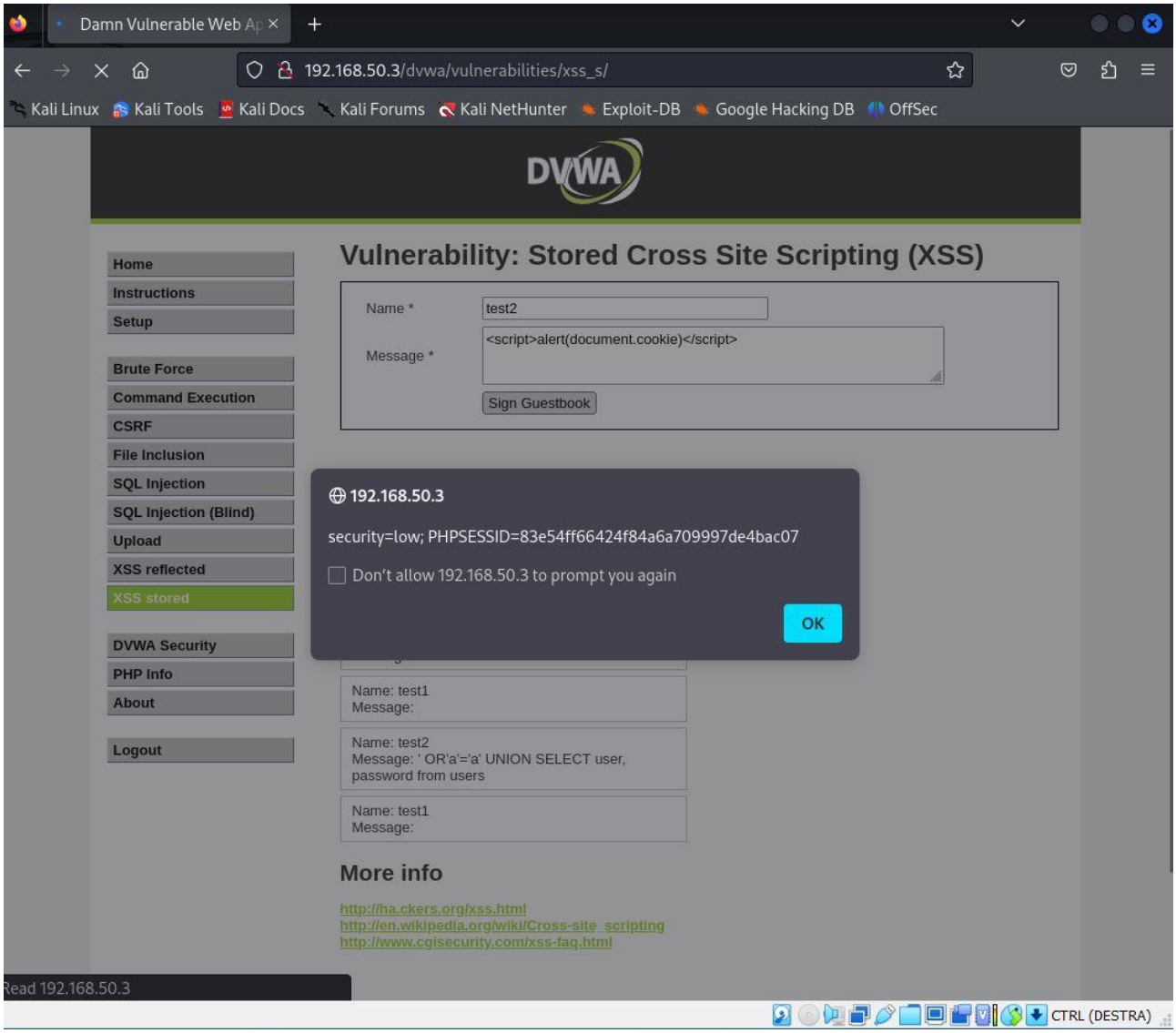
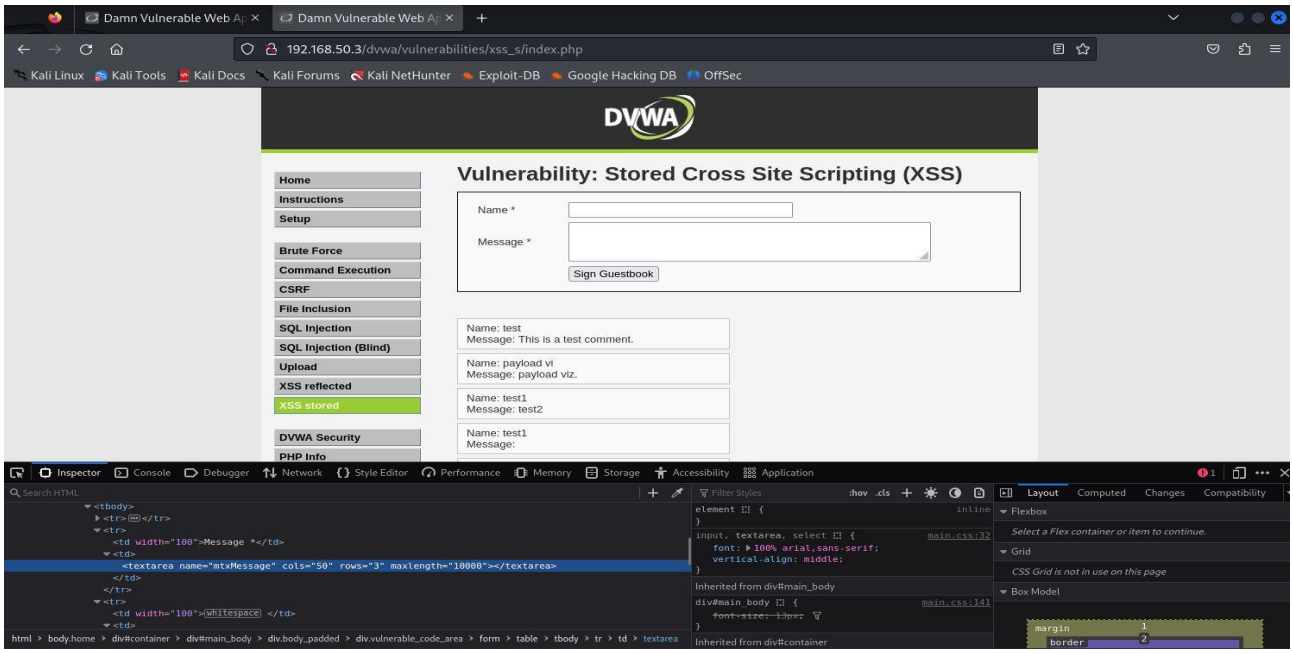
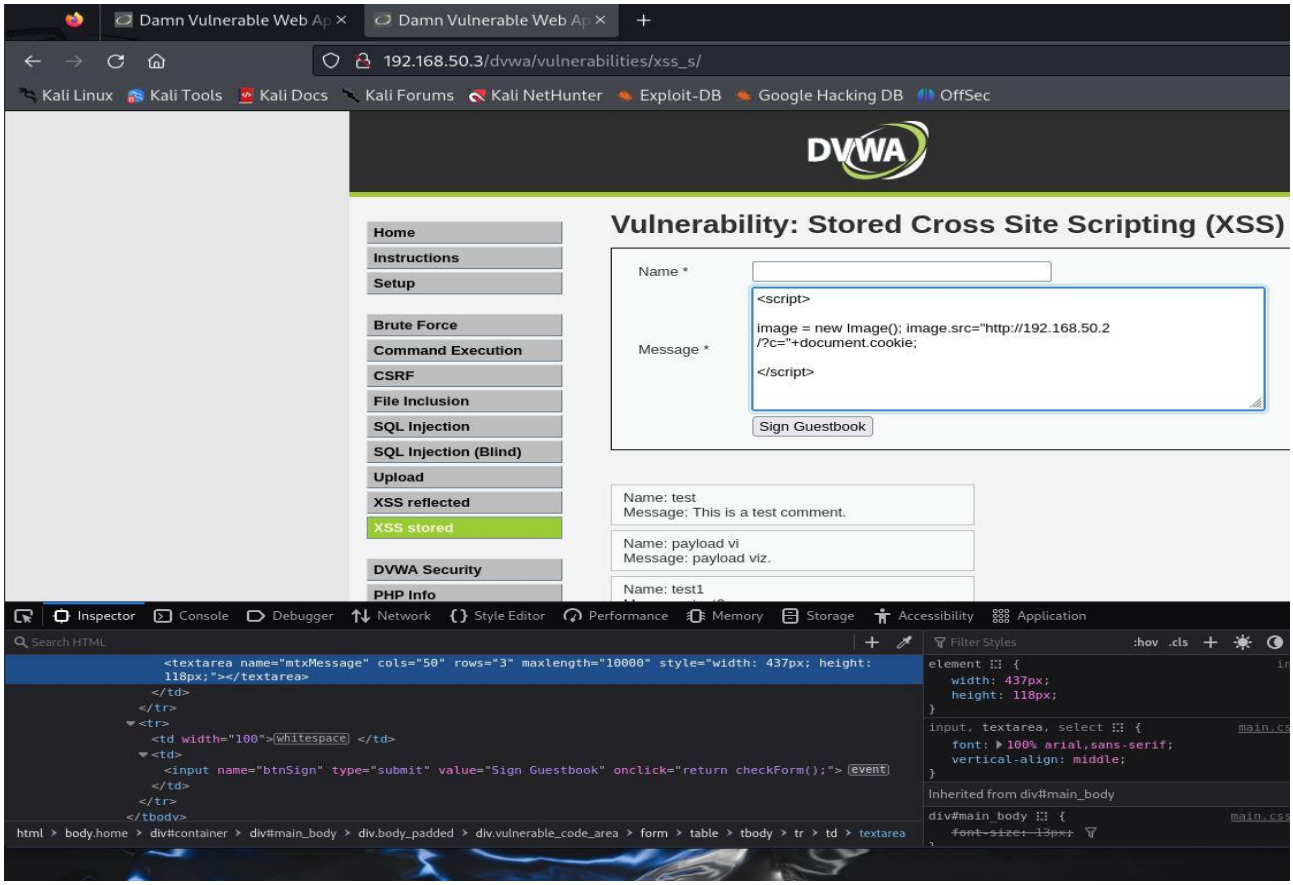
Verifichiamo prima che la pagina sia vulnerabile a questo tipo di attacco immettendo lo script sottostante che dovrebbe far comparire un popup con i cookie di sessione:



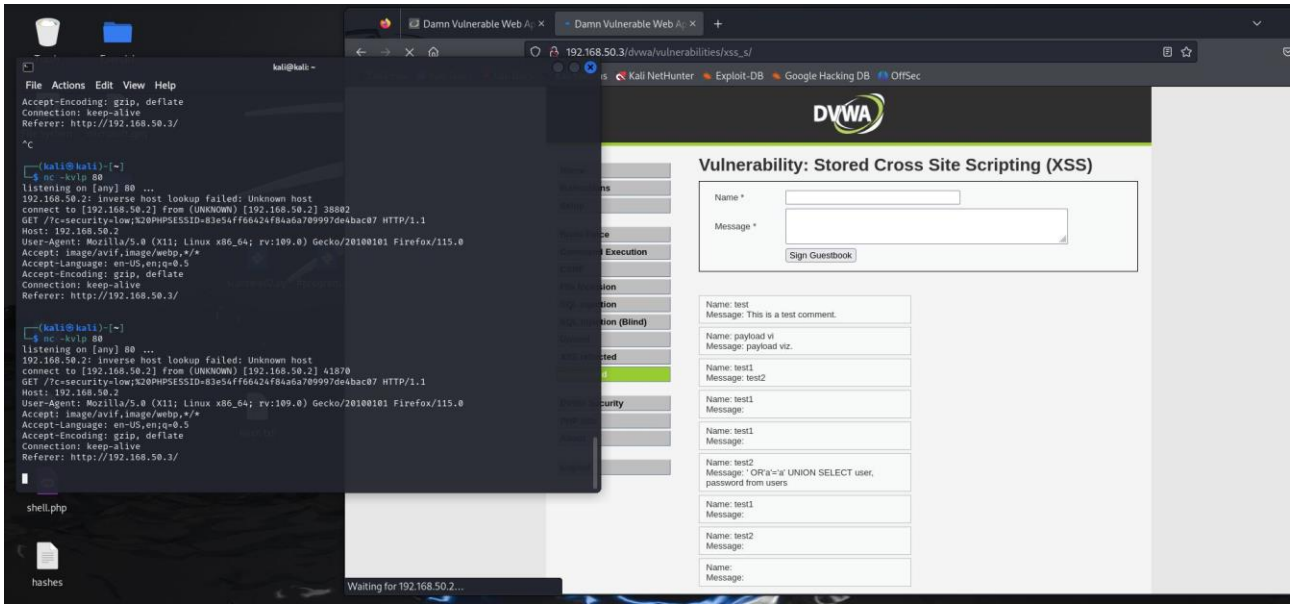
Assodata la vulnerabilità del sistema a questo tipo di attacco, creiamo uno script che va ad inviare i cookie di sessione sulla macchina Kali (IP: 192.168.50.2), per far ciò bypassiamo prima il limite di caratteri presenti nel riquadro “Message” modificando nell’inspector di pagina il parametro “max lenght” con una cifra di nostro piacimento:



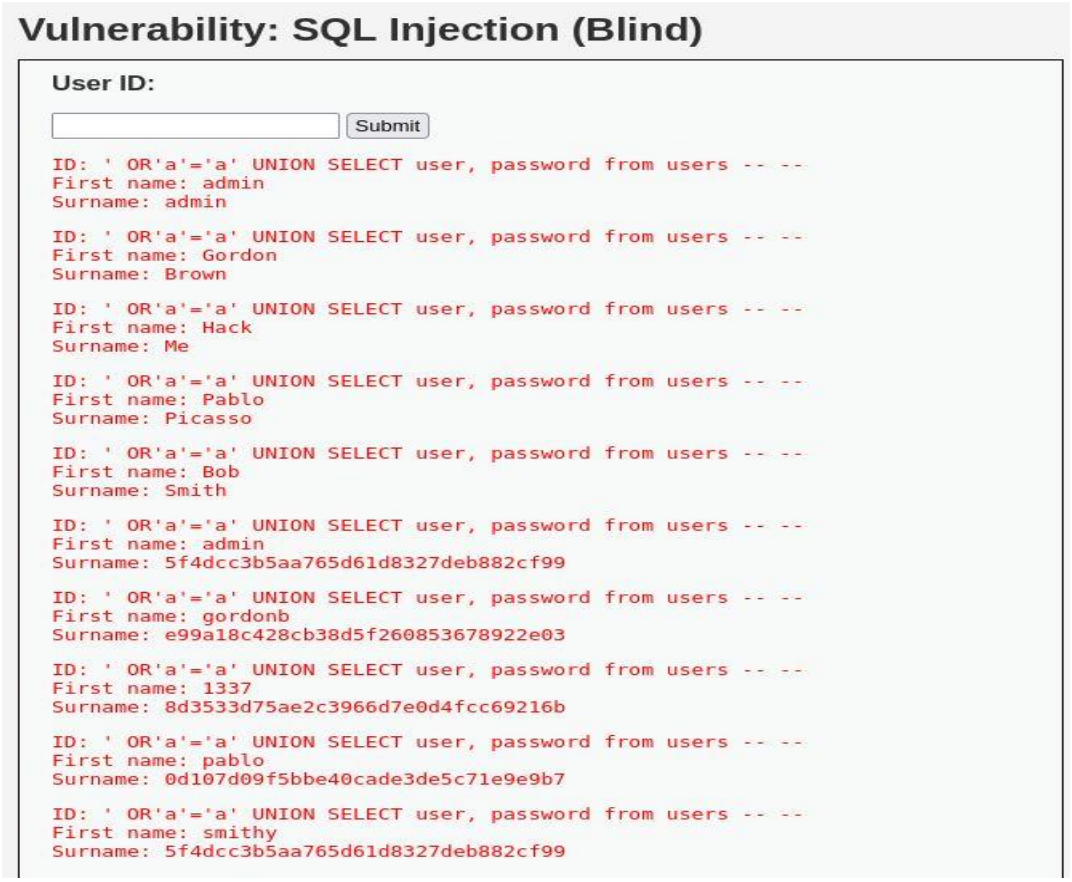
Ora possiamo immettere il nostro script, aprendo prima un listening con Netcat in modo verboso su tutte le porte 80:



Come possiamo osservare i cookie vengono catturati qualvolta un utente entri sulla pagina XSS stored:



Per quanto riguarda la SQLi per recuperare le password dal database, sfruttiamo la debole sanitizzazione presente nel codice sorgente andando ad adoperare lo stesso script già visto ‘ OR’a’=’a’ UNION SELECT user, password from users -- -- :



Andiamo ora a decriptare le password con il tool John the ripper: