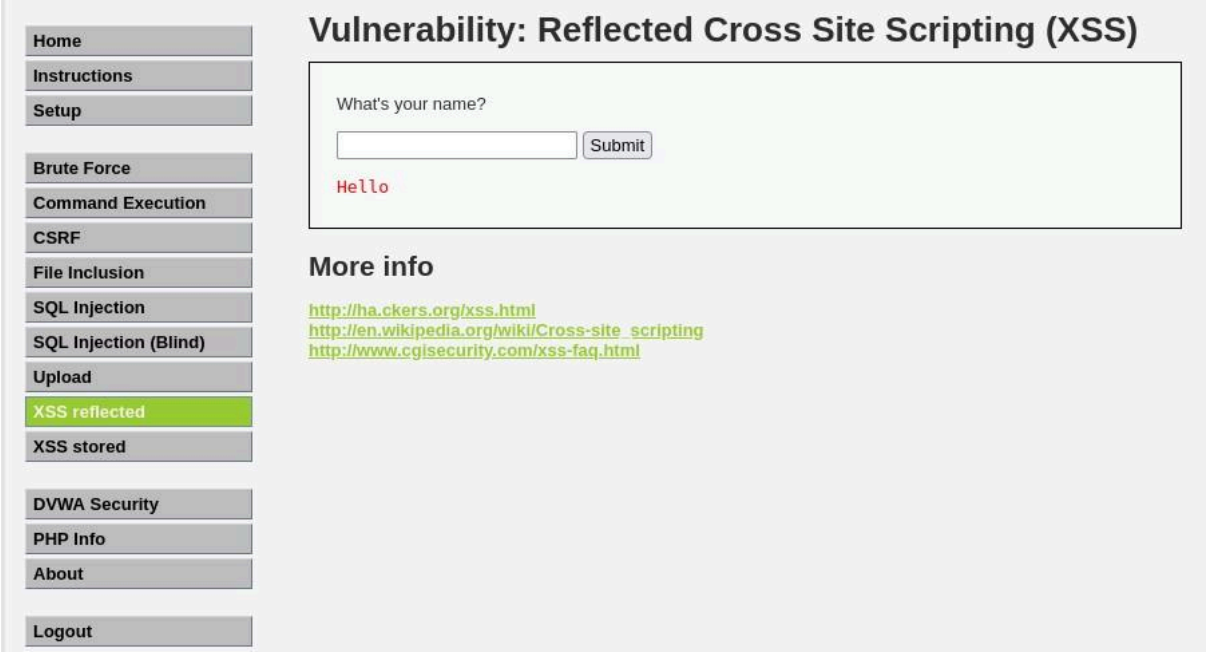
S6/L2

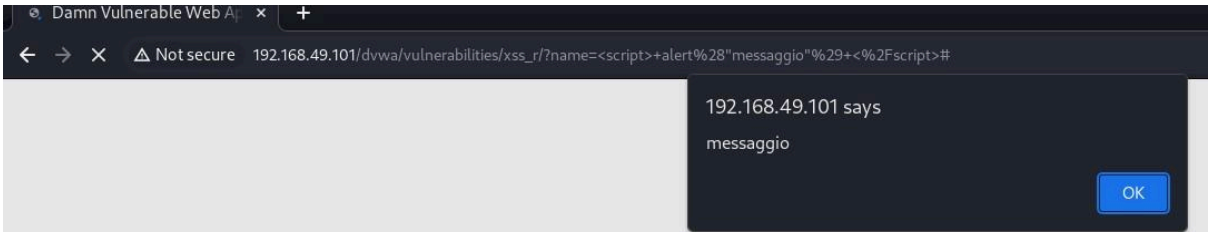
Il compito di oggi consiste in 2 lavori separati, XSS reflected e SQL injection.

Il Cross site scripting (XSS) è una famiglia di vulnerabilità che permettono ad un potenziale attaccante di prendere il controllo su una Web App e sulle sue componenti con impatti molto gravi sugli utenti.

Vedremo adesso l'esercizio svolto su DVWA.
Inseriamo nel riquadro lo script: <script> alert(“messaggio”) </script>



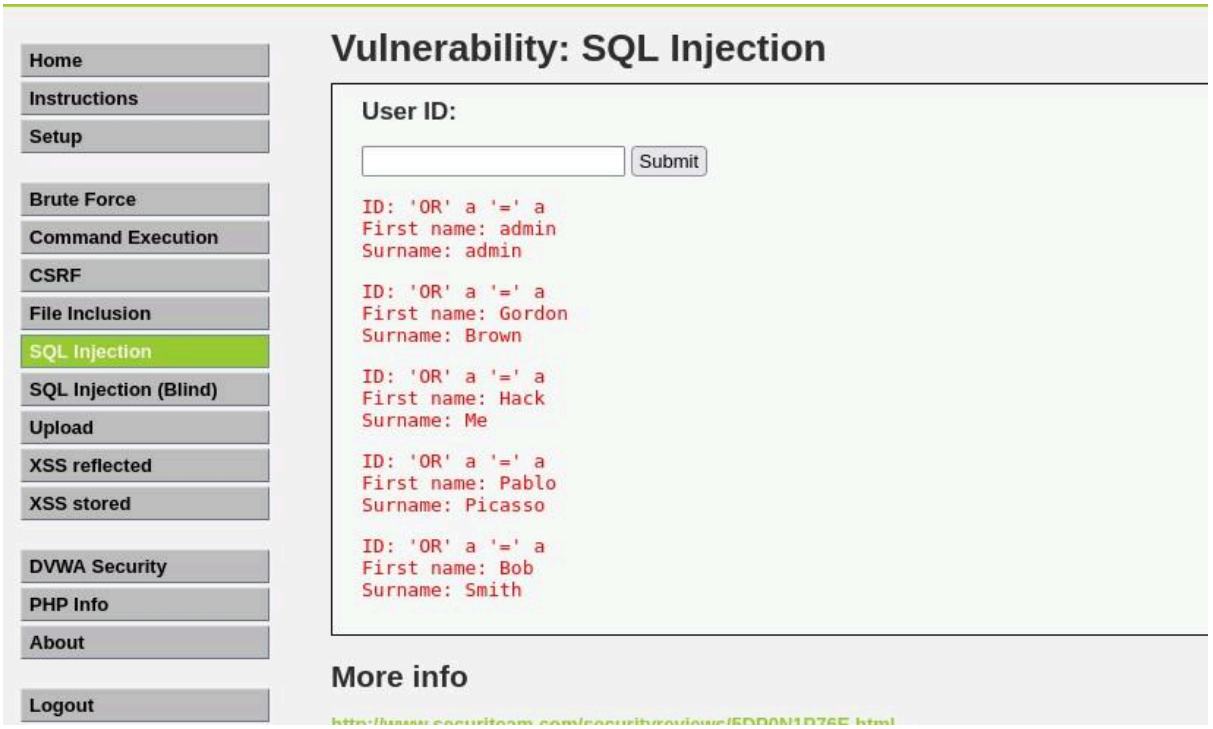
Il sito ci restituirà la stringa che abbiamo scritto nella parentesi.



SQL INJECTION

Un attacco di tipo SQL injection (SQLi) permette ad un utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un'applicazione Web. Questa tipologia di attacco ha impatti negativi enormi sui siti web.

Nel nostro caso dovremmo individuare il database nel quale sono contenute le credenziali degli account collegati al sito. Utilizziamo l'operatore 'OR' nel codice 'OR' a'='a; Poniamo la a uguale ad un'altra a per determinare una condizione sempre vera così da restituire tutti i nomi del database.



L'ultimo passaggio da fare, sempre con il comando "UNION" è quello di trovare username e password.

Scriviamo il codice ' UNION SELECT user, password FROM users#’ e troviamo username e password del database