Cool Math Games Write Up

Analysis

The server.py is a script that generates a bunch of 32 length random characters from ascii_lowercase, ascii_uppercase, and digits using random.choice. The random is seeded with the seed env variable. It prints the 1st randomly generated string and asks u to guess the next 160.

In the startup.sh, we can see that seed is $RANDOM which is a random int from 0 to 32767.

Solving

We can nc and get the 1st randomly generated string which is printed for us, and then bruteforce all possible seeds from 0 to 32767 and see which one matches with the string. Afterwards, predict the next few 160 and send it automatically with a script.

Here's an example script to do it.

```
import socket
import re
import random
from string import digits, ascii_lowercase, ascii_uppercase
import time

host = "tcp.ybn.sg"
port = 28480

repeats = 160

try:
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
        s.connect((host, port))
        print(f"Connected to {host}:{port}")
        initial_message = s.recv(1024).decode()
        print("Initial message from server:")
        print(initial_message.strip())

        match = re.search(r'Your user ID is "([^"]+)"', initial_message)
        if match:
            user_id = match.group(1)
            print(f"Extracted User ID: {user_id}")
        else:
            print("User ID not found in the server message.")
            exit()
```

```
        initial = user_id
        for i in range(32768):
            random.seed(i)
            if "".join([random.choice(ascii_lowercase + ascii_uppercase + digits) for _ in
range(32)]) == initial:
                break

        for i in range(repeats):
            bruhmoment = "".join([random.choice(ascii_lowercase + ascii_uppercase + digits) for
_ in range(32)]) + "\n"
            s.sendall(bruhmoment.encode())
            response = s.recv(1024).decode()
            print(f"Attempt {i + 1}: {response.strip()}")
            time.sleep(0.1)

        print("Interaction completed.")
except Exception as e:
    print(f"An error occurred: {e}")
```