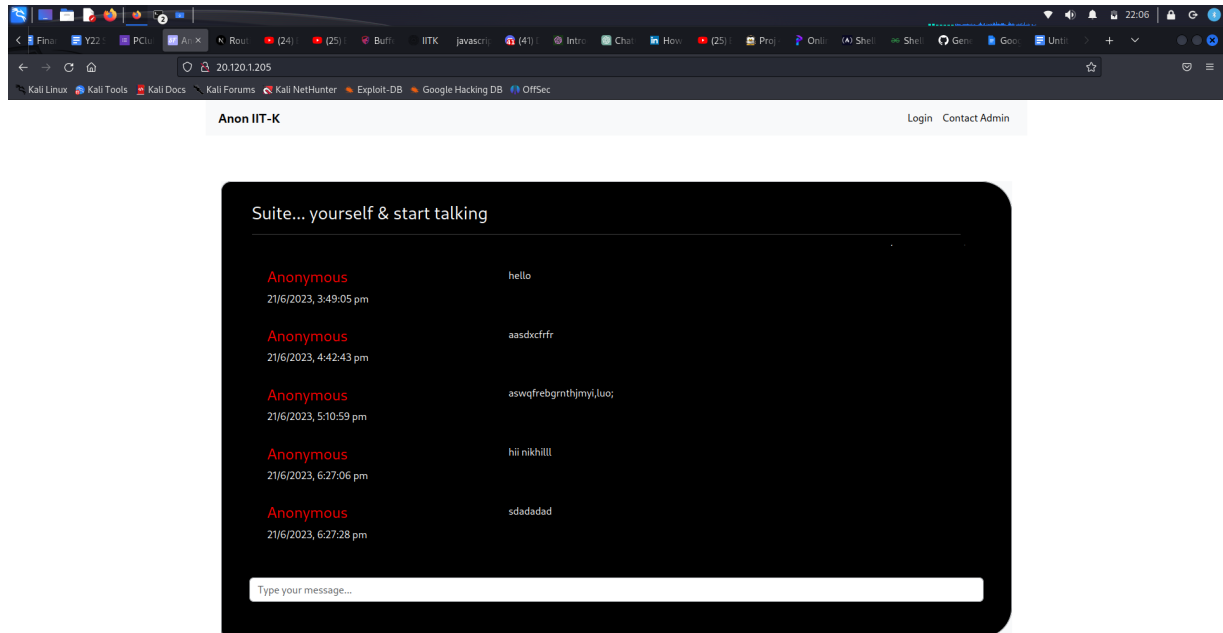


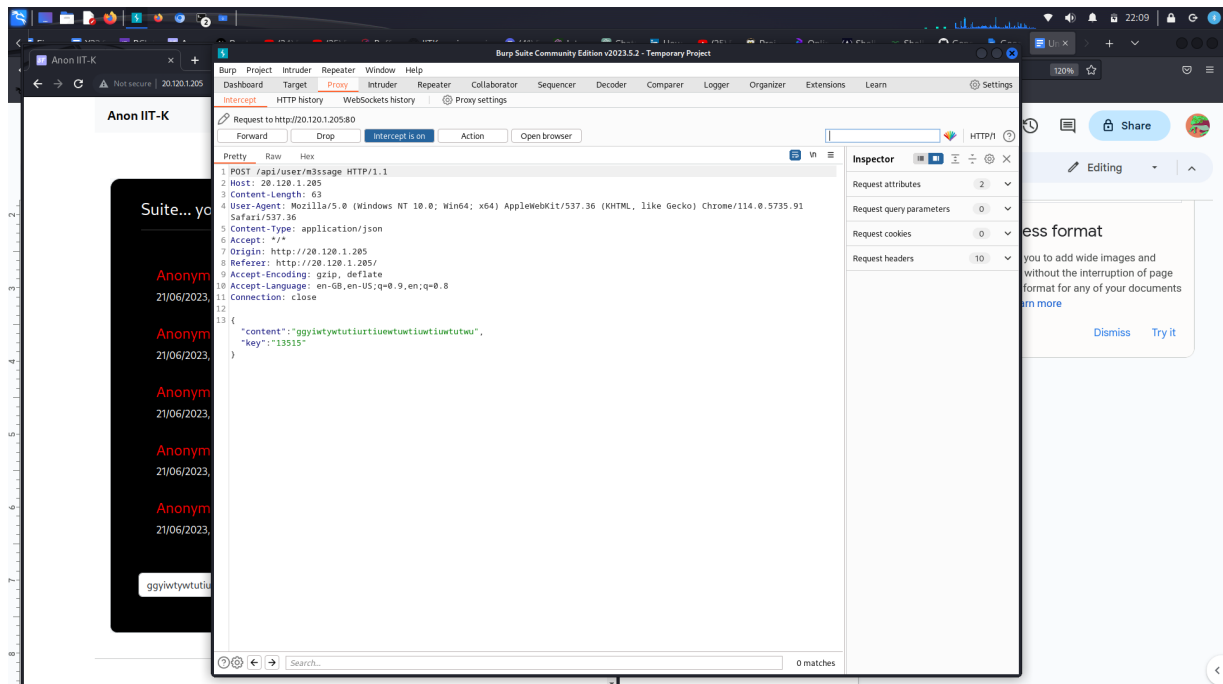
Infosec P-club task

First of all I ran the ip and it opened a site

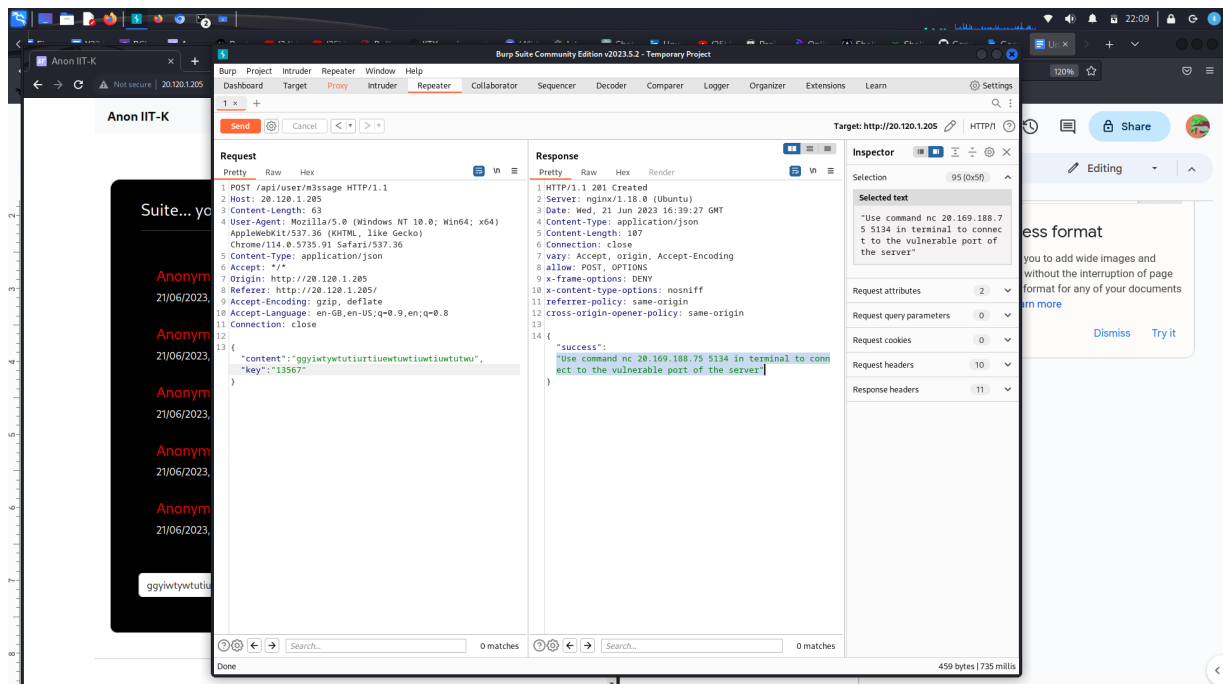


I tried many command in site and tried to find a executable command thinkin that the Chatbox will serve as a terminal.

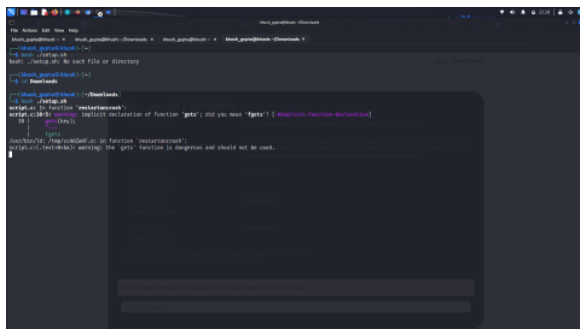
Open Burpsuite and whenever you are writing a chat intercept the site



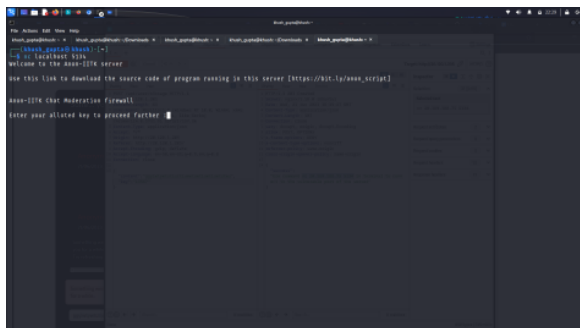
Now send the request to the repeater and simply change the key value to anything else to get a message like this



Run the following netcat command and it will take you to a script.c file and you can also download setup.sh file from there. Fix the errors in the script.c file and make it executable by running the following command `bash ./setup.sh`

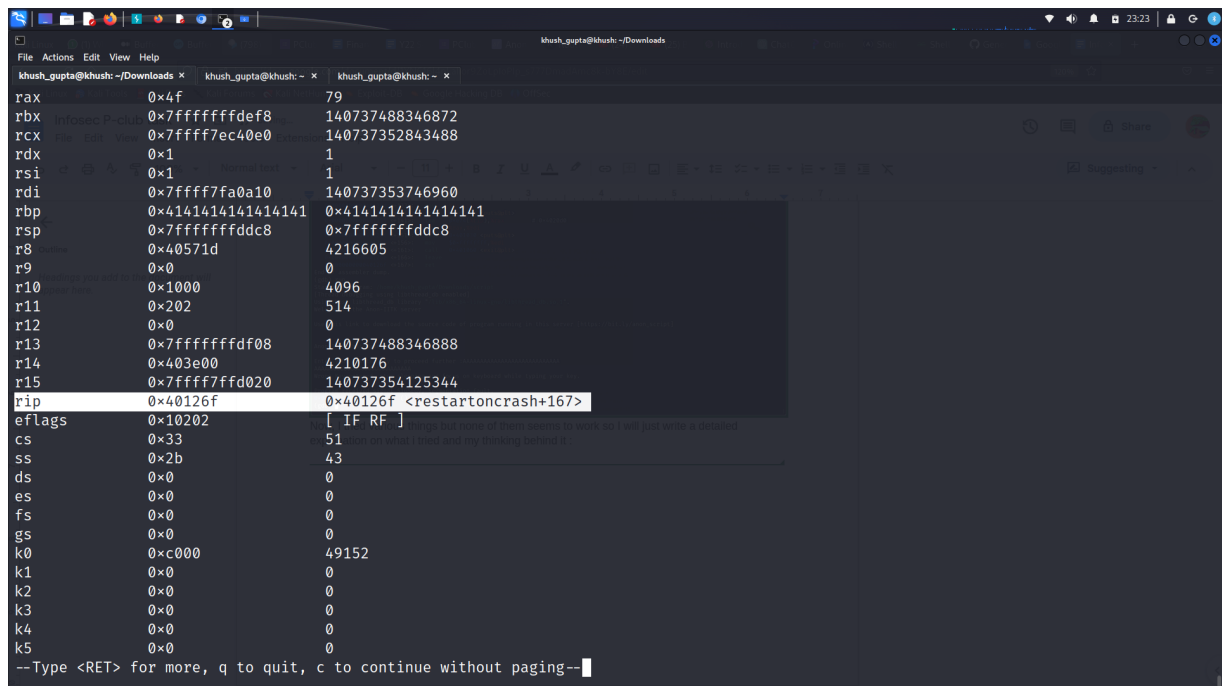


Setup connection with the localhost as in picture



Now open gdb by going to the folder containing both files and write the following command `gdb ./script`. I learned how to use gdb and read the most basic Assembly language. Disassemble the main and restartoncrash functions.

Entered info reg after putting A's to see how away i am from the return pointer which is the rip in the below image



```
File Actions Edit View Help
khush_gupta@khush: ~/Downloads khush_gupta@khush: ~ khush_gupta@khush: ~
rax 0x4f 79
rbx 0x7fffffffdef8 140737488346872
rcx 0x7ffff7ec40e0 140737352843488
rdx 0x1 1
rsi 0x1 1
rdi 0x7ffff7fa0a10 140737353746960
rbp 0x4141414141414141 0x4141414141414141
rsp 0x7ffff7fddc8 0x7ffff7fddc8
r8 0x40571d 4216605
r9 0x0 0
r10 0x1000 4096
r11 0x202 514
r12 0x0 0
r13 0x7ffff7fdd08 140737488346888
r14 0x403e00 4210176
r15 0x7ffff7ffd020 140737354125344
rip 0x40126f 0x40126f <restartoncrash+167>
eflags 0x10202 [ IF RF ]
cs 0x33 51
ss 0x2b 43
ds 0x0 0
es 0x0 0
fs 0x0 0
gs 0x0 0
k0 0xc000 49152
k1 0x0 0
k2 0x0 0
k3 0x0 0
k4 0x0 0
k5 0x0 0
--Type <RET> for more, q to quit, c to continue without paging--
```

Tried to add breakpoints on the main and restartoncrash function and also on “gets” in restartoncrash as suggested by some of the tutorials.

Problems i faced:

- 1) After finding the suitable no's of A don,t know how to add and subtract the digits to fit our shellcode.
- 2) Also didn't knew how to find shellcode or how to write one (every google site is telling something else about it).
- 3) The return address shown above does not seem to be working and when i do like this `python -c "print('A'*100+'\0x50\0x10\0x40)"` it does not return to the called function.(Don't understand why).