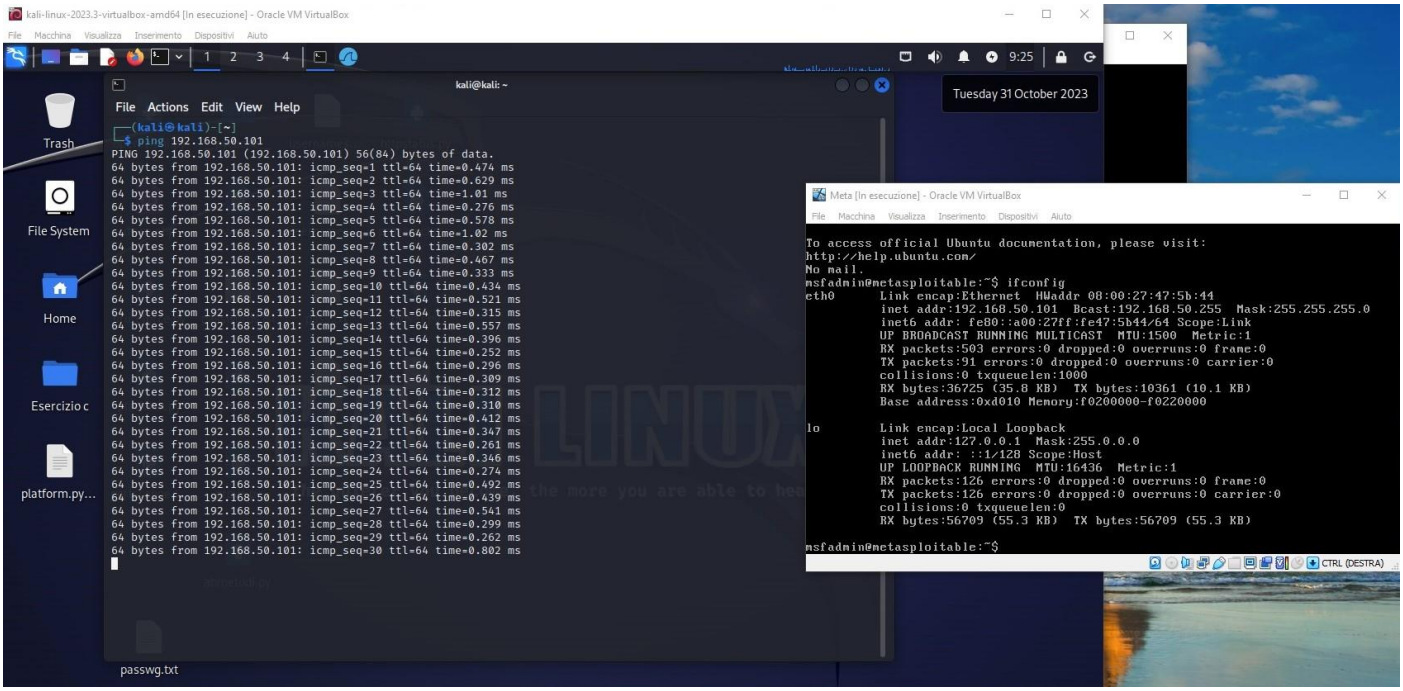
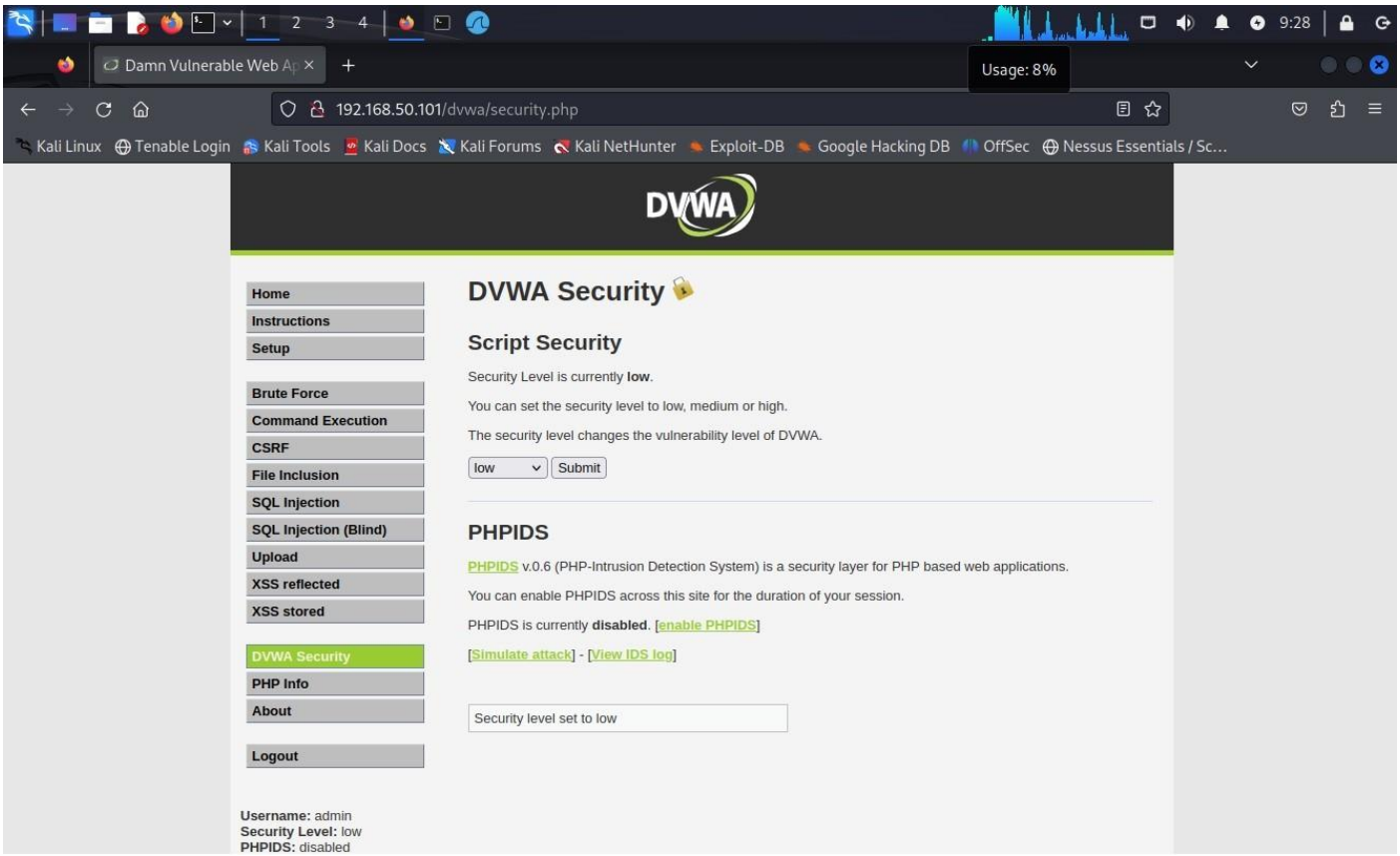
Esercizio 31/10/2023

Nell'esercizio odierno ci viene richiesto di scegliere una delle vulnerabilità XSS e un'altra per SQL Injection su DVWA e sfruttarle con successo con le tecniche viste durante la lezione teorica.

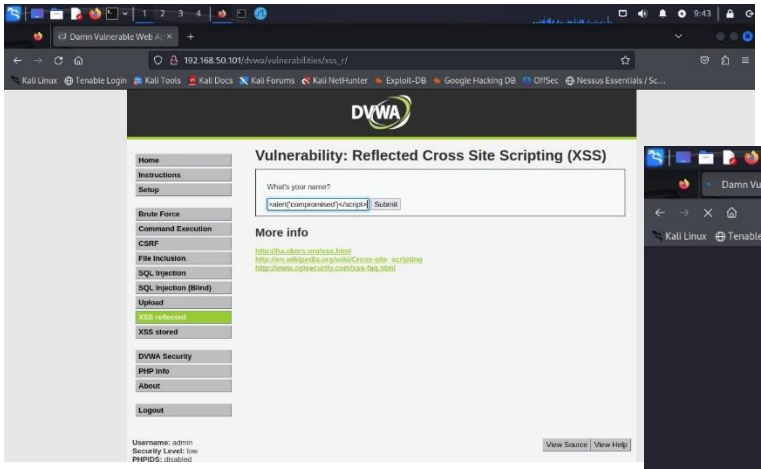
Come di consueto controllo che le macchine virtuali dialoghino tra loro attraverso il ping

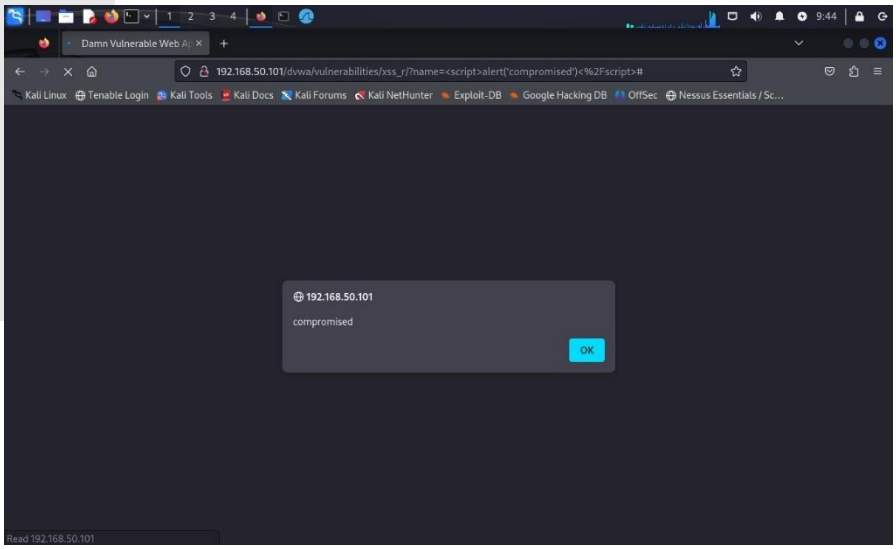


Fatto questo, come richiesto dall'esercizio, imposto su DVWA il livello di sicurezza basso

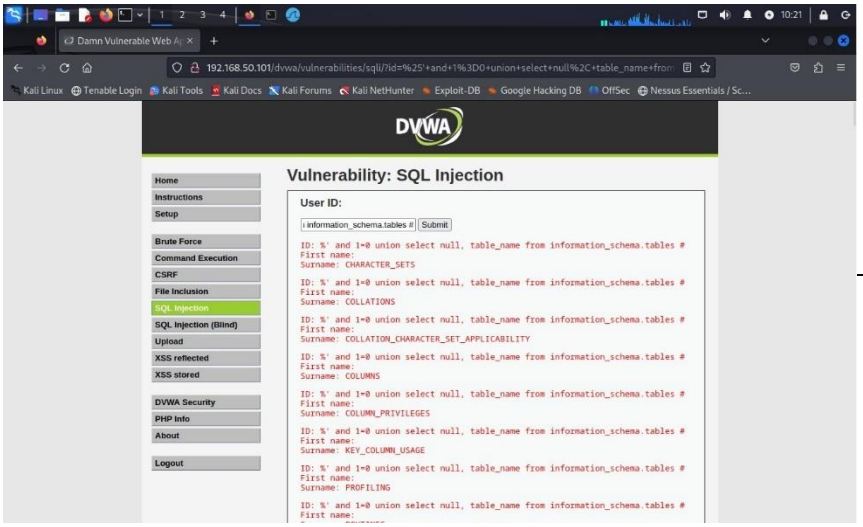


Dopo di che procedo con l'attacco XSS reflected (cioè una tecnica che, attraverso uno script, consente di riflettere immediatamente il codice inserito, o messaggio di alert in questo caso, sul sito)





Procedo, infine, all'attacco SQL Injection (una tecnica che rende l'attaccante amministratore del database, il che significa che può inserire qualsiasi input, il server sta dicendo al database che qualunque cosa inserisce, essendo l'amministratore, è lecito). L'attacco, quindi, permette ad un utente non autorizzato di prendere i comandi SQL utilizzati da una web app e ha l'obiettivo di alterare il contenuto del database.



INFO TABELLE

VISUALIZZAZIONE UTENTE DEL DATABASE