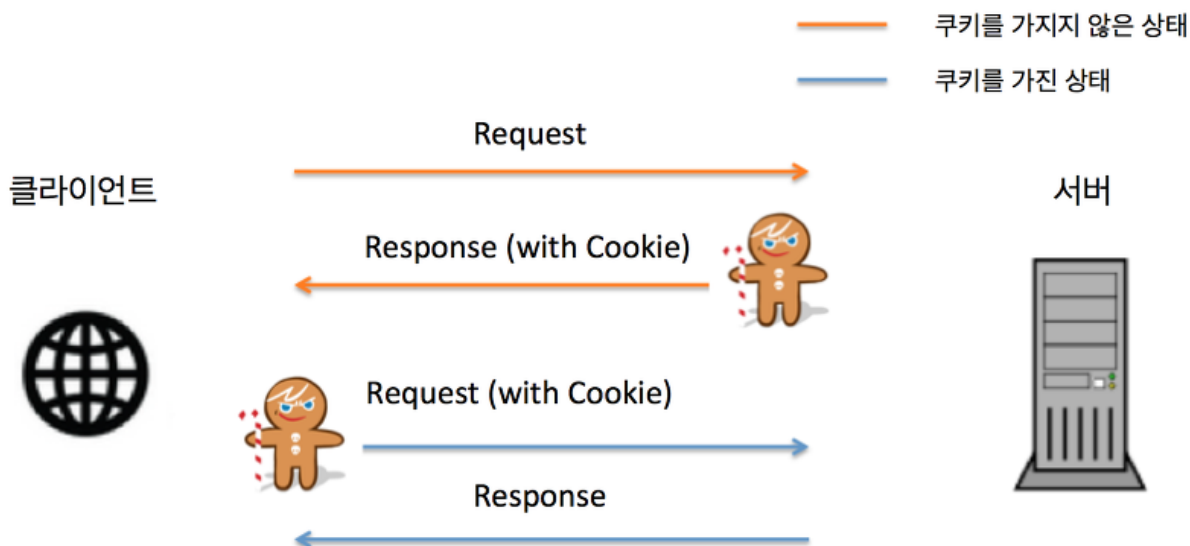


# Cookie

web

## 🍪 Cookie란?



인터넷 사용자가 어떤 웹 사이트를 방문할 때 해당 웹사이트에서 사용자의 컴퓨터 또는 장치에 저장되는 작은 파일이다. 즉, 그 사이트가 사용하게 되는 일련의 작은 기록 파일이라고 할 수 있다. 이 파일은 인터넷 사용자의 브라우저에 의해 읽히며, 해당 웹 사이트를 방문할 때마다 인터넷 사용자의 정보를 수집하고 저장한다.

## 🍪 Cookie 구조

- key-value 형식의 문자열 형태로 저장

서버가 클라이언트에 정보를 전달할 때 저장하고자 하는 정보를 응답 헤더에 저장하여 전달한다.

```
{  "Set-Cookie" : "id=user123",
  "Set-Cookie" : "pw=pw1234@"
}
```

## 문제

### 문제 설명

쿠키로 인증 상태를 관리하는 간단한 로그인 서비스입니다.

admin 계정으로 로그인에 성공하면 플래그를 획득할 수 있습니다.

플래그 형식은 DH{...} 입니다.

### Reference

[Introduction of Webhacking](#)

 [Translate](#)

- admin 계정으로 로그인에 성공하여 FLAG 획득하기



접속 화면

```

#!/usr/bin/python3
from flask import Flask, request, render_template, make_response

app = Flask(__name__)

try:
    FLAG = open('./flag.txt', 'r').read()
except:
    FLAG = '**FLAG**'

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

@app.route('/')
def index():
    username = request.cookies.get('username', None)
    if username:
        return render_template('index.html', text=f'Hello {username}')
    return render_template('index.html')

@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);'
        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);'

app.run(host='0.0.0.0', port=8000)

```

문제의 코드를 보면 **[guest]**와 **[admin]** 계정이 있다는 것을 확인할 수 있다.

**[admin]** 계정으로 로그인 될 시 **FLAG** 값이 함께 나타나고, 아닐 경우에는 “**you are not admin**” 문구가 출력 됨을 알 수 있다.

The screenshot shows a web application interface with a navigation bar containing links for 'Cookie', 'Home', 'About', and 'Login'. The main content area is titled 'Login' and contains two input fields: 'username' with the value 'guest' and 'password' with masked characters '.....'. A 'Login' button is positioned below the password field.

Below the login form, the browser's address bar shows the URL 'host3.dreamhack.games:9401'. The page content displays 'Welcome !' followed by the message 'Hello guest, you are not admin'.

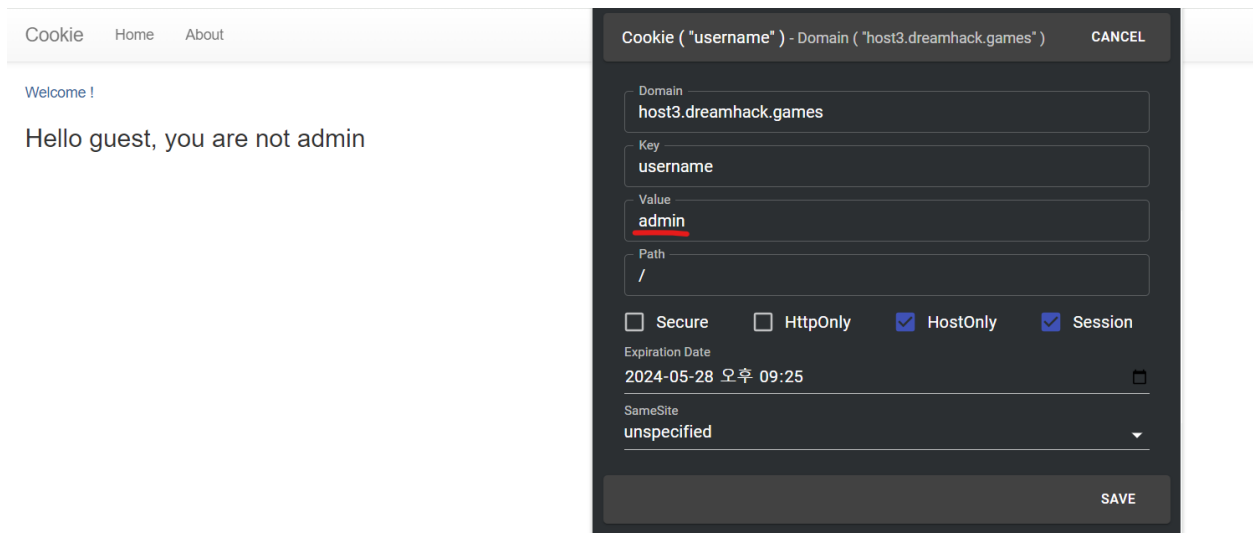
A cookie inspector extension is open, showing the following details:

- Domain: host3.dreamhack.games
- Cookie Count: 1 cookie (13 bytes)
- Search: (empty)
- Cookie List:
 

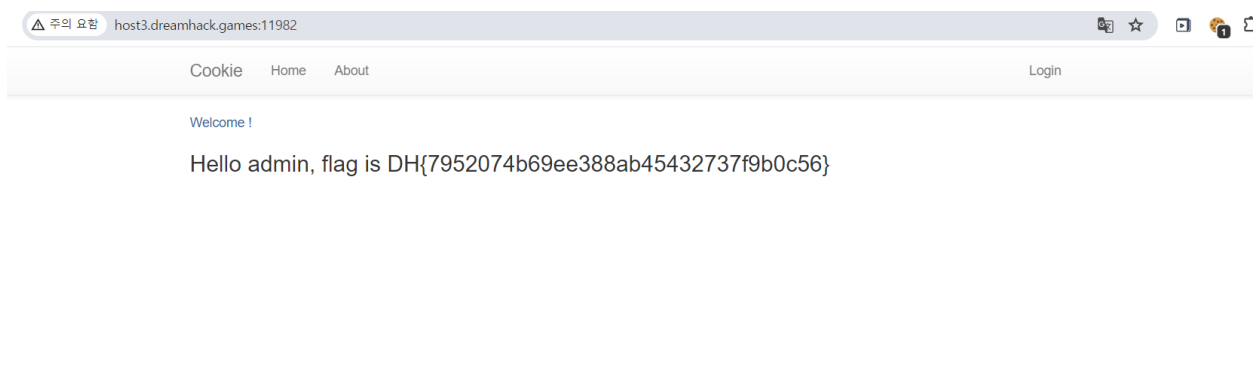
Key	Value
username	guest
- Age: Session
- Size: 13 bytes
- Buttons: ADD, CLEAR ALL, CLEAR ALL

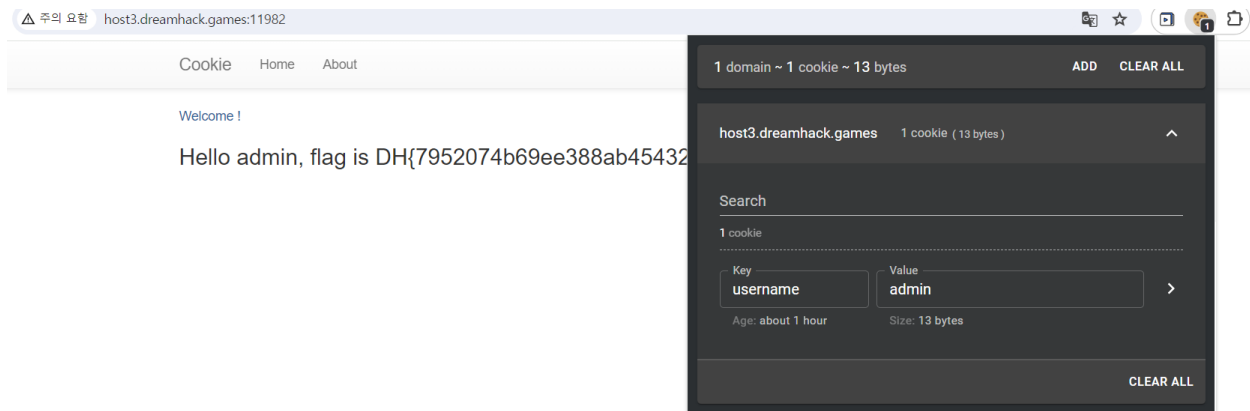
**[guest]** 계정으로 로그인을 시도해보았을 때 **“Hello guest, you are not admin”**이라는 문구를 확인할 수 있었고 **[guest]** 계정의 쿠키 값이 생성된 것을 볼 수 있었다.

쿠키 확인은 **[EditThisCookie]**를 사용하였다.



**username**의 값이 **[admin]**일 경우 **FLAG** 값을 알려주기 때문에 **[guest]** 계정으로 생성된 쿠키의 **Value** 값을 **[admin]**으로 수정하였다.





새로 고침을 하니 위와 같은 FLAG 값을 얻을 수 있었다.

Flag 입력

DH{7952074b69ee388ab45432737f9b0c56}

제출하기

풀이 531



대단해요! 정답을 맞추셨네요. 문제를 어떻게 해결하셨나요?

[풀이 작성하고 포인트 받기](#) >




성공!

## 참고

## Cookie란 무엇인가

사이트가 사용하게 되는 작은 기록 파일 Cookie는 인터넷 사용자가 어떤 웹사이트를 방문할 때 해당 웹사이트에서 사용자의 컴퓨터 또는 장치에 저장되는 작은 파일입니다. 즉, 그 사이트가 사용하게 되는 일련의 작은 기록

 <https://velog.io/@beneficial/Cookie란-무엇인가>

