Cyber Youth Singapore

repeat after me!

horizontal line

**Creator Name: Kok Rui**

# Setup:

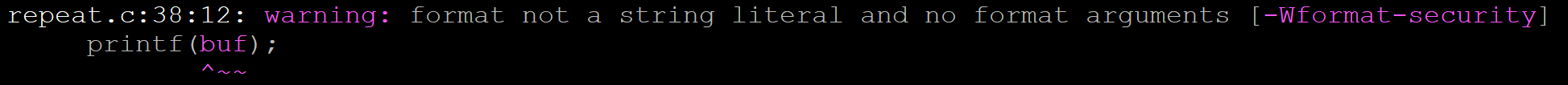
## **Static Files:**

* 1. repeat.c (source for participants)
  2. repeat (binary)
  3. flag.txt

## **Usage:**

* 1. Host chall: nohup sudo tcpserver -t 50 -RHl0 0.0.0.0 <port> ./repeat
  2. Make sure flag.txt is in same folder
  3. In CTFd, give participants repeat.c and repeat

# Description:

* **Description:**
  + My grandma can shout louder than you!
  + Give them the netcat command here thx
* **Hint:**
  + Nothing to overflow here
  + There’s a line in the program that uses a certain function with a certain component missing
  + 
  + <either paid hint or just remove> hey, here’s a convenient page with a table explaining what all the “%d”s and “%c”s in printf do… how nice! <https://owasp.org/www-community/attacks/Format_string_attack>

# Solution

1. Basic format string, they can just leak the string at every address (bruteforce %n$s) (since flag\_ptr is put directly on stack) and eventually they’ll leak the flag