lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

-SQL Injection (non blind).

-XSS reflected

SQL INJECTION

Nell’esercizio è stato inserito una query per mostrarci le pasword degli user presenti nel database, questo è il risultato (le password sono protette da codice hash)

A screenshot of a computer

Description automatically generated

Quello che abbiamo inserito è riportato nella foto successiva.

Abbiamo preso il codice sorgente scritto in php cliccando su view source e lo scopo dell’attacco consisteva nel sostituire ‘$id’ con il segunete parametro ' UNION SELECT user\_id,password FROM users #'";

l comando UNION, esegue un’unione tra due risultati (per esempio tra due SELECT). quindi apriamo un apice per inserire il corpo della query dove andremo a dire seleziona user id e dammi la password per ogni user successivamente abbiamo messo il cancelletto per andare a commentare il ‘”; del database vero e propri.

Cosi facendo abbiamo inserito all’interno della query questa nostra richiesta di ottenere le password

A screenshot of a computer

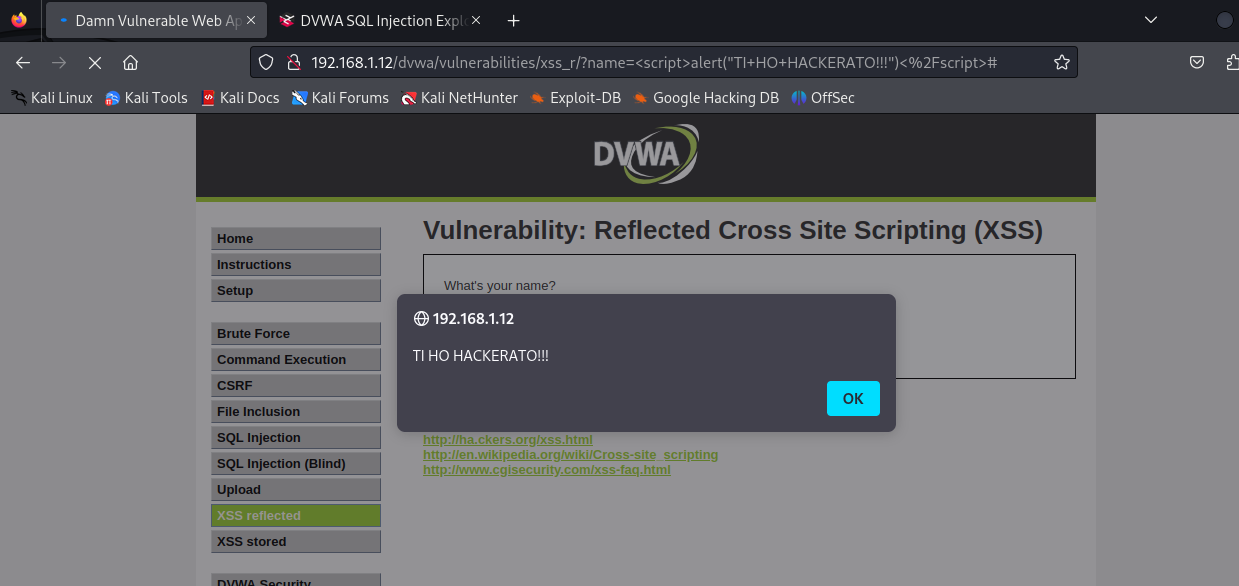
Description automatically generated

XSS reflected

Gli attacchi di tipo XSS riflesso avvengono quando il payload malevolo viene trasportato dalla richiesta che il browser della vittima invia al sito vulnerabile.

Nell’esercizio ci è bastato scrivere un banalissio script in js che abbiamo fatto eseguire dal browser.

Il risultato è il seguente



Lo script eseguito è un semplice all’alert dove abbiamo scritto al suo interno TI HO HACKERATO!!!