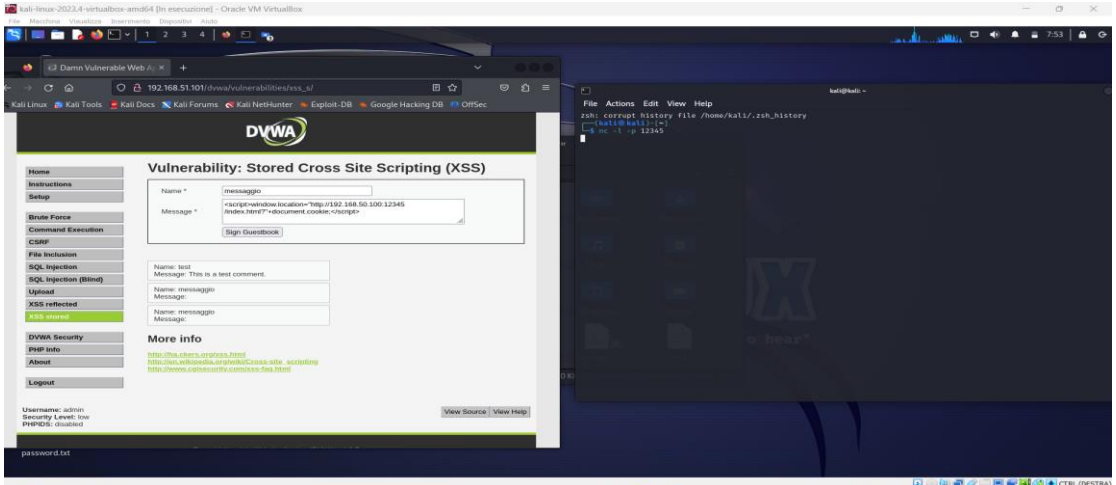
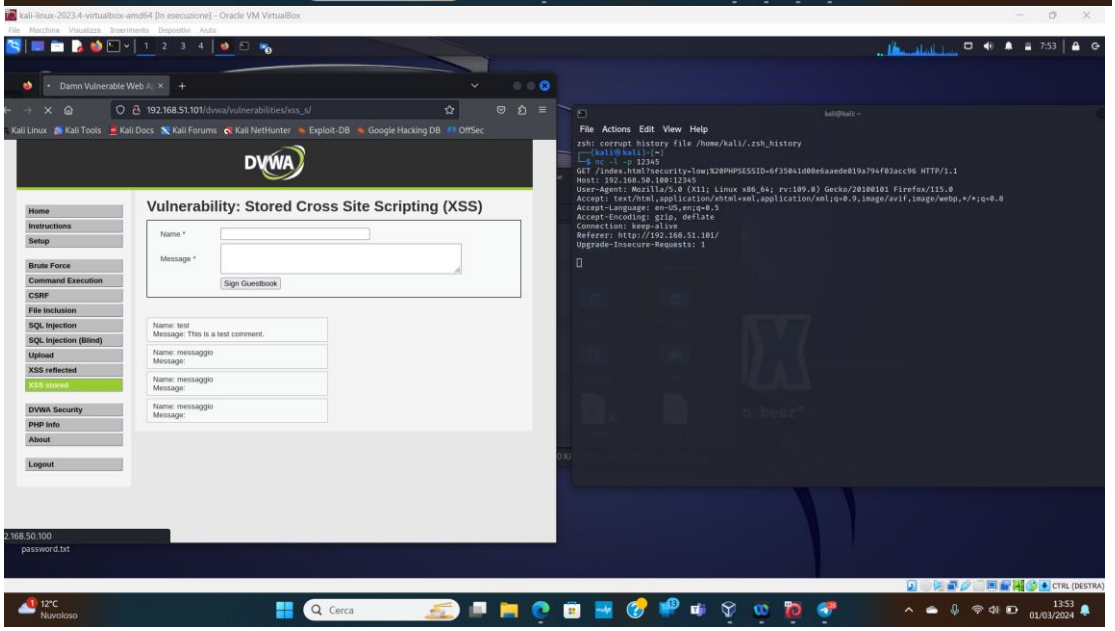
XSS stored

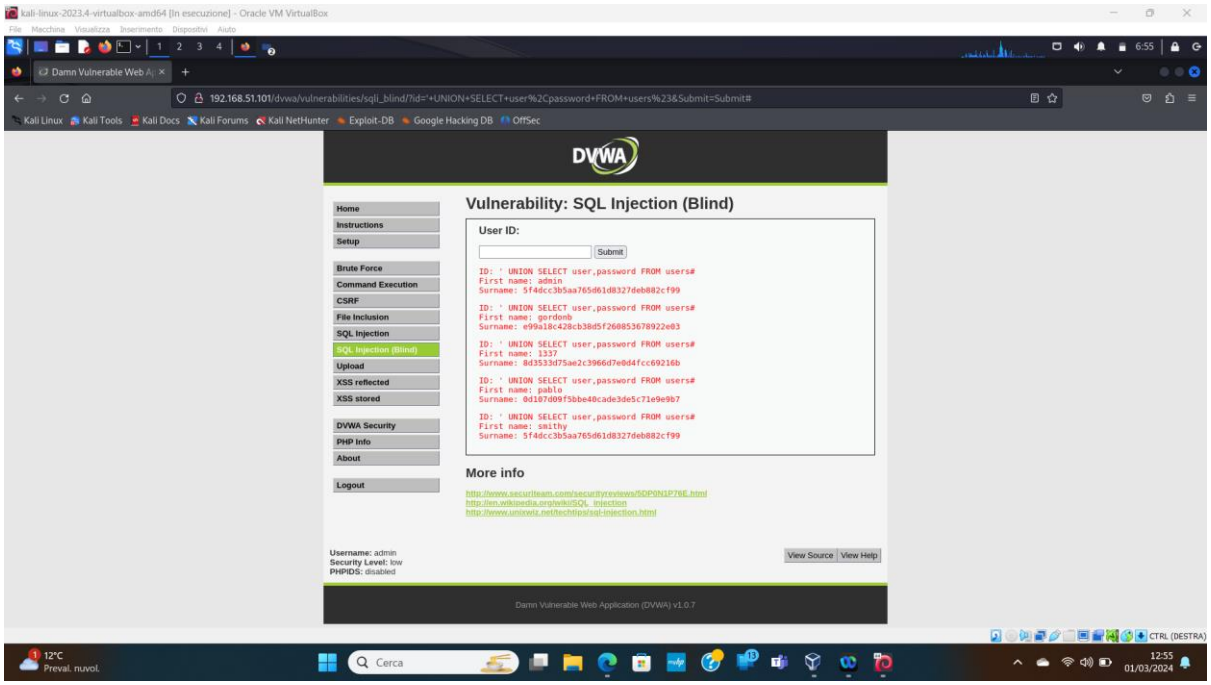
L'attacco XSS stored è una forma di attacco informatico che sfrutta le vulnerabilità nelle applicazioni web per inserire script dannosi nei dati memorizzati sul server e visualizzati agli utenti. Questi script dannosi vengono quindi eseguiti sul browser degli utenti che accedono alla pagina web, consentendo agli attaccanti di rubare informazioni sensibili o danneggiare l'esperienza dell'utente. Oggi andremo a inserire uno script (modifichiamo tramite l'ispezionamento la quantità massima di caratteri da poter inserire) che andrà a rubare i cookie di accesso della vittima indirizzandola al nostro ip e porta in modo tale da usare kali per metterci in ascolto e inserire quei cookie rubati nell'ispezionamento della pagina bypassando il login.

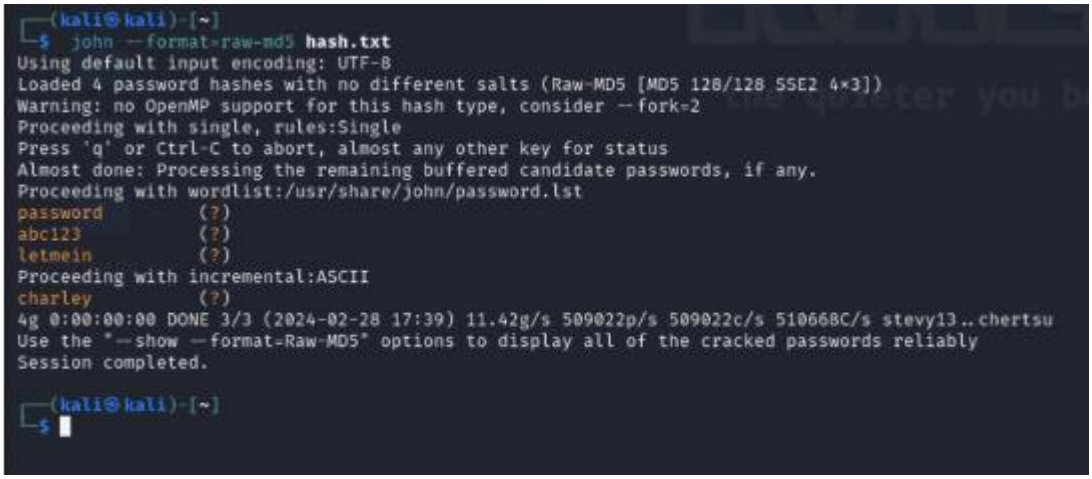




SQL injection (blind)

Un attacco di SQL injection è una vulnerabilità informatica che consente a un aggressore di inserire codice SQL dannoso all'interno di un'applicazione web o di un'interfaccia utente che interagisce con un database. Questo tipo di attacco sfrutta le falle di sicurezza nelle query SQL, permettendo agli aggressori di manipolare il comportamento del database e ottenere informazioni non autorizzate o eseguire azioni non consentite. Oggi con questo attacco entreremo nel database della web app per cercare di estrapolare tutte le informazioni sensibili che essa ha conservato su questo database, forzandola a farci tornare tutte quelle informazioni a cui noi non dovremmo avere accesso.
Utilizziamo la union per unire due query, dopo aver fatto vari test siamo riusciti a capire il numero di colonne da far combaciare, e scrivendo ' UNION SELECT user,password FROM users# otteniamo il risultato della tabella users.





Successivamente volendo abbiamo la possibilità di utilizzare john the ripper fornendo un file di hash che abbiamo catturato nel database.