

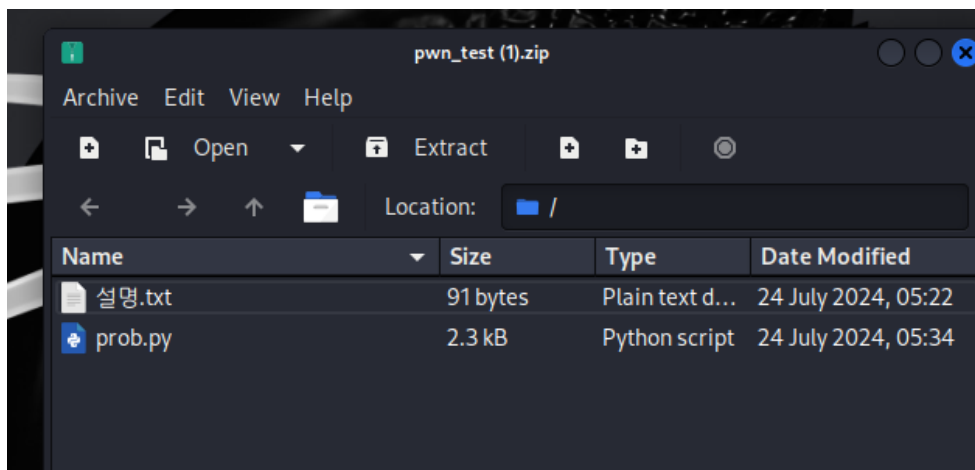
PWN TEST

32기 김효주

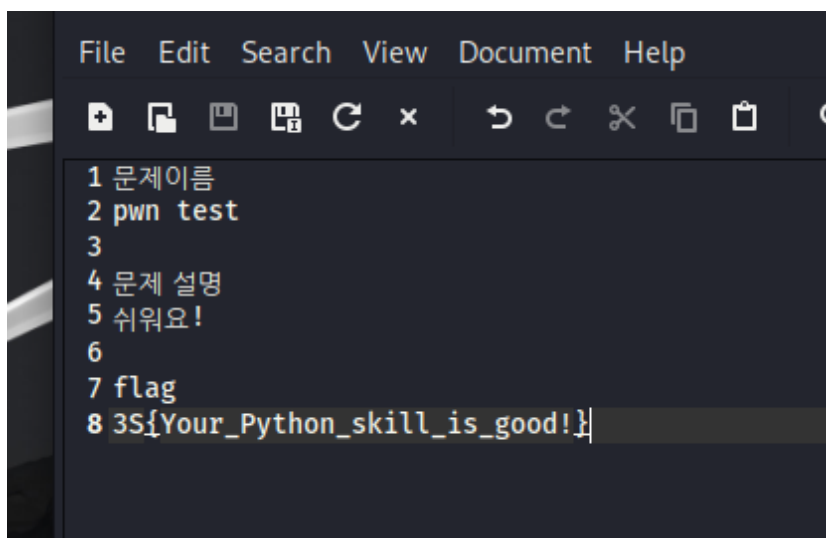
이것도 포너블 문제니까 일단 리눅스를 켜준다

엄청 쉽다고 하시니...제발 풀 수 있었으면 좋겠다

리눅스에서 파일을 다운받고 확인해보자



앵 근데 설명.txt를 열자마자 플래그가 보인다



이게 맞나?

일단 제껴두고 파이썬 파일을 열어보자

```
1 '''
2     return code
3
4 def generate_random_string(length):
5     letters = string.ascii_letters + string.digits
6     result_str = ''.join(random.choice(letters) for i in range(length))
7     return 'flag{' + result_str + '}'
8
9 def main():
10    n = random.randint(10, 20)
11    print("Welcome to easy pwn test")
12    print(f"You have to pass {n} tests")
13    ok = input("If you are ready, please enter 3S\n→ ")
14    assert ok == "3S"
15    for i in range(n):
16        print(f"test {i + 1}")
17        unique_id = str(uuid.uuid4())
18        source_file = f'{unique_id}.c'
19        executable = f'{unique_id}'
20        try:
21            with open(source_file, 'w') as cfile:
22                cfile.write(compile(random.randint(0x10, 0x50)).strip())
23            compile_process = subprocess.run(['gcc', '-no-pie', '-z relro',
24            source_file, '-o', executable],
25            stdout=subprocess.PIPE,
26            stderr=subprocess.PIPE, timeout=5)
27            assert compile_process.returncode == 0
28            os.system(f'strip {executable}')
29            with open(executable, 'rb') as prob:
30                print(base64.b64encode(prob.read()))
31            flag_str = generate_random_string(random.randint(0x18, 0x28))
32            with open(f'flag', 'w') as flag:
33                flag.write(flag_str)
34            os.system(f'./{executable}')
35            check = input("flag → ")
36
37 def main():
38    n = random.randint(10, 20)
39    print("Welcome to easy pwn test")
40    print(f"You have to pass {n} tests")
41    ok = input("If you are ready, please enter 3S\n→ ")
42    assert ok == "3S"
43    for i in range(n):
44        print(f"test {i + 1}")
45        unique_id = str(uuid.uuid4())
46        source_file = f'{unique_id}.c'
47        executable = f'{unique_id}'
48        try:
49            with open(source_file, 'w') as cfile:
50                cfile.write(compile(random.randint(0x10, 0x50)).strip())
51            compile_process = subprocess.run(['gcc', '-no-pie', '-z relro',
52            source_file, '-o', executable],
53            stdout=subprocess.PIPE,
54            stderr=subprocess.PIPE, timeout=5)
55            assert compile_process.returncode == 0
56            os.system(f'strip {executable}')
57            with open(executable, 'rb') as prob:
58                print(base64.b64encode(prob.read()))
59            flag_str = generate_random_string(random.randint(0x18, 0x28))
60            with open(f'flag', 'w') as flag:
61                flag.write(flag_str)
62            os.system(f'./{executable}')
63            check = input("flag → ")
64            except AssertionError:
65                print(f"test {i + 1} fail")
66                exit()
67            finally:
68                os.system(f'rm flag {source_file} {executable}')
69            print("3S{Your_Python_skill_is_good!}")
70
71 if __name__ == "__main__":
72     main()
```

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

```
76     print(f"test {i + 1} fail")
77     exit()
78     finally:
79         os.system(f'rm flag {source_file} {executable}')
80     print("3S{Your_Python_skill_is_good!}")
81
```

결국 처음에 txt 파일에서 발견한 플래그가 진짜였다

물론 이렇게 푸는 게 아니겠지만 어쨌거나 답은 찾았으니까...

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