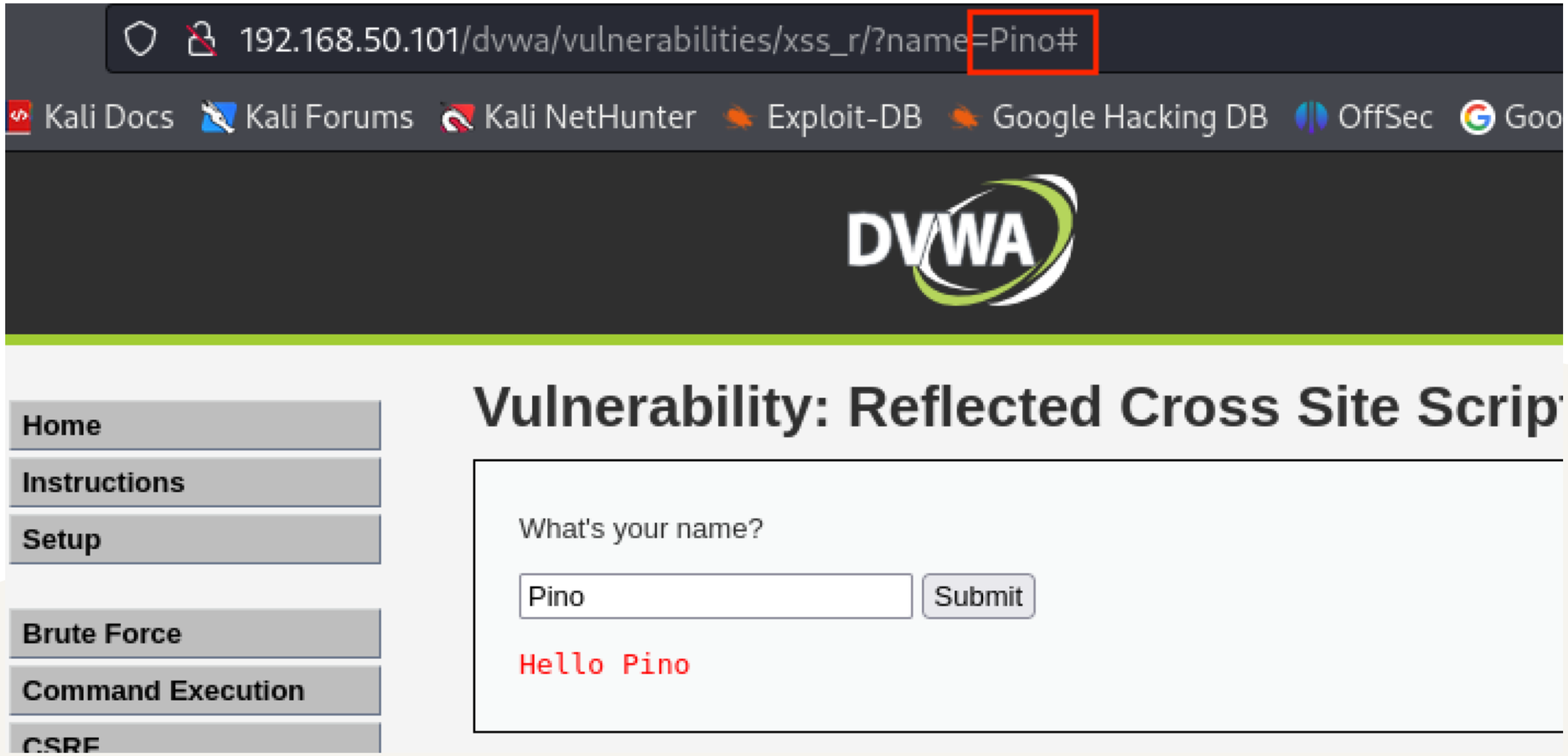
Consegna S6/L2

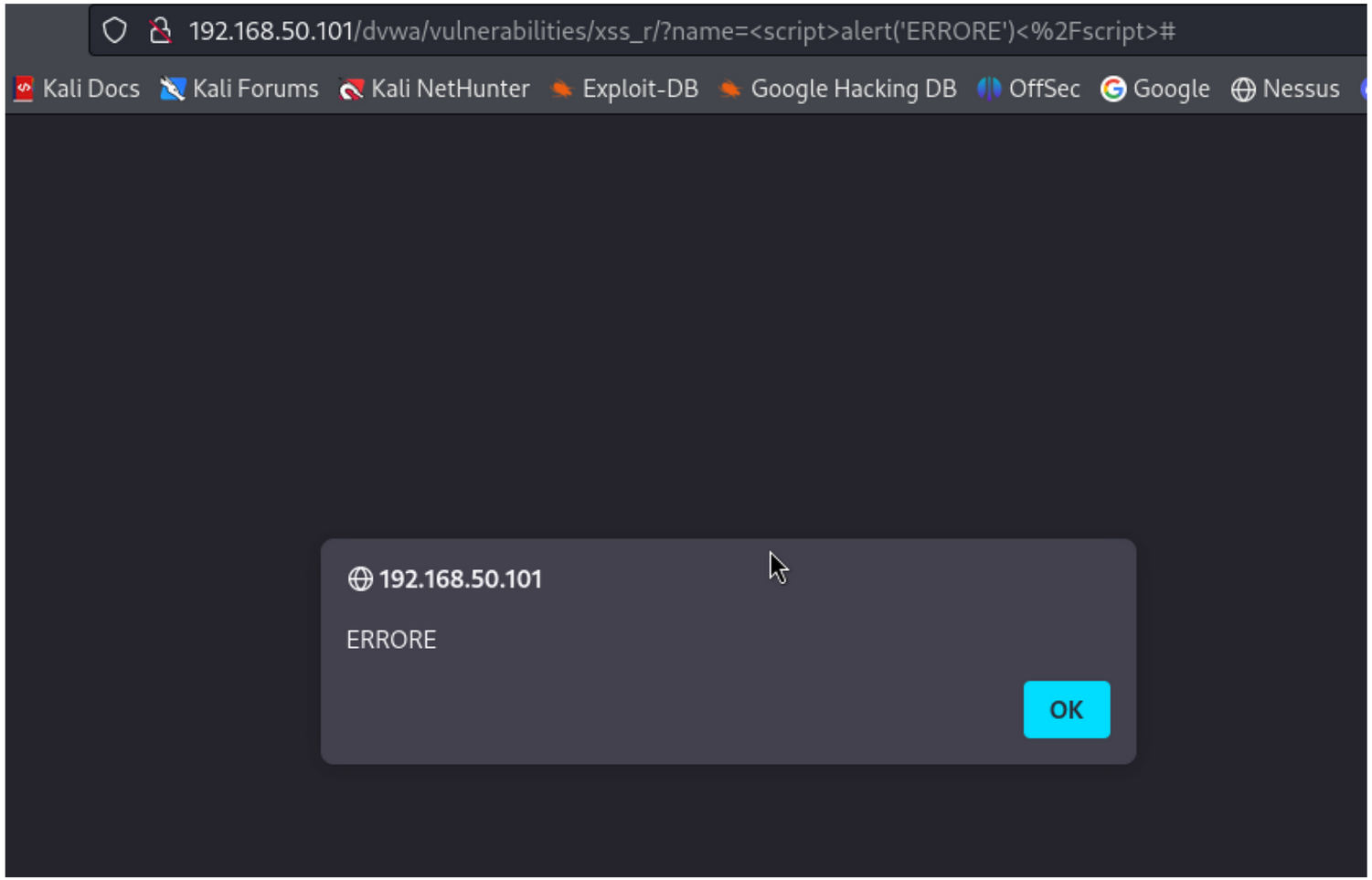
di Giuseppe Lupoi

XSS Reflected

In questa sezione abbiamo a disposizione un campo dove inserire un nome, successivamente noteremo che lo stesso nome inserito dall'utente verrà inserito anche nell'url

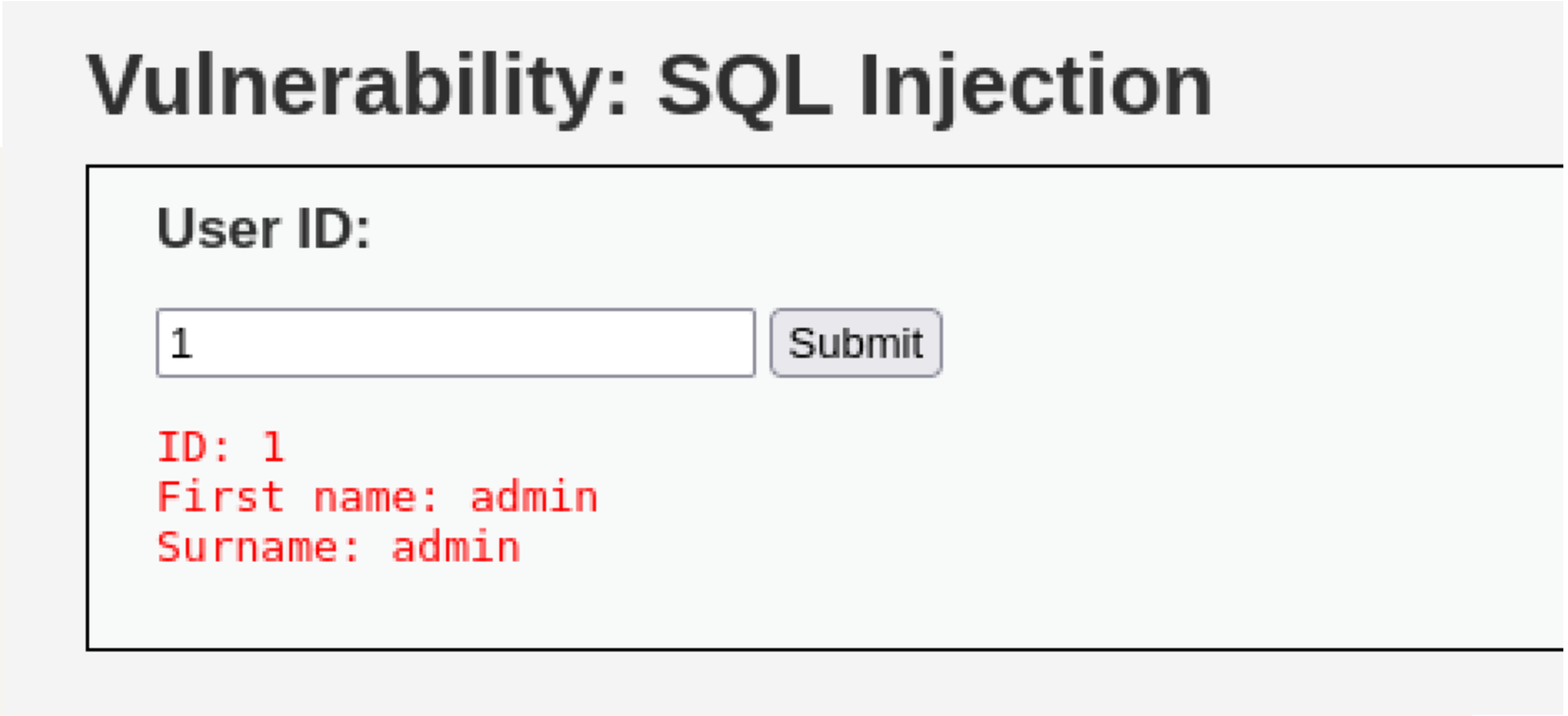


Proviamo dunque ad inserire uno script nello stesso campo dove prima abbiamo inserito il nome “Pino”.
Andremo quindi a scrivere:
<script>alert(‘ERRORE’)</script>
Se tutto funziona correttamente vedremo su schermo un pop-up che riporta il messaggio che abbiamo precedentemente inserito nello script

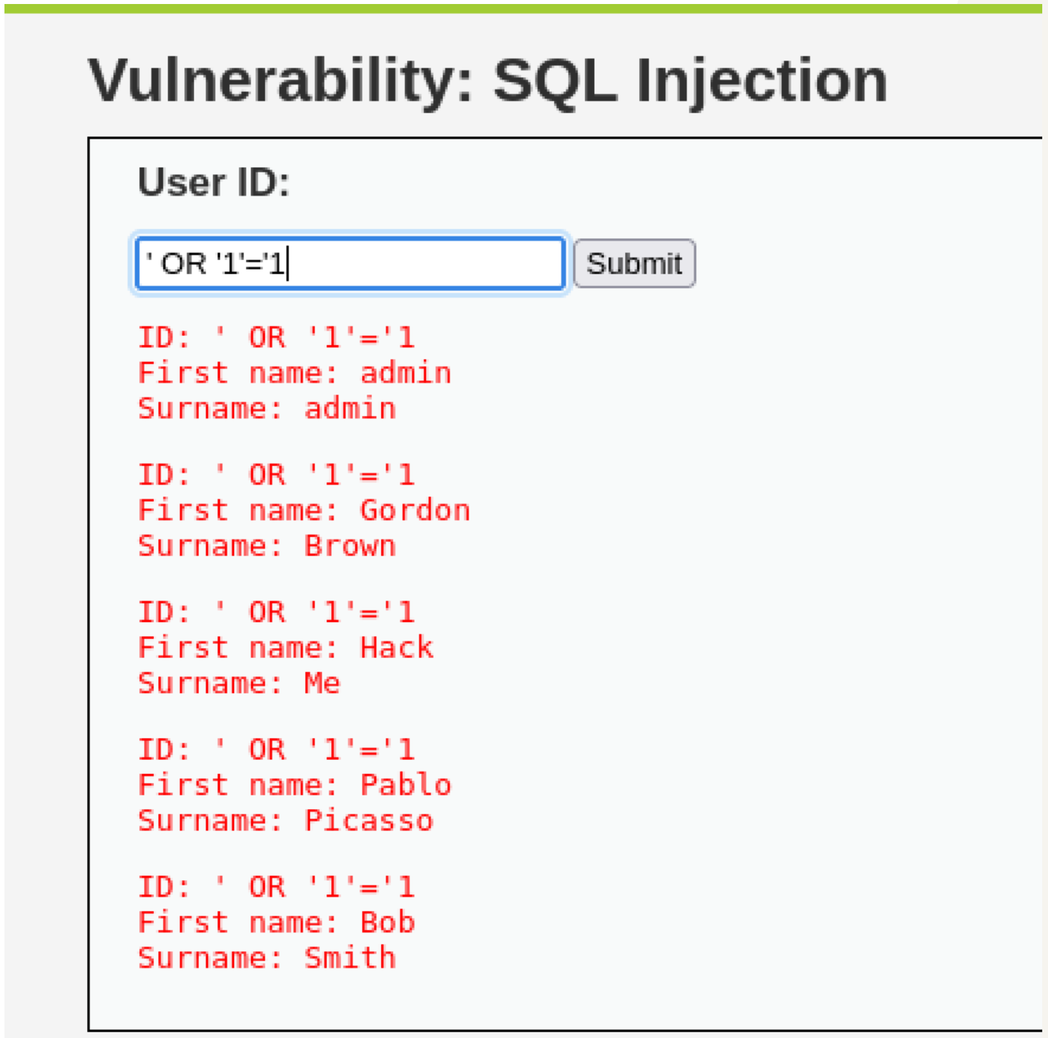


SQL Injection

La pagina **SQL Injection** ci permette, tramite l’inserimento nel suo campo, di avere in output gli user corrispondenti all’input ed attivi sul server



Possiamo provare ad inserire una condizione sempre vera per ricevere in output la lista completa degli user.
Per esempio: **‘ OR ‘1’=’1**



Arrivati a questo punto proveremo ad ingannare il server con una query **UNION**, per farlo dovremmo sapere il numero di parametri richiesti, sappiamo già che sono due: First name, Surname.
Scriveremo quindi: **1'UNION SELECT user, password FROM users#**
L'errore in output sarà quello di mostrare in **First name** il nome dell' user, e come **Surname** la sua password corrispondente cifrata