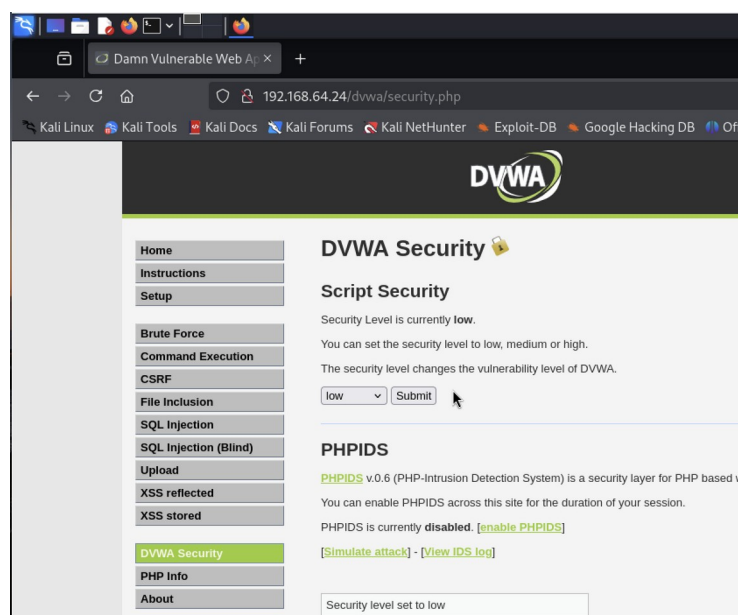


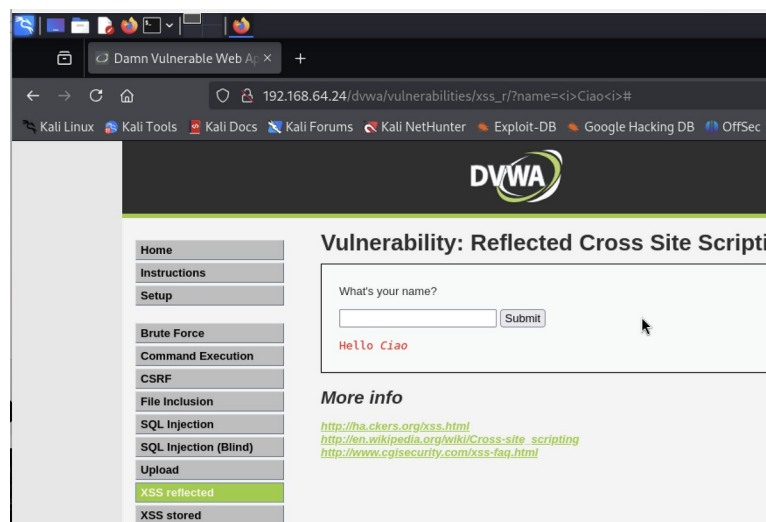
L'esercitazione di oggi prevedeva di:

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

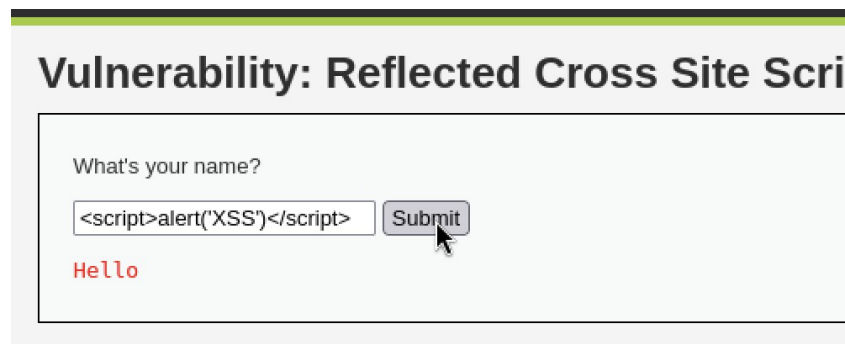
Il primo passo è fare il ping tra Metasploit e Kali per verificare la connessione, quindi ping <ip>, prima dal indirizzo di kali a metasploit e poi viceversa, verificata la connessione procediamo come segue l'immagine, ossia rechiamoci sulla DVWA di Metasploit e della sezione DVWA security scegliamo LOW e clicchiamo submit, per aggiornare il livello di sicurezza



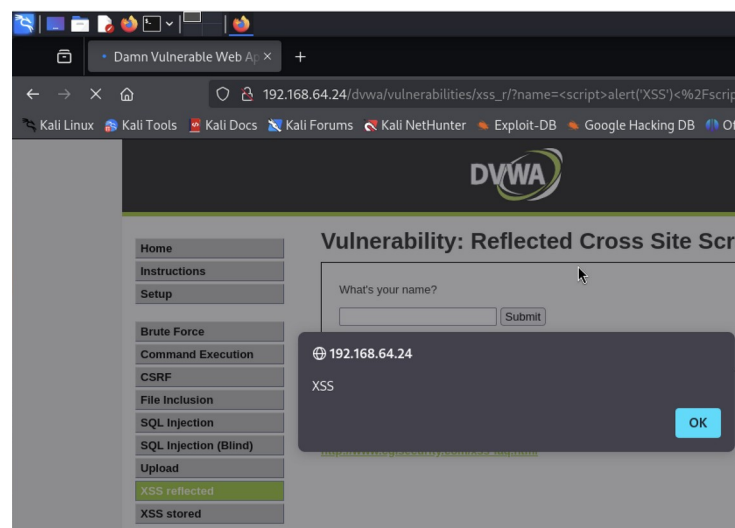
Modificando il livello di sicurezza, procediamo con un clic sulla sezione **XSS reflected**. Come prova per verificarne il funzionamento, inseriamo nel campo di input il seguente codice: <i>Ciao</i>. Come risultato, vediamo che la parola 'Ciao' viene visualizzata in corsivo (italic)



Conclusa la prova, ora inseriamo, tramite JavaScript, un alert() come mostrato nell'immagine sottostante.



Ora come risulatiat, otteniamo l'alert come prevsito e clichiamo su ok



Adesso passiamo alla sezione **SQL Injection (Blind)**. Per estrarre dati dal database, inseriamo semplicemente un numero. In questo esempio, ho utilizzato 1 come input.

