cookie

문제 파일을 다운로드 받아서 살펴보자!

```python
@app.route('/')
def index():
    username = request.cookies.get('username', None)
    if username:
        return render_template('index.html', text=f'Hello {username}, {"flag is " + FLAG if username == "admin" else "you are n
    return render_template('index.html')
```

그럼 'username'이라는 쿠키를 받아오는데 username == "admin"이면 flag를 보여준다.

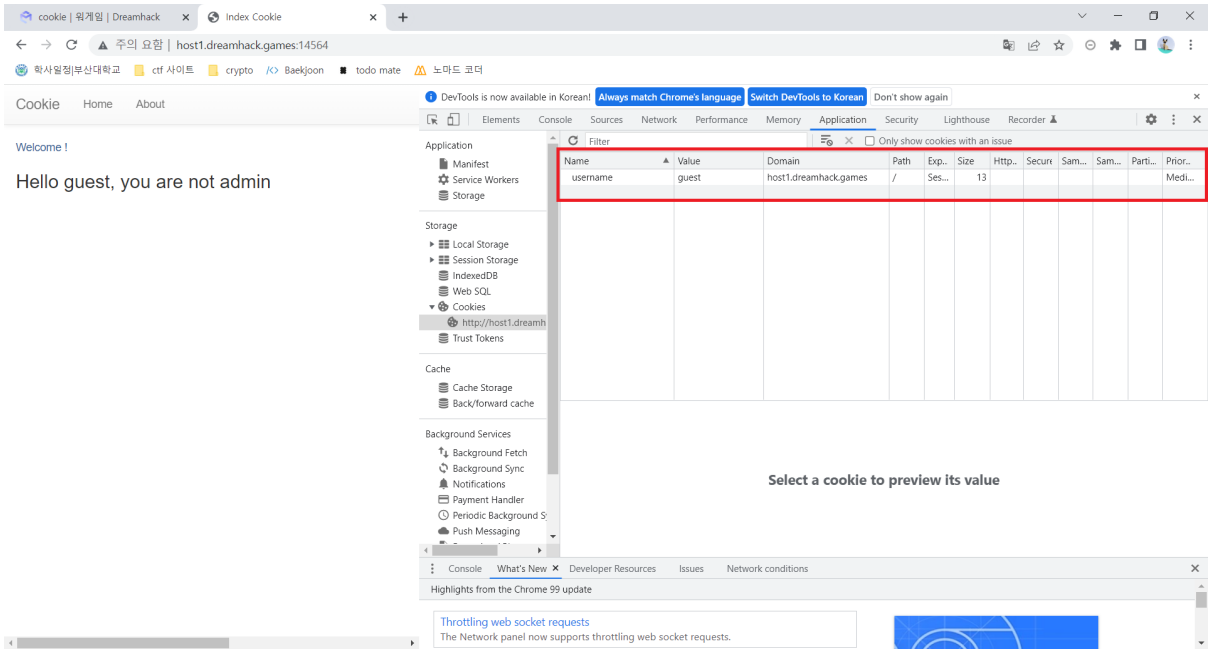
로그인 페이지를 살펴보면 로그인한 계정으로 쿠키를 생성해준다.

```python
@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'GET':
        return render_template('login.html')
    elif request.method == 'POST':
        username = request.form.get('username')
        password = request.form.get('password')
        try:
            pw = users[username]
        except:
            return '<script>alert("not found user");history.go(-1);</script>'
        if pw == password:
            resp = make response(redirect(url for('index')) )
            resp.set_cookie('username', username)
            return resp
        return '<script>alert("wrong password");history.go(-1);</script>'
```

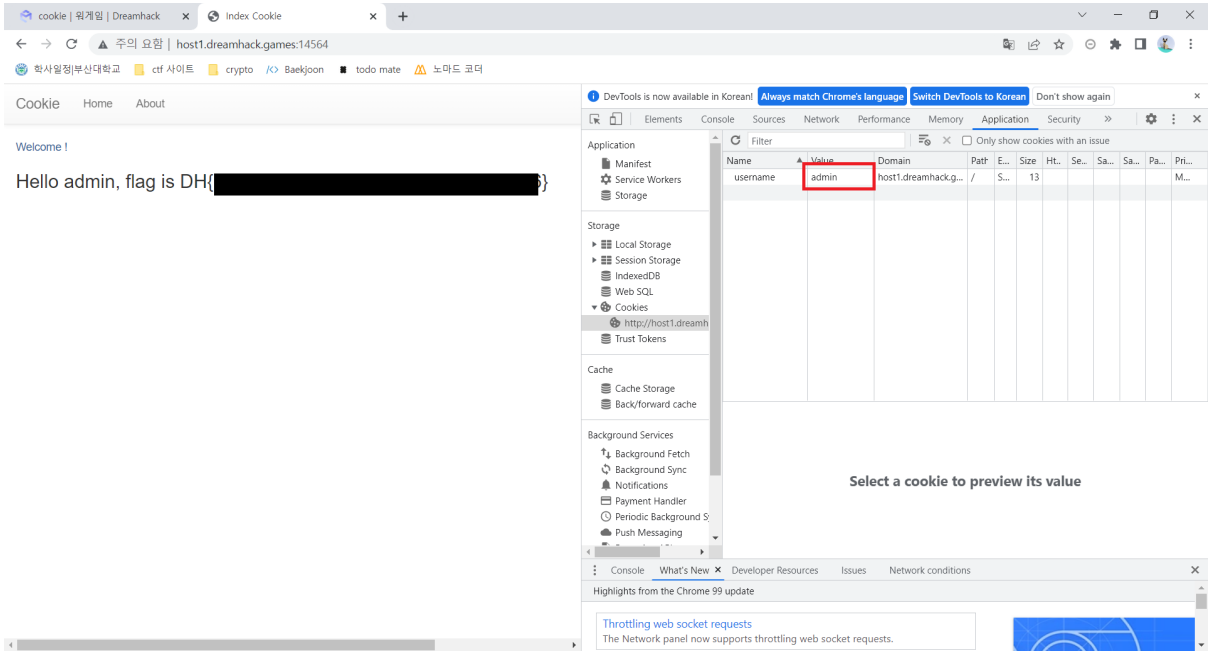
하지만 admin의 비밀번호를 모른다...

```python
users = {
    'guest': 'guest',
    'admin': FLAG
}
```

그래도 guest의 계정을 아니 guest로 로그인한 뒤에 쿠키가 생성되면 guest에서 admin으로 바꿔주면 될것 같다!



로그인해서 쿠키가 생성됐다!



admin으로 바꾸고 새로고침하니! flag가 보인다! 끝!!!!!