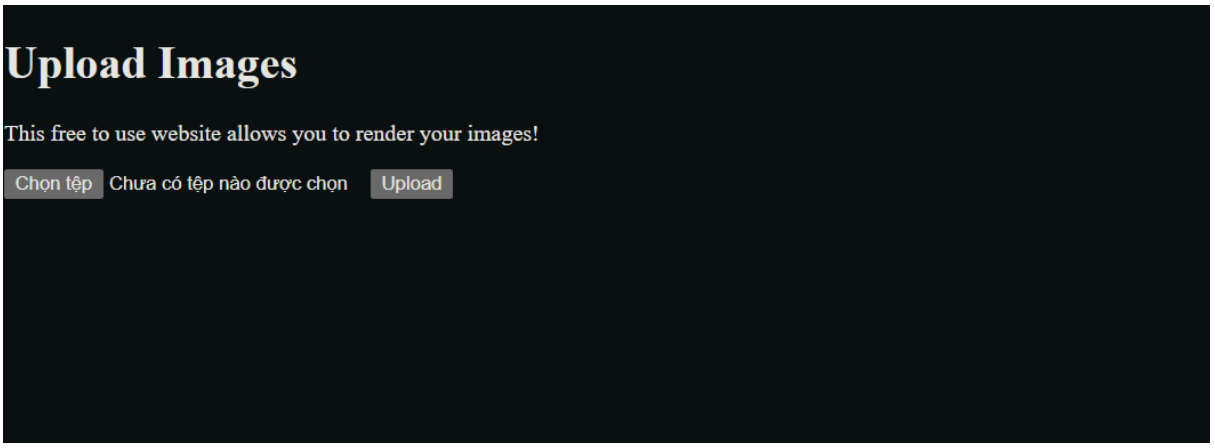
Script CTF 2025

Firstblood: Renderer



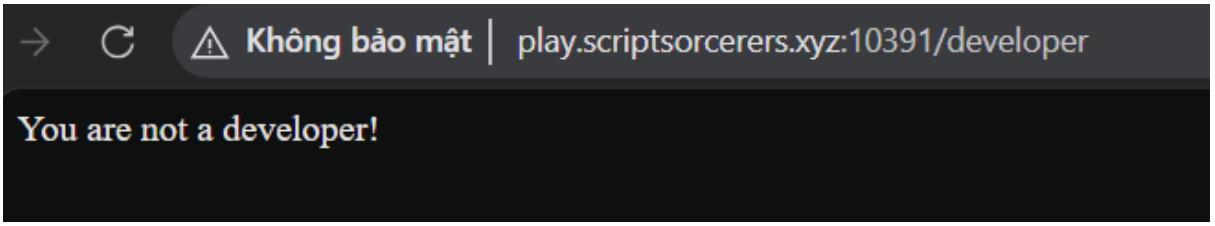
Ban đầu thì t đã tưởng là sẽ dùng XXE Injection để chèn tệp vào nhưng nó không thật sự làm được gì cả.

```
from flask import Flask, request, redirect, render_template, make_response,
url_for
app = Flask(__name__)
from hashlib import sha256
import os
def allowed(name):
    if name.split('.')[1] in ['jpg','jpeg','png','svg']:
        return True
    return False

@app.route('/',methods=['GET','POST'])
def upload():
    if request.method == 'POST':
        if 'file' not in request.files:
            return redirect(request.url)
        file = request.files['file']
        if file.filename == '':
```

```
            return redirect(request.url)
        if file and allowed(file.filename):
            filename = file.filename
            hash = sha256(os.urandom(32)).hexdigest()
            filepath = f'./static/uploads/{hash}.{filename.split(".")[1]}'
            file.save(filepath)
            return redirect(f'/render/{hash}.{filename.split(".")[1]}')
    return render_template('upload.html')

@app.route('/render/<path:filename>')
def render(filename):
    return render_template('display.html', filename=filename)

@app.route('/developer')
def developer():
    cookie = request.cookies.get("developer_secret_cookie")
    correct = open('./static/uploads/secrets/secret_cookie.txt').read()
    if correct == '':
        c = open('./static/uploads/secrets/secret_cookie.txt','w')
        c.write(sha256(os.urandom(16)).hexdigest())
        c.close()
    correct = open('./static/uploads/secrets/secret_cookie.txt').read()
    if cookie == correct:
        c = open('./static/uploads/secrets/secret_cookie.txt','w')
        c.write(sha256(os.urandom(16)).hexdigest())
        c.close()
        return f"Welcome! There is currently 1 unread message: {open('flag.tx
t').read()}"
    else:
        return "You are not a developer!"

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=1337)
```

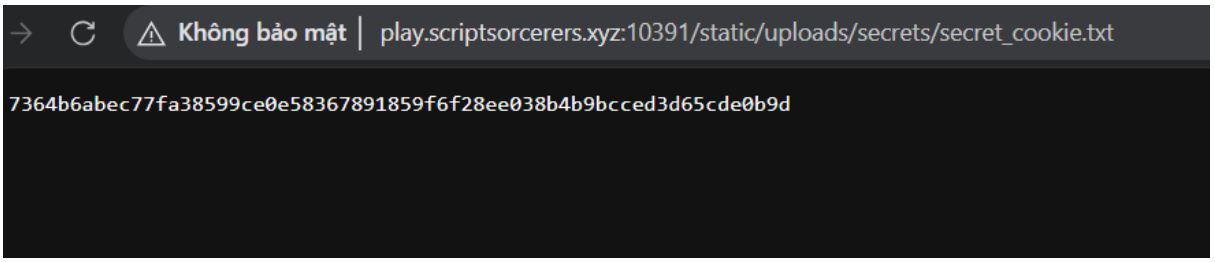
Có thể thấy ở phần developer có vài dòng lệnh khá hay ho

Thử /developer trước nhé.



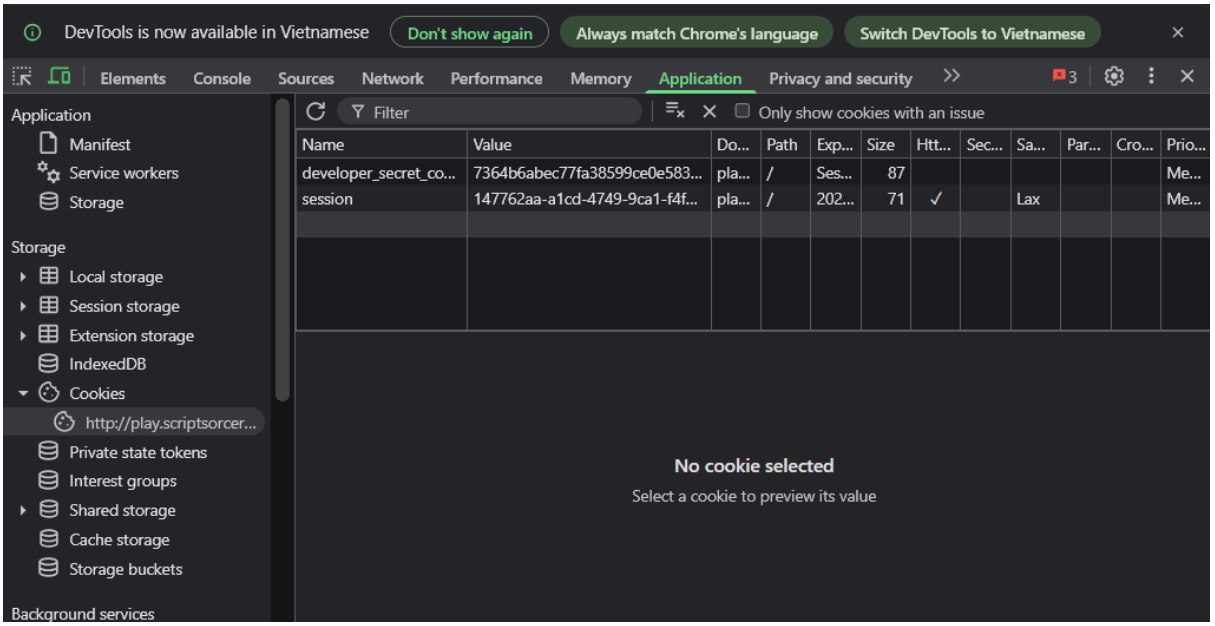
Nếu mà vào /static/uploads/secrets/secret_cookie.txt luôn mà không vào /developer từ trước thì nó sẽ không tạo ra 16 kí tự ngẫu nhiên nên phải vào /developer trước dù muốn hay không.

Giờ mới vào /static/uploads/secrets/secret_cookie.txt nè.



Copy dòng quan trọng.

Tạo 1 cookie với dòng như thế này:



developer_secret_cookie

7364b6abec77fa38599ce0e58367891859f6f28ee038b4b9bcced3d65cde0b9d

Giải thích sơ qua thì cookie là thứ dùng để ghi nhớ bạn là ai để lần sau không phải đăng nhập lại hay đăng kí lại nữa. Trong trường hợp này là ta đã ăn cắp được cookie của admin nên web cũng sẽ tự nhận diện ta là admin giống như vậy.

Nhận xét: Giải này khá là khó, vì trừ cái đầu ổn thì mấy cái sau đều rất khó và nằm trong phạm trù bảnh chưa gặp bao giờ nên thật sự là cũng không thể đánh giá công tâm các challenge sau được.

https://medium.com/@D4LTON/write-up-wizard-gallery-scriptctf-783f88486a89

Writeup: Wizard Gallery