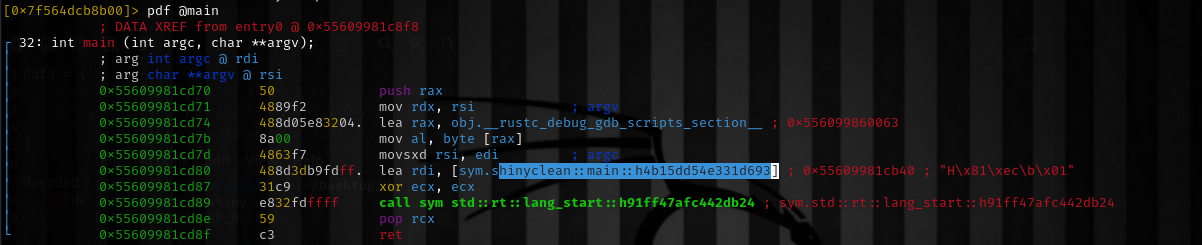
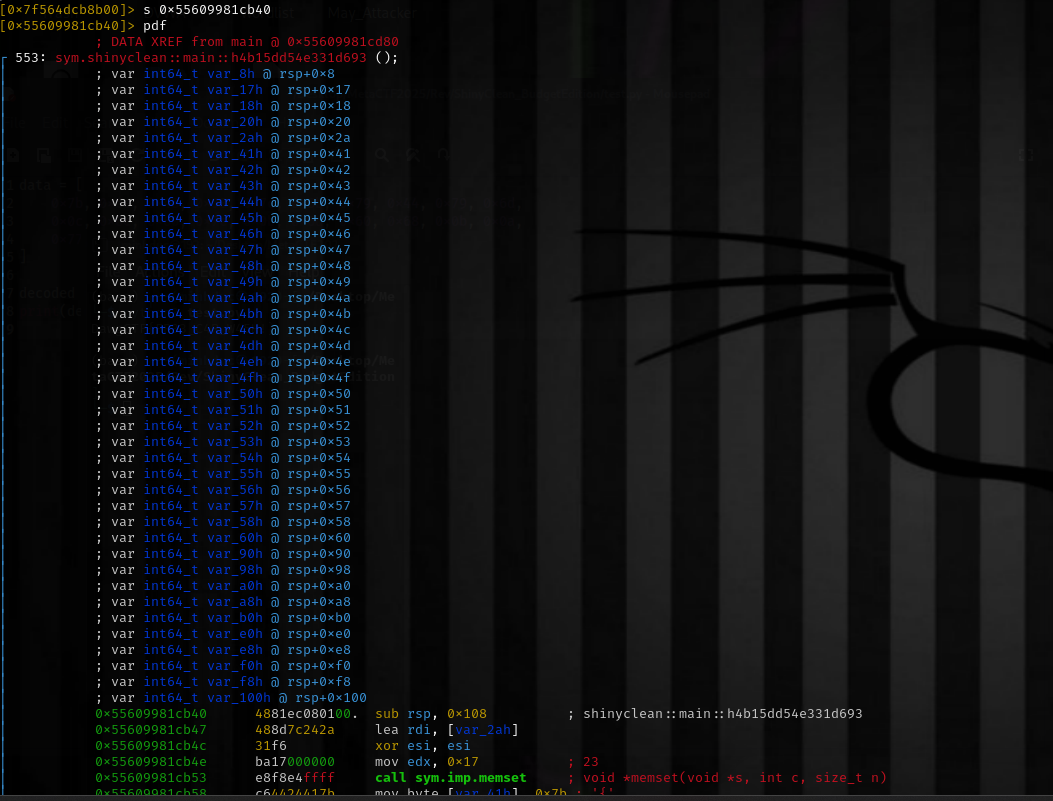
Phân tích hàm main trong file bằng radare2



**phân tích hàm shinyclean::main::h4b15dd54e331d693 tại địa chỉ 0x55609981cb40**.



Kéo xuống



có thể thấy hàm sym.shinyclean::main::h4b15dd54e331d693 đang xử lý một mảng các byte, thực hiện thao tác XOR với 0x3f, và dường như đang "giải mã" một chuỗi nào đó

Đây là một chuỗi ký tự được ghi vào vùng nhớ tạm ở rsp+0x41 trở đi.

**Vòng lặp giải mã:**

“

mov al, byte [rsp + rax + 0x41]

xor cl, 0x3f

mov byte [rsp + rax + 0x2a], cl

“

Nghĩa là từng byte của chuỗi đó được XOR với 0x3f, và ghi vào vùng nhớ mới bắt đầu từ rsp + 0x2a

**Vòng lặp chạy với rax từ 0 đến 22 (0x17):**

cmp rax, 0x17

**Giá trị đầu vào ban đầu:**

0x7b, 0x5e, 0x48, 0x58, 0x7c, 0x6b, 0x79, 0x44, 0x79, 0x6d, ...

Đến đây ta viết script để XOR từng byte với 0x3f:

data = [

0x7b, 0x5e, 0x48, 0x58, 0x7c, 0x6b, 0x79, 0x44, 0x79, 0x6d,

0x0c, 0x0c, 0x60, 0x7c, 0x0b, 0x6d, 0x60, 0x68, 0x0b, 0x0a,

0x77, 0x1e, 0x42

]

decoded = ''.join(chr(b ^ 0x3f) for b in data)

print(decoded)

