



Medium Reverse Engineering picoCTF 2021

AUTHOR: THELSHELL

Description

Best Stuff - Cheap Stuff, Buy Buy Buy...

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: NOT_RUNNING

[Launch Instance](#)

Hints ?

1

Hint :

1. Always check edge cases when programming

File yang didapat dari problem tersebut :

1. Source

```
source
Shop % file source
source: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, Go BuildID=4B889tc1TRgpS9czhvct/FgQ1iPCpaksezCsvmIRb/JEuIrSM0u7bsenZgEPQP/pVFuNtB-YiGf_M2pZFLj, with debug_info, not stripped
Shop %
```

2. nc wily-courier.picoctf.net 64783

Dari file source yang berjenis ELF, aku sudah coba analisis dengan menggunakan binary ninja dan mendapatkan kebingungan sehingga memutuskan untuk menggunakan netcat yang diberikan.

Program netcat menampilkan output seperti berikut :

```
Shop % nc wily-courier.picoctf.net 64783
Welcome to the market!
=====
You have 40 coins
      Item        Price   Count
(0) Quiet Quiches    10      12
(1) Average Apple    15       8
(2) Fruitful Flag   100       1
(3) Sell an Item
(4) Exit
Choose an option:
```

Langsung saja aku pilih fruitfull flag ternyata coinnya tidak cukup untuk beli, setelah itu aku coba beli di Quiet Quiches sebanyak 1 alhasil koinku berkurang menjadi 25 dari 40. Aku coba-coba untuk membeli sebanyak minus 10 di Average Apple alhasil koinku malah

bertambah menjadi 100-an. Lalu aku putuskan untuk langsung membeli Fruitful Flag dan muncul output sebagai berikut :

```
Item          Price   Count
(0) Quiet Quiches    10      12
(1) Average Apple   15      18
(2) Fruitful Flag    100     1
(3) Sell an Item
(4) Exit
Choose an option:
2
How many do you want to buy?
1
Flag is: [112 105 99 111 67 84 70 123 98 52 100 95 98 114 111 103 114 97 109 10
9 101 114 95 48 55 55 97 53 98 49 48 50 125 10]
```

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various categories like Operations, Favourites, Data format, etc. The main area has three tabs: Recipe, Input, and Output. In the Recipe tab, it says "From Charcode". In the Input tab, there is a large hex string: 112 105 99 111 67 84 70 123 98 52 100 95 98 114 111 103 114 97 109 109 101 114 95 48 55 55 97 53 98 49 48 50 125 10. In the Output tab, the result is shown as picoCTF{b4d_brogrammer_077a5b102}. At the bottom, there's a green button labeled "BAKE!" with a checkmark next to it.

Flag : picoCTF{b4d_brogrammer_077a5b102}