DreamHack csrf-1문제

2021-09-05

```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
```

사이트에서 XSS를 방지하기위한 필터링을 3가지 단어에 걸어 두었다.

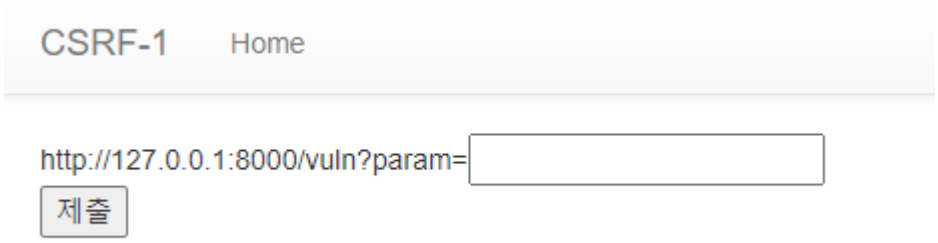
```python
memo_text = ""


@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)
```

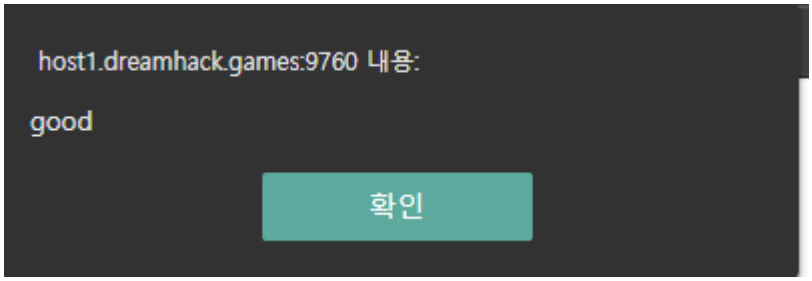
```python
@app.route("/admin/notice_flag")
def admin_notice_flag():
    global memo_text
    if request.remote_addr != "127.0.0.1":
        return "Access Denied"
    if request.args.get("userid", "") != "admin":
        return "Access Denied 2"
    memo_text += f"[Notice] flag is {FLAG}\n"
    return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

이 두코드를 보면 전역변수인 memo_test가 있고 여기에 추가를 하여 memo를 적는 것을 확인할 수 있다. Flag를 보기위해선 /admin/notice_flag 페이지에 127.0.0.1의 주소(localhost)로 접속하고 userid가 admin이여야 한다. XSS를 이용해 location.href를 쓰기엔 필터링에 의해 사용할 수 없다.

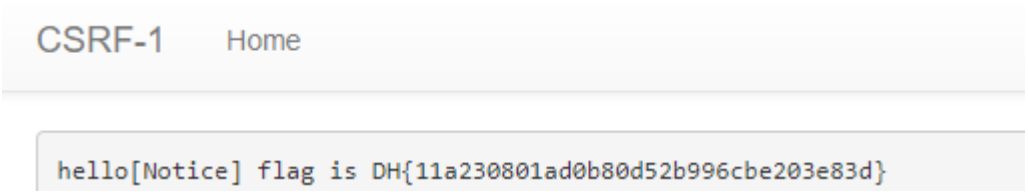
하지만 필터링 되어있지 않은 태그중 img태그의 src를 사용하면 접근은 할 수 있다.



이부분에 <img src="/admin/notice_flag?userid=admin"> 이라 적어주고 제출하였다.



이후 memo 부분을 확인해보면 memo_text에 Flag가 추가되어있어 memo에 추가되기 때문에



이와 같이 flag를 볼 수 있다.