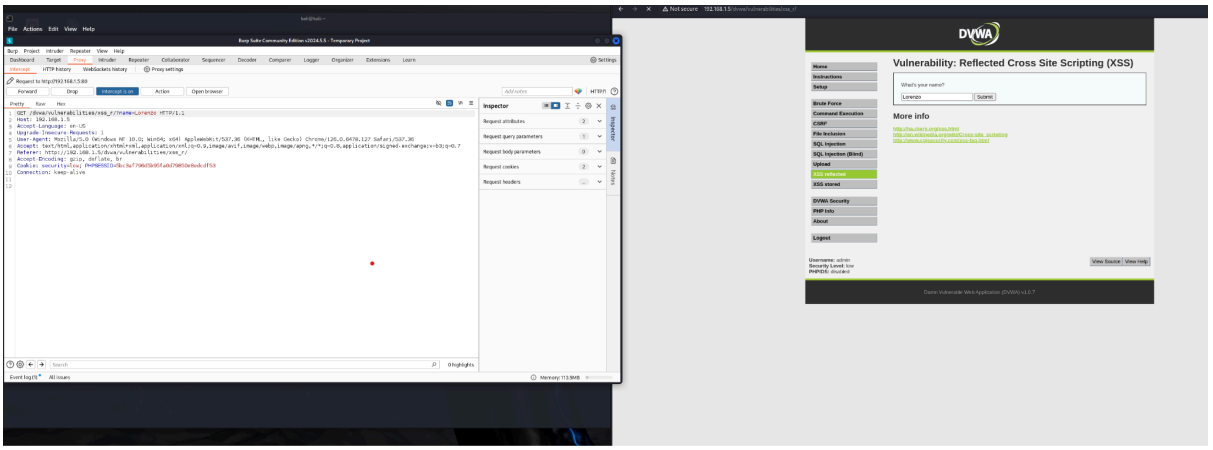
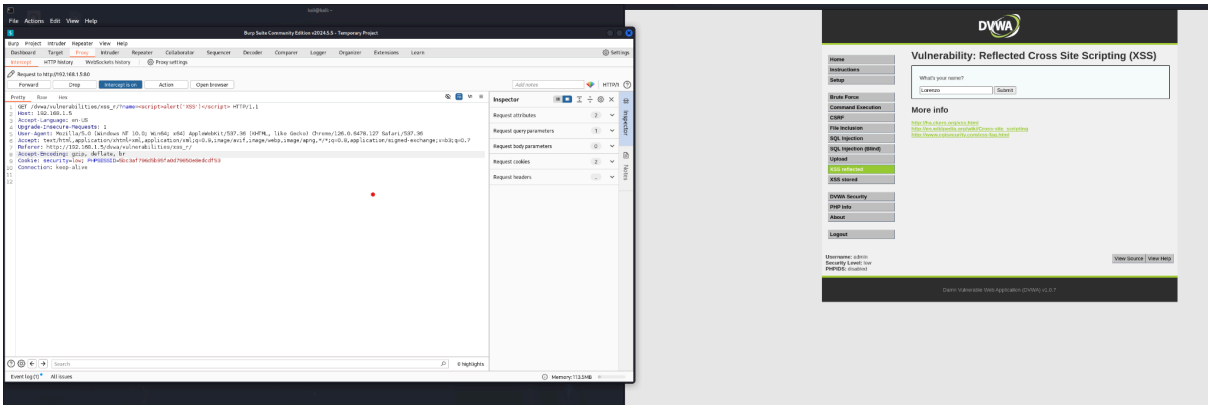
Esercizio S6L2 - Attacchi XXS Reflected e SQL Injection

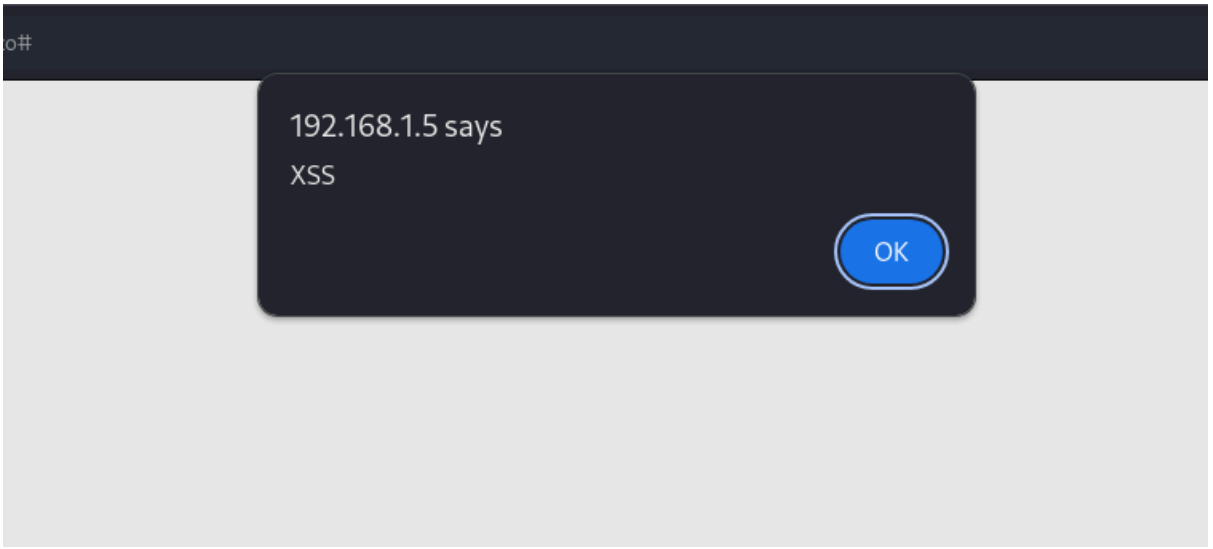
L’esercizio di oggi prevedeva l’applicazione pratica fra Kali e Metasploitable2 di attacchi XXS Reflected e SQL Injection: dopo aver configurato la corretta comunicazione fra i dispositivi, apriamo direttamente la macchina DVWA e come prima cosa, proviamo con un attacco XXS Reflected dalla tab corrispondente:



^ Inseriamo il nome, e intercettiamo con BurpSuite:

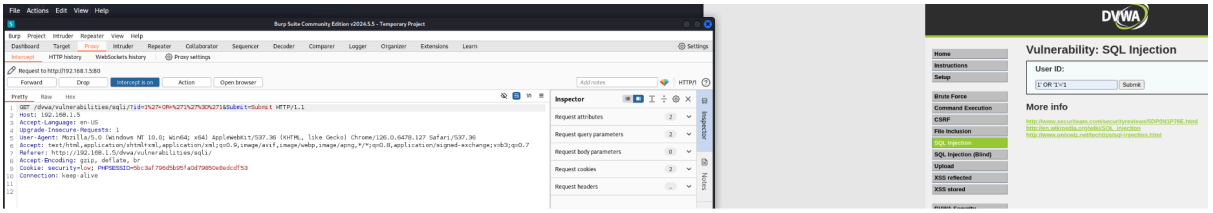


^ Modifichiamo il campo name per includere uno script di alert da far eseguire alla pagina in un popup:



Come ci aspettavamo la richiesta di un XXS Reflected è istantantea e possiamo visualizzarla immediatamente in quanto al contrario dell'XXS Stored viene eseguita immediatamente da chi clicka il link.

Passiamo invece alla SQL Injection:



^ Inserendo un termine come 1' OR '1' = '1 andiamo a comunicare al programma di rendere sempre vera la condizione, permettendo così all'attaccante di accedere non autorizzato ai dati nel database. In pratica è come applicare un filtro di Excel.

Otteniamo così una lista di utenti della macchina DVWA che possiamo ora consultare a piacimento.