**一、靶场搭建**

1、Vulhub启动

C:\Users\Toby\AppData\Local\Temp\1653485469(1).jpg

2、访问8080端口的/cgi-bin/index



**二、漏洞复现**

1、写入动态链接库源码

#include <unistd.h>

static void before\_main(void) \_\_attribute\_\_((constructor));

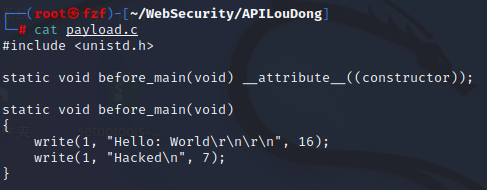
static void before\_main(void)

{

write(1, "Hello: World\r\n\r\n", 16);

write(1, "Hacked\n", 7);

}



2、编译源码

C:\Users\Toby\AppData\Local\Temp\1653486530(1).jpg

3、创建poc.py文件

引用文件：https://github.com/vulhub/vulhub/blob/master/goahead/CVE-2021-42342/poc.py

4、使用编译后的脚本发送恶意数据包，劫持代码成功被执行

