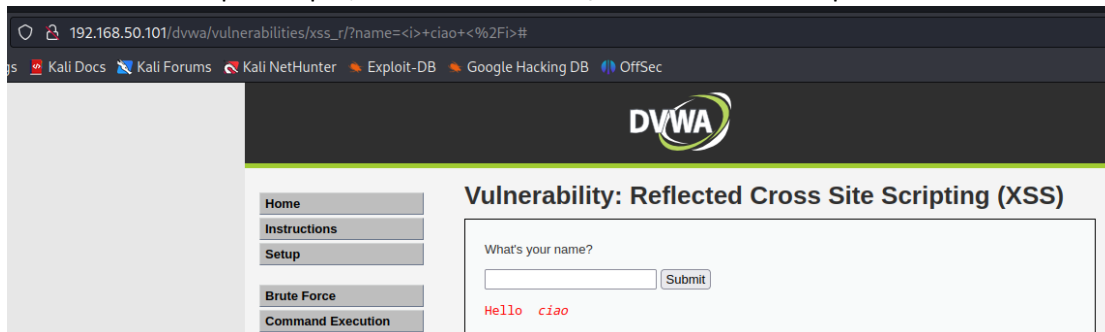


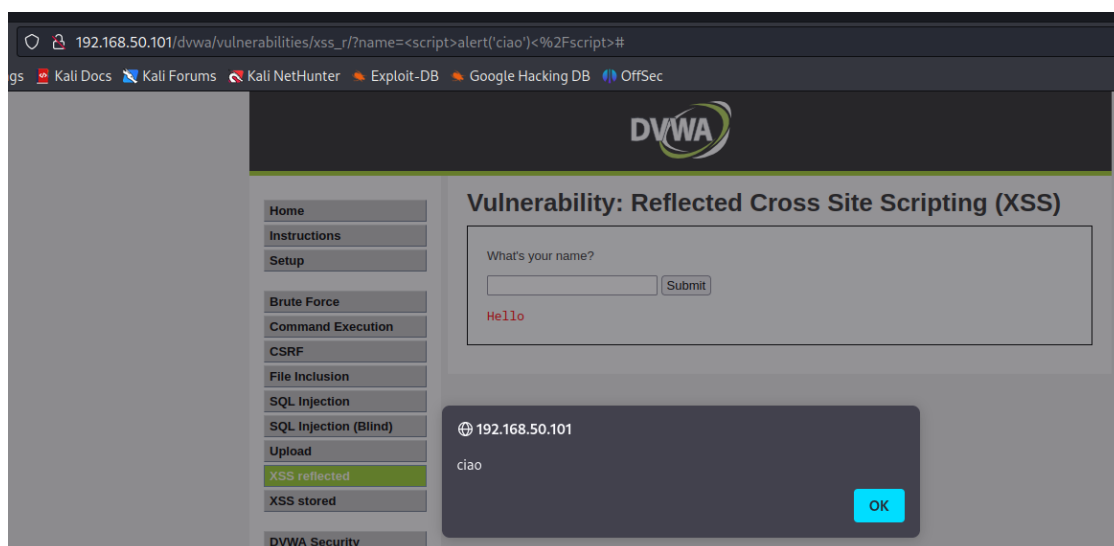
XSS

Raggiungo la DVWA e setto il livello di sicurezza a <low>. Andando sulla schermata di XSS, provo vari comandi come negli screen di seguito.

Nel campo di input, inserisco `<i> ciao </i>` mi restituisce l'input in corsivo.

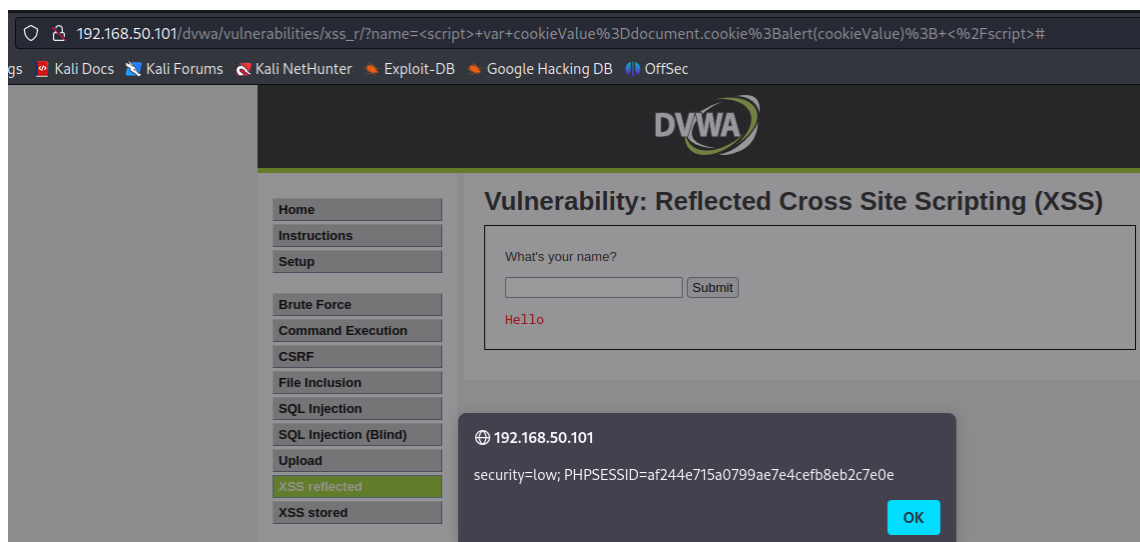


Qui invece vado ad inserire uno script per lanciare un alert a schermo, `<script>alert('ciao')</script>`



Nell'esempio che segue, ho scritto uno script che mi manda in alert, la sessione dell'utente.

`<script>var cookieValue=document.cookie;alert(cookieValue);</script>`



SQL Injection

Con la stringa **1' or '1' = '1**, mi manda in input tutti gli utenti registrati in database, con first name e surname. La condizione è sempre vera, quindi mi manda tutti gli id presenti nel database



Invece con la stringa **' UNION SELECT user, password FROM users#** vado a selezionare gli user e le password da users. Così manda a schermo il nome utente con la relativa password.

