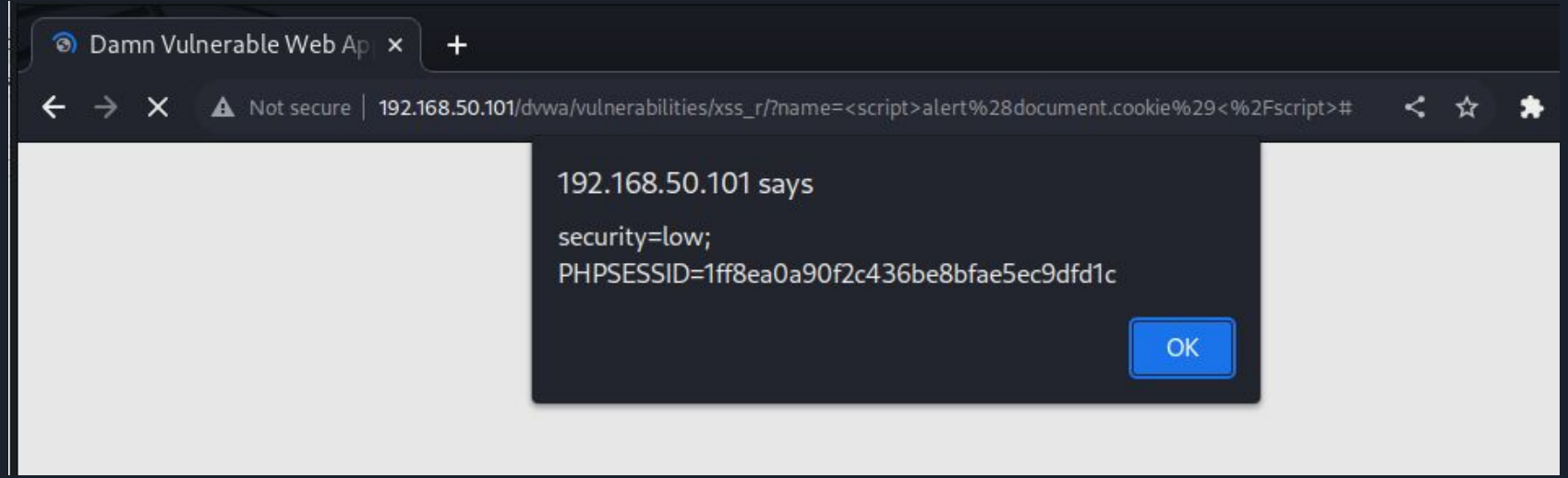
Esercizio S6 L2

XSS Reflected:

Per effettuare un attacco XSS Reflected è sufficiente andare ad inserire uno script nel campo di input della pagina. La scelta dello script da inserire dipende dalla natura dello script in sè e da quello che è il risultato desiderato dell'attacco, per questo esempio ho usato il seguente:

<script>alert(document.cookie)</script>

questo script restituisce lo ID di sessione dell'utente che lo inserisce. Per completare l'attacco è sufficiente inviare il link malevolo all'utente bersaglio tramite social engineering



SQL Injection:

Questo attacco ci permette di ottenere la lista completa degli utenti presenti nel database, scrivendo nel campo:

‘ OR ‘a’=’a

quando il sito andrà a controllare che l’user ID combaci troverà una variabile sempre vera.