Название:	Котик и фл@г
Категория:	Реверс-инжиниринг
Уровень:	Средний
Очки:	550
Описание:	Это AAA-котик?
Теги:	C, патчинг функций
Автор:	ROP

Прохождение:

Препятствие для решающих под номером 1.

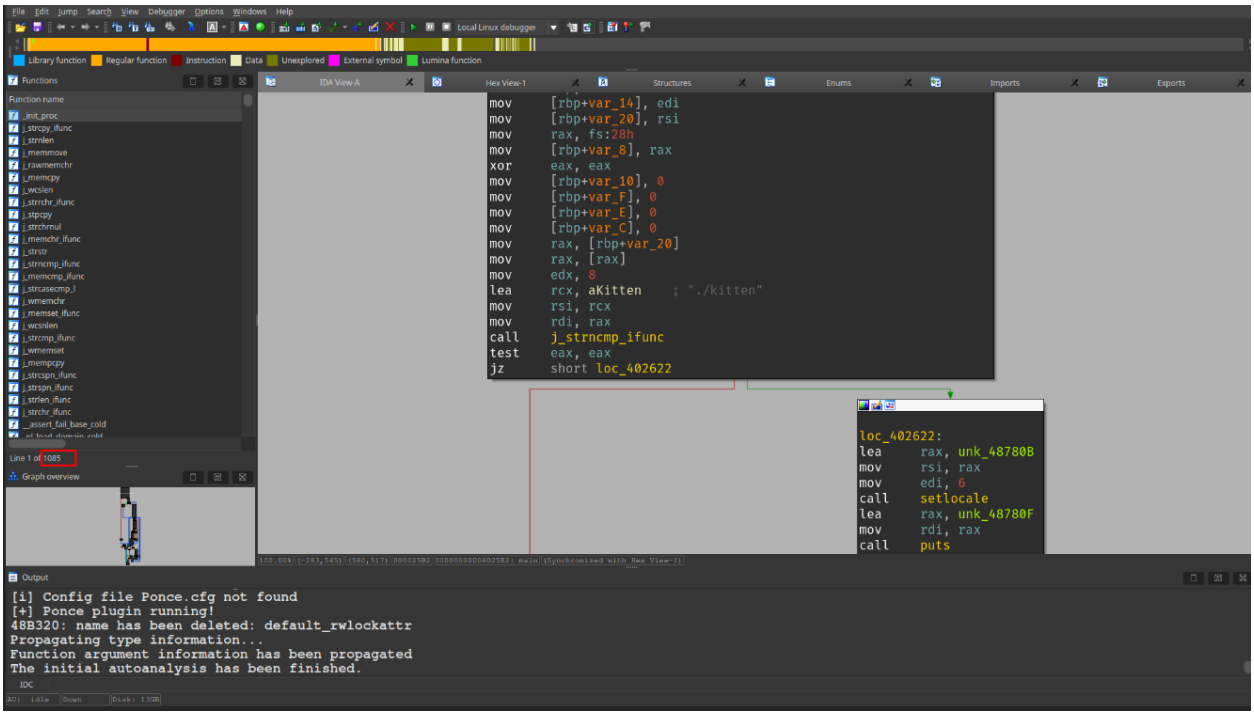
Первое препятсвие это то, что в ELF-файле есть проверка на имя программы. Оно должно быть "./kitten".

Если это не kitten или программа запущена под IDA, то происходит выход из приложения.

```
Ошибка!
~/CDB_CTF/reverse/april_ctf/Кот_да_еда ❯
```

Препятствие для решающих под номером 2.

Файл статический, поэтому там находятся все библиотечный функции из заголовочных файлов, которые были использованы в программе. Из-за этого поиск немного усложнится.



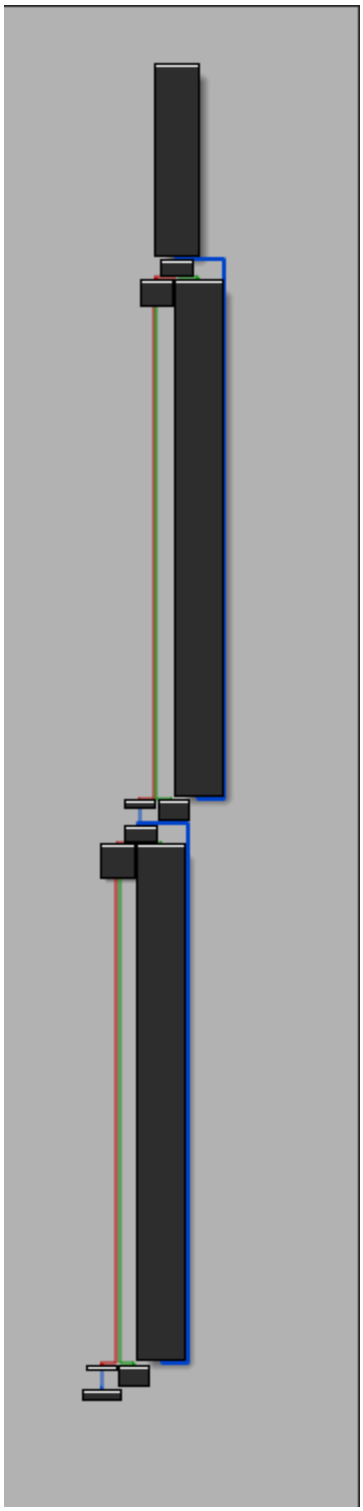
Препятствие для решающих под номером 3.

Файл упакован через UPX. И в нём изменён заголовок, чтобы нельзя было просто его распаковать.

Ложный вектор.

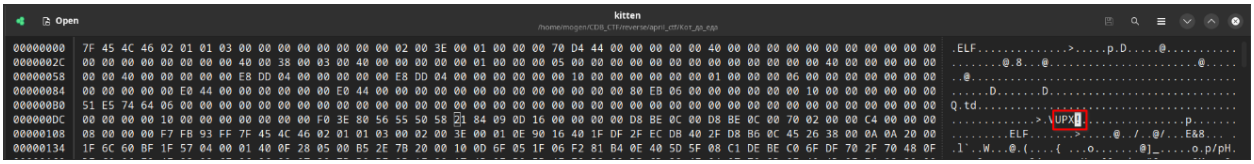
Самый главный ложный вектор - это пытаться выйграть в игре и изучать алгоритм для дешифровки в функции `give_flag`. Там ложный

флаг :)



Правильное решение.

Снимаем UPX, поменяв нужный заголовок через HEX-редактор.

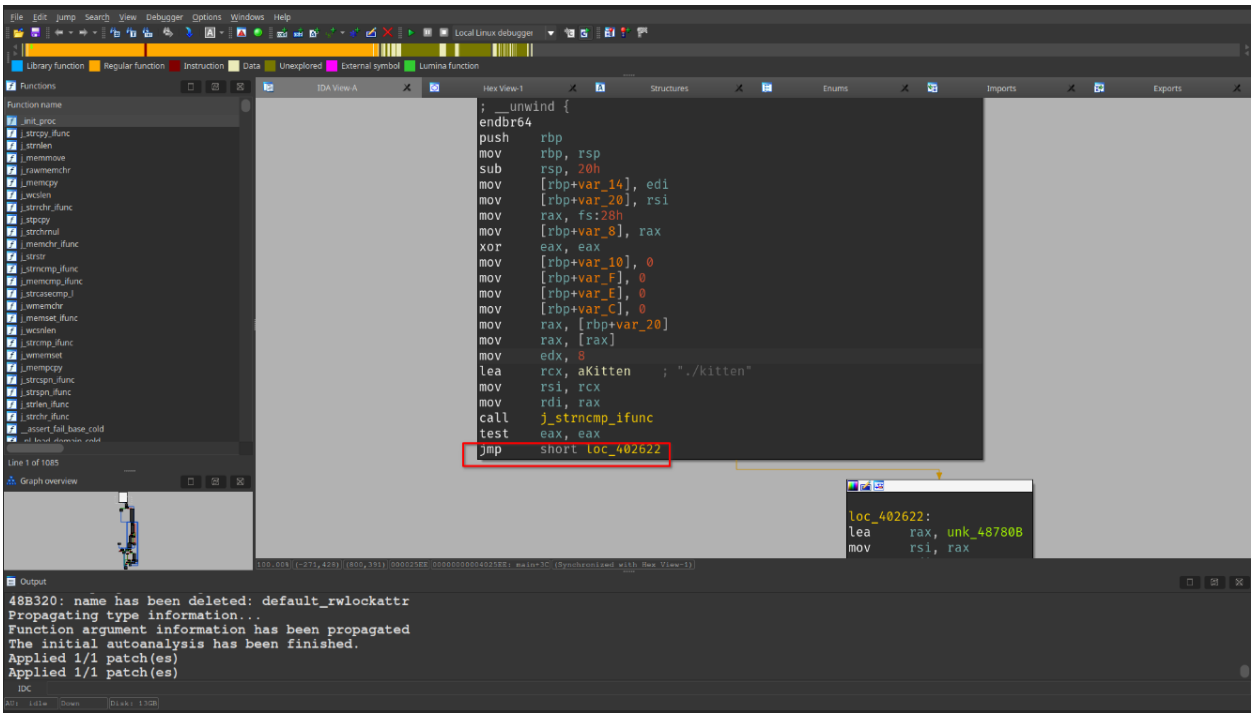


Такой должен быть.

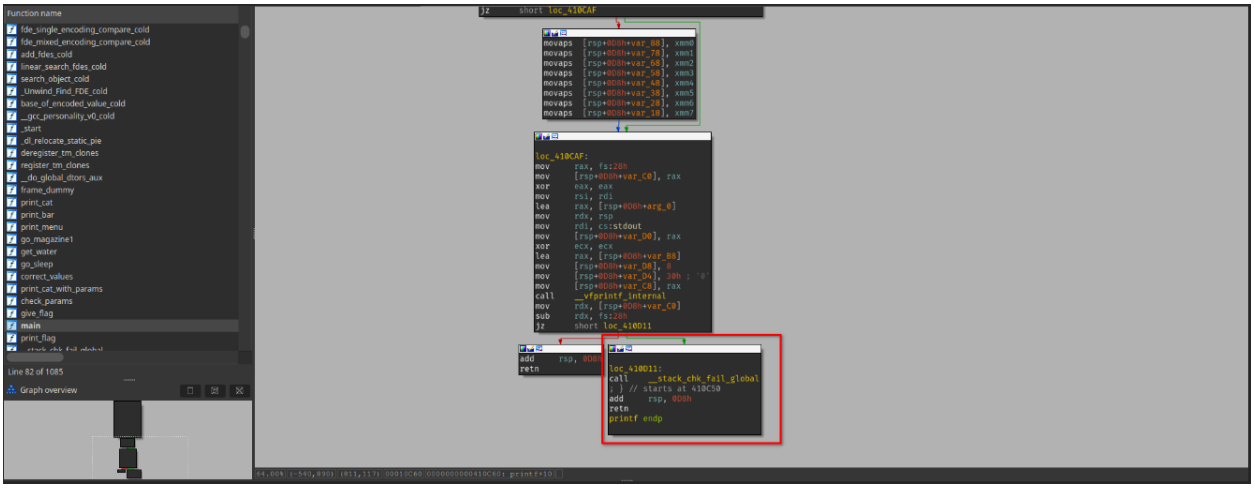
Потом используем `upx -d файл`.

```
❯ upx -d kitten
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96        Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    835288 <-    349244   41.81%   linux/amd64   kitten

Unpacked 1 file.
~/CDB_CTF/reverse/april_ctf/Кот_да_еда ❯
```

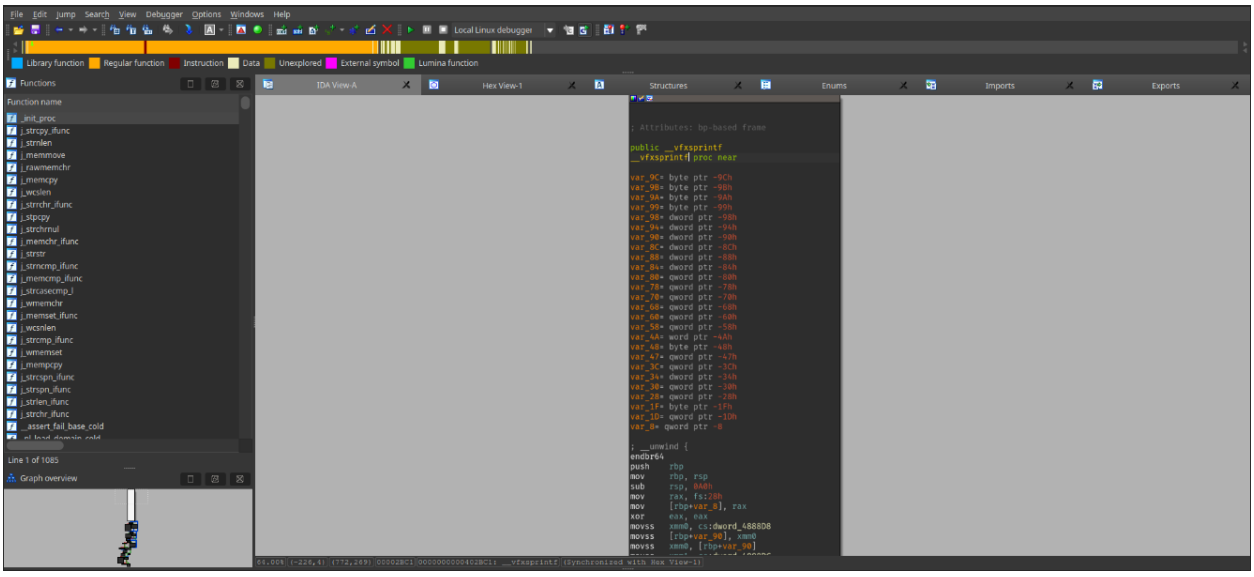
Патчим проверку имени.



(вариант 1) Изучаем функции в `main` и понимаем, что функция `printf` была изменена автором этого таска.



```
; Attributes: bp-based frame

public __stack_chk_fail_global
__stack_chk_fail_global proc near
; __unwind {
endbr64
push    rbp
mov     rbp, rsp
mov     eax, 0
call    __vfxsprintf
nop
pop     rbp
retn
; } // starts at 402BAC
__stack_chk_fail_global endp
```



В этой функции происходит вся магия. Просто её сложно найти.

Изучаем этот блок кода и понимаем, что программа хочет, чтобы у нас была системная переменная `cDb_rEv2rE` со значением флага. И ещё должна быть системная переменная `g00d_oR_bad` со значением 1.

Только в этом случае программа напечатает флаг.