LOTTERY

The lottery shows its source code at the beginning of the execution. Also, it makes you to wait 5 minutes to enter a lottery number, so it evades bruteforce attacks.

```
C:\Users\giygas\Desktop\prng>python lottery.py
Trust in Lotto-Win. Trust in open source:
def next(seed):
        # Max winner number
        MAX = 2000000000
        # Min winner number
        MIN = 1

        # Change of the seed
        seed = seed * seed + seed

        # Truncation of the seed
        if (seed > 0xFFFFFFFF):
                seed = int(hex(seed)[-8:], 16)

        # Return of [new seed, new winner number]
        return [seed, seed % (MAX - MIN) + MIN]

# Initialization of random seed
seed = random.randint(0x1337, 0xFFFFFFFF)



Last Lottery numbers:
19088396
361347183
203687859
1866050424
108956123
Wait 5 minutes to play the next round of lottery...
```

After seeing the source code, we can tell that is vulnerable to number prediction since it's using a very weak "Pseudorandom Number Generator".

We only need to know the seed's value so we can generate a number equal to the first winner number (19088396), and then predict a sequence of numbers with that seed.

To do so, we will generate a number for every single value the seed is able to own until we generate a number that matches the first winner number.

Once that occurs, we will know the initial seed value, and we will be able to predict the sequence of number, and win the lottery.

A documented PoC exploit can be found in this folder, by the name of prng_exploit.py