1 Web Application Testing

In Web application testing, we have to test the DVWA to check weather we can find any vulnerabilities through sql injection or XSS.

First, open a url http://127.0.0.1/DVWA and set the security as low and later you can test different attack methods such as sql injection, Xss.

I used the tools to test the DVWA i.e Burp suite, SQLmap, OWASP ZAP and nikto.

1.1 Recon using Nikto

Use the command in your kali linux as

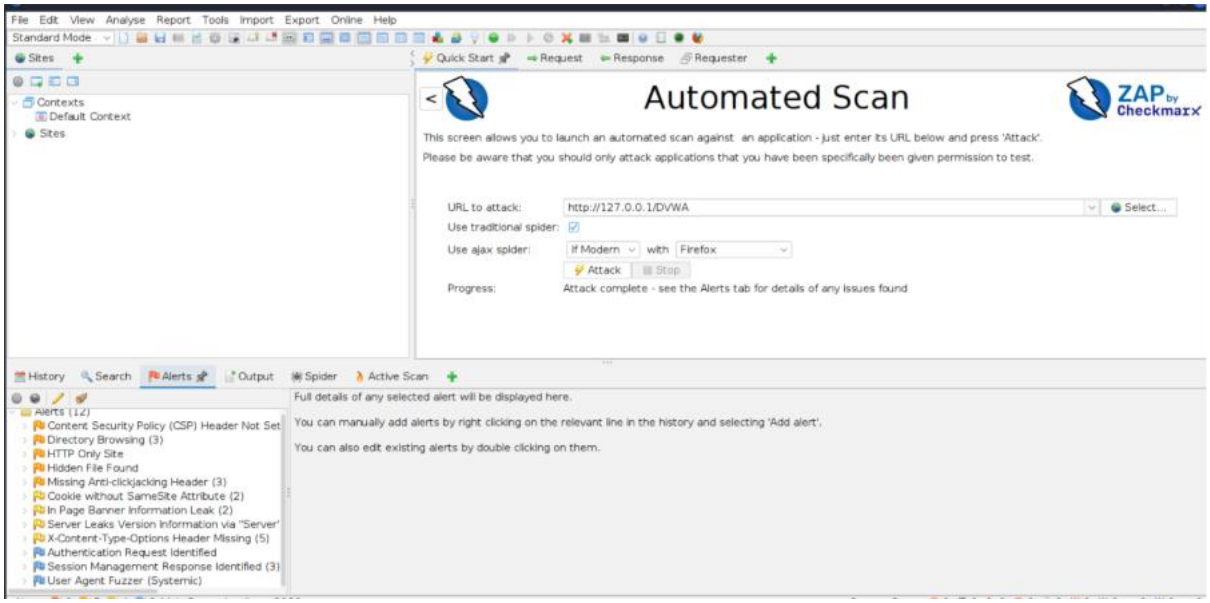
nikto -h http://127.0.0.1/DVWA -output DVWA.txt

1.2 Recon using OWASP ZAP

First, we have to setup the OWASP ZAP by downloading it in the browser and then install in your kali linux through the official website as

https://www.zaproxy.org/

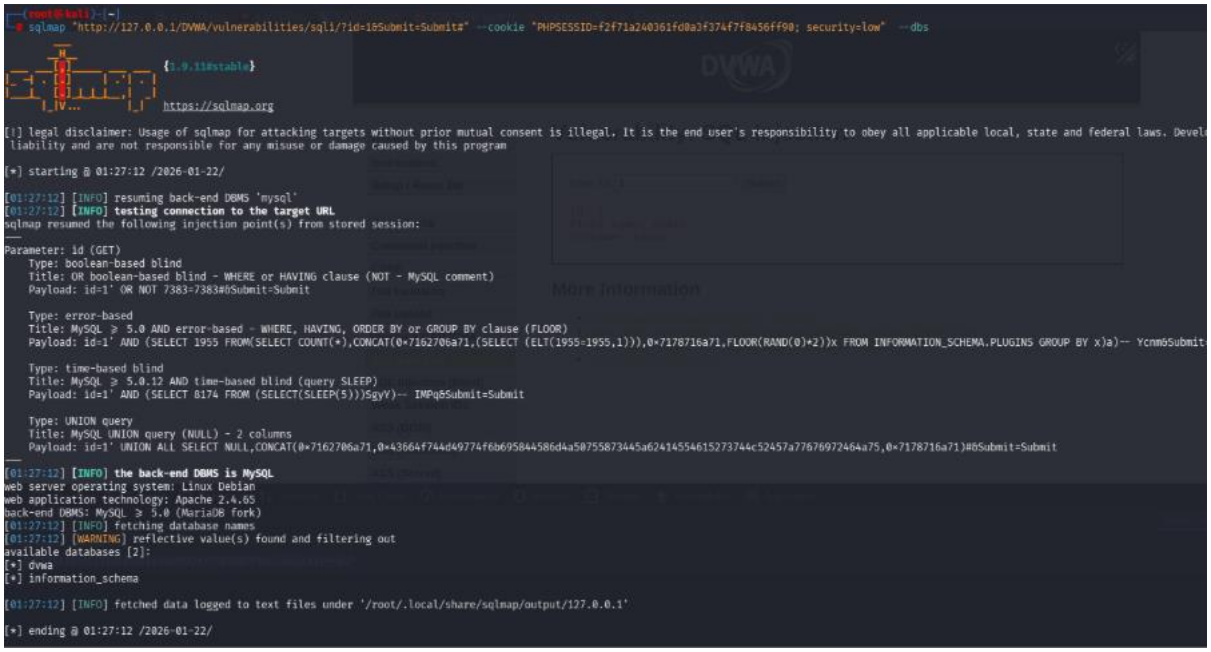
Scan the taget url such as http://127.0.0.1/DVWA in OWASP ZAP



1.3 Automated Testing for SQLi

Using the sqlmap we have to test the DVWA to check whether the databases are found or not by using the following command as

sqlmap "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "PHPSESSID=f2f71a240361fd0a3f374f7f8456ff90; security=low" --dbs

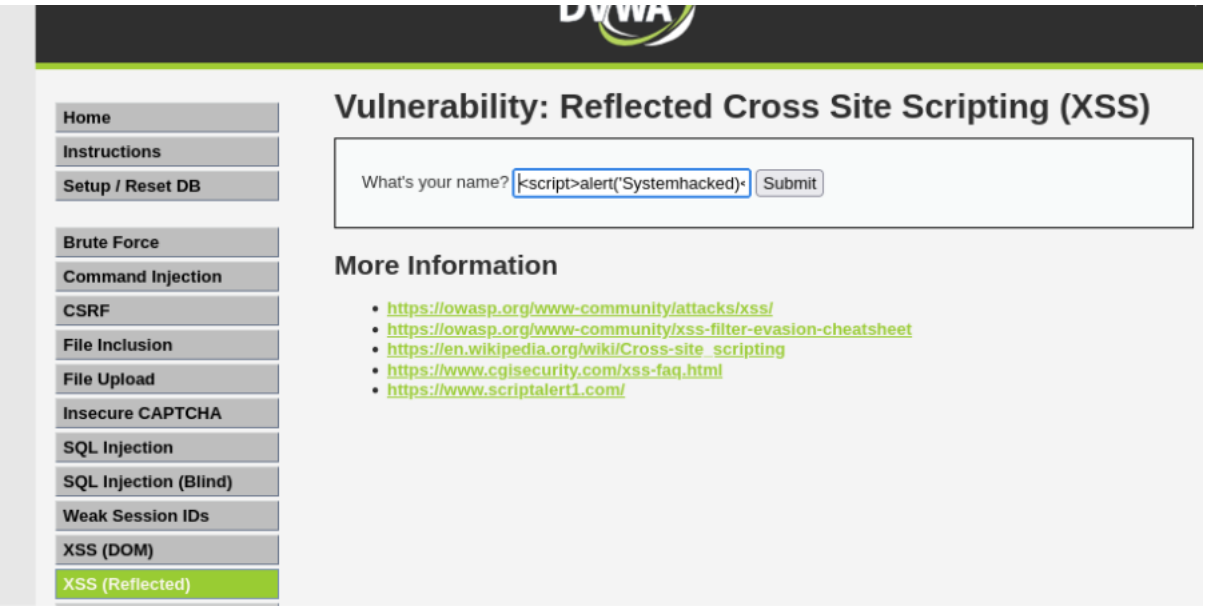


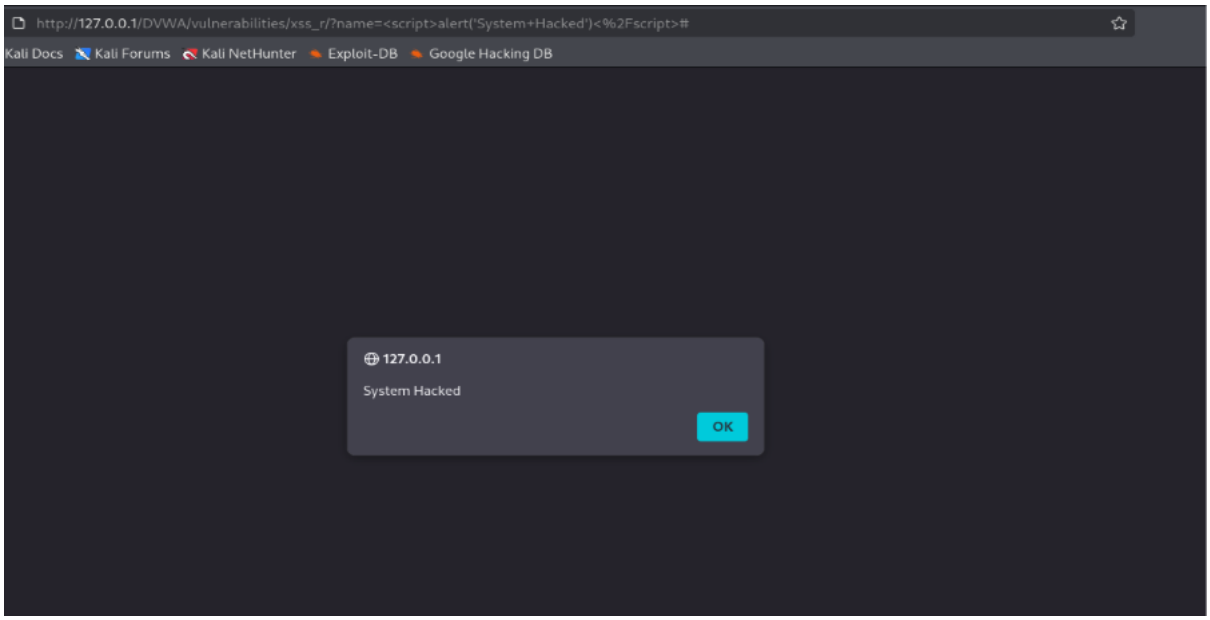
In the above results, we have identified the two databases found such as dvwa and information_schema.

1.4 Automated Testing for XSS

We have to use the automated script in the XSS section in DVWA and the query as

<script>alert('System Hacked')</script>





1.5 Manual Testing for SQLi

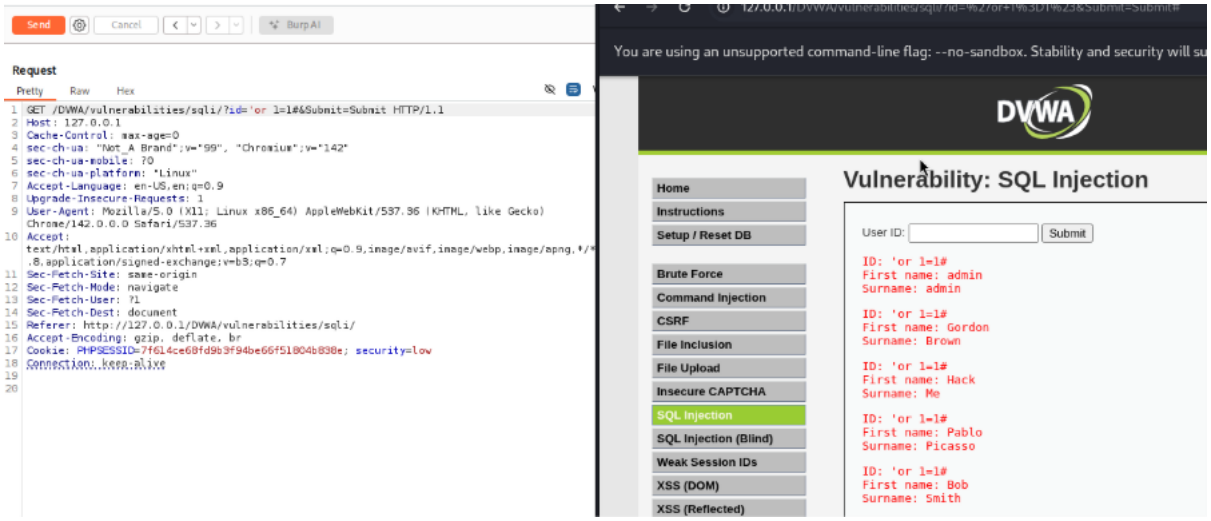
Using the Burp suite we have to capture the http request and changing the id and upload the SQL query in the request and then forward to the browser.

Configure the browser to use burp suite as proxy

Login to 'DVWA' and go to Sql injection section and then enter '1' and submit

Capture the url and send the http request to repeater in Burpsuite

In repeater change the id to an SQl query as ‘or 1=1# and later forward that request in to the browser.



1.6 Manual Testing for XSS

First, configure the bowser to Burp suite as proxy and then login to ‘DVWA’.

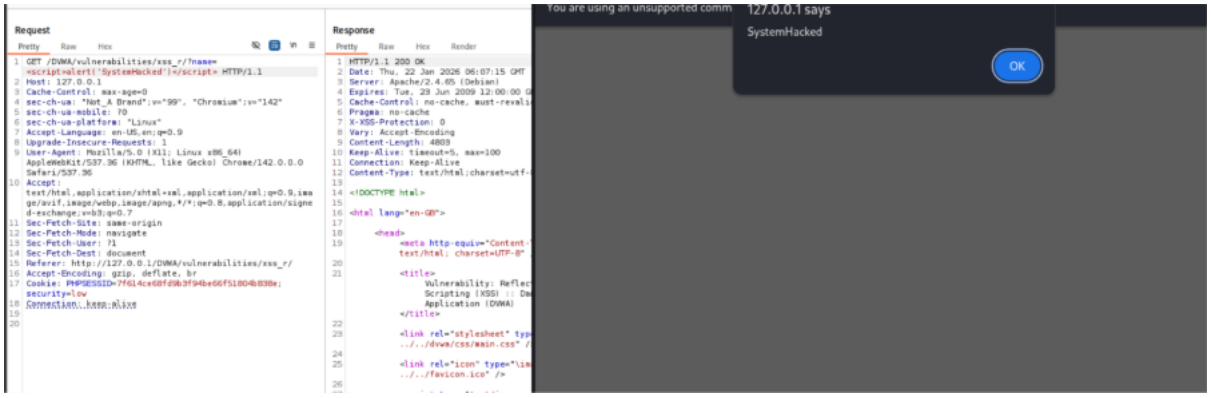
Go to XSS (Reflected) section and enter any text and later copy the url and send it in Burp

In Burp , capture the request and send it to the repeater

In repeater, change the name and enter the script which i provided in the below

<script>alert(‘SystemHacked’)</script>

Then, forward the request to the browser



TEST ID	VULNERABILITY	SEVIERITY	TARGET URL
001	SQL injection	Critical	http://127.0.0.1/DVWA/vulnerabilities/sqli/
002	XSS Reflected	Medium	http://127.0.0.1/DVWA/vulnerabilities/xss_r/