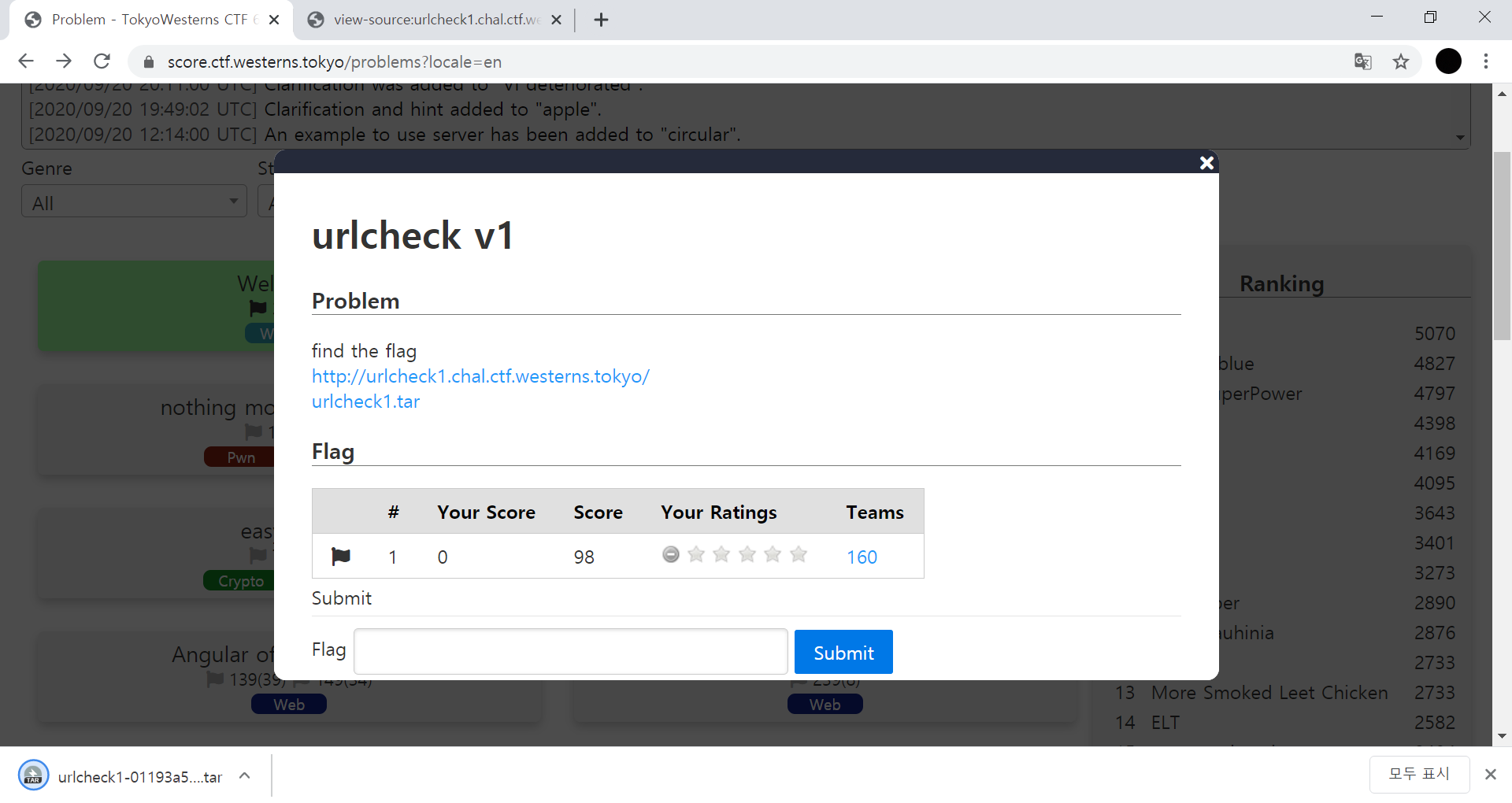
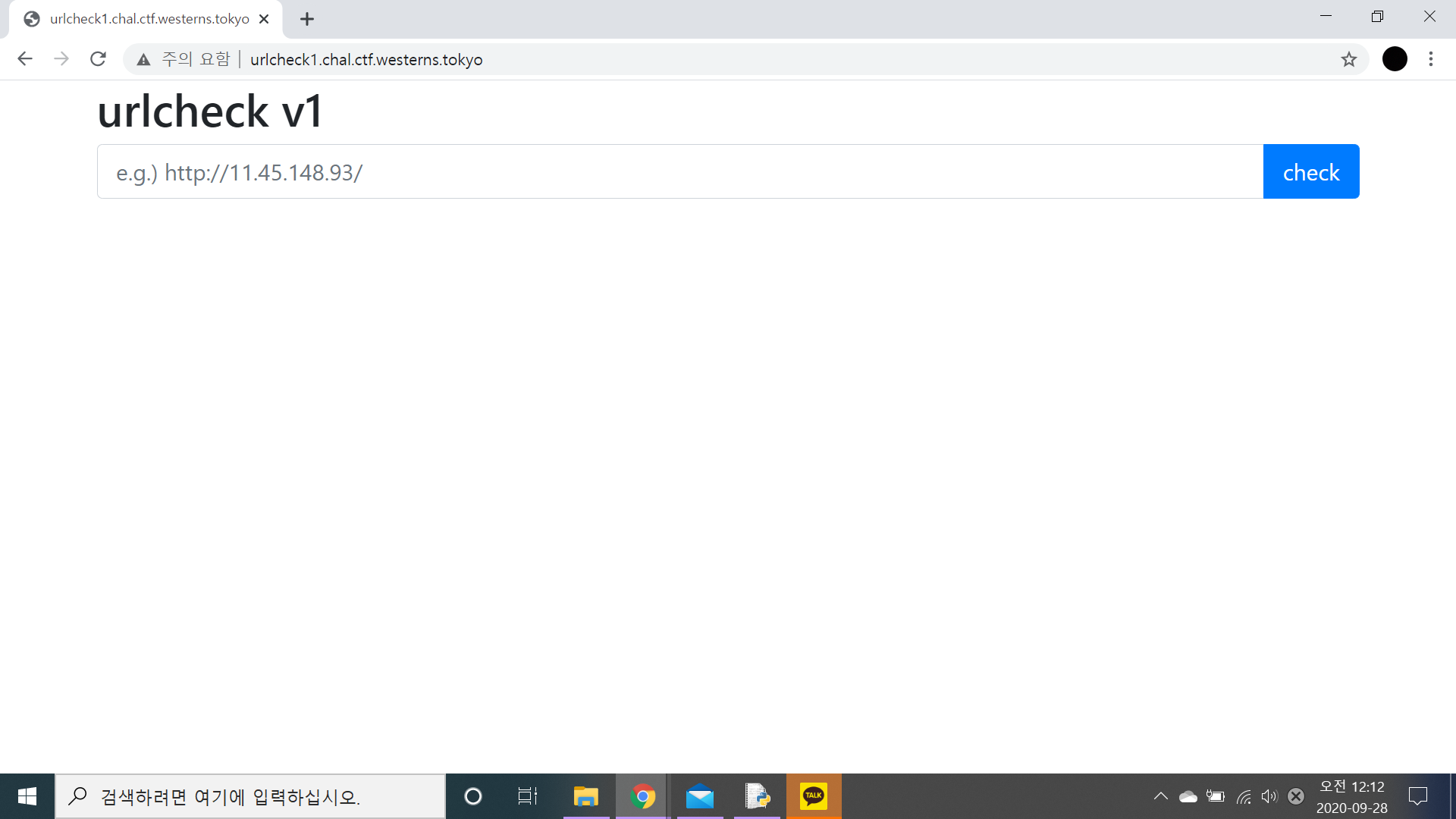
1. 문제 확인



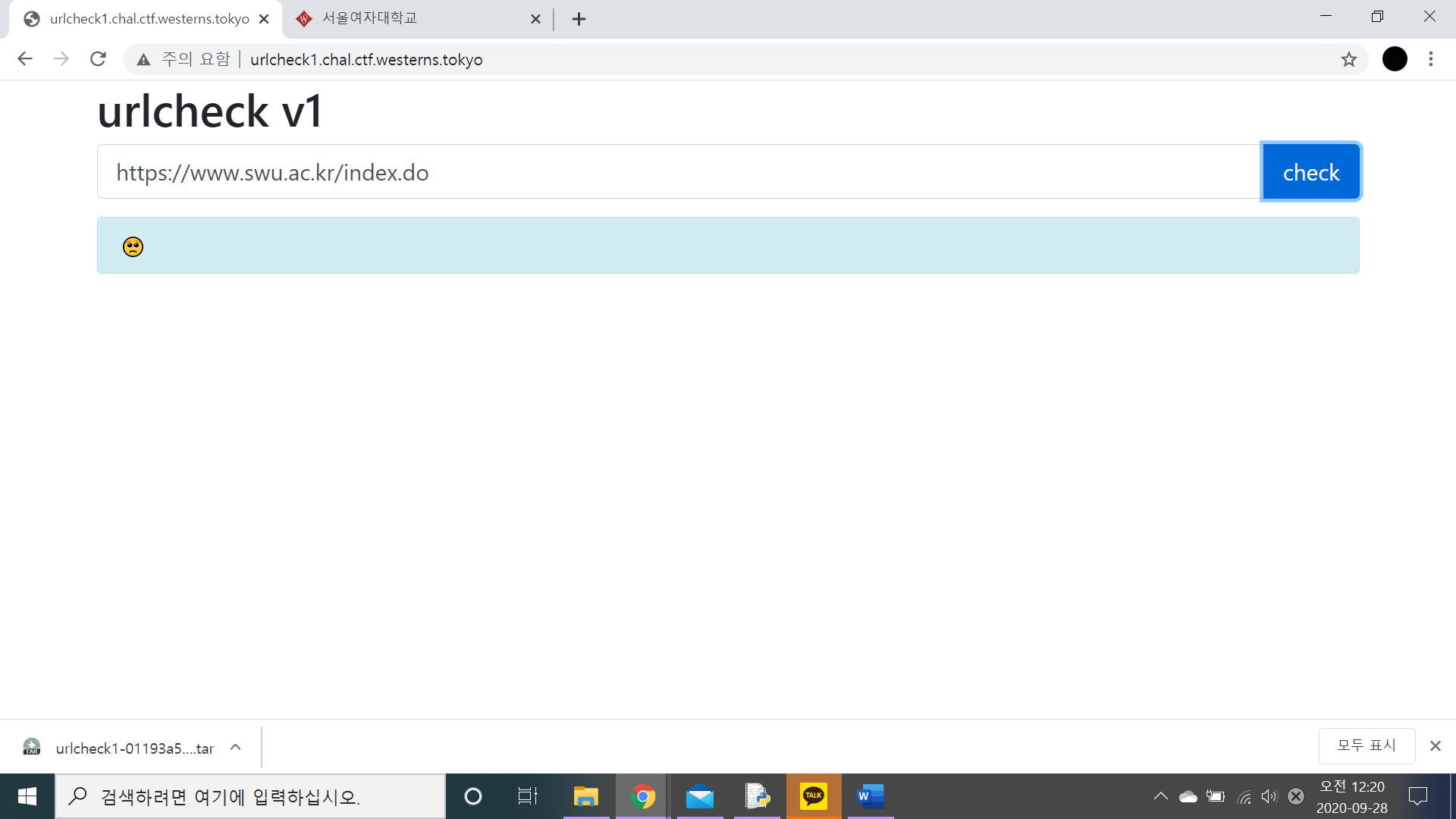
2. 과정

문제에 있는 링크로 들어가 보았다.



위처럼 url을 전송하는 것 같은 폼과 체크 버튼이 존재한다.

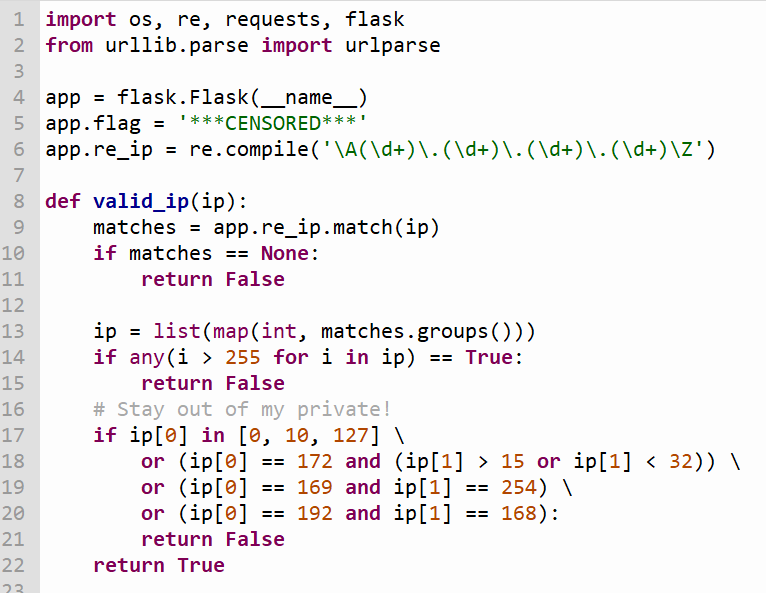
url을 입력하면 뭐가 나오나 싶어서 학교 홈페이지 url을 넣어보았다.

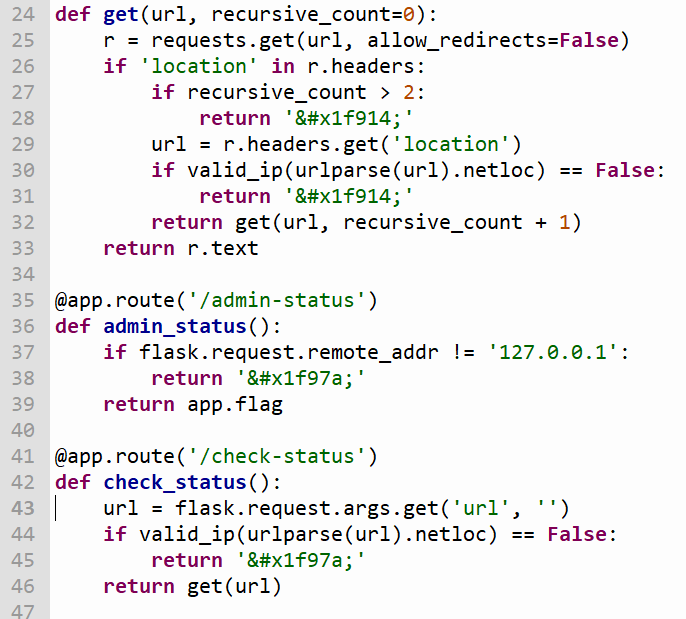


우는 표정의 이모지만 나오고 아무런 반응이 없었다.

다른 값을 넣어도 반응은 같았다.

첨부된 파일을 열어서 파이썬 코드를 확인해 보았다.





코드를 살펴보면

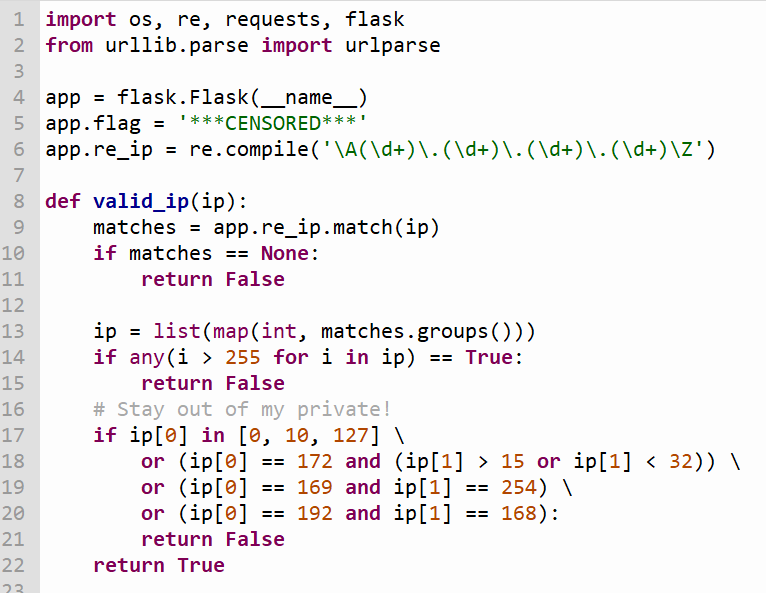
admin\_status()에 flask.request.remote\_addr이 127.0.0.1이 아니면 $#x1f97a(우는 표정 이모지)를 리턴하고,

아니면 flag를 리턴 한다고 한다.

그래서 바로 127.0.0.1/admin-status를 폼에 입력해 전송해보았지만

우는 표정 이모지가 리턴 됐다.

다시 코드를 계속 보았다.



valid\_ip()에서 매개 값을 ip로 받아 matches.groups()를 int 형으로 바꾸고 ip 값을 검사하고 있다.

여기서 ip 값 체크를 마치고 True 값이 나온다면 127.0.0.1에 요청을 보내 플래그를 얻을 수 있을 것 같다.

이 valid\_ip(ip)의 조건 검사를 우회할 수 있는 방법을 한참 헤매다가

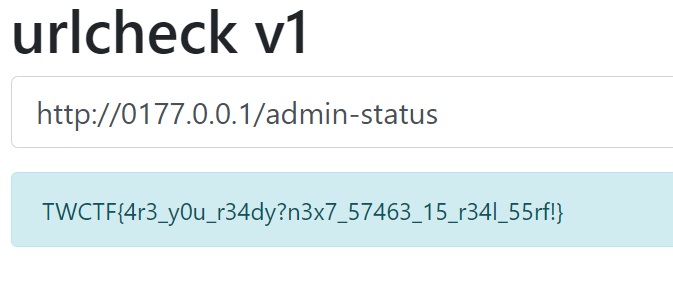
다른 분들의 라업을 참고하고서 방법을 알 수 있었다.

기존에 넣으려던 값을 8진수로 변환하여 url을 요청하면 해결할 수 있다고 한다.

그래서 127 -> 0177으로 바꾸고

0177.0.0.1/admin\_statue

폼에 입력 후 전송했다.

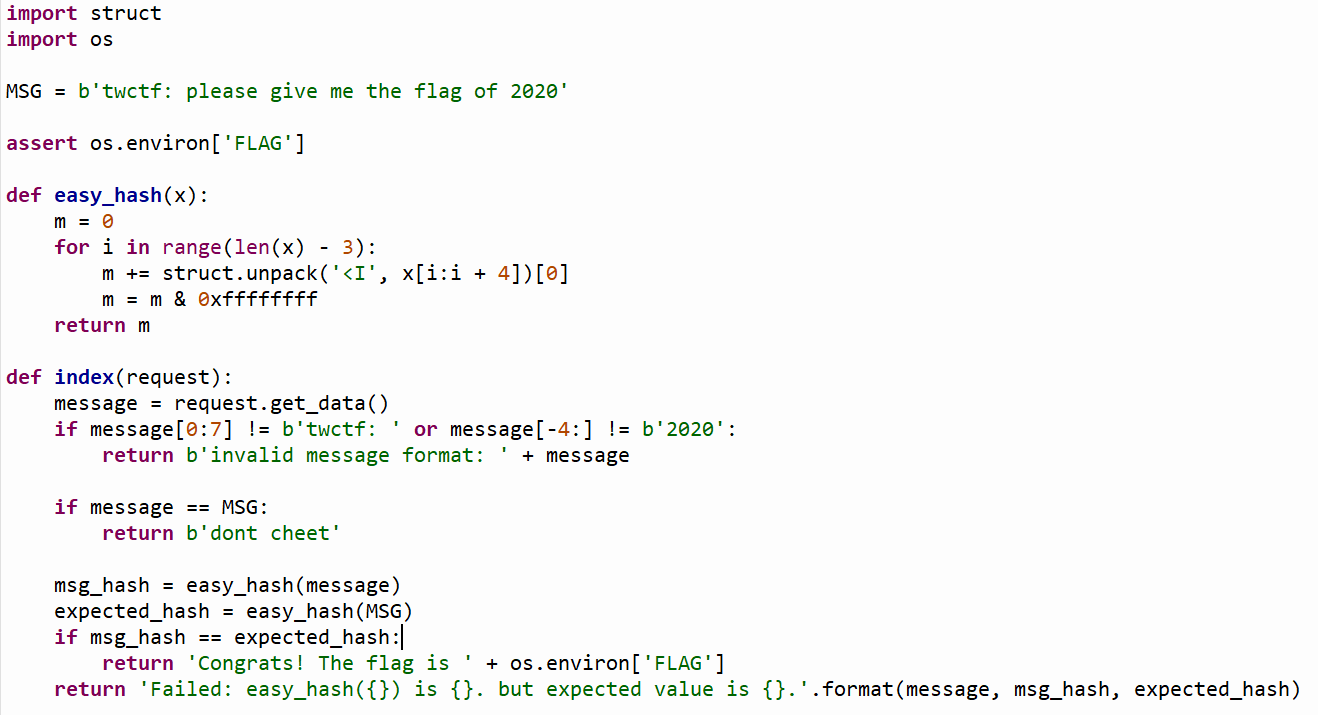


1. 문제 확인



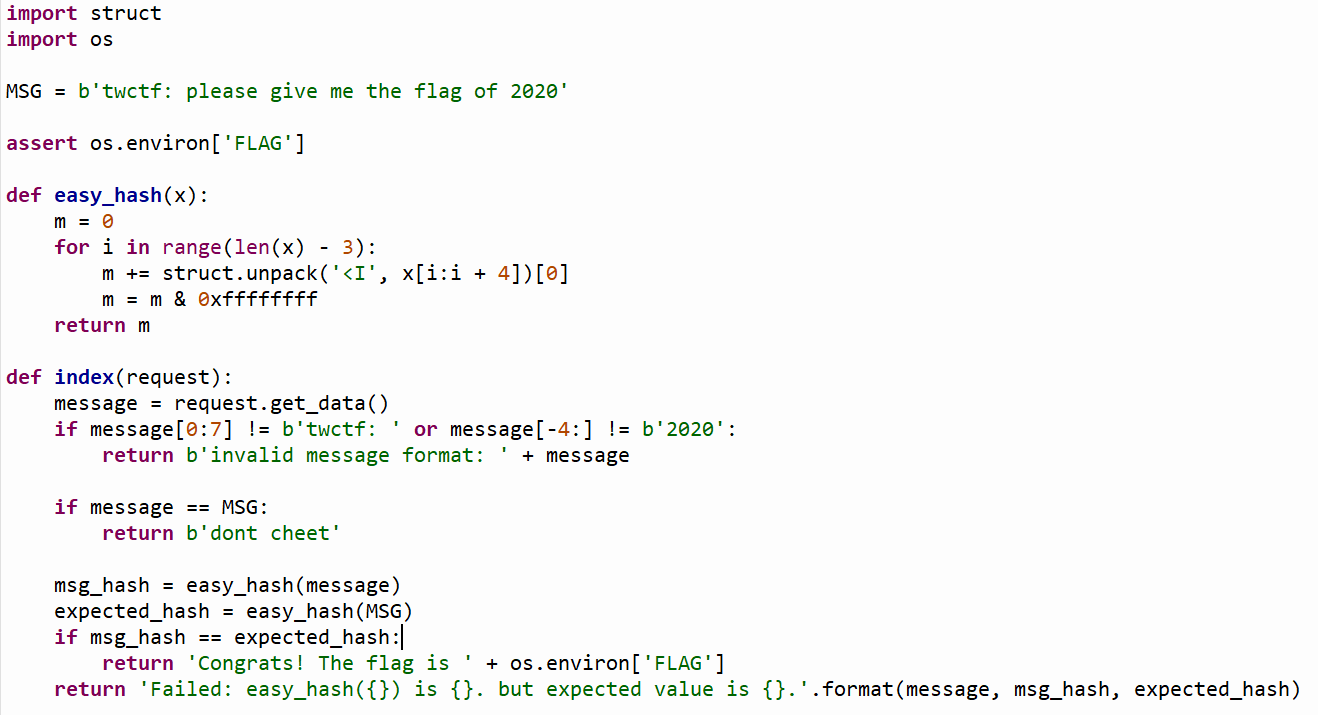
2. 과정

문제 확인하고 첨부된 파일을 열어 파이썬 코드를 살펴봤다.



easy\_hash()를 이용해 message와 MSG를 해쉬 값으로 만든 뒤 둘의 값이 일치하면 플래그를 얻을 수 있는 것 같다.

여기서 m값을 보낼 때 b’twctf: ‘ 와 b’2020’ 두 부분은 필수적으로 들어가야 하며 MSG와 같은 내용은 보낼 수 없다고 한다.



이제 easy\_hash(x)를 보면

솔직히 unpack()과 ‘<I’ 는 초면이라 검색으로 찾아봤는데 아직 제대로 이해하지 못했다.

그냥 훑어본 바로는 매개 값 x를 struct.unpack() 모듈로 값을 쌓아가는 것 같은데

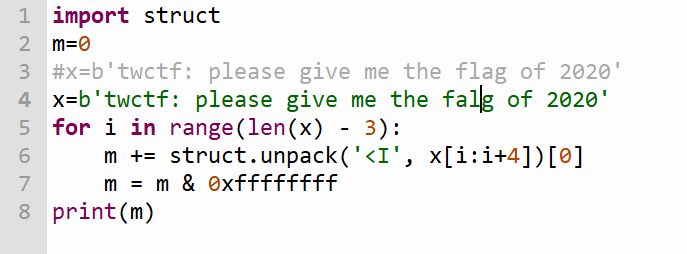
중요한 건 easy\_hash(x)와 easy\_hash(MSG)의 값이 동일한 경우를 찾는 것이다.

여기에서 이 분의 라업(<https://ctftime.org/writeup/23579>)을 보고 도움을 받았는데

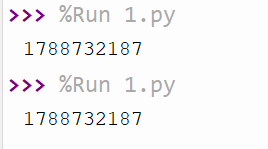
이 해쉬 함수는 easy\_hash('xabx') == easy\_hash('xbax')의 결과를 낸다고 한다.

즉, 문자열 내의 문자 구성은 동일하나 그 문자의 순서는 일치하지 않아도 된다고 한다.

바로 코드를 가져와 확인해보았다.

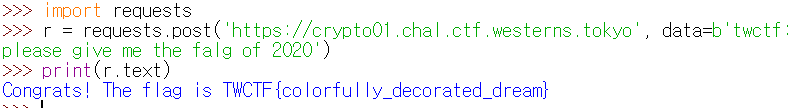


처음 x 값은 MSG 값을, 두 번째로 대입한 x의 값은 flag를 falg로 바꾼 값을 넣어 실행해보았다.



정말 다행이게도 m의 값이 동일하게 나왔다.

이제 변형한 x의 값으로 m을 서버로 보냈다.



TWCTF{colorfully\_decorated\_dream}