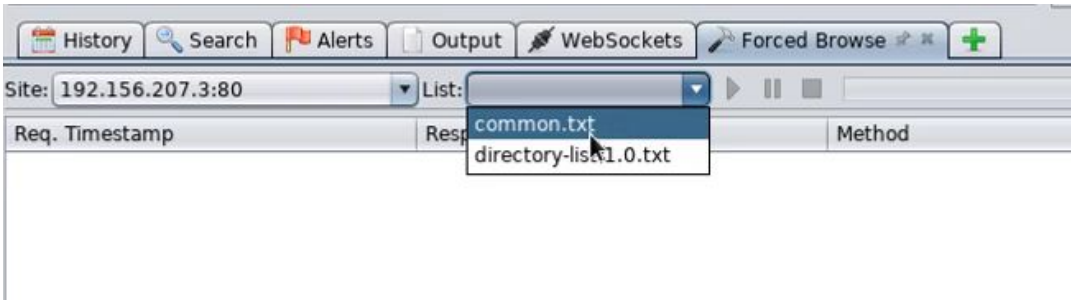
Step 7: Right Click on the target site under Sites, navigate to Attack and click on "Forced Browse Directory" .



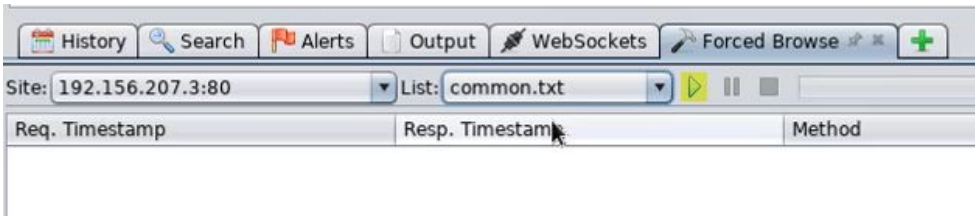
A new tab will appear on the bottom window:



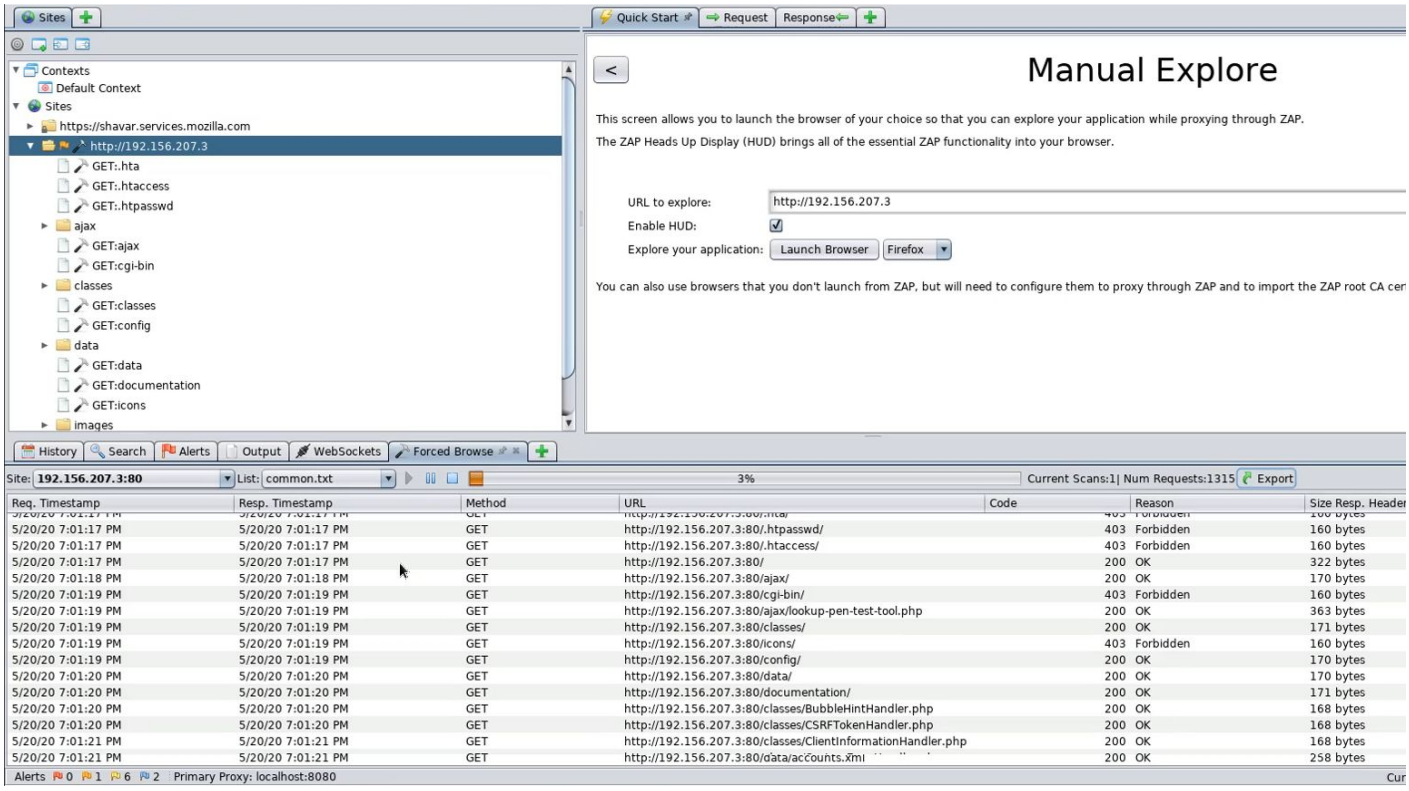
Step 8: Click on the List dropdown and select the common.txt wordlist.



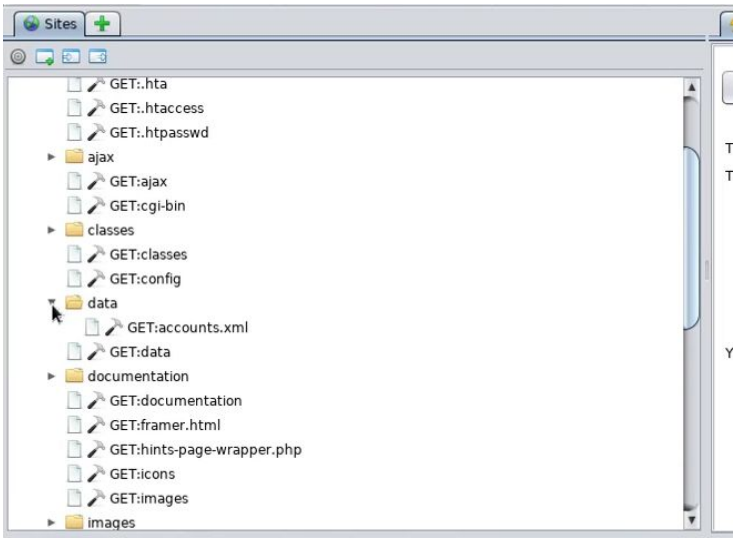
Step 9: Start the attack by clicking the play button.



The scan will start and the found directories and files will be added to the sitemap.

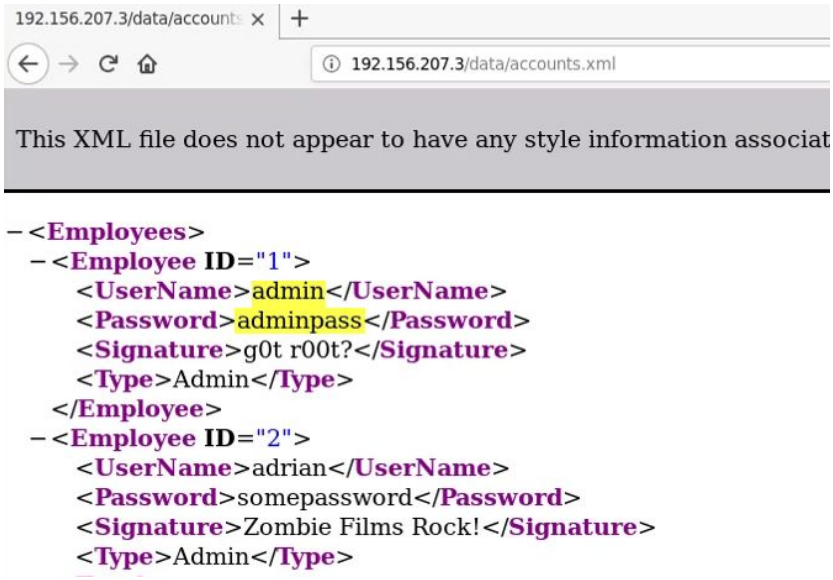


Step 10: After the scan completes, expand the directories. Check the files in data folder.



Step 11: Access the "data" directory in the browser.

Step 12: Click on the "accounts.xml" file.



The login credentials were revealed.

References:

1. OWASP Zed Attack Proxy (https://www.zaproxy.org/)
2. Mutillidae II (https://sourceforge.net/projects/mutillidae/)