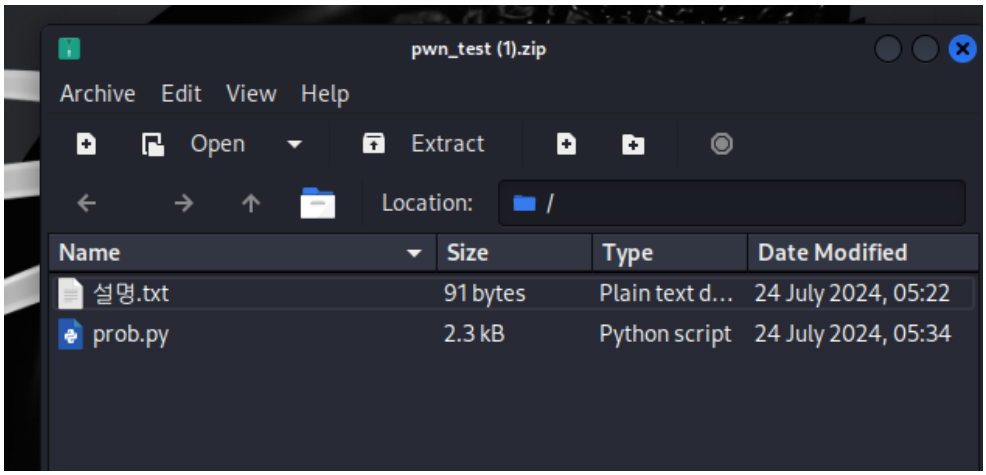
PWN TEST

32기 김효주

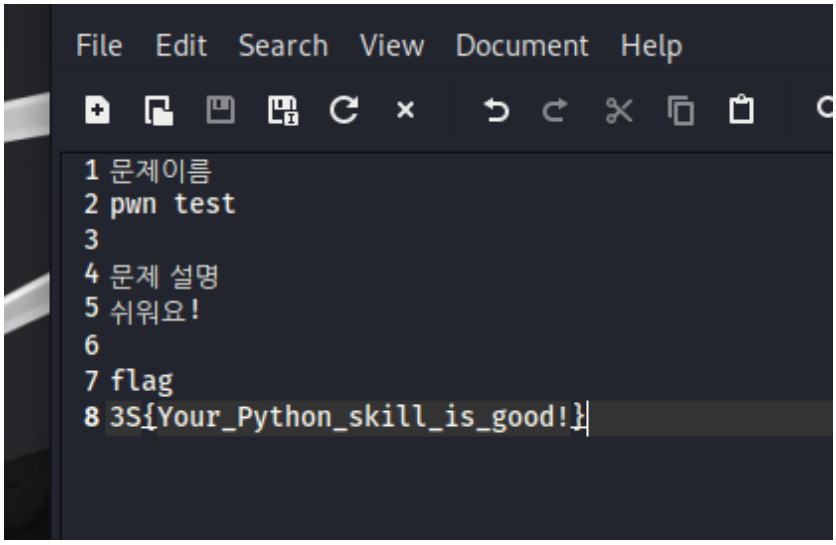
이것도 포너블 문제니까 일단 리눅스를 켜준다

엄청 쉽다고 하시니...제발 풀 수 있었으면 좋겠다

리눅스에서 파일을 다운받고 확인해보자

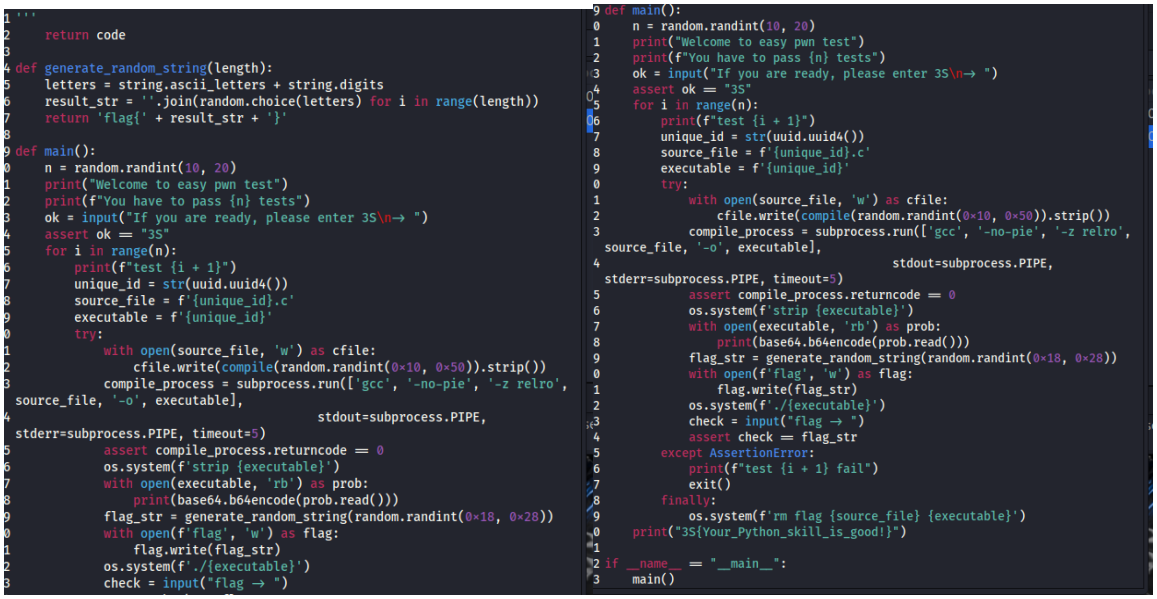


엥 근데 설명.txt를 열자마자 플래그가 보인다



이게 맞나?

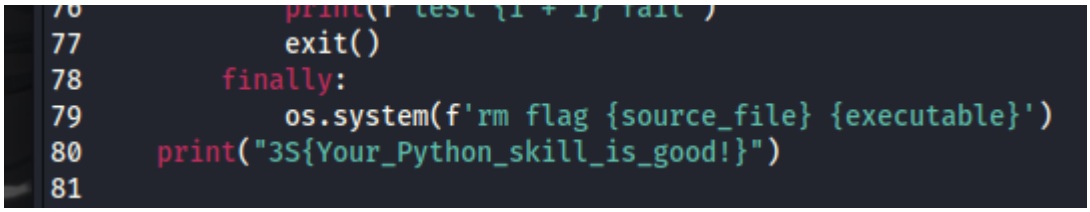
일단 제껴두고 파이썬 파일을 열어보자



```
'''
    return code

def generate_random_string(length):
    letters = string.ascii_letters + string.digits
    result_str = ''.join(random.choice(letters) for i in range(length))
    return 'flag{' + result_str + '}'

def main():
    n = random.randint(10, 20)
    print("Welcome to easy pwn test")
    print(f"You have to pass {n} tests")
    ok = input("If you are ready, please enter 3S\n→ ")
    assert ok == "3S"
    for i in range(n):
        print(f"test {i + 1}")
        unique_id = str(uuid.uuid4())
        source_file = f'{unique_id}.c'
        executable = f'{unique_id}'
        try:
            with open(source_file, 'w') as cfile:
                cfile.write(compile(random.randint(0×10, 0×50)).strip())
            compile_process = subprocess.run(['gcc', '-no-pie', '-z relro',
source_file, '-o', executable],
                                             stdout=subprocess.PIPE,
stderr=subprocess.PIPE, timeout=5)
            assert compile_process.returncode == 0
            os.system(f'strip {executable}')
            with open(executable, 'rb') as prob:
                print(base64.b64encode(prob.read()))
            flag_str = generate_random_string(random.randint(0×18, 0×28))
            with open(f'flag', 'w') as flag:
                flag.write(flag_str)
            os.system(f'./{executable}')
            check = input("flag → ")
```

```
def main():
    n = random.randint(10, 20)
    print("Welcome to easy pwn test")
    print(f"You have to pass {n} tests")
    ok = input("If you are ready, please enter 3S\n→ ")
    assert ok == "3S"
    for i in range(n):
        print(f"test {i + 1}")
        unique_id = str(uuid.uuid4())
        source_file = f'{unique_id}.c'
        executable = f'{unique_id}'
        try:
            with open(source_file, 'w') as cfile:
                cfile.write(compile(random.randint(0×10, 0×50)).strip())
            compile_process = subprocess.run(['gcc', '-no-pie', '-z relro',
source_file, '-o', executable],
                                             stdout=subprocess.PIPE,
stderr=subprocess.PIPE, timeout=5)
            assert compile_process.returncode == 0
            os.system(f'strip {executable}')
            with open(executable, 'rb') as prob:
                print(base64.b64encode(prob.read()))
            flag_str = generate_random_string(random.randint(0×18, 0×28))
            with open(f'flag', 'w') as flag:
                flag.write(flag_str)
            os.system(f'./{executable}')
            check = input("flag → ")
            assert check == flag_str
        except AssertionError:
            print(f"test {i + 1} fail")
            exit()
        finally:
            os.system(f'rm flag {source_file} {executable}')
    print("3S{Your_Python_skill_is_good!}")

if __name__ == "__main__":
    main()
```

엄청 긴데 대충 단계를 거치다가 마지막까지 답을 잘 입력하면 다음과 같이 출력된다



```
            print(f"test {i + 1} fail")
            exit()
        finally:
            os.system(f'rm flag {source_file} {executable}')
    print("3S{Your_Python_skill_is_good!}")

```

결국 처음에 txt 파일에서 발견한 플래그가 진짜였다

물론 이렇게 푸는 게 아니겠지만 어쨌거나 답은 찾았으니까...

그래서 플래그는 3S{Your_Python_skill_is_good!} !!!!