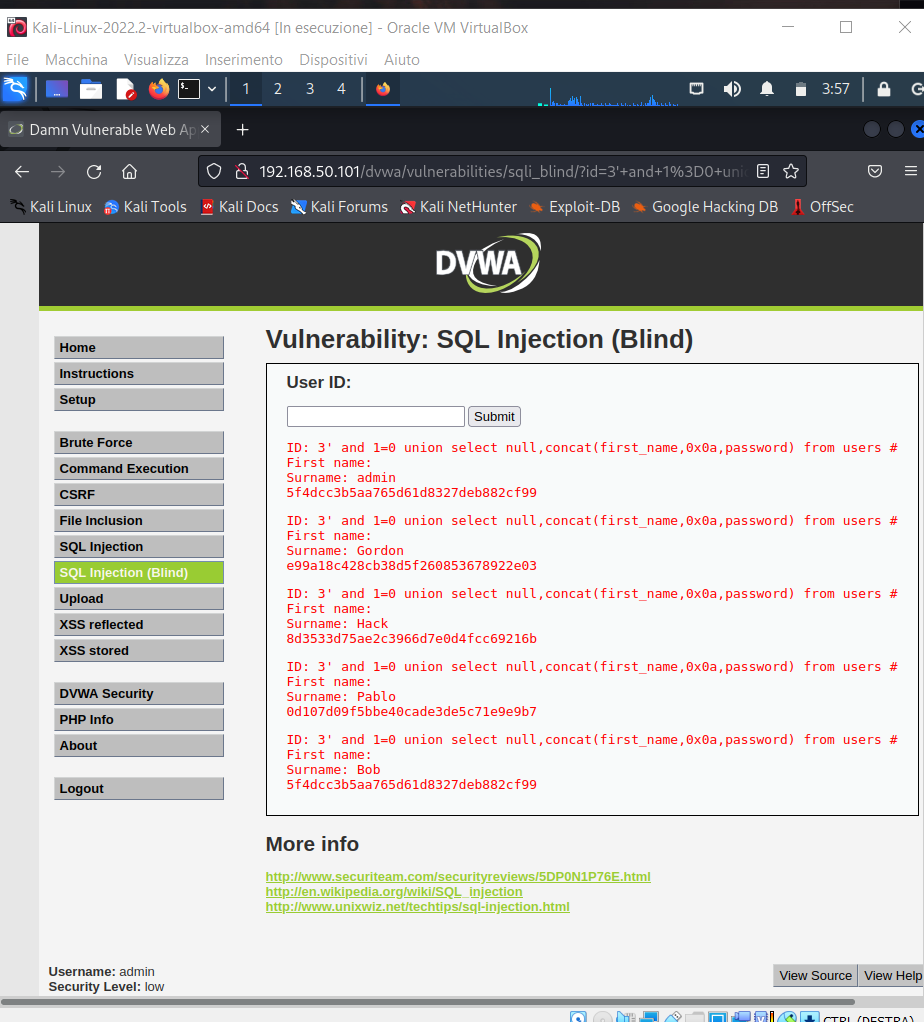
Esercizio settimanale

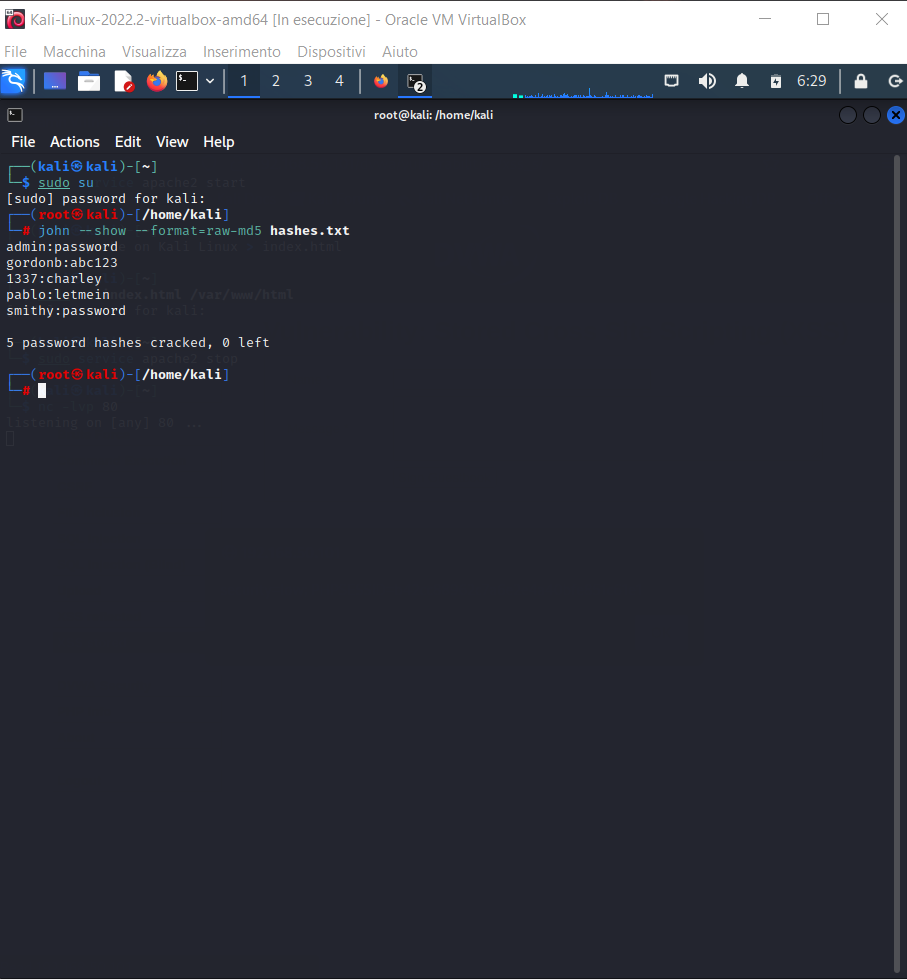
Nella prova di oggi bisognava recuperare le password e gli utenti del database tramite SQL, per poi trovarne i cookie.

Recupero password e utenti



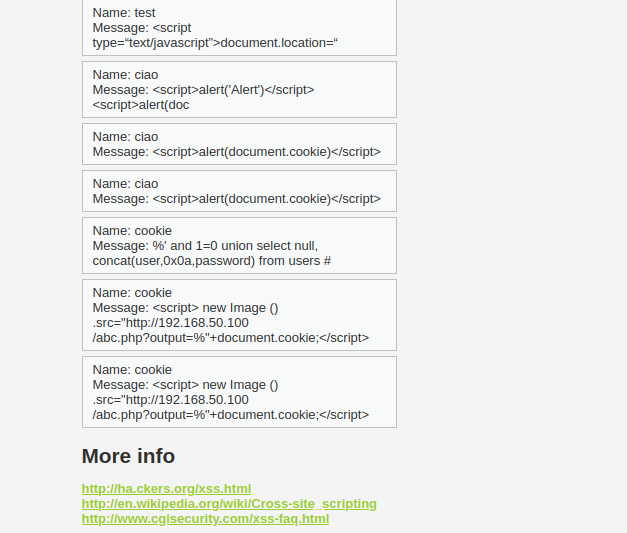
Per prima cosa tramite SQL ho trovato gli utenti e le loro password in formato md5, che poi ho convertito con john per ricavare la password decriptata.

Decriptazione password



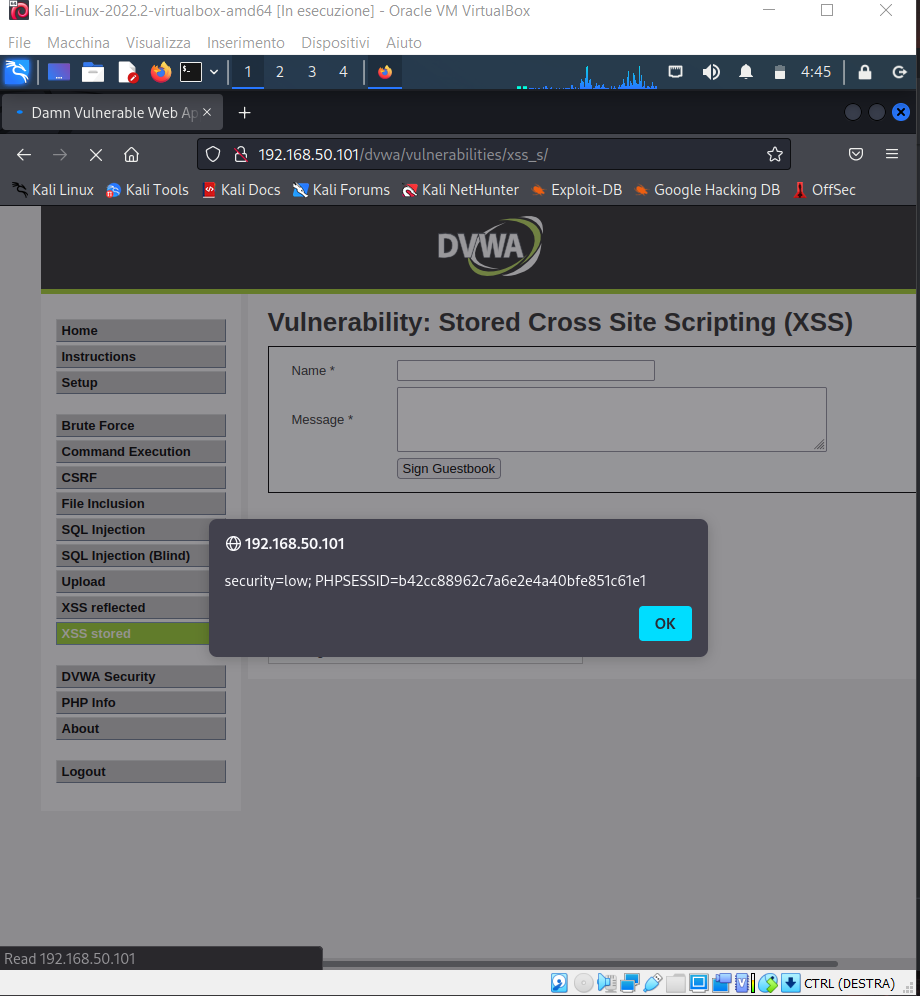
Questo è il risultato della decriptazione, qui possiamo notare l’username e la password in chiaro.

Script per i cookie

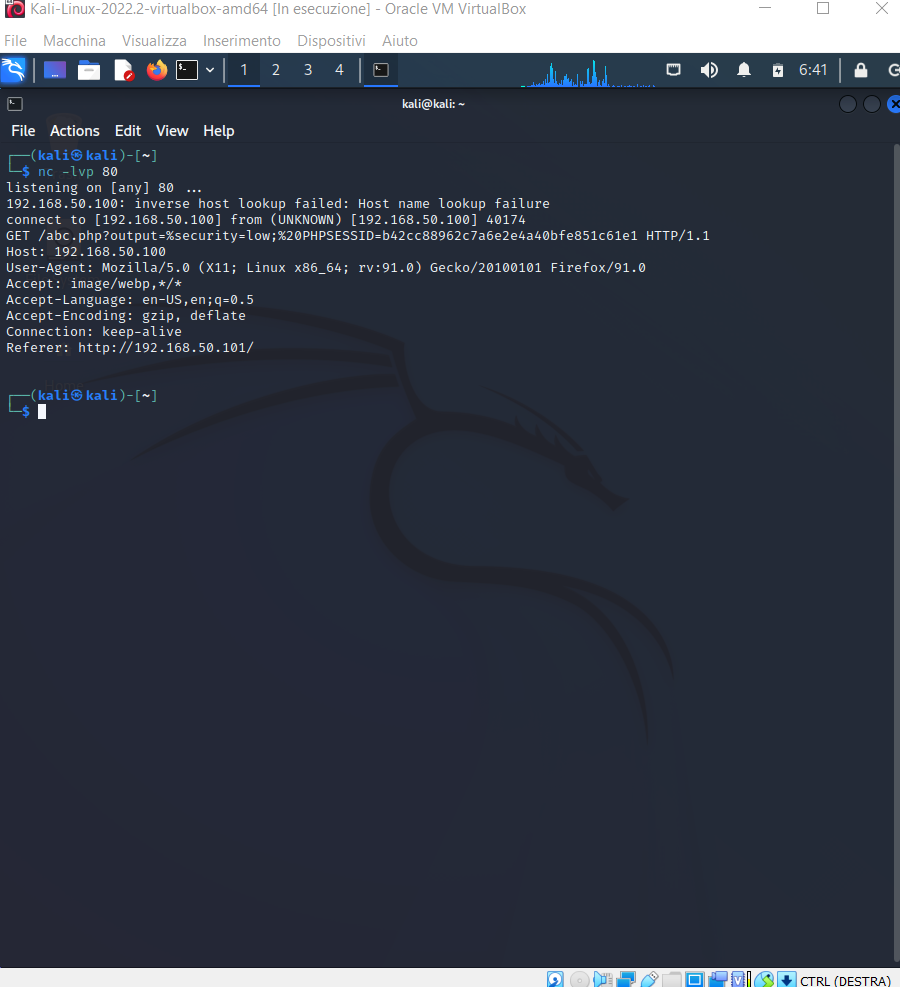


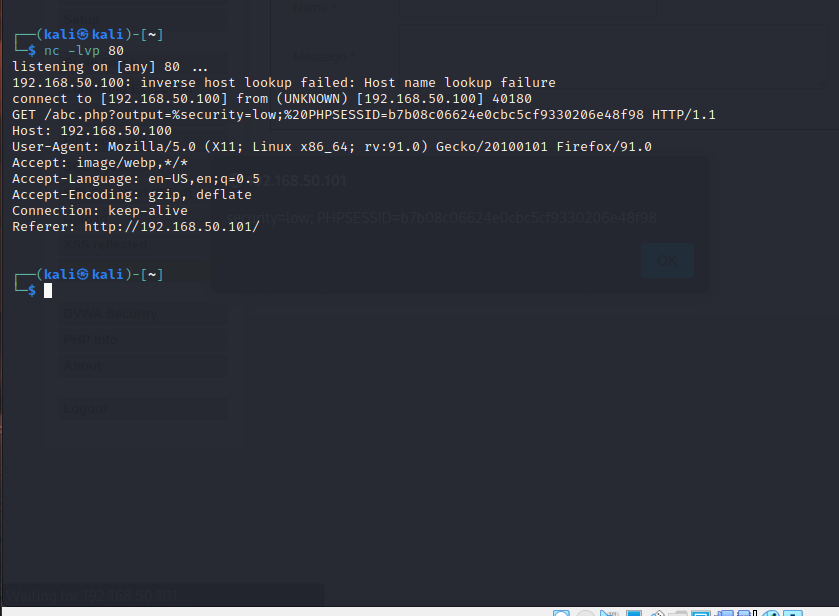
Tramite uno script che ho inserito in XSS stored sono riuscito a ricavare i cookie di sessione dell’utente.

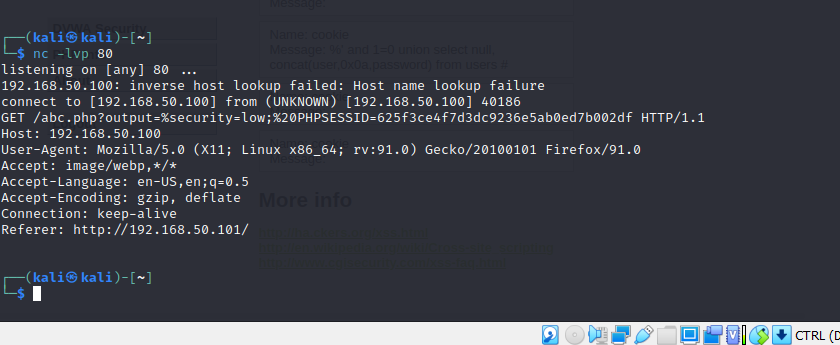
Questo è il risultato del comando:

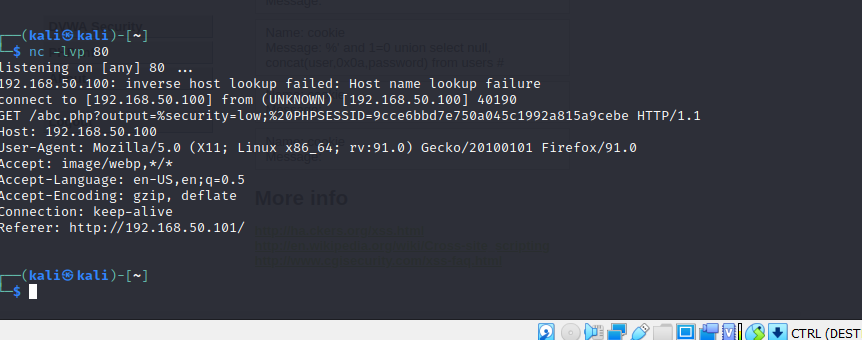


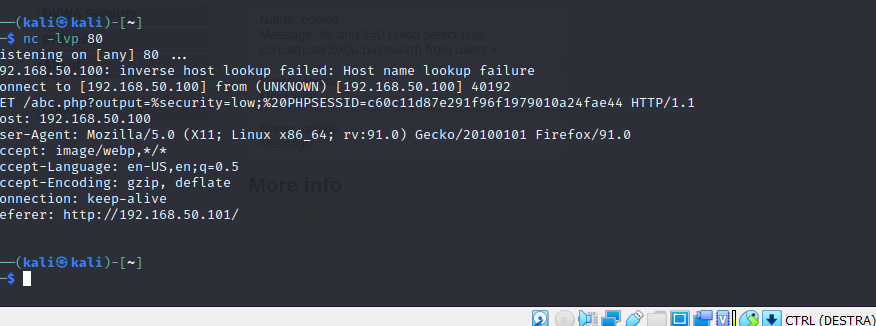
Cookie dei vari utenti











Una volta scoperto il meccanismo per recuperare il cookie di un utente, ho ripetuto questa operazione per tutti gli utenti.

Per fare tutto questo ho usato netcat in quanto può essere usato come server per ricevere le informazioni.