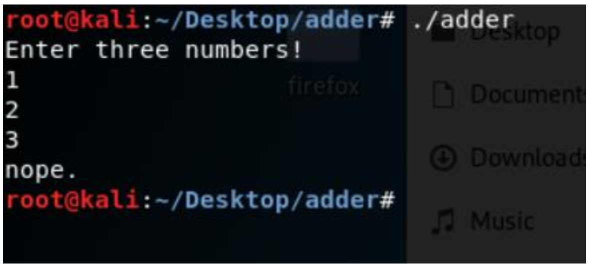
./adder

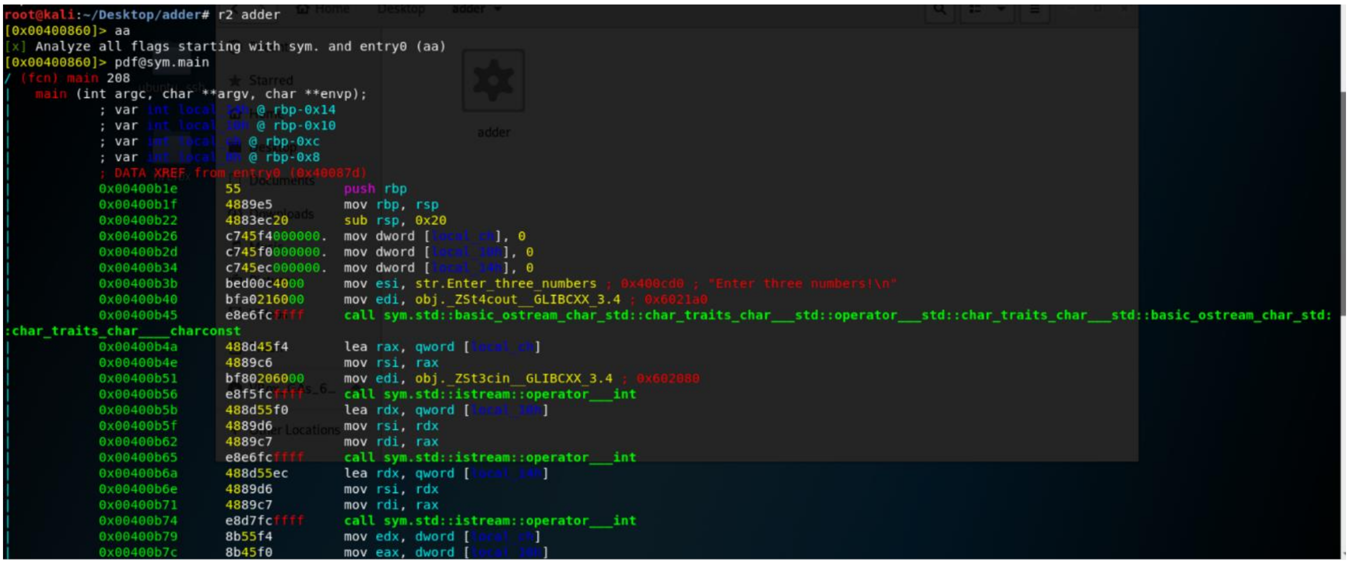


```
root@kali:~/Desktop/adder# ./adder
Enter three numbers!
1
2
3
nope.
root@kali:~/Desktop/adder#
```

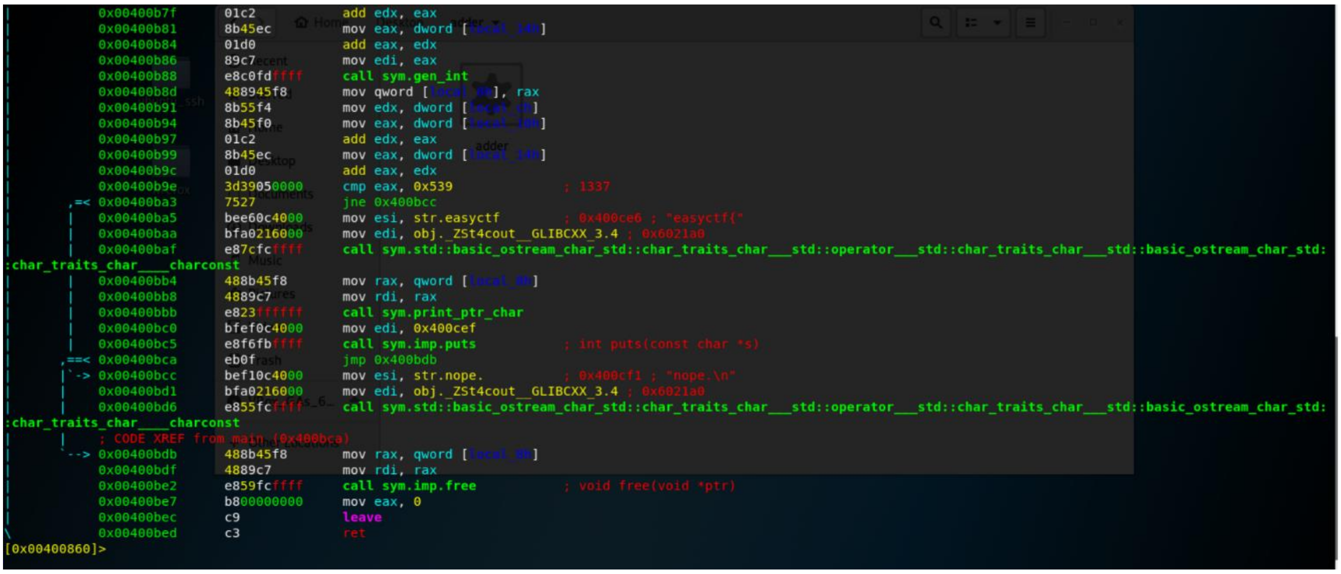
r2 adder

aa

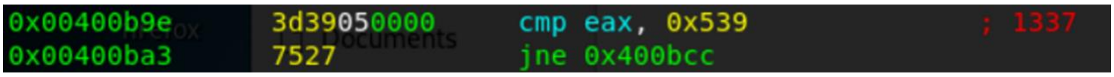
pdf@sys.main



```
root@kali:~/Desktop/adder# r2 adder
[0x00400860]> aa
[x] Analyze all flags starting with sym. and entry0 (aa)
[0x00400860]> pdf@sym.main
/ (fcn) main 208
|   main (int argc, char **argv, char **envp);
|           ; var int local_14h @ rbp-0x14
|           ; var int local_10h @ rbp-0x10
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; DATA XREF from entry0 (0x40087d)
|           0x00400b1e      55             push rbp
|           0x00400b1f      4889e5         mov rbp, rsp
|           0x00400b22      4883ec20       sub rsp, 0x20
|           0x00400b26      c745f4000000.  mov dword [local_ch], 0
|           0x00400b2d      c745f0000000.  mov dword [local_10h], 0
|           0x00400b34      c745ec000000.  mov dword [local_14h], 0
|           0x00400b3b      bed00c4000     mov esi, str.Enter_three_numbers ; 0x400cd0 ; "Enter three numbers!\n"
|           0x00400b40      bfa0216000     mov edi, obj._ZSt4cout__GLIBCXX_3.4 ; 0x6021a0
|           0x00400b45      e8e6fcffff     call sym.std::basic_ostream_char_std::char_traits_char___std::operator___std::char_traits_char___std::basic_ostream_char_std:
:char_traits_char____charconst
|           0x00400b4a      488d45f4       lea rax, qword [local_ch]
|           0x00400b4e      4889c6         mov rsi, rax
|           0x00400b51      bf80206000     mov edi, obj._ZSt3cin__GLIBCXX_3.4 ; 0x602080
|           0x00400b56      e8f5fcffff     call sym.std::istream::operator___int
|           0x00400b5b      488d55f0       lea rdx, qword [local_10h]
|           0x00400b5f      4889d6         mov rsi, rdx
|           0x00400b62      4889c7         mov rdi, rax
|           0x00400b65      e8e6fcffff     call sym.std::istream::operator___int
|           0x00400b6a      488d55ec       lea rdx, qword [local_14h]
|           0x00400b6e      4889d6         mov rsi, rdx
|           0x00400b71      4889c7         mov rdi, rax
|           0x00400b74      e8d7fcffff     call sym.std::istream::operator___int
|           0x00400b79      8b55f4         mov edx, dword [local_ch]
|           0x00400b7c      8b45f0         mov eax, dword [local_10h]
```



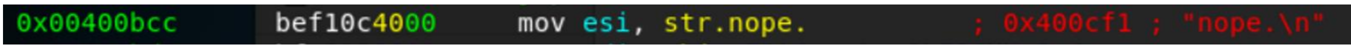
```
|           0x00400b7f      01c2           add edx, eax
|           0x00400b81      8b45ec         mov eax, dword [local_14h]
|           0x00400b84      01d0           add eax, edx
|           0x00400b86      89c7           mov edi, eax
|           0x00400b88      e8c0fdffff     call sym.gen_int
|           0x00400b8d      488945f8       mov qword [local_8h], rax
|           0x00400b91      8b55f4         mov edx, dword [local_ch]
|           0x00400b94      8b45f0         mov eax, dword [local_10h]
|           0x00400b97      01c2           add edx, eax
|           0x00400b99      8b45ec         mov eax, dword [local_14h]
|           0x00400b9c      01d0           add eax, edx
|           0x00400b9e      3d39050000     cmp eax, 0x539              ; 1337
|       ,=< 0x00400ba3      7527           jne 0x400bcc
|       |   0x00400ba5      bee60c4000     mov esi, str.easyctf        ; 0x400ce6 ; "easyctf{"
|       |   0x00400baa      bfa0216000     mov edi, obj._ZSt4cout__GLIBCXX_3.4 ; 0x6021a0
|       |   0x00400baf      e87cfcffff     call sym.std::basic_ostream_char_std::char_traits_char___std::operator___std::char_traits_char___std::basic_ostream_char_std:
:char_traits_char____charconst
|       |   0x00400bb4      488b45f8       mov rax, qword [local_8h]
|       |   0x00400bb8      4889c7         mov rdi, rax
|       |   0x00400bbb      e823ffffff     call sym.print_ptr_char
|       |   0x00400bc0      bfef0c4000     mov edi, 0x400cef
|       |   0x00400bc5      e8f6fbffff     call sym.imp.puts           ; int puts(const char *s)
|      ,==< 0x00400bca      eb0f           jmp 0x400bdb
|      |`-> 0x00400bcc      bef10c4000     mov esi, str.nope.          ; 0x400cf1 ; "nope.\n"
|      |    0x00400bd1      bfa0216000     mov edi, obj._ZSt4cout__GLIBCXX_3.4 ; 0x6021a0
|      |    0x00400bd6      e855fcffff     call sym.std::basic_ostream_char_std::char_traits_char___std::operator___std::char_traits_char___std::basic_ostream_char_std:
:char_traits_char____charconst
|      |    ; CODE XREF from main (0x400bca)
|      `--> 0x00400bdb      488b45f8       mov rax, qword [local_8h]
|           0x00400bdf      4889c7         mov rdi, rax
|           0x00400be2      e859fcffff     call sym.imp.free           ; void free(void *ptr)
|           0x00400be7      b800000000     mov eax, 0
|           0x00400bec      c9             leave
\           0x00400bed      c3             ret
[0x00400860]>
```



```
0x00400b9e      3d39050000     cmp eax, 0x539              ; 1337
0x00400ba3      7527           jne 0x400bcc
```

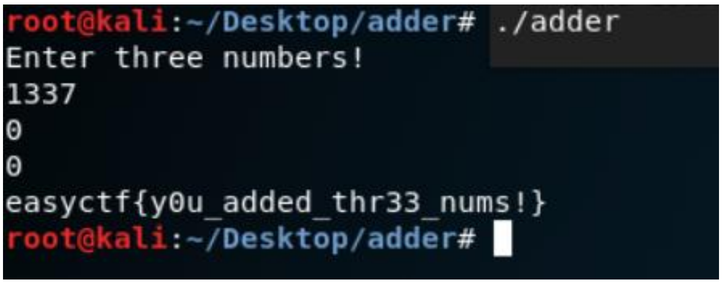
在這行指令中發現了 cmp 指令與 1337 這個數字，推測 1337 可能是 adder 所想

要的答案，因為下一個 instruction 是 jne 0x400bcc，也就是 jump if not equal. 然後在 ox400bcc 我們發現了 nope 這個字串。



```
0x00400bcc      bef10c4000      mov esi, str.nope.       ; 0x400cf1 ; "nope.\n"
```

此時去試試看 1337 這個值



```
root@kali:~/Desktop/adder# ./adder
Enter three numbers!
1337
0
0
easyctf{y0u_added_thr33_nums!}
root@kali:~/Desktop/adder#
```

得到 flag