02/10/2019 - Francesco Penasa - Homework-3

XSS_2

- Try to add a Button with text me “Click Me”. The button click must trigger an alert with the content “You have a Virus!”

To exploit `xss_2.py` I wrote some html code to close the previously opened `<a>` tag and to display a button with an onclick action.
Furthermore, I hide the rest of the line, opening a new `<a>` tag and setting his CSS to not display it.

```
http://localhost:5000/hello?name="></a>  <!-- close the previous tag -->
<button type="button" onclick="alert('You have a virus!')">Click Me</button>  <!-- define the butt
on and his onclick function -->
<a style="display: none;" href="
```

- Fix the vulnerability

We can sanitize the input parameter using the function `escape` from `html` module, following is showed the piece of code modified in order to fix the XSS vulnerability. `name = escape(request.args.get('name'));`

XSS_3

- The returned website will set you a random cookie. Get that cookies and pass it to GET /secret?cookies= `<your-cookies>`

Using Postman we can send the GET request on `http://localhost:5000/hello?name=Emanuele` this will result in a body representing the content of the webpage, next to the “Body” tab we can see the “Cookies (1)” tab. In such tab we can find the cookie value. In my case the cookie value is `80ff5b23-573e-4a01-ac81-941f9f111ba6`
Otherwise, it is possible to use the `Inspect Element` function of Firefox and search for the cookie in the “Storage” tab, to use it in the next point.

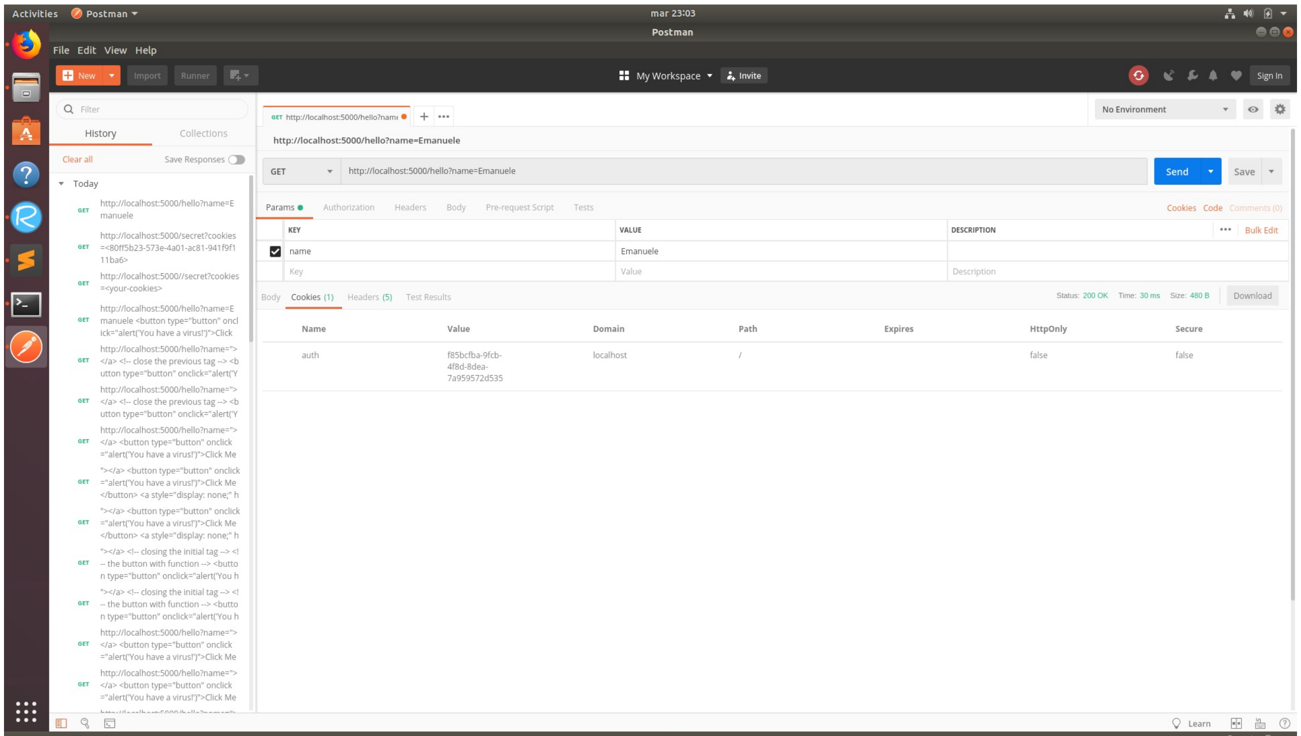
- Assert the cookie is correct, you will receive a webpage with `Congrats!`

Simply call the webpage
`http://localhost:5000/secret?cookies=80ff5b23-573e-4a01-ac81-941f9f111ba6`

- Fix it

As `xss_2.py` we fix this program sanitizing his input variables.
`name = escape(request.args.get('name'))`
`cookies = escape(request.args.get('cookies'))`

In the following pages some screenshots are displayed for more clarity.



http://localhost:5000/hello?name=Emanuele

GET http://localhost:5000/hello?name=Emanuele

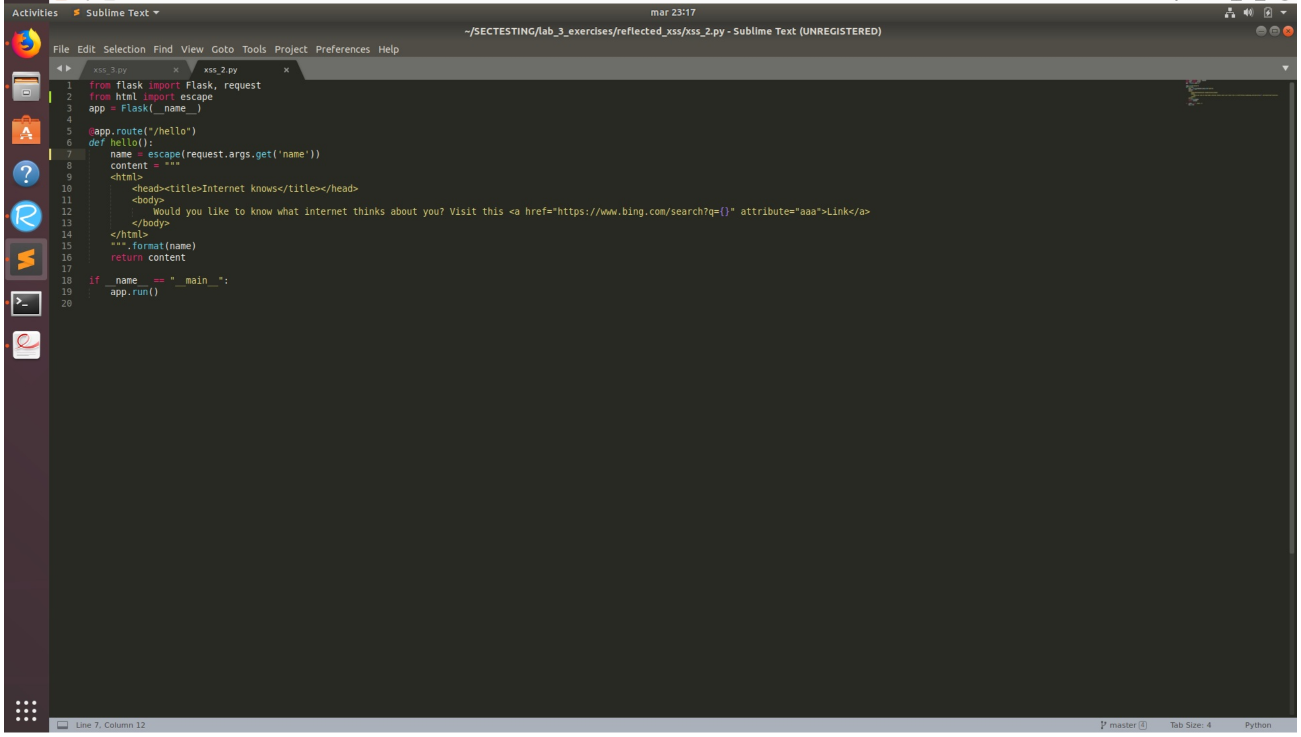
KEY	VALUE	DESCRIPTION
name	Emanuele	

Status: 200 OK Time: 30 ms Size: 480 B

Name	Value	Domain	Path	Expires	HttpOnly	Secure
auth	f85bcfba-9fcb-4f8d-8dea-7a959572d535	localhost	/		false	false

History – Today:

```
GET http://localhost:5000/hello?name=Emanuele
GET http://localhost:5000/secret?cookies=<80ff5b23-573e-4a01-ac81-941f9f111ba6>
GET http://localhost:5000//secret?cookies=<your-cookies>
GET http://localhost:5000/hello?name=Emanuele <button type="button" onclick="alert('You have a virus!')">Click
GET http://localhost:5000/hello?name="></a> <!-- close the previous tag --> <button type="button" onclick="alert('Y
GET http://localhost:5000/hello?name="></a> <!-- close the previous tag --> <button type="button" onclick="alert('Y
GET http://localhost:5000/hello?name="></a> <button type="button" onclick="alert('You have a virus!')">Click Me
GET "></a> <button type="button" onclick="alert('You have a virus!')">Click Me</button> <a style="display: none;" h
GET "></a> <button type="button" onclick="alert('You have a virus!')">Click Me</button> <a style="display: none;" h
GET "></a> <!-- closing the initial tag --> <!-- the button with function --> <button type="button" onclick="alert('You h
GET "></a> <!-- closing the initial tag --> <!-- the button with function --> <button type="button" onclick="alert('You h
GET http://localhost:5000/hello?name="></a> <button type="button" onclick="alert('You have a virus!')">Click Me
GET http://localhost:5000/hello?name="></a> <button type="button" onclick="alert('You have a virus!')">Click Me
```



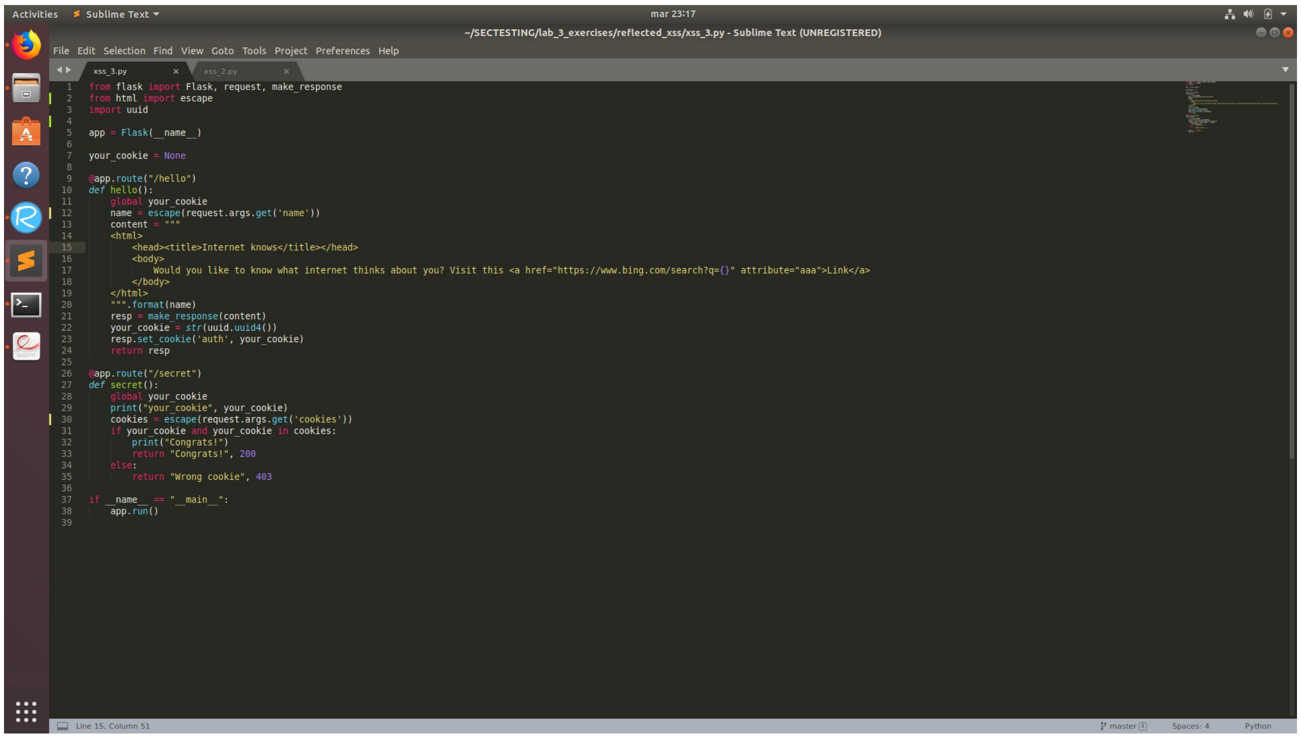
~/SECTESTING/lab_3_exercises/reflected_xss/xss_2.py - Sublime Text (UNREGISTERED)

```python
from flask import Flask, request
from html import escape
app = Flask(__name__)

@app.route("/hello")
def hello():
    name = escape(request.args.get('name'))
    content = """
    <html>
        <head><title>Internet knows</title></head>
        <body>
            Would you like to know what internet thinks about you? Visit this <a href="https://www.bing.com/search?q={}" attribute="aaa">Link</a>
        </body>
    </html>
    """.format(name)
    return content

if __name__ == "__main__":
    app.run()
```

Line 7, Column 12


Activities
Sublime Text
mar 23:17
~/SECTESTING/lab_3_exercises/reflected_xss/xss_3.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
xss_3.py
xss_2.py

```python
from flask import Flask, request, make_response
from html import escape
import uuid

app = Flask(__name__)

your_cookie = None

@app.route("/hello")
def hello():
    global your_cookie
    name = escape(request.args.get('name'))
    content = """
    <html>
        <head><title>Internet knows</title></head>
        <body>
            Would you like to know what internet thinks about you? Visit this <a href="https://www.bing.com/search?q={}" attribute="aaa">Link</a>
        </body>
    </html>
    """.format(name)
    resp = make_response(content)
    your_cookie = str(uuid.uuid4())
    resp.set_cookie('auth', your_cookie)
    return resp

@app.route("/secret")
def secret():
    global your_cookie
    print("your_cookie", your_cookie)
    cookies = escape(request.args.get('cookies'))
    if your_cookie and your_cookie in cookies:
        print("Congrats!")
        return "Congrats!", 200
    else:
        return "Wrong cookie", 403

if __name__ == "__main__":
    app.run()

```