

# Simple-web-request

| web

## 문제

### 문제 설명

#### Description

STEP 1~2를 거쳐 FLAG 페이지에 도달하면 플래그가 출력됩니다.

모든 단계를 통과하여 플래그를 획득하세요. 플래그는 flag.txt 파일과 FLAG 변수에 있습니다.

플래그 형식은 DH{...} 입니다.

#### 📖 웹앱 실행 가이드

본 문제는 웹앱 프레임워크인 Flask로 작성된 웹 페이지입니다. 문제에서 접속 호스트와 포트를 제공하고 있어 url로 접속할 수 있으나, 직접 웹앱을 실행해 보고 싶은 분들을 위해 가이드를 준비했습니다.

문제에 주어진 `deploy` 디렉토리를 이용하면 웹앱을 실행하고 Flask 웹 서버에 접속할 수 있습니다. 방법은 다음과 같습니다.

1. 터미널 창을 열고 `deploy` 디렉토리로 이동합니다.
2. Flask가 처음이라면 `pip install flask` 명령어로 Flask를 설치합니다.
3. `python app.py` 명령어로 파이썬 파일을 실행합니다.
4. 출력된 웹 주소를 복사하여 브라우저에서 접속합니다.

해당 웹 서버에서 문제를 풀면 sample flag가 출력됩니다! ▶

[🌐 Translate](#)

## 풀이

Simple Web   Home

STEP 1

STEP 2

FLAG

첫 서버 화면이다.

Simple Web Home

제출

param :  
param2 :

[STEP 1] 화면이다.

Simple Web Home

제출

param : 1  
param2 : 2

`param`에는 1 `param2`에는 2를 넣어보았다.

함수의 소스 코드를 확인해보자.

```

20 @app.route("/step1", methods=["GET", "POST"])
21 def step1():
22
23     ##### 풀이외 관계없는 치팅 방지 코드
24     global step1_num
25     step1_num = int.from_bytes(os.urandom(16), sys.byteorder)
26     #####
27
28     if request.method == "GET":
29         prm1 = request.args.get("param", "")
30         prm2 = request.args.get("param2", "")
31         step1_text = "param : " + prm1 + "\nparam2 : " + prm2 + "\n"
32         if prm1 == "getget" and prm2 == "rerequest":
33             return redirect(url_for("step2", prev_step_num = step1_num))
34         return render_template("step1.html", text = step1_text)
35     else:
36         return render_template("step1.html", text = "Not POST")
37

```

```

39 @app.route("/step2", methods=["GET", "POST"])
40 def step2():
41     if request.method == "GET":
42
43         ##### 풀이와 관계없는 치팅 방지 코드 #####
44         if request.args.get("prev_step_num"):
45             try:
46                 prev_step_num = request.args.get("prev_step_num")
47                 if prev_step_num == str(step1_num):
48                     global step2_num
49                     step2_num = int.from_bytes(os.urandom(16), sys.byteorder)
50                     return render_template("step2.html", prev_step_num = step1_num, hidden_num = step2_num)
51             except:
52                 return render_template("step2.html", text="Not yet")
53             return render_template("step2.html", text="Not yet")
54         #####
55
56     else:
57         return render_template("step2.html", text="Not POST")

```

prm1 에 'getget'을 prm2 에 'rerequest' 를 넣으면 step2 함수 를 호출하고 파라미터 prev\_step\_num=step1\_num 와 함께 redirect 시킬 것이다.

주요 요점 host3.dreamhack.games:22880/step2?prev\_step\_num=172262296237668012197411317880807570498

---

Simple Web Home

param

param2

위의 값을 넣었더니 url이 step2?prev\_step\_num=172262296237668012197411317880807570498 로 이동되었다.

```

60 @app.route("/flag", methods=["GET", "POST"])
61 def flag():
62     if request.method == "GET":
63         return render_template("flag.html", flag_txt="Not yet")
64     else:
65
66         ##### 풀이와 관계없는 치팅 방지 코드 #####
67         prev_step_num = request.form.get("check", "")
68         try:
69             if prev_step_num == str(step2_num):
70                 #####
71
72                 prm1 = request.form.get("param", "")
73                 prm2 = request.form.get("param2", "")
74                 if prm1 == "pooost" and prm2 == "requeeeest":
75                     return render_template("flag.html", flag_txt=FLAG)
76                 else:
77                     return redirect(url_for("step2", prev_step_num = str(step1_num)))
78                 return render_template("flag.html", flag_txt="Not yet")
79             except:
80                 return render_template("flag.html", flag_txt="Not yet")
81
82
83 app.run(host="0.0.0.0", port=8000)

```

이번에는 prm1 에 pooost 를 prm2 에는 requeeeest 를 넣으면 될 것 같다.

Simple Web Home

param

param2

제출

host3.dreamhack.games:23626/flag

Simple Web Home

DH{ c46b414ddb26adfa4606c59655bda0a18fbe260606b042b52d865e0160eea0e }

플래그 값 획득

풀이 57

🔍 ↕

대단해요! 정답을 맞추셨네요. 문제를 어떻게 해결하셨나요?

[풀이 작성하고 포인트 받기 >](#)



이step2 함수 하나하나 보면서 개발자 도구 이용해 이것저것 만져보았는데...

그냥 코드만 보고 대입하면 되는 거였다..ㅎ

## 참고

<https://taehyeki.tistory.com/150>