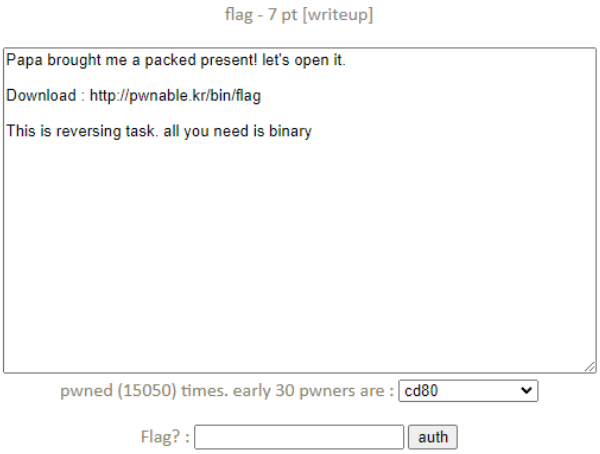
Pwnable.kr
- flag -

Download : http://pwnable.kr/bin/flag

0. 문제 살펴보기



문제에서는 bof 때와 같이 파일을 다운로드하여 살펴보는 것 같다.
원격 접속 주소가 존재하지 않으니, 해당 파일에 flag가 숨겨져 있는 것으로 생각된다.
이 문제는 리버싱에 관한 것이라고 하며 바이너리가 필요하다고 한다.

1. 파일 다운로드 및 살펴보기

```
┌──(kali㉿kali)-[~]
└─$ wget http://pwnable.kr/bin/flag
--2024-01-31 14:24:51--  http://pwnable.kr/bin/flag
Resolving pwnable.kr (pwnable.kr)... 128.61.240.205
Connecting to pwnable.kr (pwnable.kr)|128.61.240.205|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 335288 (327K)
Saving to: 'flag'

flag                                100%[=============================================================>] 327.43K   429KB/s    in 0.8s

2024-01-31 14:24:52 (429 KB/s) - 'flag' saved [335288/335288]
```

```
┌──(kali㉿kali)-[~]
└─$ file flag
flag: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.24, BuildID[sha1]=96ec4cc272aeb383bd9ed26c0d4ac0eb5db41b16, not
 stripped
```

wget 명령을 이용하여 파일을 다운로드하고 flag 파일을 살펴보았다.
file 명령을 이용하여 해당 파일이 무엇인지 확인해보았더니 실행 파일인 것을 확인할 수 있었다.

```
┌──(kali㉿kali)-[~]
└─$ ./flag
I will malloc() and strcpy the flag there. take it.
```

flag 파일을 실행해보니 malloc과 strcpy를 했고 flag는 그곳에 있다고 한다.

2. gdb

```
┌──(kali㉿kali)-[~]
└─$ gdb flag
GNU gdb (Debian 13.2-1) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from flag...
(No debugging symbols found in flag)
(gdb) disas main
No symbol table is loaded.  Use the "file" command.
```

디버깅 정보를 확인하기 위해 gdb를 이용하여 flag 파일을 열어 main 함수의 어셈블리어를 보려고 하였으나, 심볼이 존재하지 않다며 확인이 불가능한 것을 볼 수 있다.

3. 바이너리 확인

문제에서 우리는 binary가 필요하다고 하였다. 그렇기 때문에 xxd를 이용하여 flag 파일을 binary로 확인하였다.
그러자 UPX라는 한 단어가 눈에 띈다. 이 파일은 현재 압축되어 있어 gdb가 정상적으로 작동하지 않은 것으로 생각된다.

> ※ UPX
> 수많은 파일 포맷을 지원하는 오픈소스 실행 파일 압축 프로그램이다.
> 압축은 UCL이라는 이름의 데이터 압축 알고리즘을 사용한다.
> 압축 해제는 “in-place technic”과 “임시 파일로의 해제” 이렇게 두 가지의 메커니즘을 지원한다.

4. 압축 해제 및 gdb

flag 파일이 upx로 압축되었다는 것을 알았으니 해제할 차례이다.
upx의 -d 옵션을 이용하여 flag 파일을 압축 해제하였다.

이후, gdb로 flag 파일을 열자 정상적으로 작동하는 것을 볼 수 있다.
main의 어셈블리어를 확인하자 한 가지 눈에 띄는 문구가 발견되었다.
“0x6c2070 <flag>” 혹시 몰라 해당 위치의 값을 확인해보았다.

그랬더니 어떠한 문장이 등장하였다. 우리가 다른 단계에서 보았던 문장과 같이 어떠한 대화 방식의 문장이어서 사이트에서 flag로 입력하였더니 올바른 문장이었다.