i春秋 - Exploit-Exercises: Nebula - level04

原创

jchalex 于 2017-02-25 22:22:38 发布 1049 收藏

分类专栏： exploit 文章标签： exploit

About

This level requires you to read the token file, but the code restricts the files that can be read. Find a way to bypass it :)

Source

```c
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <sys/types.h>
#include <stdio.h>
#include <fcntl.h>

int main(int argc, char **argv, char **envp)
{
  char buf[1024];
  int fd, rc;

  if(argc == 1) {
      printf("%s [file to read]\n", argv[0]);
      exit(EXIT_FAILURE);
  }

  if(strstr(argv[1], "token") != NULL) {
      printf("You may not access '%s'\n", argv[1]);
      exit(EXIT_FAILURE);
  }

  fd = open(argv[1], O_RDONLY);
  if(fd == -1) {
      err(EXIT_FAILURE, "Unable to open %s", argv[1]);
  }

  rc = read(fd, buf, sizeof(buf));

  if(rc == -1) {
      err(EXIT_FAILURE, "Unable to read fd %d", fd);
  }

  write(1, buf, rc);
}
```

Nebula官网

程序逻辑

读取指定文件，但是过滤token关键字，然后输出

思路

i春秋没改这题的源码与程序，也就是说不会过滤flag关键字，所以直接运行即得flag

```
cd /home/flag04/
./flag04 flag
```

```
level04@nebula:/home/flag04$ ./flag04 flag
flag{W29MNXDT7}level04@nebula:/home/flag04$
```