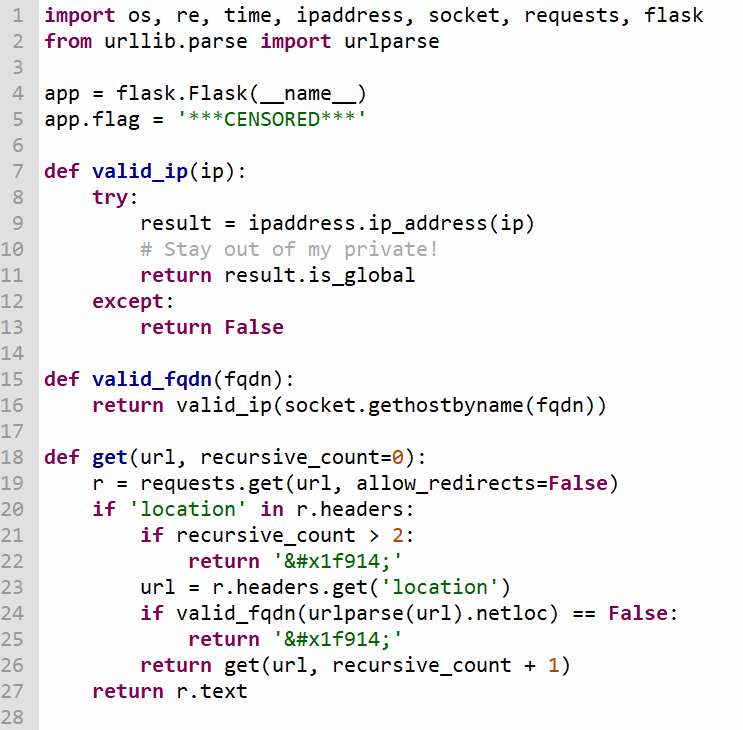
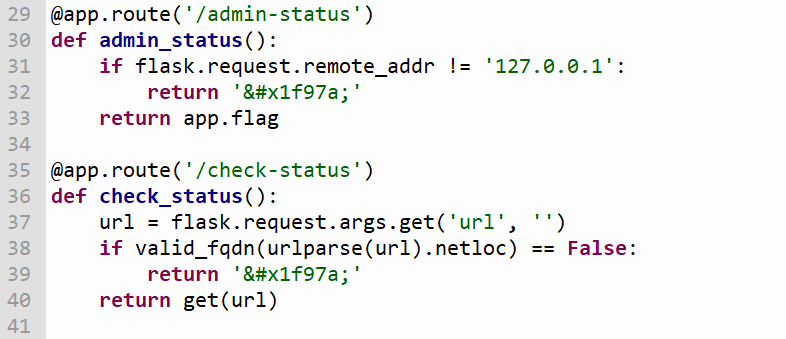
1. 문제 확인

Urlcheck\_v2와 똑 같은 폼을 가진 문제이다.

2. 과정

바로 함께 첨부된 파일의 파이썬 코드를 확인했다.



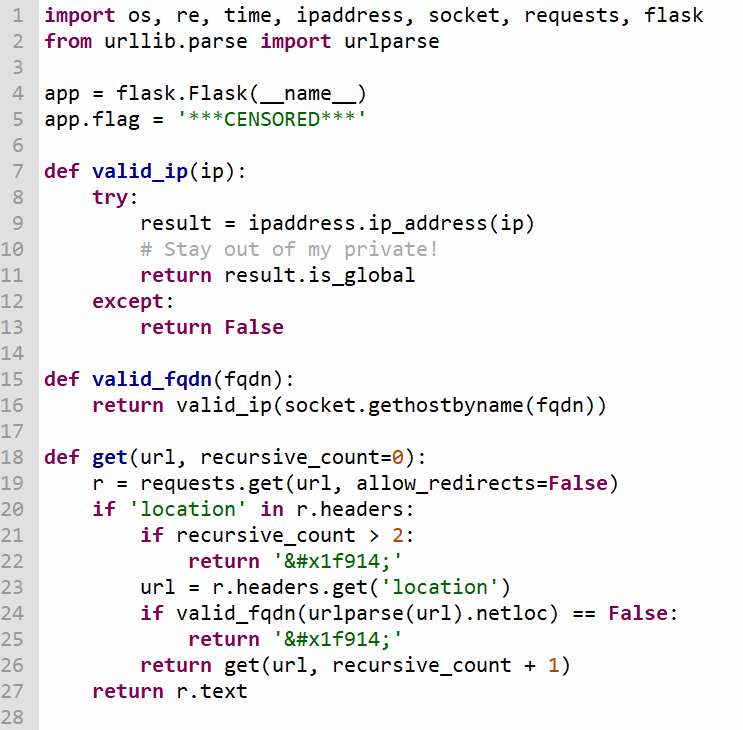


파이썬 코드도 유사한 부분이 많은 것 같다.

또 보면 admin\_status() 부분에서 127.0.0.1로 요청을 보내면 플래그를 얻을 수 있다고 한다.

그렇다면 몇 가지 검사를 우회하여 url을 요청할 수 있도록 해야 하는데

이번에는 valid\_ip(ip)와 valid\_fqdn(fqdn) 총 두 가지의 검사를 거친다.



valid\_ip(ip)를 보면 ip를 확인하는데 ip가 개인인지 공인인지 검사한다. 여기서는 공인 아이피만 가능한 것 같다.

Valid\_fqdn(fqdn)을 보면 gethostbyname()함수를 통해 호스트 이름을 IPv4 주소 형식으로 변환하는데 이렇게 얻은 ip 주소를 valid\_ip로 보낸다.

(fqdn: 전체 주소 도메인 네임)

이렇게 두 검사를 통과하면 v1 문제처럼 127.0.0.1/admin-status로 플래그를 가져올 수 있는데

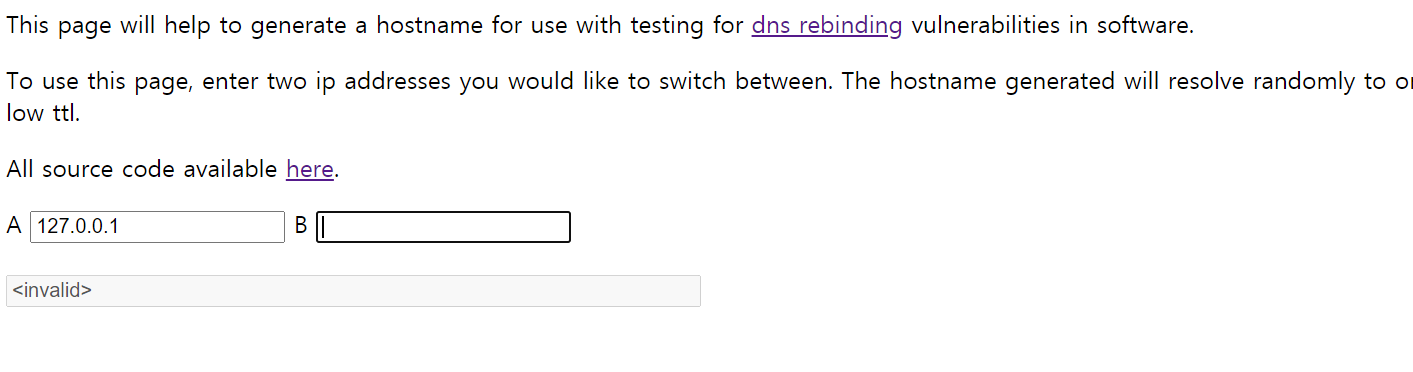
여기서 어떻게 우회를 해야 하는지 고민해야 했다.

여기선 공인 ip와 127.0.0.1을 이용해야 될 것 같았는데 계속 찾아봐도 어떤 식으로 우회할지 감이 오지 않았다.

결국 다시 다른 분의 라업을 참고해보았는데 DNS rebinding 공격을 이용할 수 있다고 한다.

DNS rebinding은 악의적인 사이트의 도메인에 할당된 IP를 잠재적인 희생자가 사이트에 들어와 있는 동안 공격하고자 하는 사이트의 IP로 바꾸어 Same Origin Policy를 우회하는 방법이라고 한다.

rbndr(<https://lock.cmpxchg8b.com/rebinder.html>)를 통해 쉽게 이용할 수 있다.



주기적으로 두개의 IP를 응답해서 보내는 것만 지원한다고 해서

하나는 127.0.0.1을, 다른 하나는 공인 ip 주소를 입력해 값을 얻었다.

이제 주어진 값을 폼에 입력해 전송해보았다.

