# Lab 13 – Automating SQL injection using SQLmap and Cross site Scripting (XSS)

**CYSE 450- Ethical Hacking and Penetration Testing**

**(Total: 100 Points)**

SQLmap is an open-source tool used as part of a penetration test to detect and exploit injection flaws. SQLmap is particularly useful as it saves time by automating the process of detecting and exploiting SQL injection.

**Lab Tool:**

Reliable internet connection, Metasploitable2 and Kali Linux.

## Task-A: (60 Points) Using SQLmap to automate SQL injection to Obtain data from DVWA Application.

1. Open terminal in Kali Linux
2. Login to Metasploitable2 VM and find the IP address.
3. In the browser, in Kali VM, type the Ip address of metasploitable2 and login to DVWA application.
4. Set the" DVWA Security" to "low", Select "SQL Injection" tab and type"1" in the User Id box. Hit the Submit button. **Don't forget to copy the URL after submitting action**. Please submit the screenshot for this step.
5. Use sqlmap tool/command to find the vulnerabilities for SQL injection in the URL copied in the above step. **Highlight** the Vulnerabilities detected for SQL injection. Please submit the screenshot for this step.
6. In Kali terminal, use SQLmap command to display all the tables used by DVWA database. Please submit the screenshot for this step.
7. Use SQLmap command to display all the users along with passwords in plaintext format in "users" table. Please submit the screenshot for this step.

## Task-B: (40 Points) Using Cross Site Scripting to Obtain data from dvwa Database

1. Login to DVWA application and set the "DVWA Security" to "low".

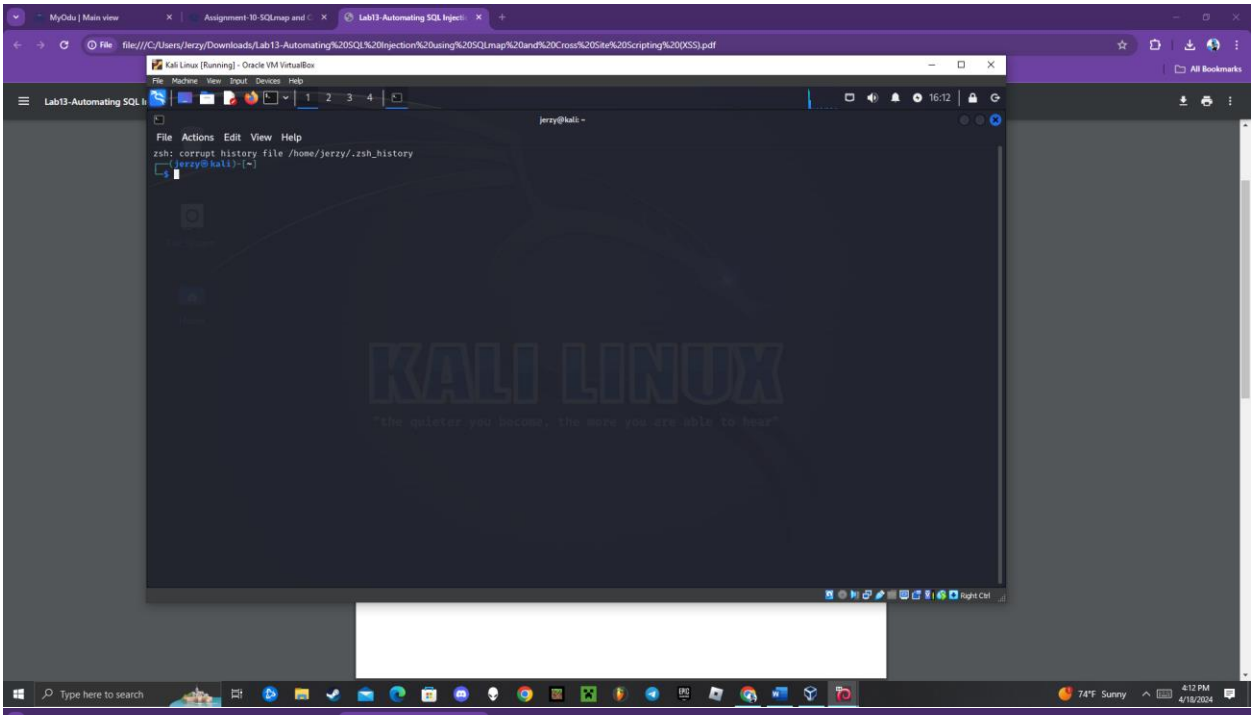
2. Select “XSS refelected” and post a Malicious Message to Display an Alert Window in DVWA application Window by embedding a JavaScript program in the “What is Your name?” field.
3. Post a malicious code to display cookies using **alert(),**as demonstrated in the class.
4. Select “XSS Stored” and in the message box, use **“<script>document.location=Ip-address of DVWA website</script>** to perform DOM based Cross site scripting.

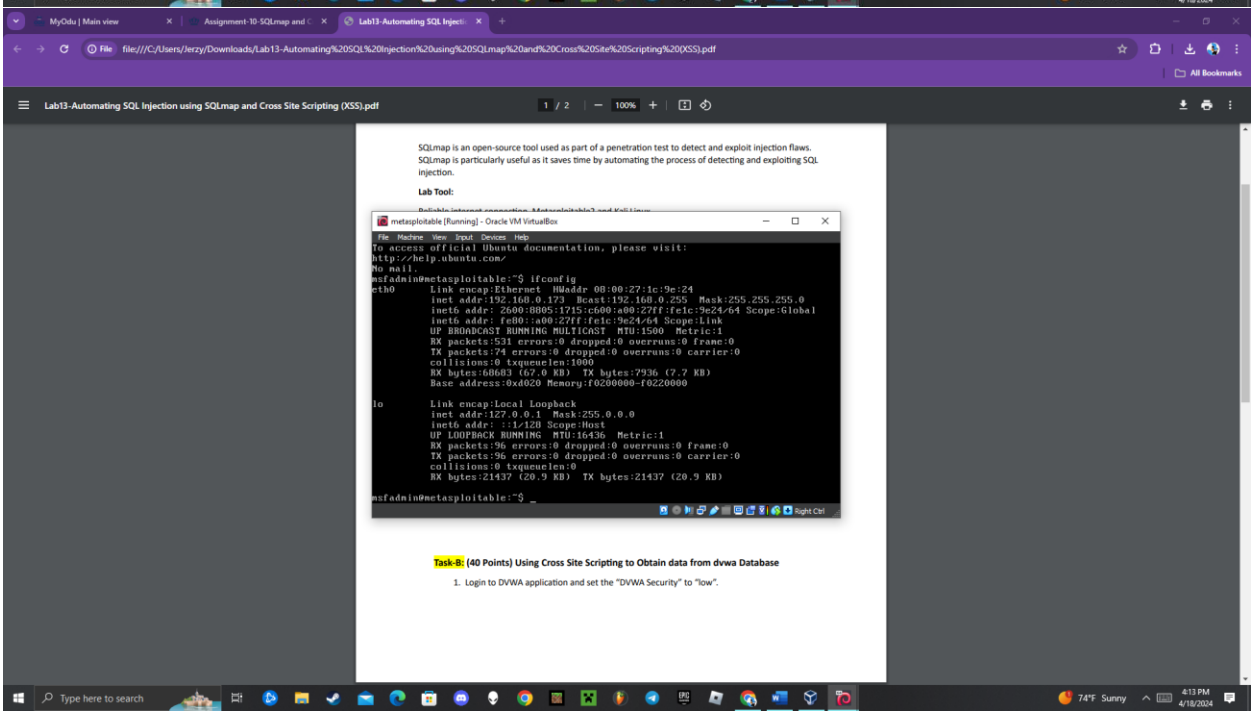
**Extra Credit (20 Points):**

In this task, Steal Cookies from the Victim’s Machine (DVWA application in metasploitable2) so that the attacker (Kali VM) can get access to that.

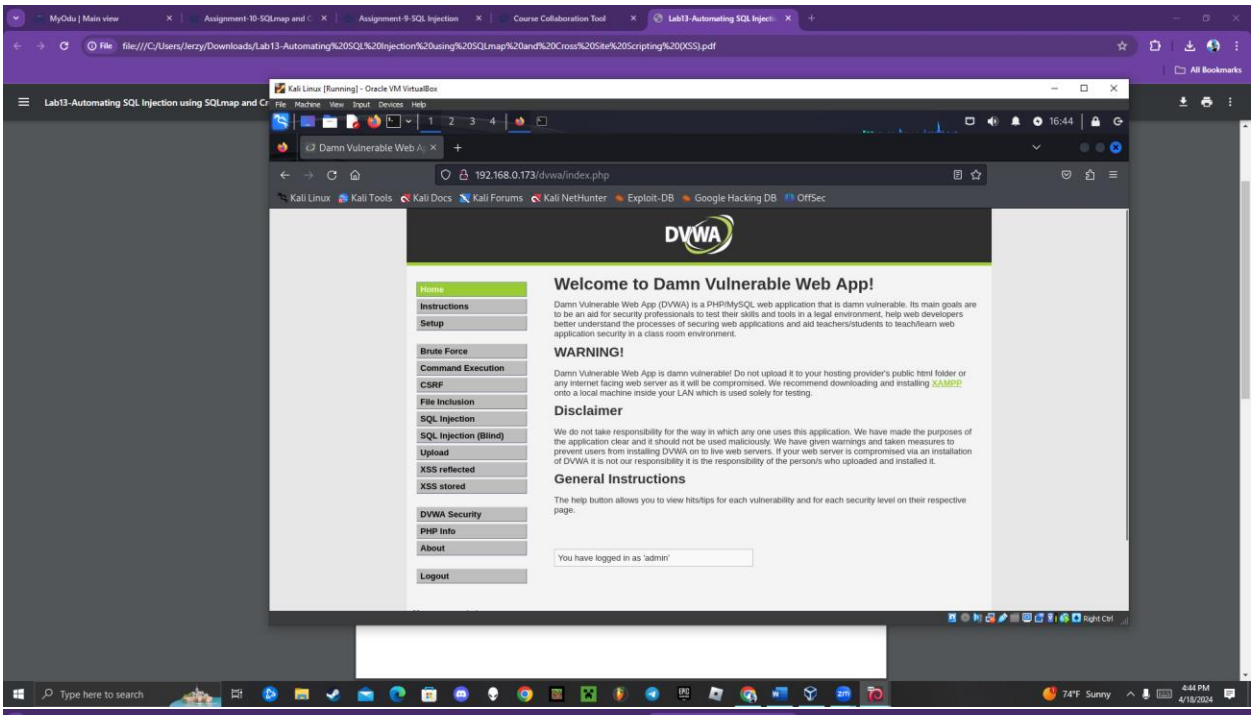
Hint: you can use “nc” tool to listen to the connection at some port (for e.g., 5000) and as soon as the malicious script get executed the cookie information is stored/displayed at attacker terminal listening at post 5000.

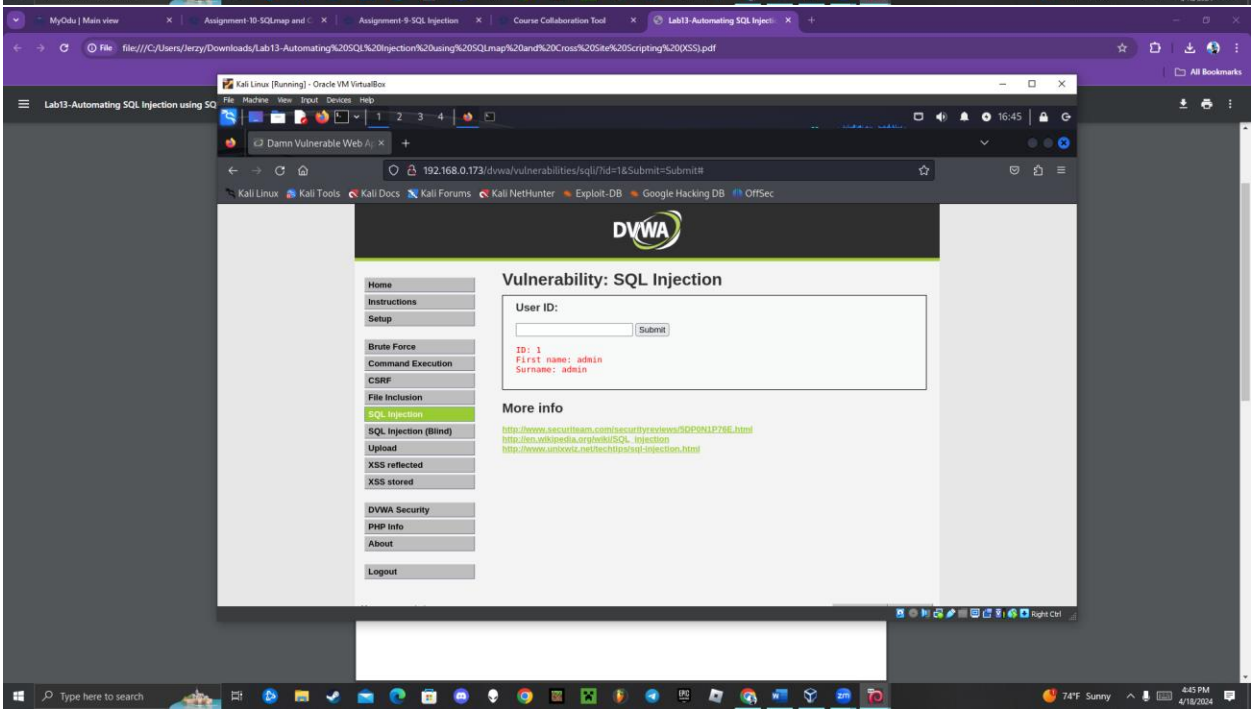
## Task A

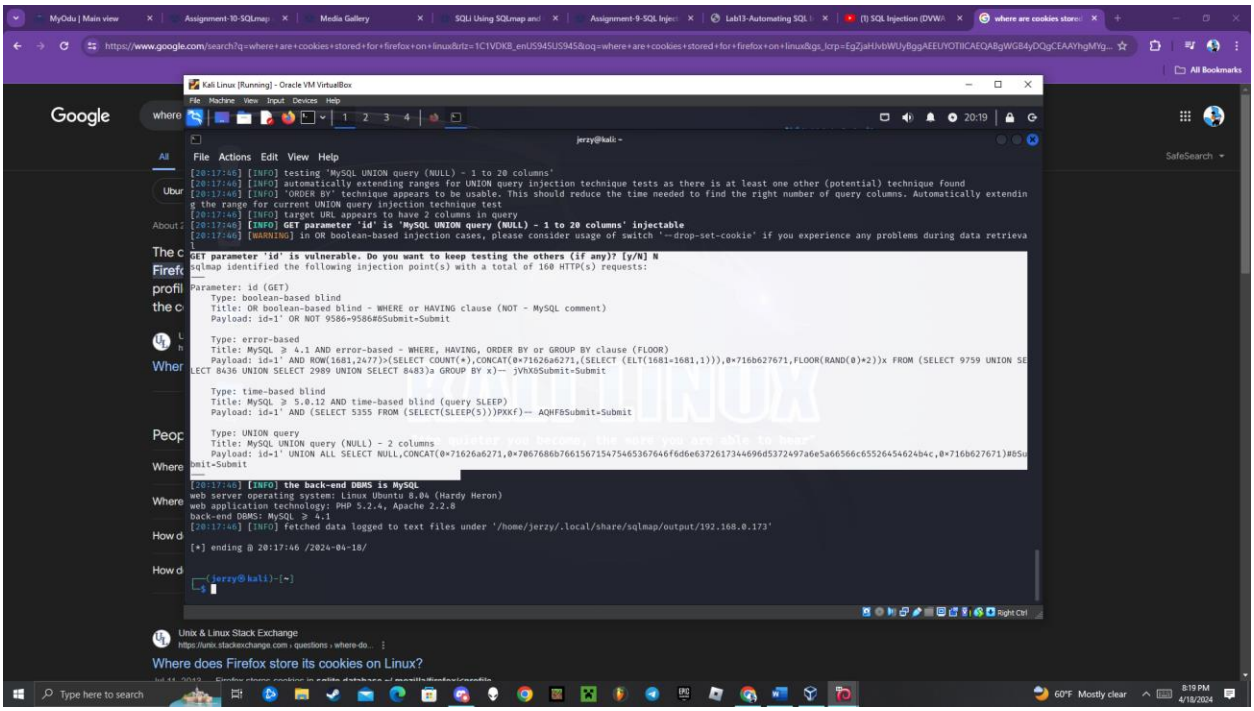
1. 


2. 

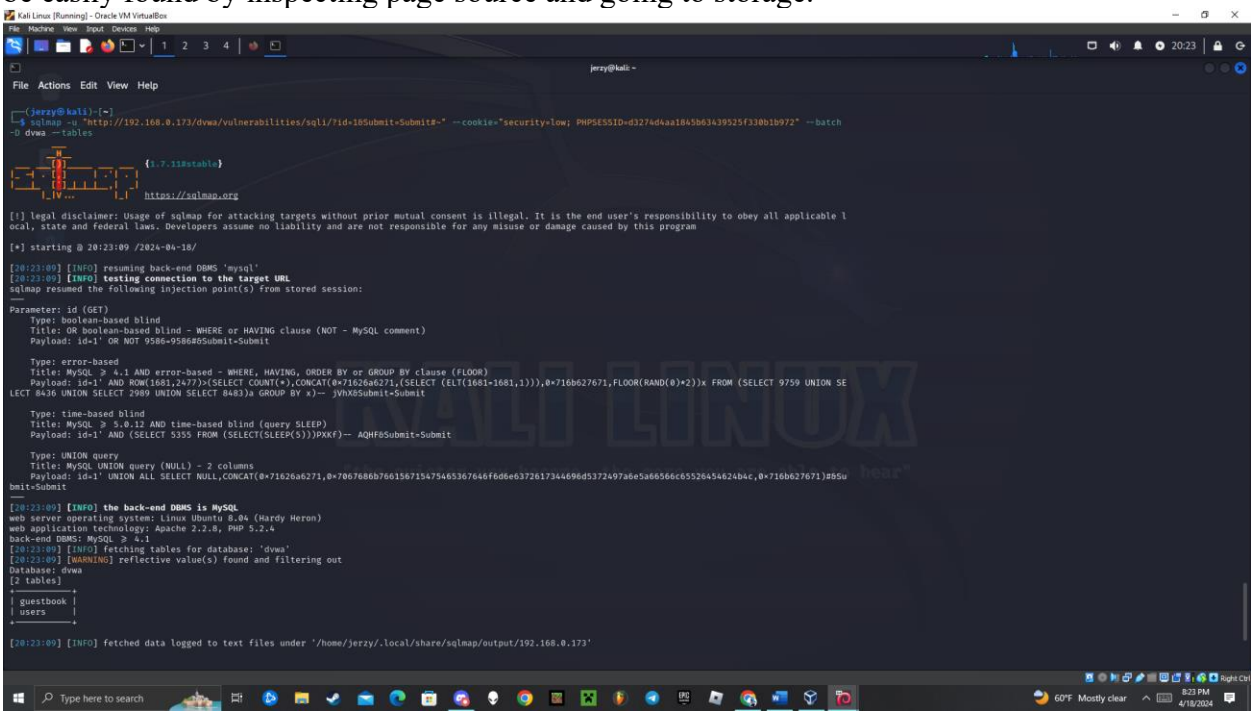

IP is 192.168.0.173.

3. 
Kali Linux [Running] - Oracle VM VirtualBox
Damn Vulnerable Web App
192.168.0.173/dvwa/index.php
DVWA
Welcome to Damn Vulnerable Web App!
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
WARNING!
Disclaimer
General Instructions
You have logged in as 'admin'

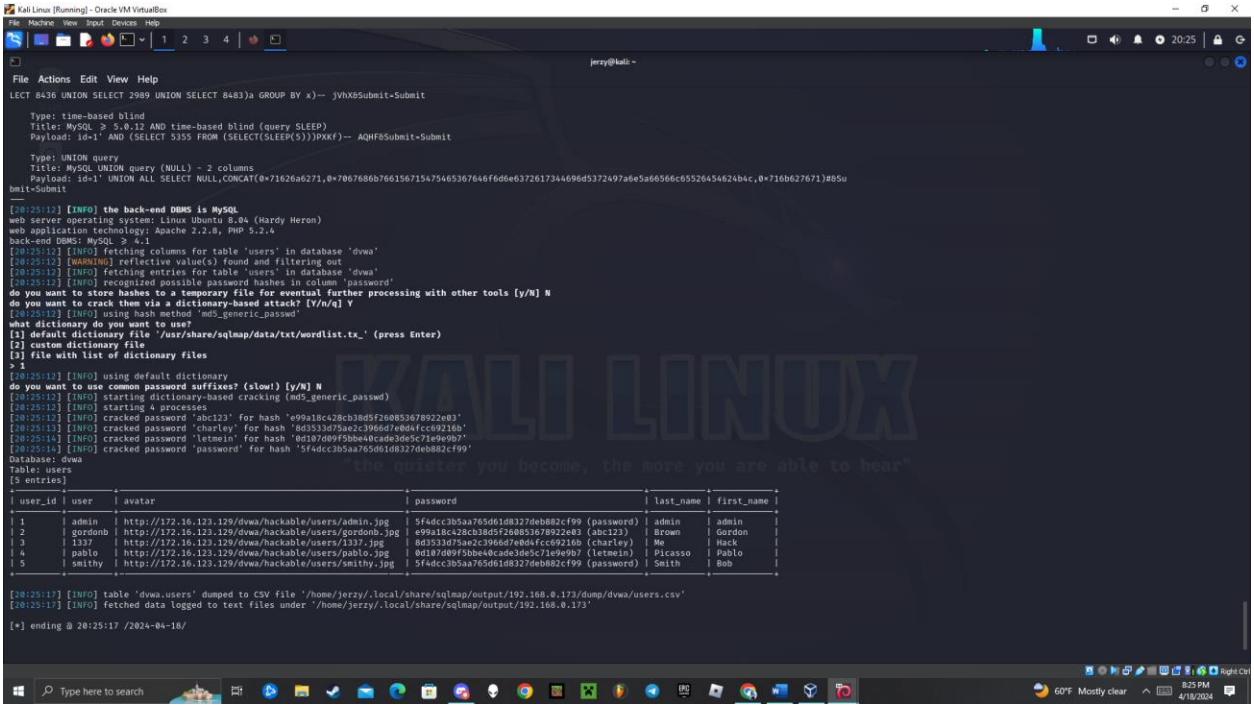
4. 
Kali Linux [Running] - Oracle VM VirtualBox
Damn Vulnerable Web App
192.168.0.173/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
DVWA
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More info
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

5. 


Used sqlmap -u URL –cookie=”security=low; PHPSESSID=cookie” –batch. Cookies can be easily found by inspecting page source and going to storage.

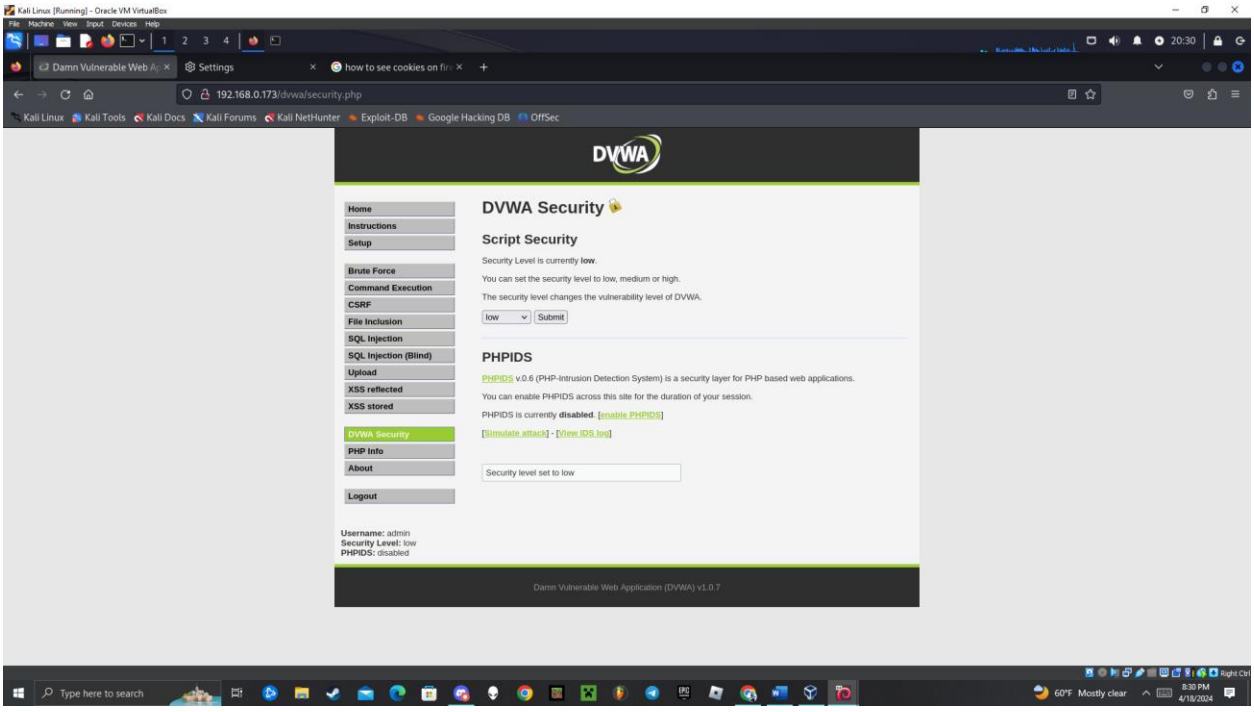
6. 

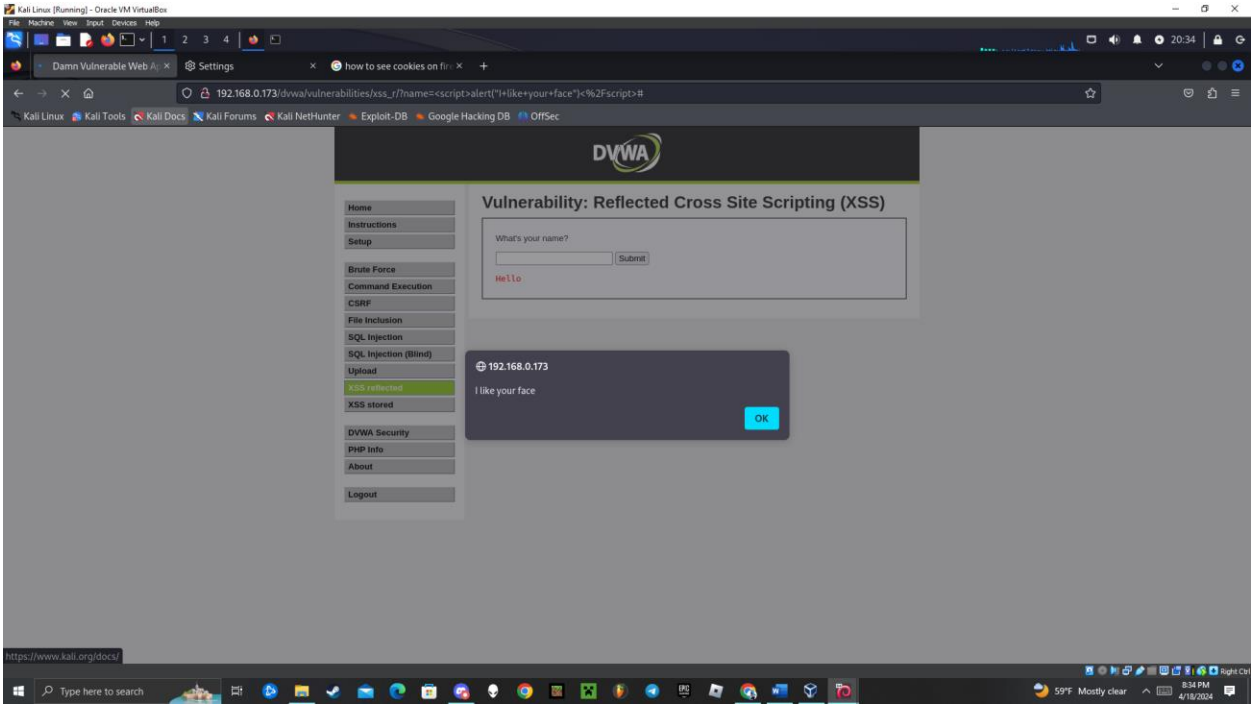

Added –tables and -D dvwa to query

7. 

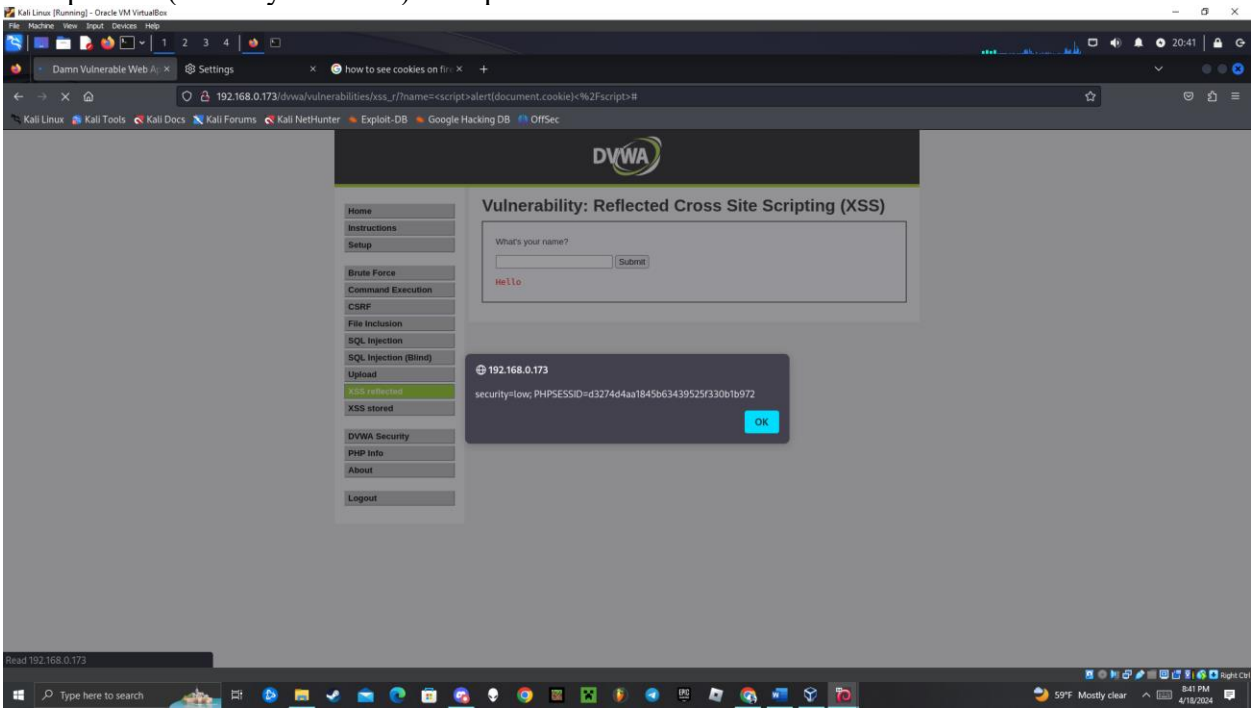

Added -T users and --dump

## Task B

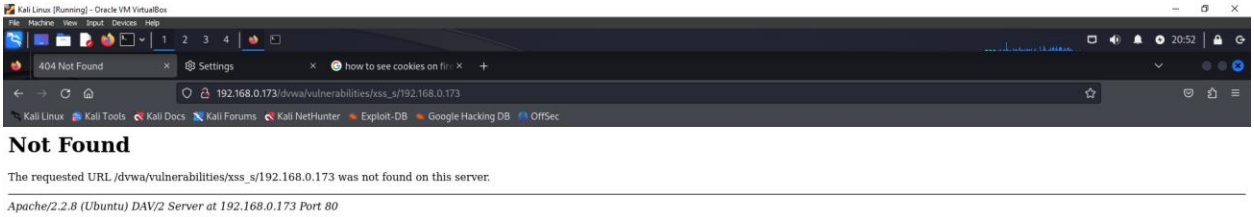
1. 

2. 


<script>alert(“I like your face”)</script>

3. 


<script>alert(document.cookie)</script>

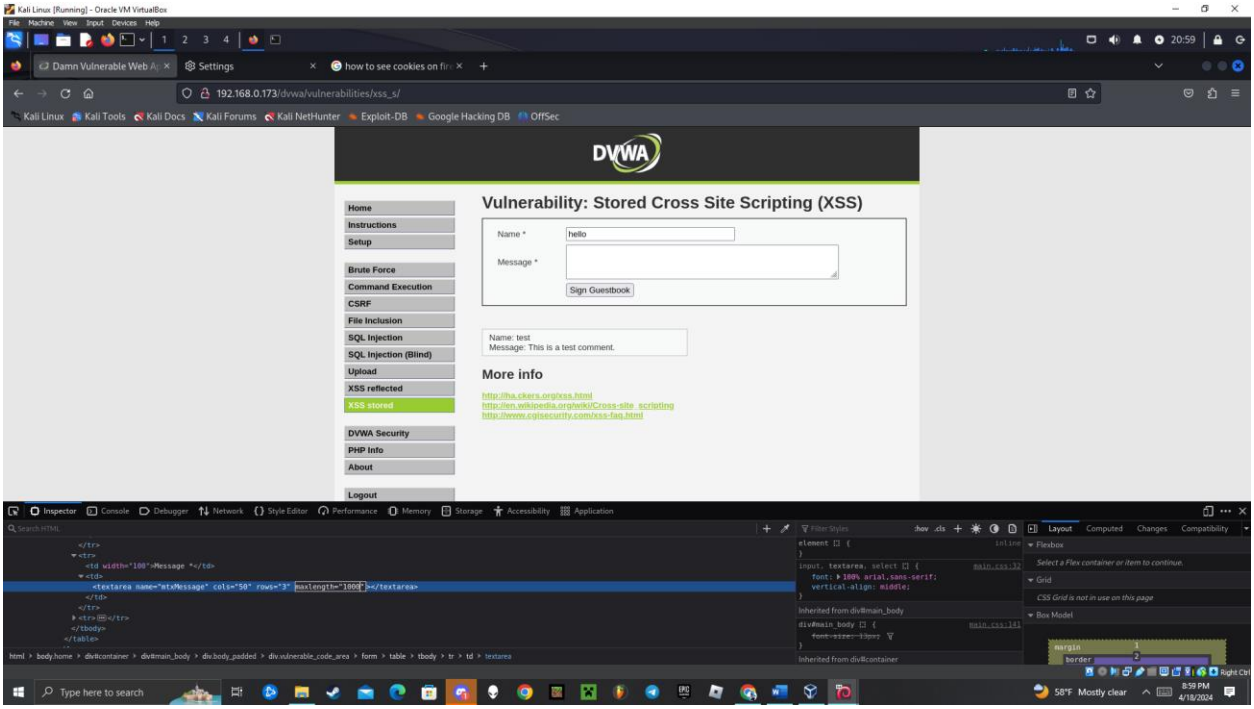


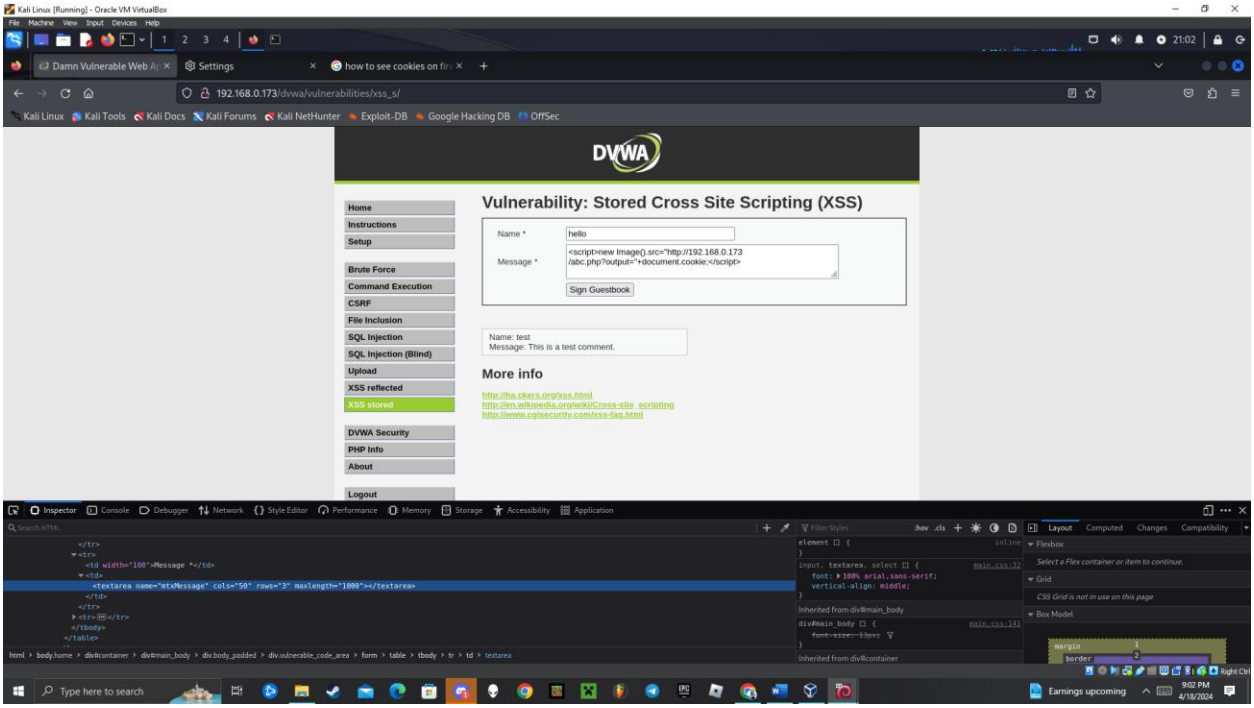

4. 

<script>document.location=”192.168.0.173”</script>

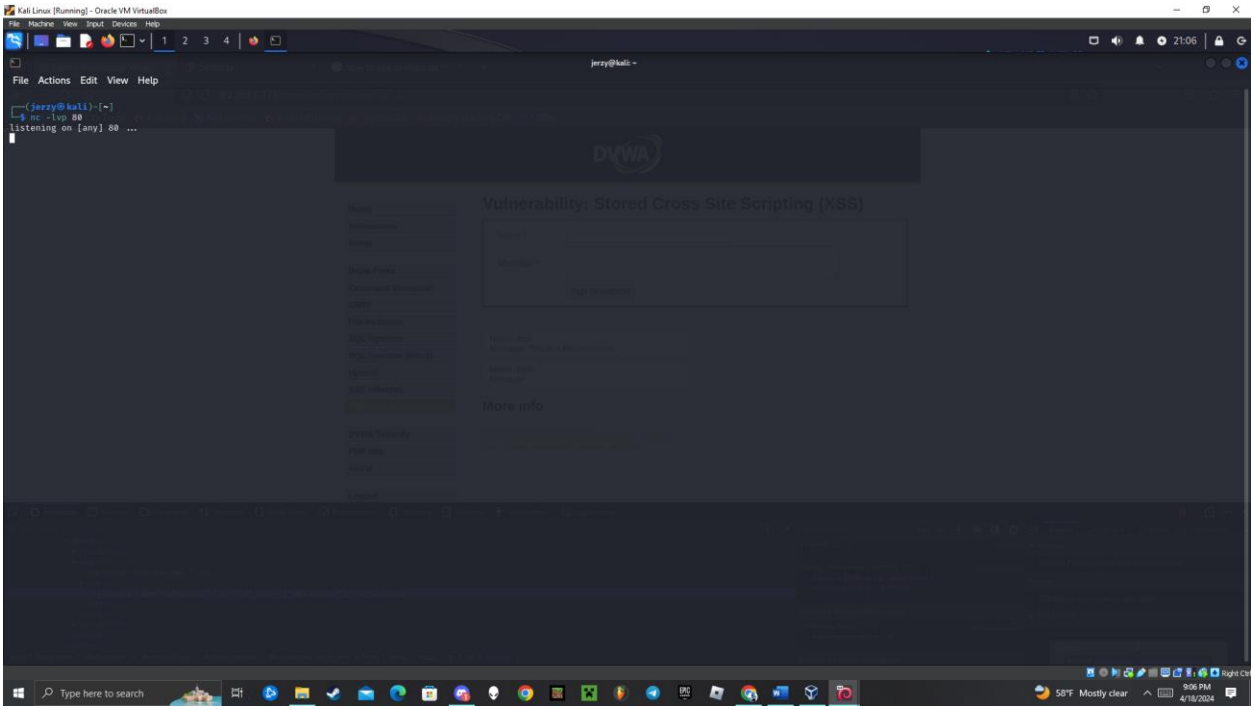
## Extra Credit

First I changed the allowed space for a XSS stored submission by inspecting and changing elements

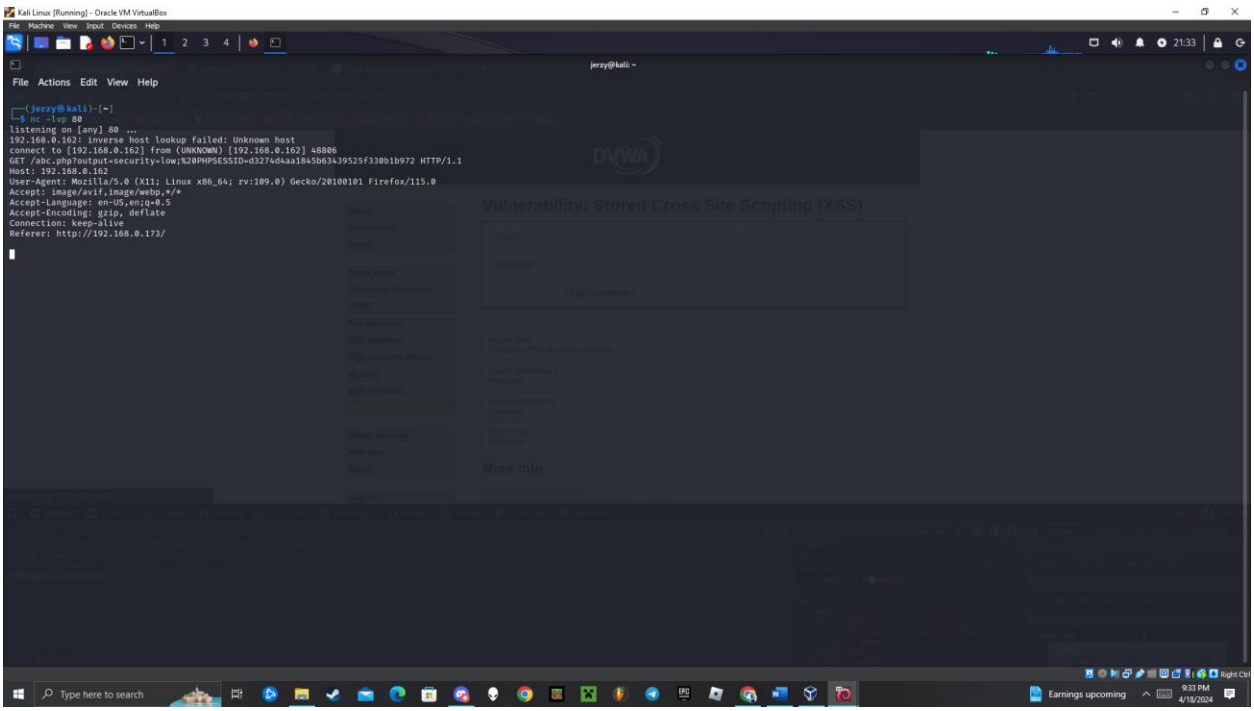





Next, I submitted the following code (I found a YouTube video demonstrating this attack online and this is the code they used). The IP address included can be changed to target anyone desired.




I start listening on my machine with this command




This is what it would look like if I accessed DVWA from the webpage provided. I couldn't figure out how to access a browser from metasploitable2 so I used another machine to demonstrate what would happen.