CTF題目 June. 23rd 2021

[Medium] [Binary] Lazy Game Challenge

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`

[Medium] [Forensics] Tux!

The flag is hidden inside the Penguin!

https://ctflearn.com/challenge/download/973

[Medium] [Programming] The Credit Card Fraudster

I just arrested someone who is probably the most wanted credit card fraudster in Europe. She is a smart cybercriminal, always a step ahead INTERPOL and she kept unnoticed for years by never buying online, but buying goods with a different card every time and in different stores. My cyber-analysts found out after collecting all evidences she hacked into one the largest payment provider in Europe, reverse-engineered the software present on the server and partly corrupted the card number validation code to accept all her payments. The change enables acceptance of any transaction with a card number multiple of 123457 and the Luhn check digit is valid.

I caught her because every year she bought a bouquet of flowers next to the same cemetery. While handcuffing her at the flower shop's exit, she said the flowers were for her lost father and today it is his death anniversary. She broke down in tears and she did some steps and threw something in the sewers. My female colleague conducted a search on her, but she couldn't find the card she used, only the receipt.

```
The little flower shop
======================

European Express Debit
Card Number: 543210******1234
SALE

Please debit my account
Amount: 25.00€
```

Can you help me to recover the card number so that I can confirm with the flower merchant's bank the card number was used in that shop and is fraudulent?

Hints:

1/ Luhn_algorithm

2/ Flag format is `CTFlearn{card_number}`

[Medium] [Reverse Engineering] Bite-code

I dunno what bytecode is. Could you tell me what input of 'checkNum' will return true? The flag is just a 32-bit signed integer as a decimal (nothing else.)

https://mega.nz/#!qfATFaKR!zaTNExq3Bm1MjJnePjTGQyvnvLX_xZxhbGaMv_ypaxo

Hints:

1/ x64 Manual: https://cs.brown.edu/courses/cs033/docs/guides/x64_cheatsheet.pdf

[Hard] [Web] Inj3ction Time

I stumbled upon this website: http://web.ctflearn.com/web8/ and I think they have the flag in their somewhere. UNION might be a helpful command

Hints:

1/ How to find database name, table name, and column name?