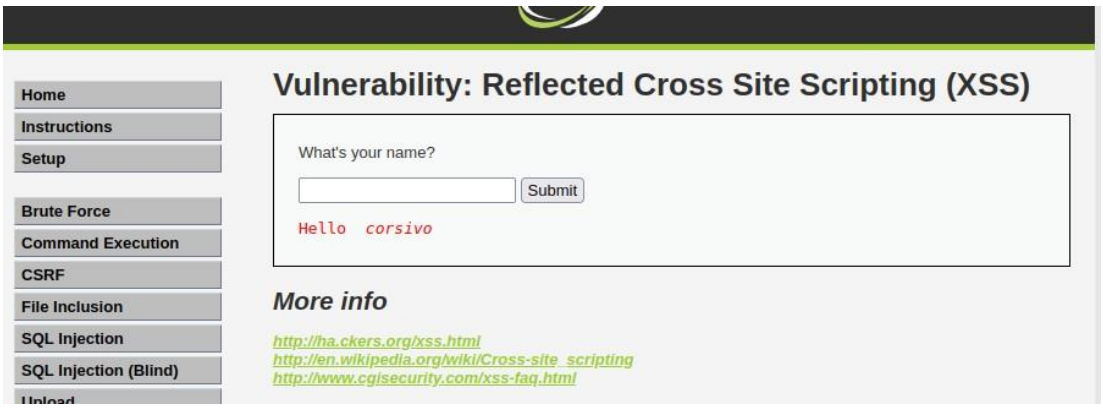
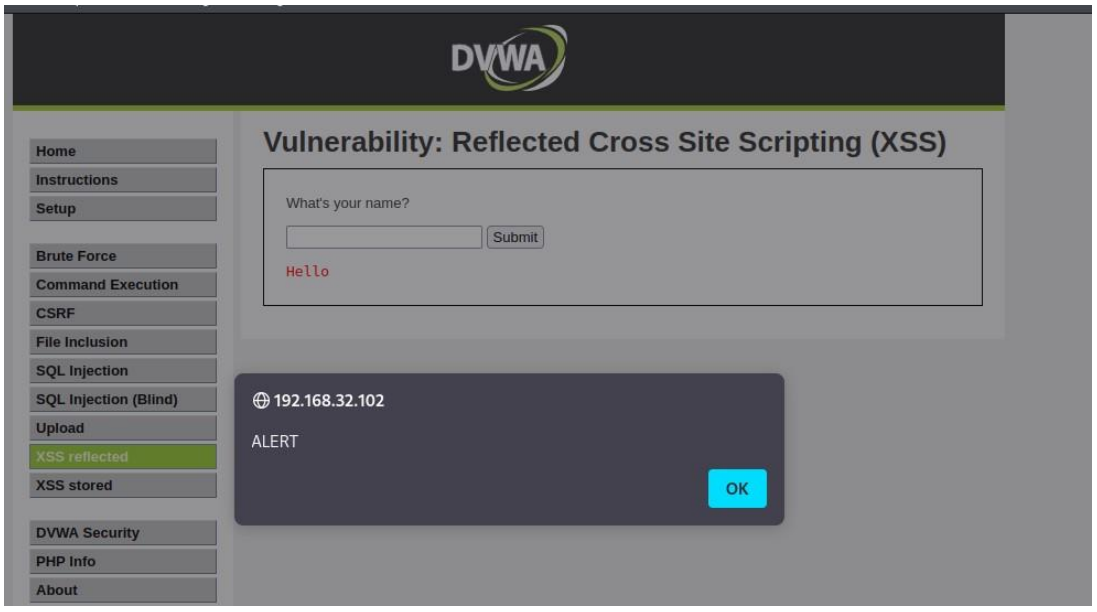
CROSS SITE SCRIPTING E MYSQL INJECTION

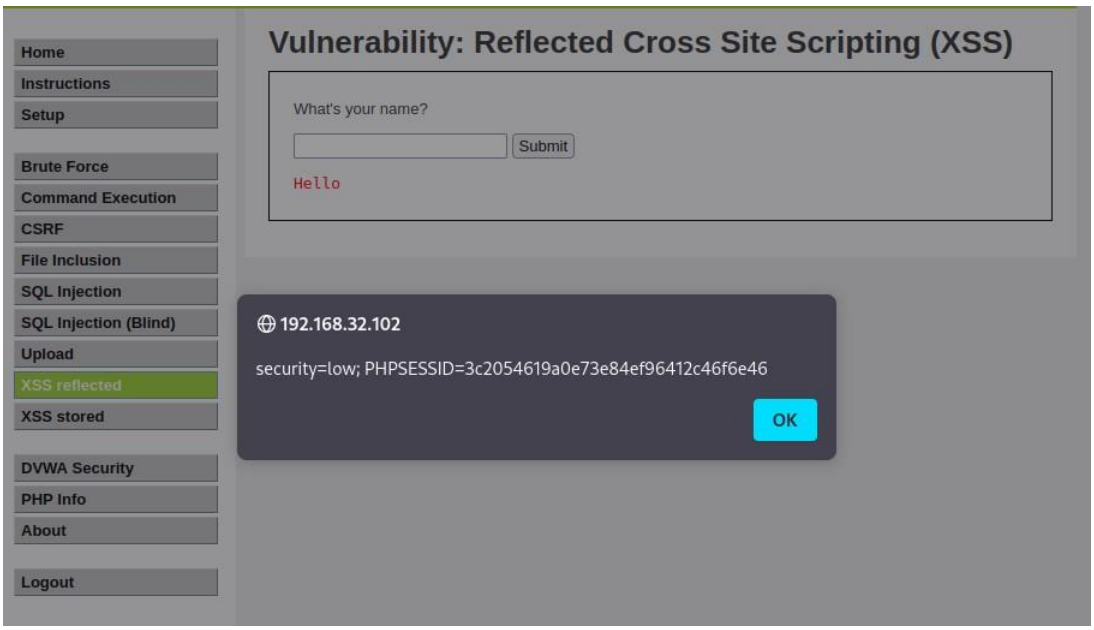
Sfruttando la vulnerabilità di DVWA, possiamo iniettare dello script malevolo all'interno del campo input della sezione XSS Reflected; scrivendo <i> e poi la parola che vogliamo (in questo caso ho messo 'corsivo'), la facciamo apparire scritta in corsivo:



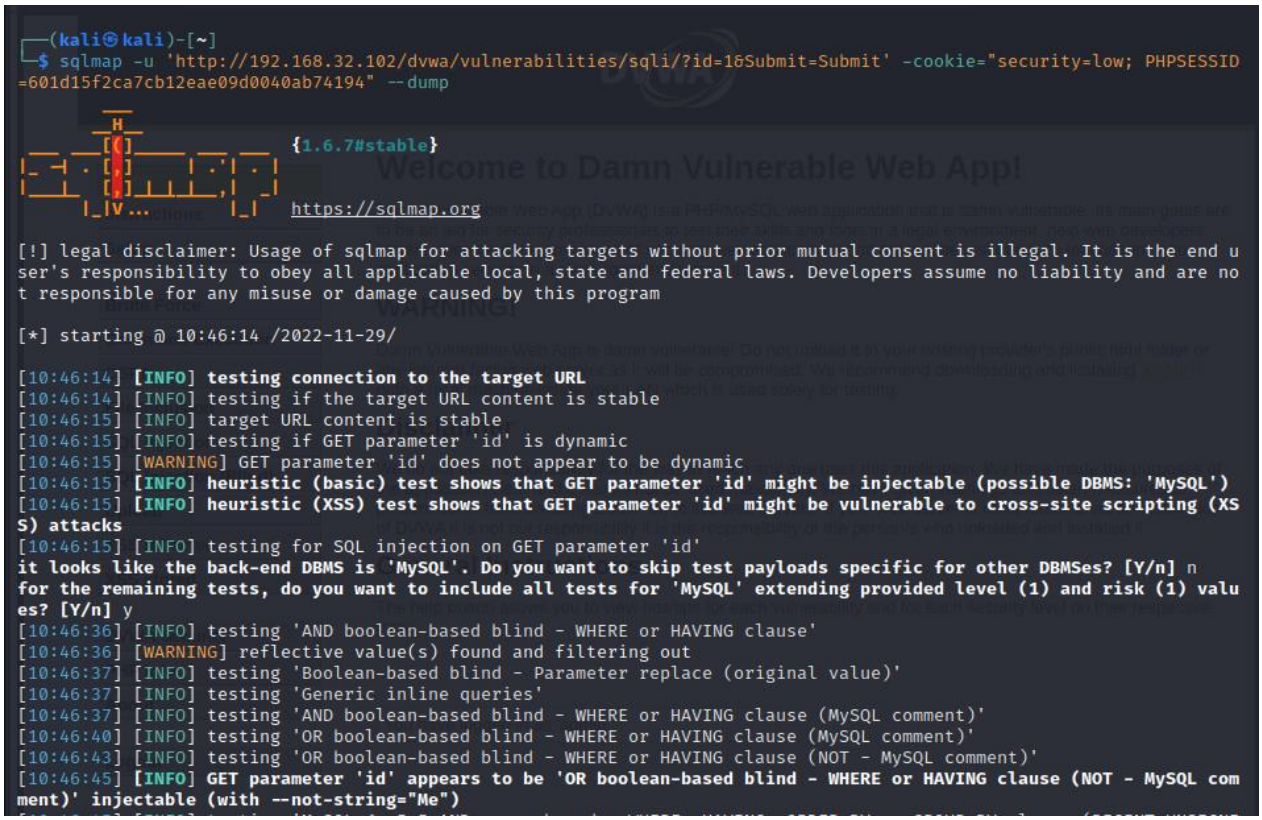
Con il codice <script>alert()</script>, facciamo apparire appunto un alert con scritto quello che abbiamo inserito all'interno delle parentesi tonde:



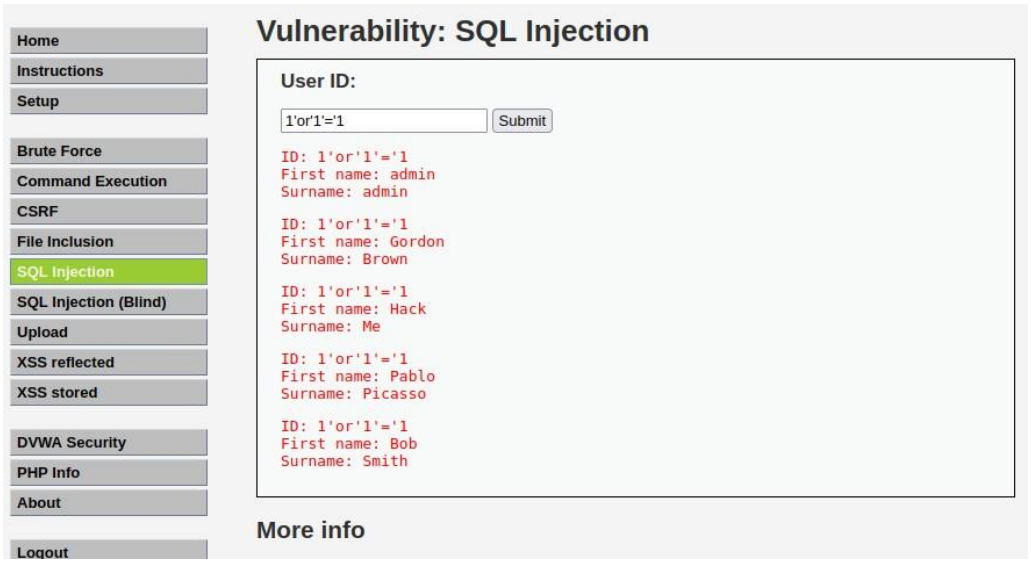
Mentre con il codice <script>alert(document.cookie)</script>, facciamo apparire a schermo il cookie di sessione:



Per i controlli di injection, utilizziamo il tool di Kali chiamato sqlmap:



Di seguito, abbiamo un esempio di 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
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

Qui con UNION: