XSS Exercises

Go to https://google-gruyere.appspot.com/ and try the exercices File Upload XSS, Reflected XSS, Stored XSS, Stored XSS via HTML Attribute and XSRF Challenge.

SQL Exercises

Start a VM. For the network you have to choose an option that allows a host (or another virtual machine if you are working in one) to connect to the VM.
Login/password for the VM: ingi/uclouvain
Inside the VM run "ifconfig" command and find its IP.

For the remaining, you don't need to work in the VM, but it must be running.
Open in your browser VM_IP/dvwa/
Username/password: admin/password

In case of problems with the website, e.g. security level is not changing or constant error "Something went wrong", try to logout, clear cookies for the website might need to restart VM.

We are going to do exercises SQL injection and SQL injection (Blind).
For both of the exercises there are several security levels that can be setup in the DVWA Security tab. The goal of both exercises is to get the list of Users.

SQL Injection:

1) Security setting Low

Hint:
[redacted]

Solution:
[redacted]

2) Security setting Medium

Now there is no input box. But there is a select box. Therefore the webpage sends the chosen value to the server. The request can be analysed in the webdevelopers tools.

Hint:
[redacted]

Solution:
[redacted]

3) Security setting Hard

The application in this setting runs a query with a LIMIT 1, that limits the output number of rows.

Hint:
[redacted]

Solution:
[redacted]

SQL Injection (Blind):

For this exercise we are going to use sqlmap tool.
sqlmap --help command shows available options
(or it could be python sqlmap.py --help)

From the webdevelopers tools you need the following information:
- Url address the request is send to
- Cookie

The request should look like :
python3 sqlmap.py -u "http://<VM_IP>/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="PHPSESSID=<Cookie>; security=low"

1) Low security:
You need to find the list of users with sqlmap. Start by enumerating databases: use an option --dbs

Hint 1
[redacted]

Hint 2
[redacted]

Guess which table contains users.

Solution
[redacted]

2) Medium security:
BEFORE starting the exersice you need to cleanup sqlmap outputs:
rename/remove the folder ‘./sqlmap/output/<VM_IP>’

Notice that url and the cookie has changed!

Hint:
[redacted]

Solution:
[redacted]