Emdee five for life

처음 접속하면 문자열을 `MD5` 해시로 만들라는 문자열이 출력된다. `MD5` 해시로 변환 후 `Submit` 버튼을 누르면 너무 느리다는 메시지가 출력된다.

```
import requests
import hashlib
from bs4 import BeautifulSoup

url = "http://167.99.85.216:32595/"

# POST 요청 보내기
response = requests.post(url)
soup = BeautifulSoup(response.text, 'html.parser')

# <h3> 태그의 텍스트 추출
string_to_encrypt = soup.find('h3').text

md5_hash = hashlib.md5()
md5_hash.update(string_to_encrypt.encode('utf-8'))
encrypted_string = md5_hash.hexdigest()

# 첫 번째 응답에서 세션 정보 가져오기
session_info = response.headers['Set-Cookie']

# 암호화한 문자열을 다시 서버로 전송
headers = {'Cookie': session_info}
second_response = requests.post(url, data={'hash': encrypted_string}, headers=headers)

# 결과 출력
print(second_response.text)
```

POST 요청을 보낸 후 `MD5` 해시로 변환해야 하는 문자열을 받은 뒤, 바로 변환하여 요청을 보내고 그 응답을 받는 코드를 작성했다.

```
$ py payload.py
<html>
<head>
<title>emdee five for life</title>
</head>
<body style="background-color:powderblue;">
<h1 align='center'>MD5 encrypt this string</h1><h3 align='center'>Q0Zs5EdoEfHqa6PR2LMm</h3><p align='center'>HTB{N1c3_ScrIpt
<input type="text" name="hash" placeholder="MD5" align='center'></input>
</br>
<input type="submit" value="Submit"></input>
</form></center>
</body>
</html>
```

해당 소스코드를 실행시키면 플래그를 획득할 수 있다. 소스코드 실행 속도에 따라 플래그가 출력되지 않는 경우도 있어서 여러 번 실행시켜야 했다.

```
import requests
import hashlib

url="http://167.99.85.216:32595"
```

```
req=requests.session()

get=req.get(url)
target_string=get.text.split("<h3 align='center'>")[1].split("</h3>")[0]
print (target_string)
hash_string=hashlib.md5(target_string.encode('utf-8')).hexdigest()
data={
    "hash": hash_string
}
post=req.post(url,data=data)
print (post.text)
```

높은 확률로 플래그를 얻을 수 있는 소스코드이다.