

[illegible]

Name	Active Crawling with ZAPProxy
URL	https://attackdefense.com/challengedetails?cid=1890
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 active crawling on the web application with ZAPProxy

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.

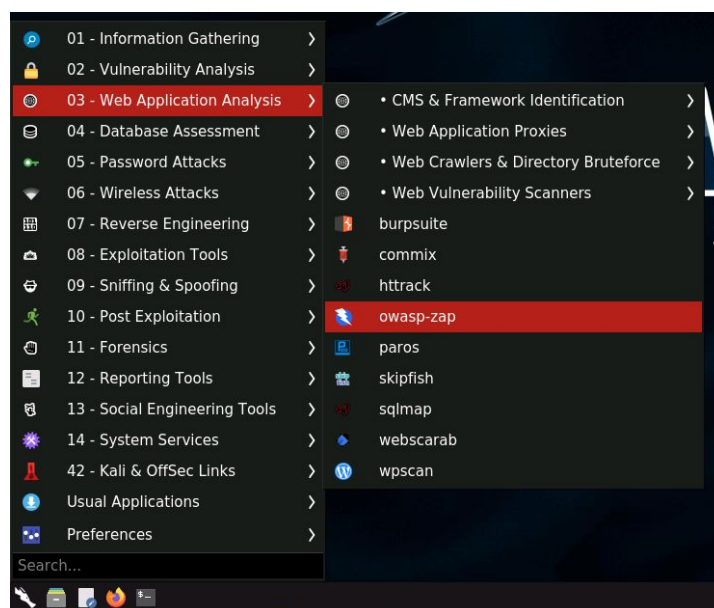
Command: nmap 192.156.207.3

```
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)

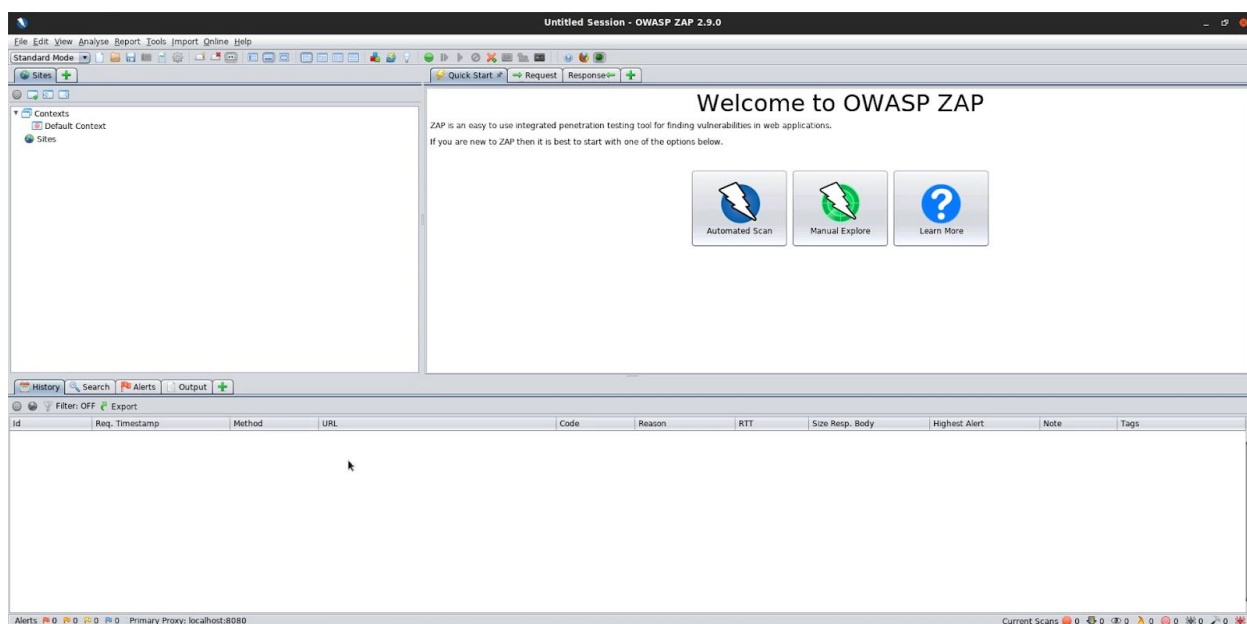
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open.

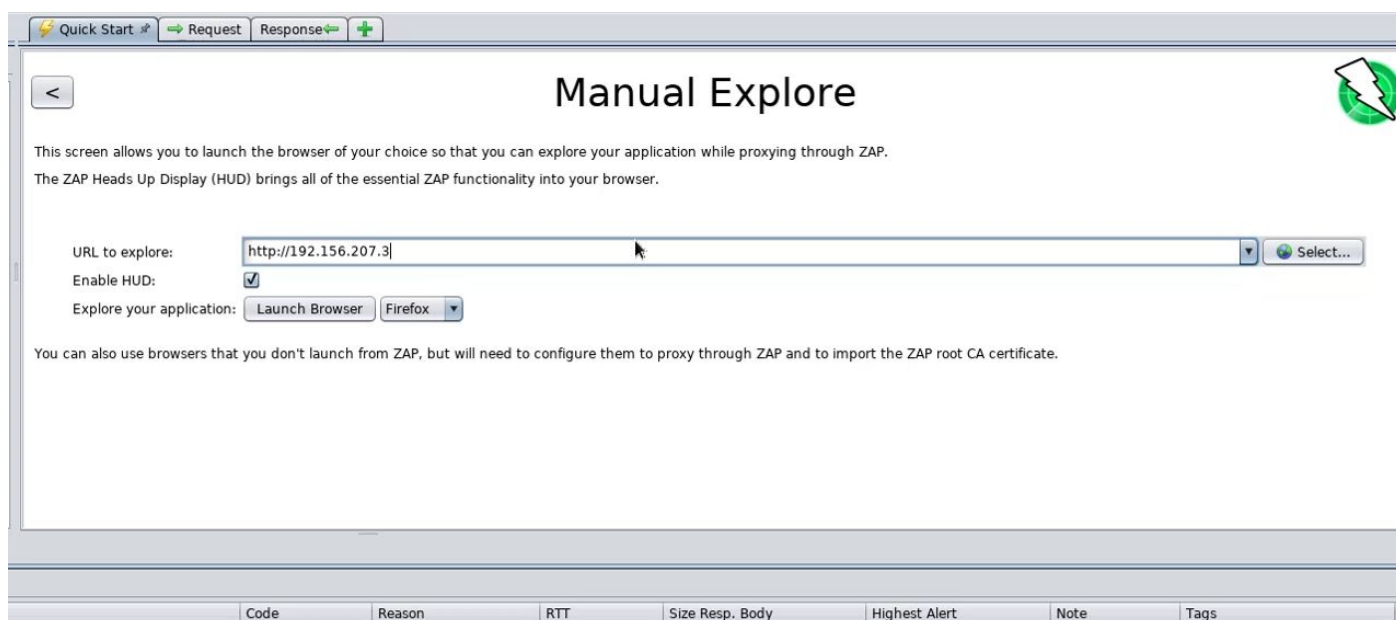
Step 3: Starting Burp Suite. Click on the Menu, Navigate to "Web Application Analysis" and click on "owasp-zap".



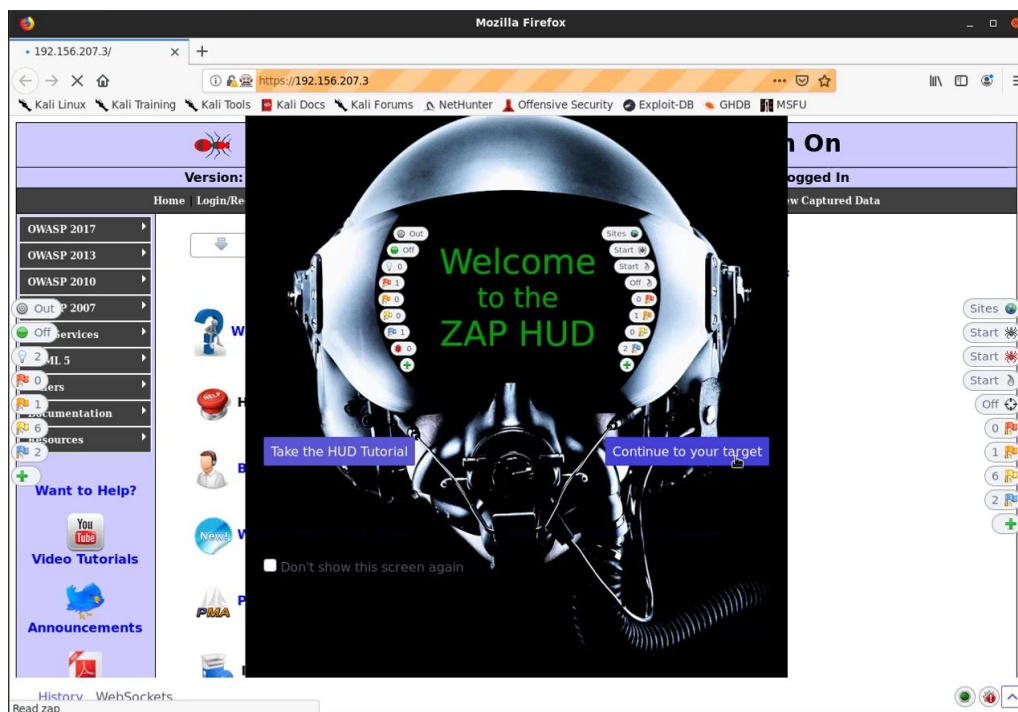
ZAP:



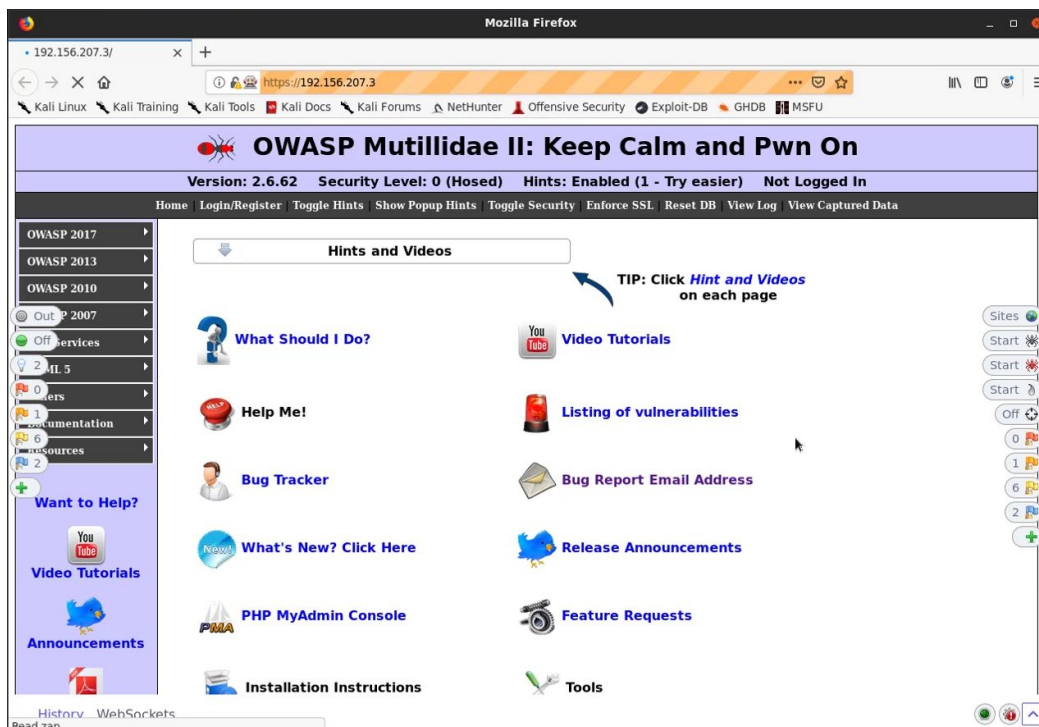
Step 4: Click on "Manual Explore", enter the target IP address in the Input field and click on "Launch Browser".



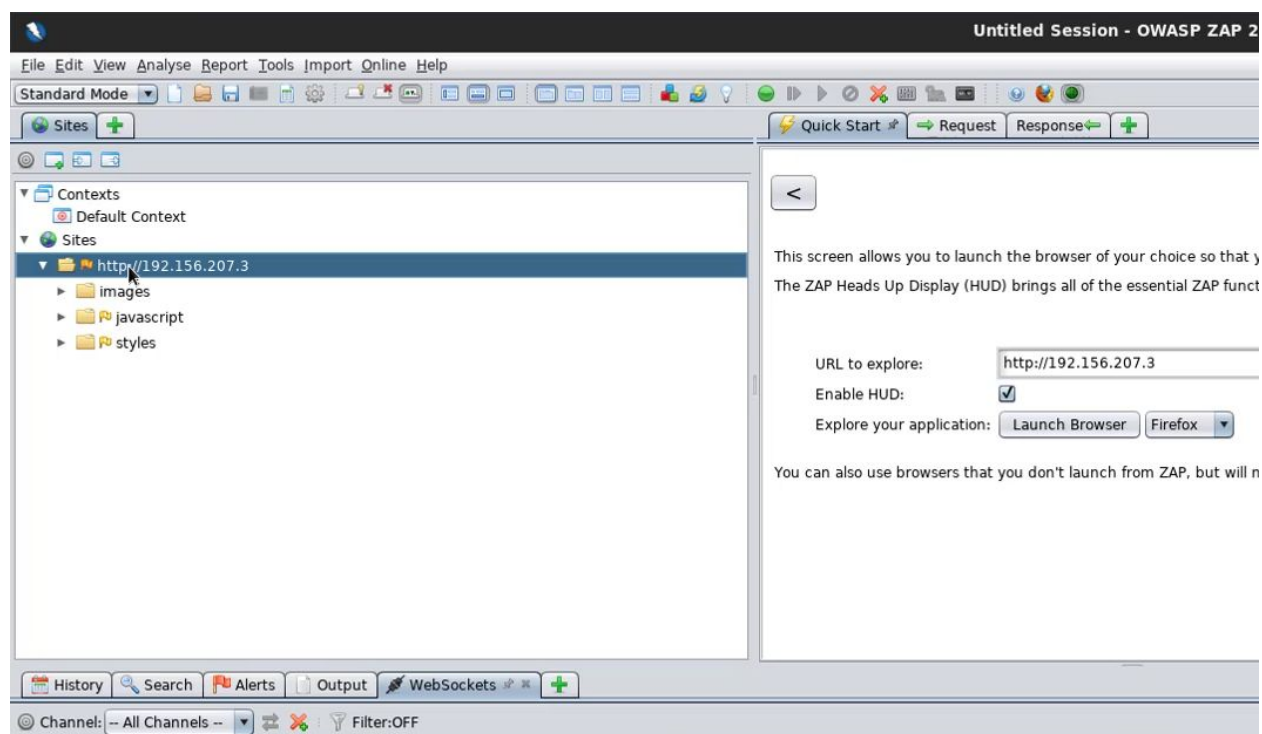
A browser session will be started with ZAP HUD.



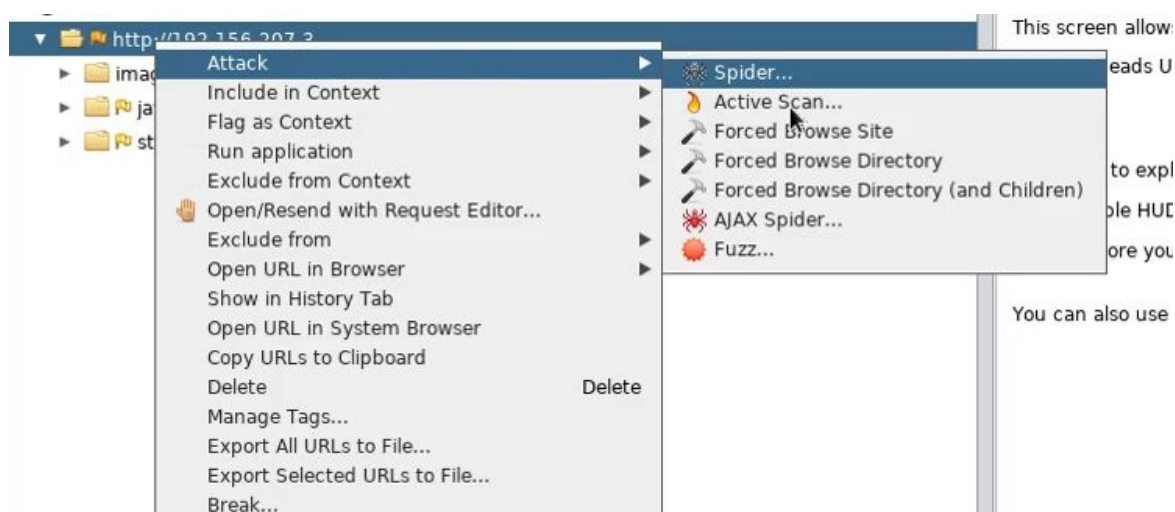
Step 5: Click on "Continue to your target".



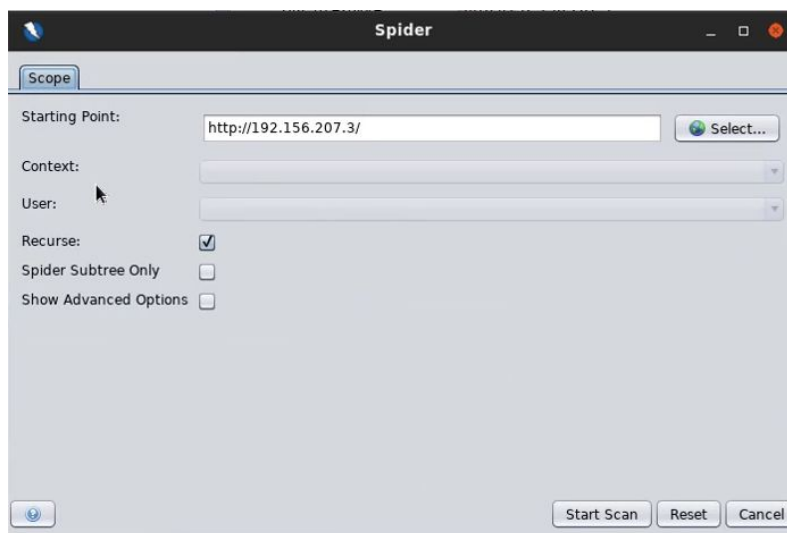
Upon visiting the website, the website will be added to the Site map.



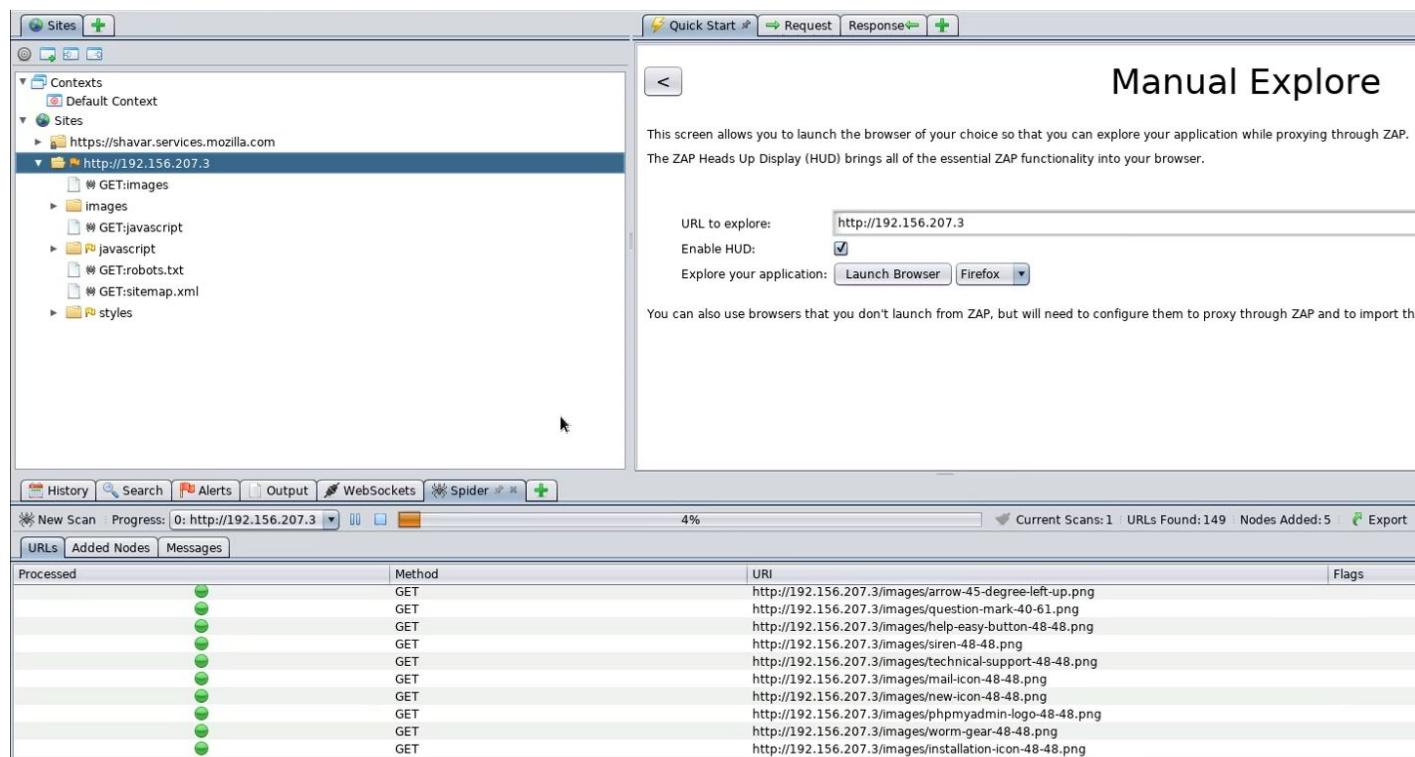
Step 6: Right Click on the target site under Sites, navigate to Attack and click on "Spider" .



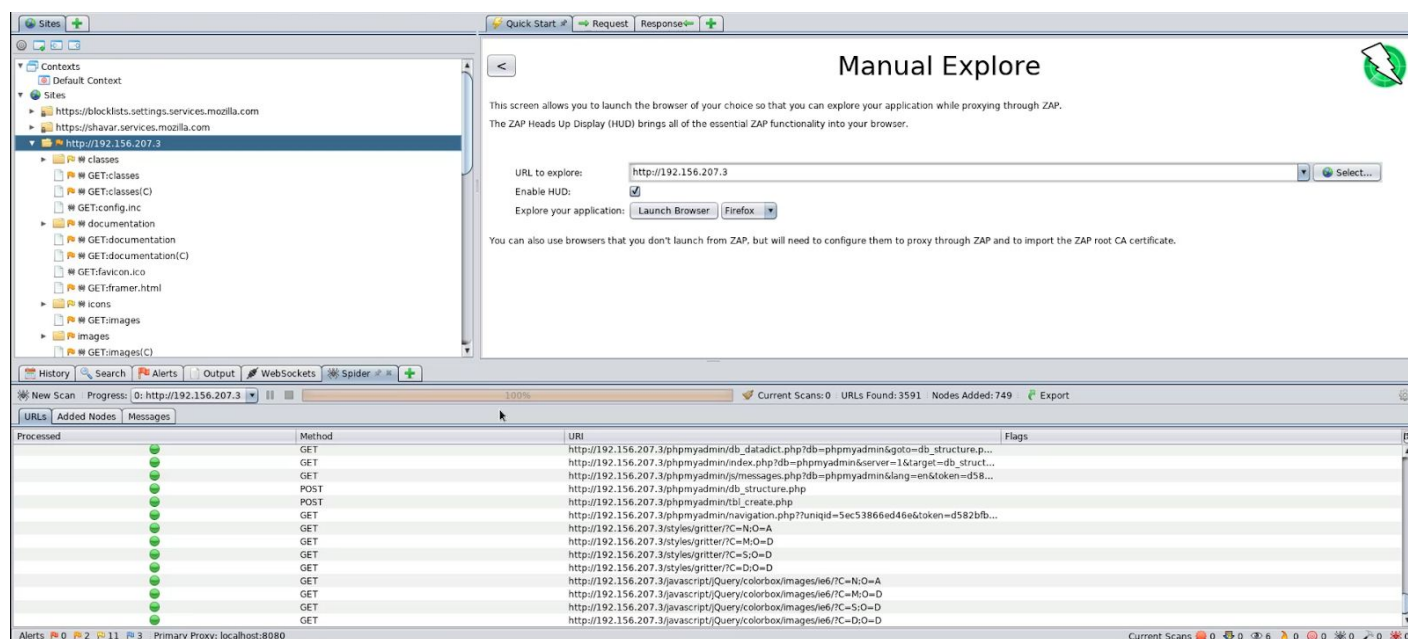
A dialog box will appear



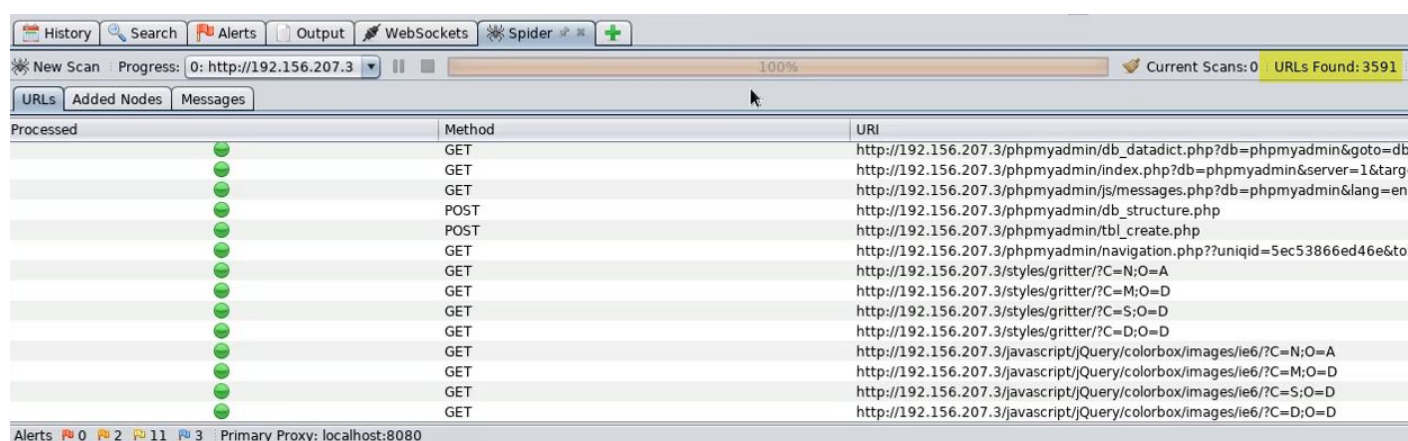
Step 7: Click on the "Start Scan" button and ZAP will start crawling the web pages.



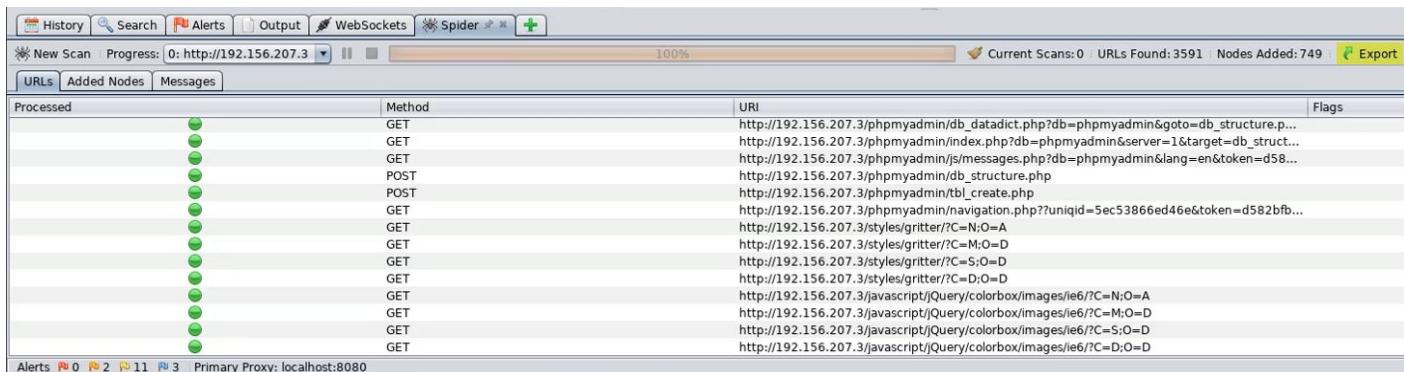
The crawled web pages and files will appear on the sitemap.



Total: 3591 URLs were found.

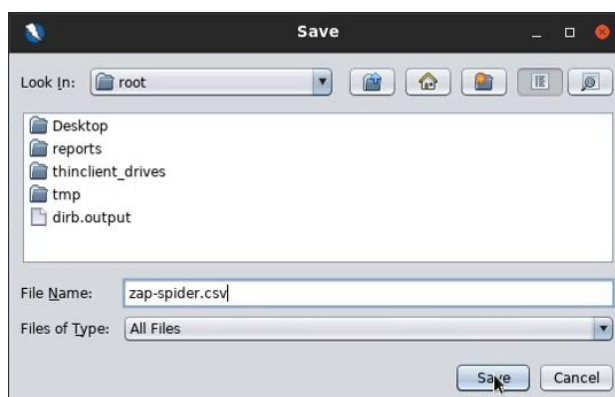


Step 8: After all the pages are crawled, Click on the Export Button.



Processed	Method	URI	Flags
●	GET	http://192.156.207.3/phpmyadmin/db_datadict.php?db=phpmyadmin&goto=db_structure.p...	
●	GET	http://192.156.207.3/phpmyadmin/index.php?db=phpmyadmin&server=1&target=db_struct...	
●	GET	http://192.156.207.3/phpmyadmin/js/messages.php?db=phpmyadmin&lang=en&token=d58...	
●	POST	http://192.156.207.3/phpmyadmin/db_structure.php	
●	POST	http://192.156.207.3/phpmyadmin/tbl_create.php	
●	GET	http://192.156.207.3/phpmyadmin/navigation.php?uniqid=5ec53866ed46e&token=d582bfb...	
●	GET	http://192.156.207.3/styles/gritter/?C=N;O=A	
●	GET	http://192.156.207.3/styles/gritter/?C=M;O=D	
●	GET	http://192.156.207.3/styles/gritter/?C=S;O=D	
●	GET	http://192.156.207.3/styles/gritter/?C=D;O=D	
●	GET	http://192.156.207.3/javascript/Query/colorbox/images/ie6/?C=N;O=A	
●	GET	http://192.156.207.3/javascript/Query/colorbox/images/ie6/?C=M;O=D	
●	GET	http://192.156.207.3/javascript/Query/colorbox/images/ie6/?C=S;O=D	
●	GET	http://192.156.207.3/javascript/Query/colorbox/images/ie6/?C=D;O=D	

Step 9: Enter a filename ("zap-spider.csv") and save the output.



Upon successful export the following message will appear.



Step 10: View the saved file.

Command: cat zap-spider.csv

