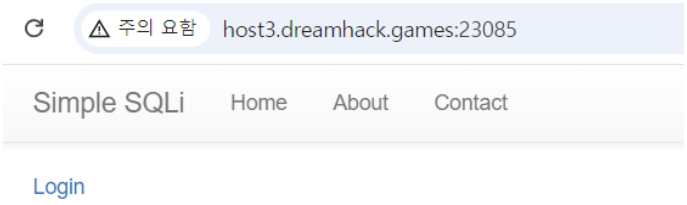
Dreamhack simple_sqil_chatgpt Writeup

먼저 서버를 열어본다.

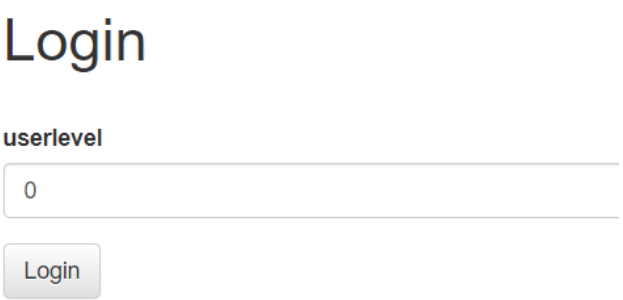


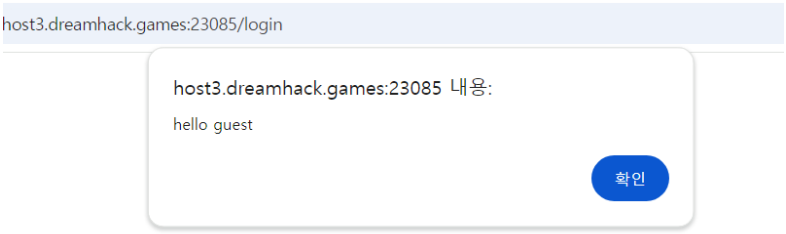
로그인 시스템만이 있는 웹사이트이다.

로그인을 할 때에는 userlevel을 이용해 로그인하게 되어있다.

```
BASE) == False:
ct(DATABASE)
 table users(userid char(100), userpassword char(100), userlevel integer);')
t into users(userid, userpassword, userlevel) values ("guest", "guest", 0), (
```

코드를 확인해보면 userlevel이 0인 guest 계정으로 로그인할 수 있음을 알 수 있다.





Userlevel을 0으로 입력하고 로그인하니 guest로 로그인되었음을 알 수 있다.

```
else:
    userlevel = request.form.get('userlevel')
    res = query_db(f"select * from users where userlevel='{userlevel}'")
    if res:
        userid = res[0]
        userlevel = res[2]
        print(userid, userlevel)
        if userid == 'admin' and userlevel == 0:
            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>'
```

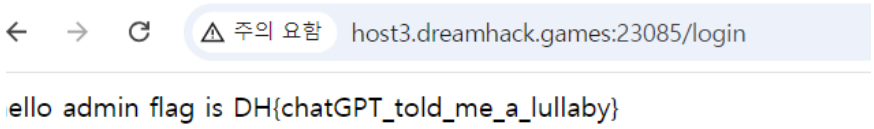
코드에서 userlevel과 관련되어 있는 것으로 보이는 부분을 가져와 분석해보았다. 이 부분은 입력한 userlevel 값을 가져와 데이터베이스에서 해당 레벨에 맞는 유저를 조회하고, 조건에 따라 다른 응답을 반환하는 역할을 한다.

더 자세히 말하자면 사용자의 userlevel 값이 입력되면 SQL 구문이 작동하여 데이터베이스의 userid 와 userlevel의 값과 비교하는데, 이때 조회된 유저가 admin이고 userlevel이 0일 경우, FLAG 값을 포함한 응답을 반환한다.

따라서 해당 SQL 구문을 조작해주면 된다. 현재의 구문은 "select * from users where userlevel='{userlevel}'"이기 때문에 여기서 원하는 userlevel과 userid를 넣어주면 된다.

그러면 입력할 구문이 select * from users where userlevel'0' AND userid='admin'이 된다.

따라서 로그인 칸에 0' AND userid='admin을 입력하여 플래그를 알아낼 수 있다.



플래그는 **DH{chatGPT_told_me_a_lullaby}** 이다.