



Challenge Name: Lazy Game Challenge

Category: Binary Exploitation

AUTHOR: JOHN_123

Description

I found an interesting game made by some guy named "John_123". It is some betting game. I made some small fixes to the game; see if you can still pwn this and steal \$1000000 from me!

To get flag, pwn the server at: [nc thekidofarcrania.com 10001](https://nc.thekidofarcrania.com/10001)

<https://ctflearn.com/challenge/691>

Learning outcome: Network, critical thinking



Solution

1. Understand its logic of the algorithm.
2. Original – your bet = your money left
3. If original you have 500, and your bet is (e.g. -1000000)
4. $500 - (-1000000) = 1000500$
5. The answer is
“CTFlearn{d9029a08c55b936cbc9a30_i_wish_real_betting_games_were_like_this!}”

```
offliner@ubuntu: ~
Welcome to the Game of Luck !.

Rules of the Game :
(1) You will be Given 500$
(2) Place a Bet
(3) Guess the number what computer thinks of !
(4) computer's number changes every new time !.
(5) You have to guess a number between 1-10
(6) You have only 10 tries !.
(7) If you guess a number > 10, it still counts as a Try !
(8) Put your mind, Win the game !..
(9) If you guess within the number of tries, you win money !
(10) Good Luck !..

theKidOfArccrania:
  I bet you cannot get past $1000000!

Are you ready? Y/N : █
```

```
offliner@ubuntu: ~
Money you have : 500$
Place a Bet : -1000000 █
```

```
offliner@ubuntu: ~
Sorry you didn't made it !
Play Again !..
Better Luck next Time !.
Sorry you lost some money !..
Your balance has been updated !.
Current balance : :
1000500$
What the... how did you get that money (even when I tried to stop you)!? I guess
you beat me!

The flag is CTFlearn{d9029a08c55b936cbc9a30_i_wish_real_betting_games_were_like_
this!}

Thank you for playing !
Made by John_123
Small mods by theKidOfArccrania
Give it a (+1) if you like !..
offliner@ubuntu:~$
```

挑戰名稱：懶惰遊戲挑戰

類別: Binary Exploitation

作者: JOHN_123

描述

我發現了一個有趣的遊戲，該遊戲是由一個名為“John_123”製作的。這是一款幸運遊戲。我對遊戲做了一些更改；看看您能否偽造並從我那裡竊取\$ 1000000！

想成都奪旗，請到此伺服器：[nc.thekidofarcrania.com 10001](http://nc.thekidofarcrania.com:10001)

<https://ctflearn.com/challenge/691>

可以學習到: 網絡知識 及 多元思考



解題

1. 了解算術的邏輯。
2. 原有的金錢 - 你打賭的金錢 = 金錢的餘額。
3. 如果你原先有 500 元並設置賭金 (e.g. -1000000)
 1. $500 - (-1000000) = 1000500$
 2. 所得的旗幟是：
“CTFlearn{d9029a08c55b936cbc9a30_i_wish_real_betting_games_were_like_this!}”

```
offliner@ubuntu: ~
Welcome to the Game of Luck !.

Rules of the Game :
(1) You will be Given 500$
(2) Place a Bet
(3) Guess the number what computer thinks of !
(4) computer's number changes every new time !.
(5) You have to guess a number between 1-10
(6) You have only 10 tries !.
(7) If you guess a number > 10, it still counts as a Try !
(8) Put your mind, Win the game !..
(9) If you guess within the number of tries, you win money !
(10) Good Luck !..

theKidOfArccrania:
I bet you cannot get past $1000000!

Are you ready? Y/N : █
```

```
offliner@ubuntu: ~
Money you have : 500$
Place a Bet : -1000000 █
```

```
offliner@ubuntu: ~
Sorry you didn't made it !
Play Again !..
Better Luck next Time !.
Sorry you lost some money !..
Your balance has been updated !.
Current balance : :
1000500$
What the... how did you get that money (even when I tried to stop you)!? I guess
you beat me!

The flag is CTFlearn{d9029a08c55b936cbc9a30_i_wish_real_betting_games_were_like_
this!}

Thank you for playing !
Made by John_123
Small mods by theKidOfArccrania
Give it a (+1) if you like !..
offliner@ubuntu:~$
```