DreamHack simple_sqli 문제

2021-09-05

```python
@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'GET':
        return render_template('login.html')
    else:
        userid = request.form.get('userid')
        userpassword = request.form.get('userpassword')
        res = query_db(f'select * from users where userid="{userid}" and userpassword="{userpassword}"')
        if res:
            userid = res[0]
            if userid == 'admin':
                return f'hello {userid} flag is {FLAG}'
            return f'<script>alert("hello {userid}");history.go(-1);</script>'
        return '<script>alert("wrong");history.go(-1);</script>'
```

서버의 코드가 이와 같기에 userid부분에서 "를 닫아주고 뒤를 주석으로 만들면 userid를 마음대로 조작하여 SQLinjection 공격으로 인해 admin으로 로그인이 가능하다.

userid에 admin"--를 적어 "를 닫고 뒤를 주석으로 만든다. Password는 어짜피 주석이라 아무거나 적어도 상관없다.

Login을 누르면

hello admin flag is DH{1f136225e316add7bff3349ab1dd5400}

Flag를 얻을 수 있다.