

# PRATICA S6L4:

## Esercizio del Giorno

**Argomento:** Password Cracking - Recupero delle Password in Chiaro

**Obiettivo dell'Esercizio:** Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

### DVWA:

Per attivare DVWA sul mio ambiente Kali Linux, ho iniziato avviando il servizio MySQL con il comando `service mysql start`, assicurandomi che il database fosse operativo. Successivamente, ho effettuato l'accesso a MariaDB come utente root usando `sudo mysql -u root -p`, inserendo la password per accedere al monitor del database. Una volta dentro, ho concesso tutti i privilegi sull'intero database DVWA all'utente kali collegato da 127.0.0.1, impostando anche la sua password come kali. Questo passaggio è stato fondamentale per permettere a DVWA di interagire correttamente con il database.

Dopo aver eseguito il comando di grant e verificato che fosse andato a buon fine, ho chiuso la sessione MariaDB con `exit`. Infine, ho avviato il server Apache2 con `service apache2 start`, rendendo DVWA accessibile via browser. Con questi passaggi, ho completato la configurazione iniziale e reso DVWA pronto per l'utilizzo.

```
(kali@kali)-[~]
└─$ service mysql start
* Starting MariaDB database server: mariadbd.
*
(kali@kali)-[~]
└─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.2-MariaDB-1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

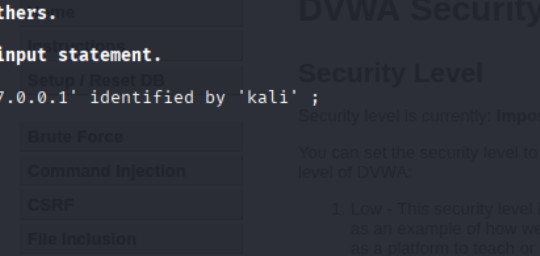
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.013 sec)

MariaDB [(none)]> exit
Bye

(kali@kali)-[~]
└─$ service apache2 start
```



## Accesso alle tabelle del database che contengono le password:

Ho eseguito una query SQL per visualizzare tutti i dati presenti nella tabella users, usando `SELECT * FROM users;`. Questo mi ha permesso di recuperare gli hash delle password associate agli utenti registrati nell'applicazione. I risultati mostrati includevano cinque utenti, ciascuno con un hash MD5 nella colonna password, che ho poi utilizzato per le sessioni di cracking. Dopo aver verificato e copiato gli hash, ho chiuso la sessione MariaDB con il comando `exit`, completando così la fase di estrazione delle password dal database DVWA.

```
(kali@kali)-[~]
└─$ sudo mysql -u root -p
[sudo] password for kali:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 11.8.2-MariaDB-1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [dvwa]> SELECT * FROM users;
+----+-----+-----+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user | password | avatar | last_login | failed_login |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | /DVWA/hackable/users/admin.jpg | 2025-08-07 07:27:50 | 0 |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38d5f260853678922e03 | /DVWA/hackable/users/gordonb.jpg | 2025-08-07 07:27:50 | 0 |
| 3 | Hack | Me | 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b | /DVWA/hackable/users/1337.jpg | 2025-08-07 07:27:50 | 0 |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 | /DVWA/hackable/users/pablo.jpg | 2025-08-07 07:27:50 | 0 |
| 5 | Bob | Smith | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 | /DVWA/hackable/users/smithy.jpg | 2025-08-07 07:27:50 | 0 |
+----+-----+-----+-----+-----+-----+-----+-----+
5 rows in set (0.000 sec)

MariaDB [dvwa]> exit
Bye
```

## Creazione del file password.txt:

Dopo aver recuperato gli hash delle password dal database DVWA, ho creato un file chiamato `password.txt` utilizzando l'editor nano, dove ho incollato tutti gli hash che intendevo craccare. Una volta salvato il file, ho verificato il suo contenuto con il comando `cat password.txt`, assicurandomi che tutti gli hash fossero correttamente inseriti. Questo file mi servirà per avviare le sessioni di cracking con lo strumento John the Ripper, con l'obiettivo di ottenere le versioni in chiaro delle password.

```
(kali@kali)-[~]
└─$ nano password.txt

(kali@kali)-[~]
└─$ echo password.txt
password.txt

(kali@kali)-[~]
└─$ cat password.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

## John the Ripper:

È uno strumento di cracking delle password, per testare la sicurezza di alcuni hash MD5. Ho eseguito il comando:

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

Questo ha caricato 5 hash di password dal file `password.txt` e ha utilizzato il formato Raw-MD5. Ho applicato il set di regole "single" e una wordlist predefinita situata in:

- `/usr/share/john/password.lst`

Il tool ha trovato le seguenti password corrispondenti agli hash:

- password
- password
- abc123
- letmein
- Charley

```
(kali@kali)-[~]
$ john --format=raw-md5 password.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
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 (2025-08-07 08:12) 10.86g/s 387717p/s 387717c/s 391056C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Alla fine della sessione, John ha fornito un riepilogo con il tempo impiegato, la velocità di guesses al secondo e il numero totale di tentativi. Per visualizzare in modo affidabile tutte le password trovate, mi è stato consigliato di usare:

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

```
(kali㉿kali)-[~]  
$ john --show --format=raw-md5 password.txt  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
5 password hashes cracked, 0 left
```

## Conclusione:

L'attività svolta ha permesso di comprendere in modo pratico le vulnerabilità legate alla gestione delle credenziali all'interno di applicazioni web non sicure come DVWA.

Attraverso l'accesso al database, l'identificazione degli hash MD5 e l'utilizzo di tool di cracking come John the Ripper e Hashcat, è stato possibile recuperare le password in chiaro degli utenti.

Questo esercizio ha evidenziato l'importanza di:

- Evitare l'uso di algoritmi di hashing obsoleti come MD5.
- Implementare misure di sicurezza come salting, hashing robusto (es. bcrypt, Argon2) e protezione del database.
- Utilizzare password complesse e non presenti in dizionari comuni.

In conclusione, il cracking delle password ha dimostrato quanto sia semplice compromettere un sistema mal configurato, sottolineando la necessità di adottare pratiche di sicurezza avanzate per proteggere le informazioni sensibili.