XSS & SQL Injection

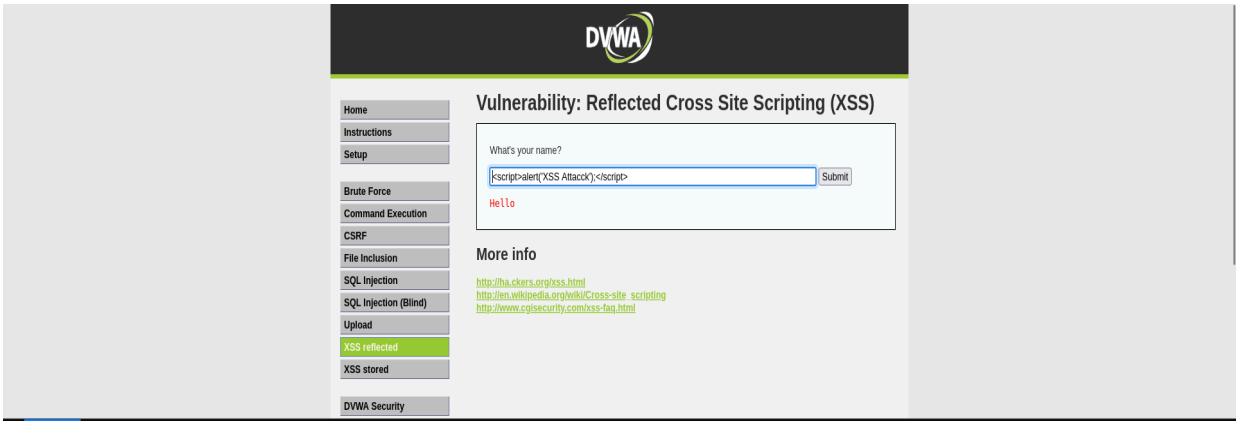
Obiettivo

Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application DVWA.

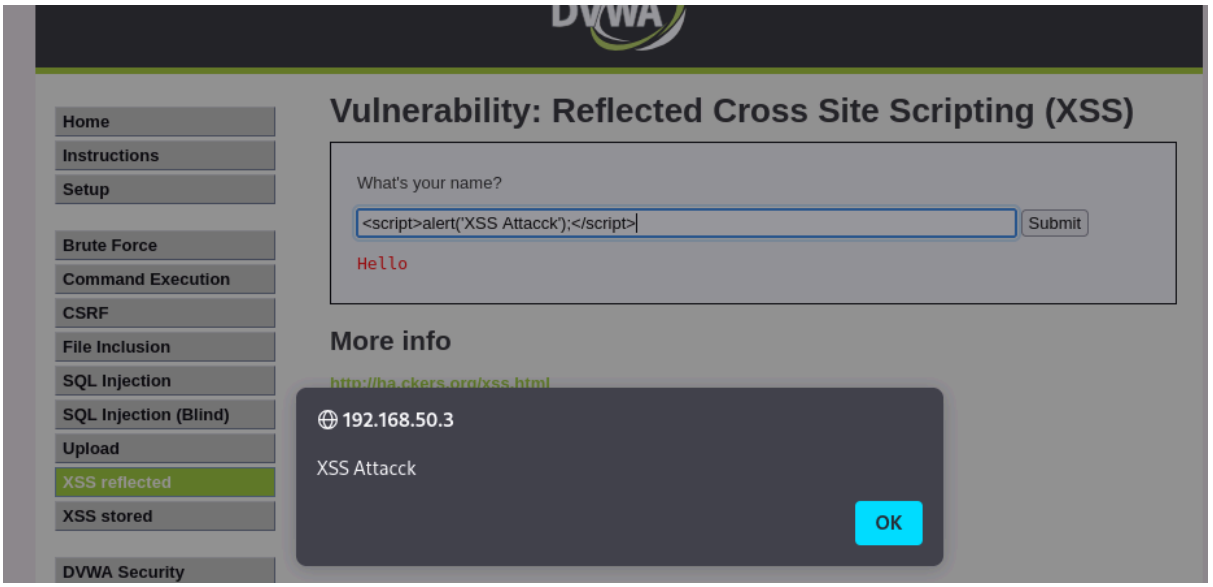
XSS Reflected

Security Low

Andiamo ora ad analizzare nello specifico ciò che concerne un tipo di attacco XSS Reflected. Come possiamo vedere negli screen sottostanti un attaccante potrebbe andare ad inserire del codice JavaScript all'interno del campo di ricerca (In questo caso <script> alert('XSS Attack');</script>)



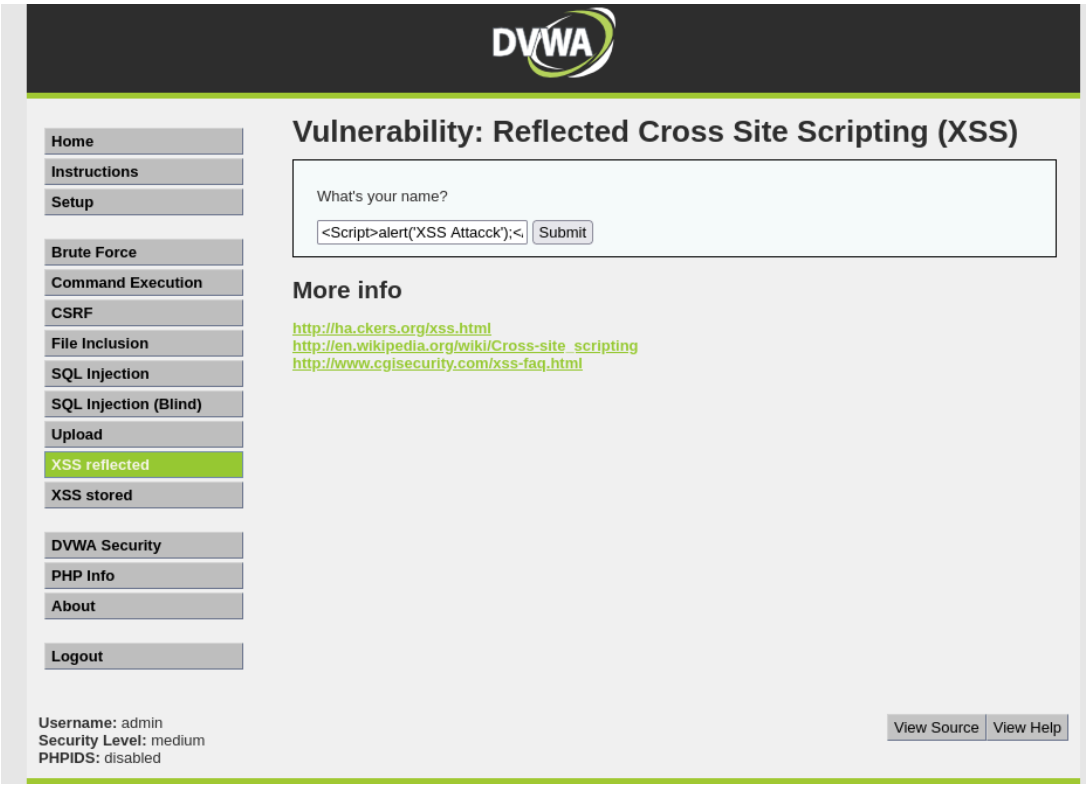
Il server prende l'input dell'utente e lo inserisce direttamente nel contenuto HTML della pagina dei risultati.



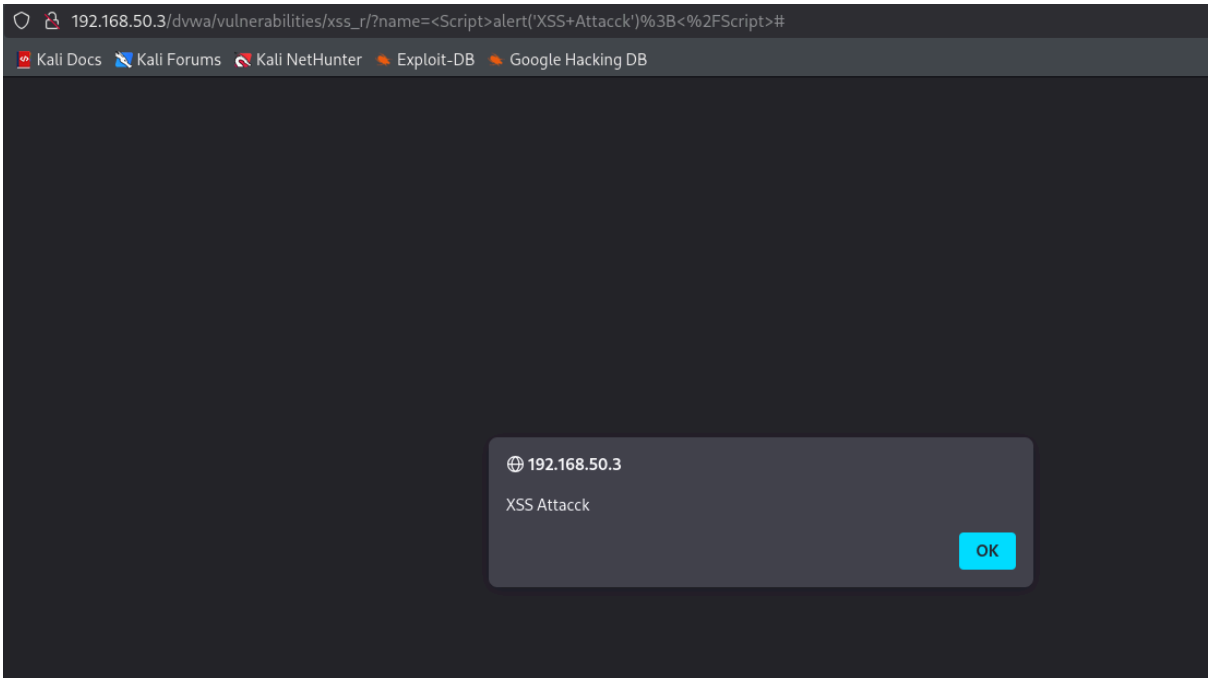
Security Medium

Per quanto riguarda il caso in cui la security impostata su Medium come possiamo vedere viene effettuata una ‘sanificazione’ dell’input (`echo 'Hello ' . str_replace('<script>', '', $_GET['name']);`

Ma questo tipo di sanificazione non è abbastanza in quanto essendo i tag di javascript casesensitive è possibile utilizzare lo stesso comando modificandolo per ottenere lo stesso risultato come mostrato in figura. Quindi modificando il tag con <Script>alert(‘testo’);</Script>



Otteniamo come aspettato



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.
La query è progettata per estrarre i nomi delle tabelle dal database dvwa e visualizzarli sull'interfaccia dell'applicazione, sfruttando una vulnerabilità SQL Injection di tipo **UNION.**

' UNION SELECT table_name,null FROM information_schema.tables WHERE table_schema = 'dvwa' -- -

Affinché **UNION** funzioni, il numero e il tipo di colonne della query iniettata devono corrispondere al numero e al tipo di colonne della query originale
-- : È il simbolo standard di commento in SQL che dice al server di ignorare tutto ciò che segue fino alla fine della riga.
- : A volte viene aggiunto per assicurare che, se l'applicazione aggiunge automaticamente una virgoletta singola o un punto e virgola dopo l'input, il commento sia comunque valido.

Come possiamo vedere dall’esecuzione della query ci vengono restituiti i nomi delle tabelle del database DVWA.