

CTF题目 June. 30th 2021

[Easy] [Reverse] Transformation

I wonder what this really is... `enc ''.join([chr((ord(flag[i]) << 8) + ord(flag[i + 1])) for i in range(0, len(flag), 2)])`

<https://mercury.picoctf.net/static/77a2b202236aa741e988581e78d277a6/enc>

Hint: You may find some decoders online

[Easy] [Cryptography] Mind your Ps and Qs

In RSA, a small `e` value can be problematic, but what about `n`? Can you decrypt this? [values](#)

<https://mercury.picoctf.net/static/b9ddda080c56fb421bf30409bec3460d/values>

Hint: Bits are expensive, I used only a little bit over 100 to save money

[Medium] [Web] It is my Birthday

I sent out 2 invitations to all of my friends for my birthday! I'll know if they get stolen because the two invites look similar, and they even have the same md5 hash, but they are slightly different! You wouldn't believe how long it took me to find a collision. Anyway, see if you're invited by submitting 2 PDFs to my website.

<http://mercury.picoctf.net:63578/>

Hint1: Look at the category of this problem.

Hint2: How may a PHP site check the rules in the description?

[Medium] [Binary] Stonks

I decided to try something noone else has before. I made a bot to automatically trade stonks for me using AI and machine learning. I wouldn't believe you if you told me it's unsecure! [vuln.c](#)

`nc mercury.picoctf.net 27912`

<https://mercury.picoctf.net/static/17ba7f9351aca192c45833c658742fe5/vuln.c>

Hint: Okay, maybe I'd believe you if you find my API key.

[Hard] [Binary] Here's a LIBC

I am once again asking for you to pwn this binary [vuln libc.so.6 Makefile](#)

`nc mercury.picoctf.net 62289`

<https://mercury.picoctf.net/static/2c327c6c08e9d1d8142dbdb85ae00574/vuln>

<https://mercury.picoctf.net/static/2c327c6c08e9d1d8142dbdb85ae00574/libc.so.6>

<https://mercury.picoctf.net/static/2c327c6c08e9d1d8142dbdb85ae00574/Makefile>

Hint: PWNTools has a lot of useful features for getting offsets.

参考资料: <https://ctf-wiki.org/pwn/linux/stackoverflow/basic-rop/>

