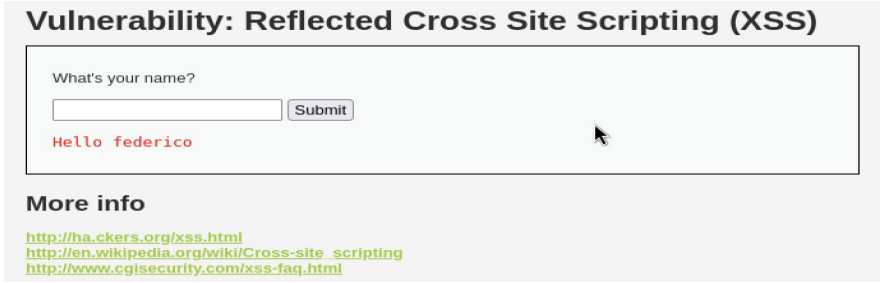
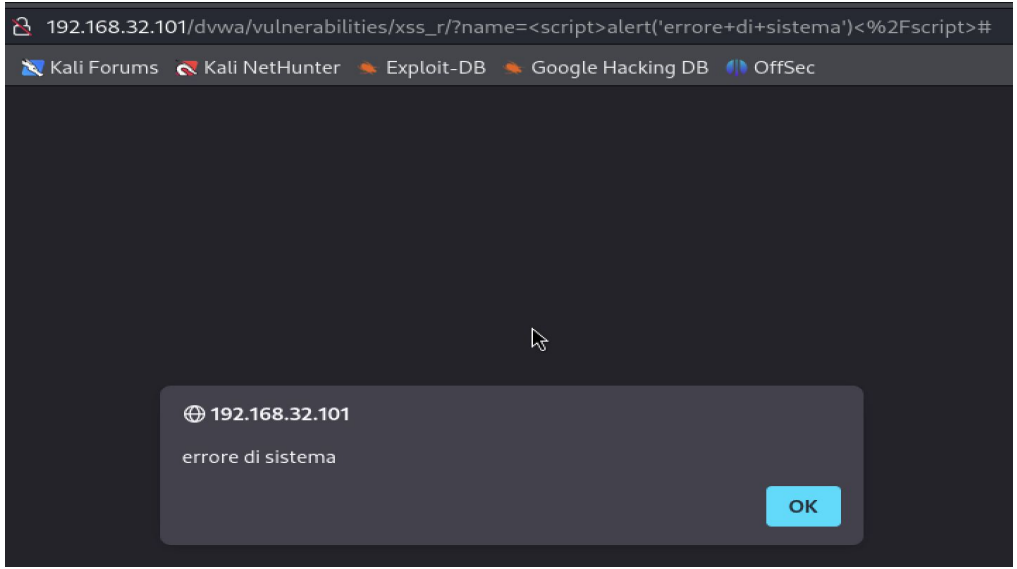
XSS

Dopo aver impostato il livello di sicurezza su low, andiamo alla pagina della vulnerabilità XSS e proviamo ad inserire il nostro nome come richiesto.



Spostandoci sull'Url della pagina possiamo notare che corrisponde il name=...il nome che abbiamo inserito, nel nostro caso federico.

Modificando l'ulr, oppure inserendo lo script direttamente nella barra di submit, possiamo inserire degli script malevoli, in questo caso faremo apparire un messaggio a schermo, nel dettaglio un alert.



SQL Injection

Tentiamo un sqlinjection a livello di sicurezza low

Nel codice sorgente andiamo a visualizzare la query che ci interessa, in questo caso $getid, quindi andiamo a sostituire user_id con una sintassi che sia letta come sempre vera. Possiamo notare che nella richiesta dell'user ID possiamo inserire direttamente la condizione sempre vera, l'output sarà la lista di tutti gli ID dei diversi user.

```
$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
$result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );
```