PicoCTF Shop 50 points

<https://mercury.picoctf.net/static/f7b8db17d0891fb38c01a716052d1c04/source>

mercury.picoctf.net 24851

We start with 2 sources, the first is the source code itself and the second a link to use with Netcat, we will first check out what that does!

A screenshot of a computer

Description automatically generated with medium confidence

It’s a simple UI like environment where you can buy and sell items

When opening the file in a hex editor you can se .ELF at the start meaning its an ELF file

Graphical user interface, text, application

Description automatically generated

Ofcorse this doesn’t make a lot of sense so I decided to decompile the file using snowman: <https://github.com/yegord/snowman> in order to see the code underneath!

Graphical user interface, text, application

Description automatically generated

Then I copied it to visual studio code for easier observing!

A computer screen capture

Description automatically generated with medium confidence

After understanding that the vulnerability was that it is possible to buy negative amounts of items I bought the flag by first buying a negative amount making me gain money and afterwards buying the flag!

Text

Description automatically generated

picoCTF{b4d\_brogrammer\_532bcd98}

As I couldn’t manage to find the vulnerability myself in the code I should definitely get back to this!