



Название :	Шар предсказаний
Категория :	Реверс-инжиниринг
Уровень :	Лёгкая
Очки :	350
Описание :	Шар предскажет всё! Но кроме флага, конечно)
Теги :	Побайтовое шифрование, стековая самописня VM
Автор :	ROP

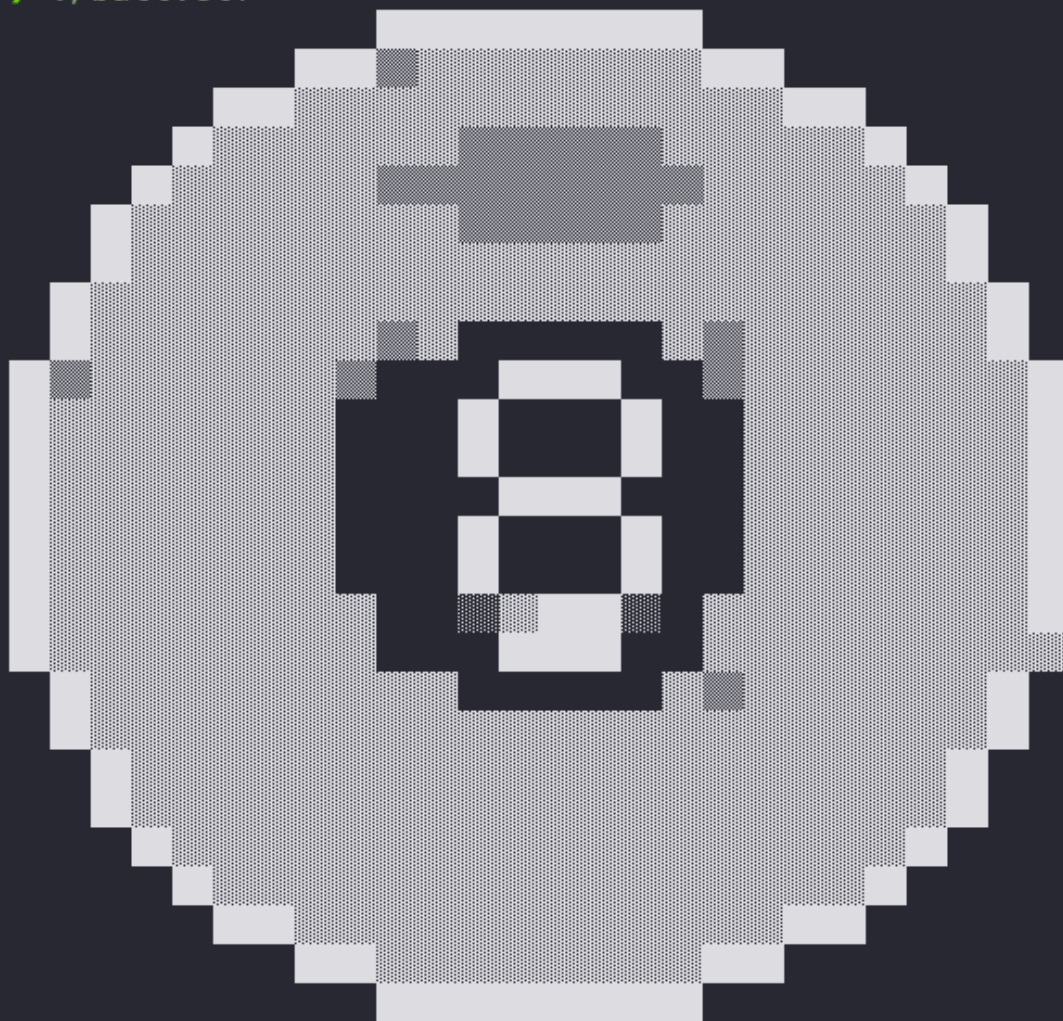
---

### Прохождение :

---

Изучаем данный нам файл.

```
> ./ball.elf
```



Я отвечу на любой вопрос!

Задать вопрос: Ты знаешь флаг?

Ты что, нет!

🔄 /tmp/Шар > █

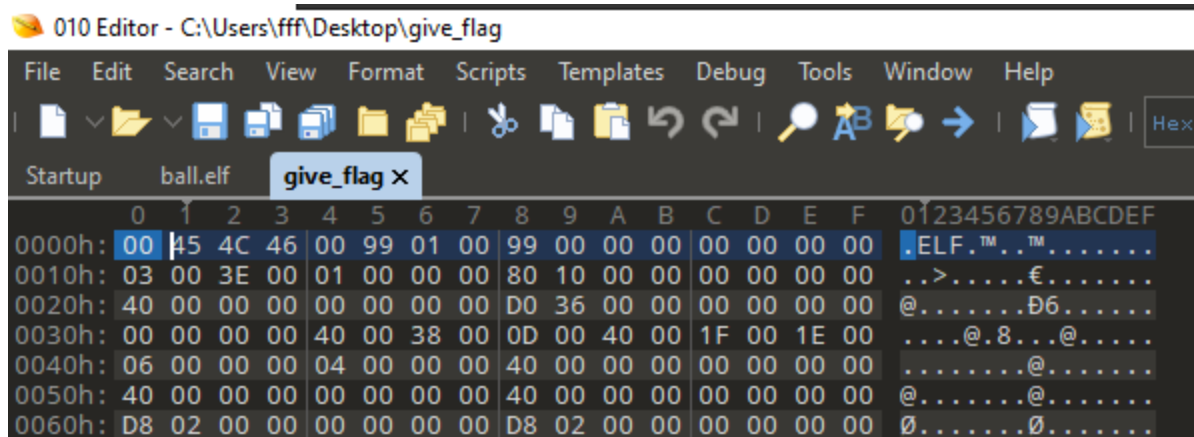
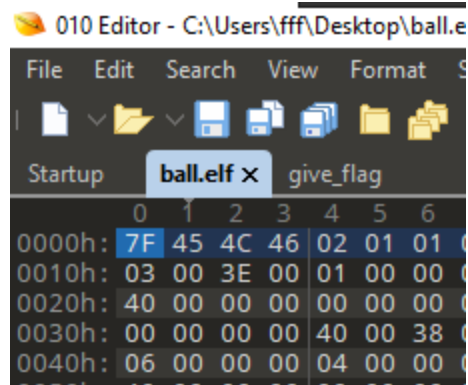
Если посмотреть строки через IDA, то можно заметить:

```

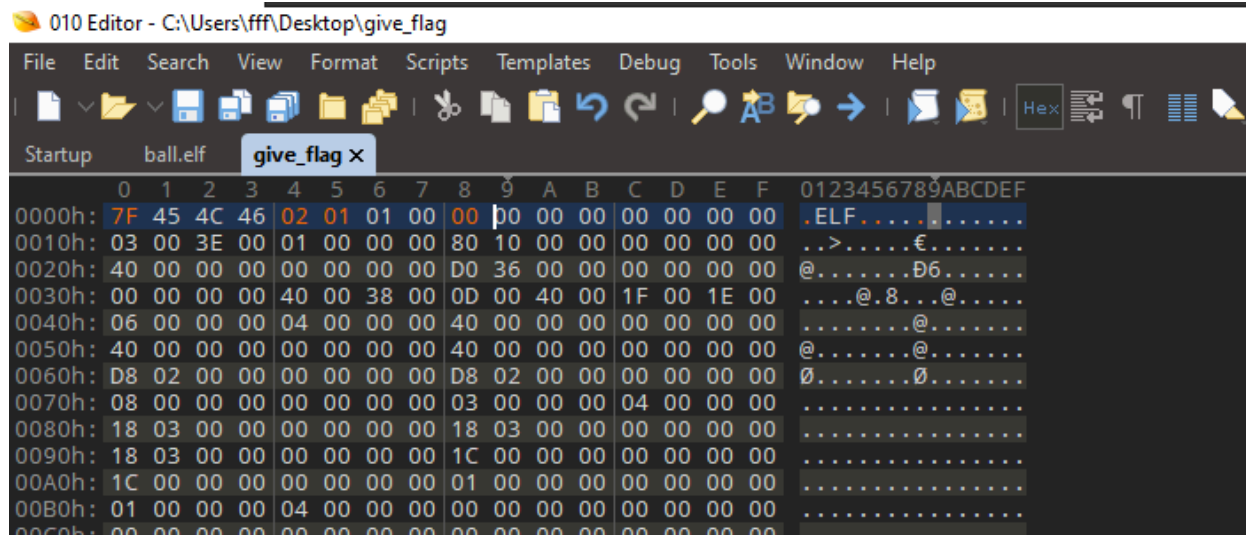
29 LOAD:0000... 0000001C C /lib64/ld-linux-x86-64.so.2
29 LOAD:0000... 00000006 C fgets
29 LOAD:0000... 00000006 C stdin
29 LOAD:0000... 00000011 C __stack_chk_fail
29 LOAD:0000... 00000012 C __libc_start_main
29 LOAD:0000... 00000006 C srand
29 LOAD:0000... 0000000F C __cxa_finalize
29 LOAD:0000... 00000007 C printf
29 LOAD:0000... 00000008 C strncmp
29 LOAD:0000... 0000000A C libc.so.6
29 LOAD:0000... 0000000A C GLIBC_2.4
29 LOAD:0000... 0000000C C GLIBC_2.2.5
29 LOAD:0000... 0000000B C GLIBC_2.34
29 LOAD:0000... 0000001C C _ITM_deregisterTMCloneTable
29 LOAD:0000... 0000000F C __gmon_start__
29 LOAD:0000... 0000001A C _ITM_registerTMCloneTable
29 .rodata:000... 00000019 C Скорее всего.
29 .rodata:000... 00000013 C Это точно.
29 .rodata:000... 00000024 C Вообще ни капельки.
29 .rodata:000... 00000007 C 1000%.
29 .rodata:000... 0000001E C Подумай об этом.
29 .rodata:000... 00000015 C Ты что, нет!
29 .rodata:000... 00000012 C : p@sS_f0R_arC1ve
29 .eh_frame:0... 00000006 C 9*3$\"
29 .data:00000... 0000003A C ;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 90\n
29 .data:00000... 0000000E C dEKXK?dXQXqjdw
29 .data:00000... 00000006 C (\\\"rb`!
29 .data:00000... 00000005 C !a:P/
29 .data:00000... 00000005 C @Al@P
29 .data:00000... 00000005 C 7.UK4
29 .data:00000... 00000006 C /uf('
29 .data:00000... 00000005 C h\\acej
29 .data:00000... 00000005 C d\\*Fw
29 .data:00000... 00000005 C z2h*^
29 .data:00000... 00000006 C Mb_Jj\\
29 .data:00000... 00000005 C \\v*h\\n
29 .data:00000... 00000007 C ]Lih63.
Line 23 of 111

```

Попробуем его на архиве, что дан вместе с файлом. Успешно подходит. Мы получили битый ELF-файл. Это можно понять, сравнив его с `ball.elf` в Нех-редакторе.



Меняем 0 на 0x7F. Также есть другие изменения в заголовках:



На скрине показан запатченный вариант. Теперь его можно открыть в IDA. Далее посмотрев код и изменения флага до `puts`, можно получить флаг.