CMPE – 279
ASSIGNMENT – 3
DVWA – Damn Vulnerable Web App

GitHub Link: https://github.com/madhuridv/CMPE-279

Completed By :

Madhuri Dhani Venu

Payal Ghule

Q1) Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?

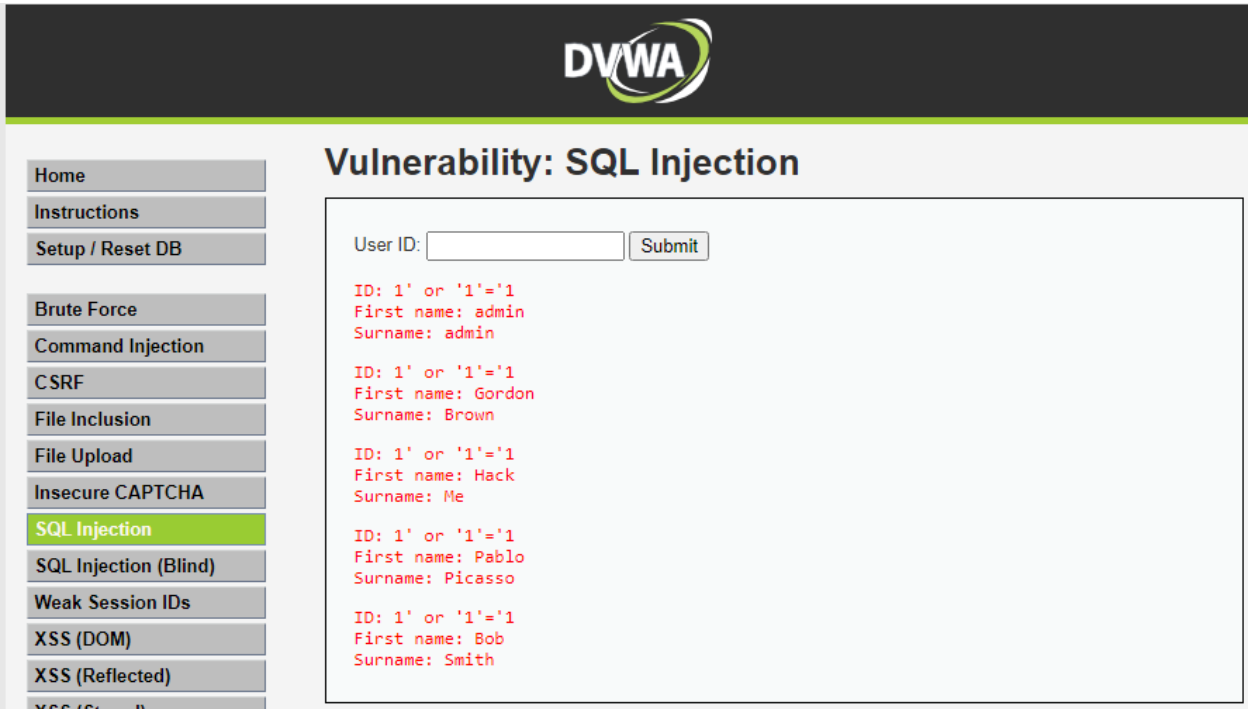
Ans: SQL Injection is a method of hacking sensitive data by modifying the SQL query.

Keeping the security to 'Low' and the input string = 1' or '1'='1

Converted the SQL Query to:

```
"SELECT first_name, last_name FROM users WHERE '1'='1;";
```

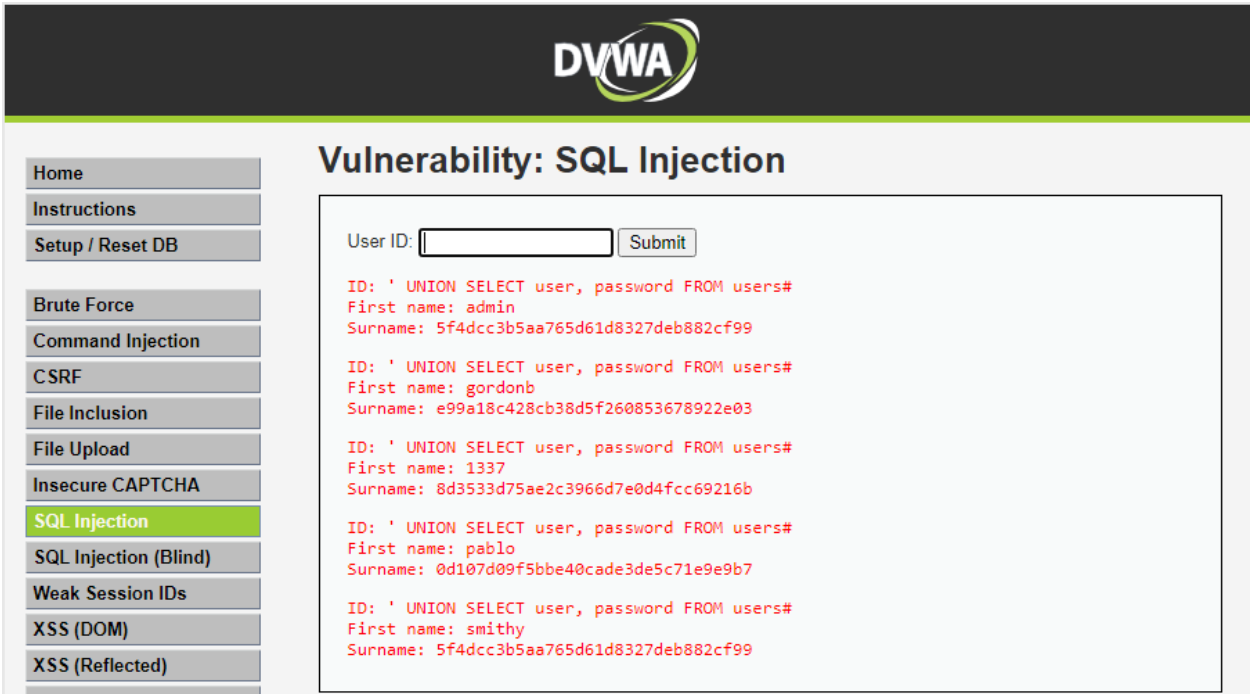
This SQL Injection was able to retrieve the following results:



Similarly, by passing the below as the input string:

' UNION SELECT user, password FROM users#

We were successful in retrieving the sensitive information like username and password from the database.



Q2) If you switch the security level in DVWA to "Medium", does the SQLi attack still work?

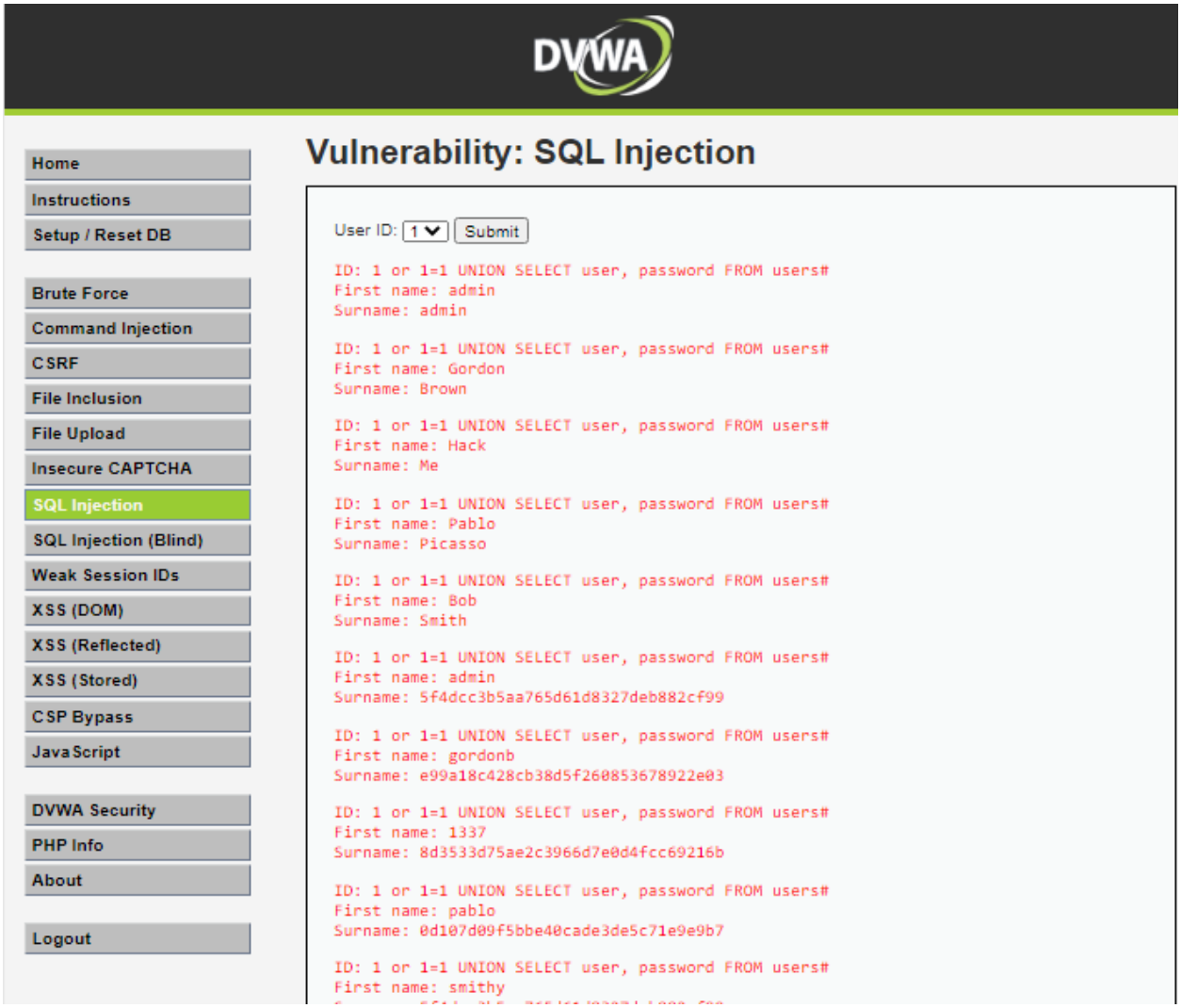
Ans: Upon switching the security levels from Low to Medium, the input type changed to a dropdown and allows the user to select from the list of options available.

In this scenario, SQL injection can be achieved by modifying the value of the dropdown list of inputs by directly injecting in the value field upon element inspection.

With the below SQL Injection:

<option value ="1 or 1=1 UNION SELECT user, password FROM users#> 1 </option>

The below results were obtained:



Q3) Describe the reflected XSS attack you used, how did it work?

Ans: Cross Site Scripting is (XSS) is a code injected security attack that targets the web Applications.

With “Low” Security and input string :

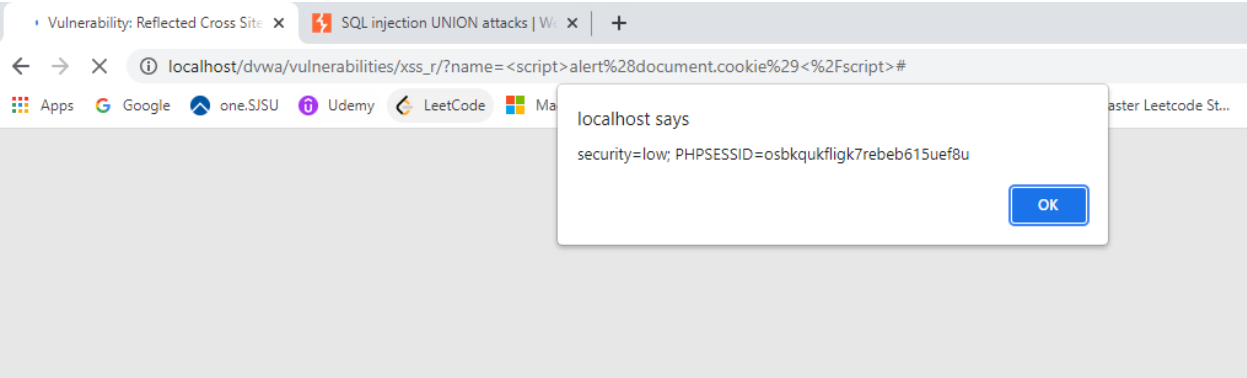
<script>alert("You have been HACKED")</script>

Displays the message in an alert box.

Similarly, when the below URL with injected code is sent to the victim, session cookies can be obtained.

http://localhost/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E#

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



Similarly, setting the window location in the script tag to redirect the victim to our configured webserver with a parameter cookie and we can set it to our cookie(document.cookie)

Q4) If you switch the security level in DVWA to "Medium", does the XSS attack still work?

<u>Ans:</u> Upon switching the security level to medium, the <script> command failed to work because the source code checked specifically for the occurrence of "<script>" word and if a match was found, request was ignored.

However, JavaScript is not case sensitive and hence by passing the same request with all letters in uppercase, we were able to successfully fetch the session cookie of the victim

Below is the command and its result:

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