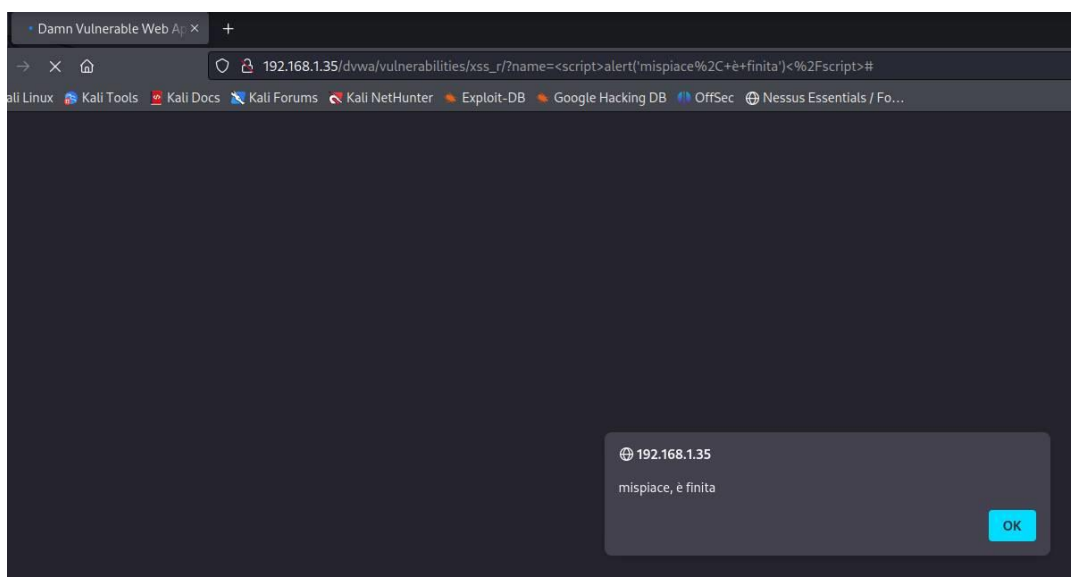
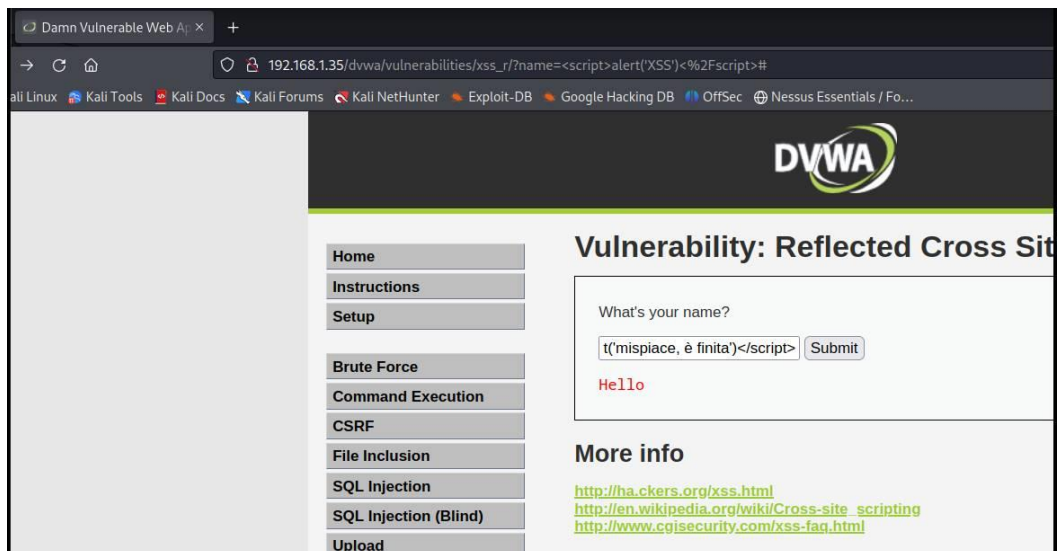


# Esercizio 2 Settimana 6

## XSS – SQL injection

Prendiamo confidenza con gli attacchi XSS e SQL Injection.

1. XSS reflected: sfrutta una vulnerabilità connessa all'esecuzione di codice (script) e all'input dell'utente. Possiamo anche inserire una stringa malevola che porta a siti fasulli e/o pop up non sicuri. Gli script inseriti sono "interpretati", cioè le righe di codice vengono eseguite subito senza salvare (a differenza del compilato). Per fare ciò inseriamo '`<script>alert('scritta')</script>`'. A quel punto basta solo mandare l'URL tramite phishing: una volta aperto il link, il codice malevolo si attiva subito e manda il Malware.



2. SQL Injection: questo attacco va ad agire direttamente sul server che andrà poi a comunicare con il database. Il server, in questo caso, comunicherà in linguaggio SQL le informazioni che verranno comparate nelle tabelle del database.

