

<PWN TEST - 포너블>

파일을 다운 받아서 압축을 풀었더니 다음과 같은 파일들이 생겨났다.

 prob		2024-07-24 오후 6:34	Python File	3KB
 설명		2024-07-24 오후 6:22	텍스트 문서	1KB

일단 문제를 풀기 전에 설명 메모를 열어보았다.



열어보니 flag 값이 적혀 있어서 살짝 당황했다.

처음에는 당연히 답이 아닐거라고 생각했다. 단순히 압축 파일을 푸는 것이 다는 아닐거니까.

그래서 prob 파일이 파이썬 코드라고 생각해서 visual studio로 열어보았다.

```
prob.py X
C: > Users > kimye > OneDrive > 바탕 화면 > pwn_test (1) > prob.py > ...
49 def main():
57     unique_id = str(uuid.uuid4())
58     source_file = f'{unique_id}.c'
59     executable = f'{unique_id}'
60     try:
61         with open(source_file, 'w') as cfile:
62             cfile.write(compile(random.randint(0x10, 0x50)).strip())
63         compile_process = subprocess.run(['gcc', '-no-pie', '-z relro', source_file, '-o', executable],
64                                         stdout=subprocess.PIPE, stderr=subprocess.PIPE, timeout=5)
65         assert compile_process.returncode == 0
66         os.system(f'strip {executable}')
67         with open(executable, 'rb') as prob:
68             print(base64.b64encode(prob.read()))
69         flag_str = generate_random_string(random.randint(0x18, 0x28))
70         with open(f'flag', 'w') as flag:
71             flag.write(flag_str)
72         os.system(f'./{executable}')
73         check = input("flag -> ")
74         assert check == flag_str
75     except AssertionError:
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
82 if __name__ == "__main__":
83     main()
```

코드를 쭉 훑어보니 놀랍게도 마지막 부분에 flag가 적혀 있는데 메모장 플래그와 동일하다.

이게 답이 맞나? 당황스럽다.