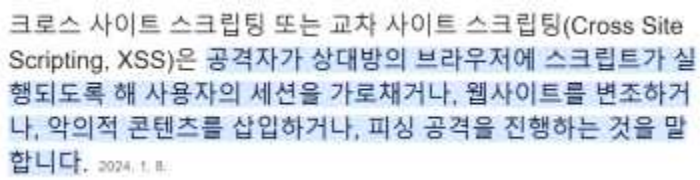
xss 문제풀이

문제를 받고 압축을 풀어보니 여러 파일이 나왔다.

app 이라는 파이썬 코드가 나왔는데 열심히 해석해보니

```python
#!/usr/bin/python3
from flask import Flask, request, render_template
from selenium import webdriver
from selenium.webdriver.chrome.service import Service
import urllib
import os

app = Flask(__name__)
app.secret_key = os.urandom(32)

try:
    FLAG = open("./flag.txt", "r").read()
except:
    FLAG = "[**FLAG**]"


def read_url(url, cookie={"name": "name", "value": "value"}):
    cookie.update({"domain": "127.0.0.1"})
    try:
        service = Service(executable_path="/chromedriver")
        options = webdriver.ChromeOptions()
        for _ in [
            "headless",
            "window-size=1920x1080",
            "disable-gpu",
            "no-sandbox",
            "disable-dev-shm-usage",
        ]:
            options.add_argument(_)
        driver = webdriver.Chrome(service=service, options=options)
        driver.implicitly_wait(3)
        driver.set_page_load_timeout(3)
        driver.get("http://127.0.0.1:8000/")
        driver.add_cookie(cookie)
        driver.get(url)
    except Exception as e:
        driver.quit()
        # return str(e)
        return False
    driver.quit()
    return True


def check_xss(param, cookie={"name": "name", "value": "value"}):
    url = f"http://127.0.0.1:8000/vuln?param={urllib.parse.quote(param)}"
    return read_url(url, cookie)
```

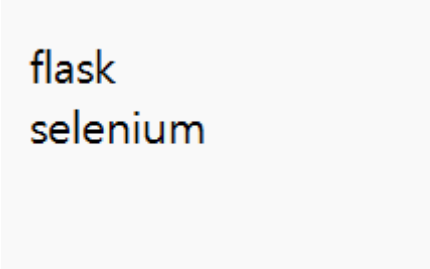
모르는 부분은 구글링을 했는데 XSS 공격 어쩌고... 내용이 나왔다.



피싱 공격의 일종인 것 같았다.

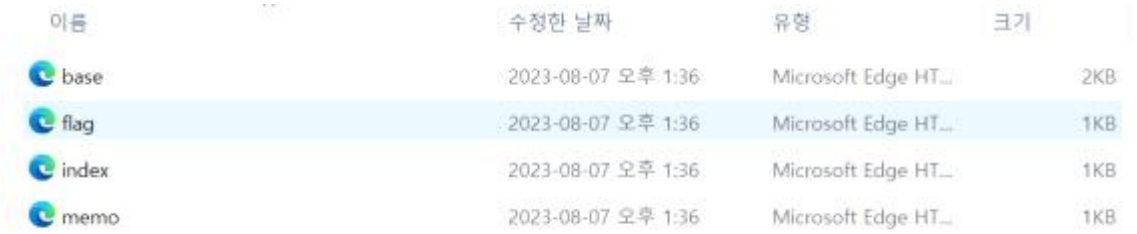
그리고 플라스크는 파이썬으로 작성된 마이크로 웹 프레임워크라고 한다.
플라스크를 이용한 어플리케이션을 구현한 코드같다.

flag라는 텍스트 파일에는 이렇게만 써있었다.



requirement 라는 텍스트 파일에는 이렇게 써있었다.

셀레늄도 엡 애플리케이션인 것 같은데
왜 메모장에 적어둔 건지는 모르겠다.



템플릿 폴더에 이렇게 웹 사이트로 열 수 있는 html 파일들이 있었다.

이건 플래그 파일이었고, 뭔가 제출하는 칸이 있었다.

혹시 몰라서 DH{**flag**} 라고 적고 제출했는데 아무 일도 일어나지 않았다.

나머지 파일들도 별 소득이 없었다.

static 폴더에 이렇게 나왔는데 css는 프로그래밍 언어인 것 같고, fonts 등이 있는 걸로 보아 어플리케이션 구현을 위해 필요한 코드들인 것 같았다.