More cookies 90 points

<http://mercury.picoctf.net:43275/>

This is the continuation of Cookies, a funny thing is that More cookies was actually more difficult than most cookies, this is one I just couldn’t find so credits to the source!

The first hint send you to a Wikipedia link: <https://en.wikipedia.org/wiki/Homomorphic_encryption> which is the encryption method used.

Within the cookies you can see that auth\_name has an encrypted value: Graphical user interface, application

Description automatically generated

R2lUL0hKamxtMkhycGFsSTJrbTVSTnhVLzVtRWRmRHVqUHNpRHF4UEJscFA0QVhOMGEydDZVSnE1b2ZDbURjYk1CMStEeXZkeTNTR0VFUGc2L1hsbGN2QnpYMm9lc0F5aEdtcm9XZmZkYWJEWDN4bHIxczEzMzlKUnNYaWZEREM=

Which is encrypted with a Homomorphic encryption stated by the hint. Homomorphic encryption allows you to perform operation on encrypted text which is really cool!

as CBC was capitalized in the explanation it indicated that cipher block chaining is used! This means its vulnerable to a bit flip! A bit flip is where you change bits hoping to change values. In this case we want to have a value like admin=0 become admin=1.

As I’m currently going through writeups I went for a nice & clean copy paste from the second writeup in the sources which gave me a bruite force algoritm to bitflip through the code!

Text

Description automatically generated

The bruite force algoritm will now bash through the possible combinations of the code and if it gets a value back that has PicoCTF{ inside it will stop the looping and return the flag

Graphical user interface, text

Description automatically generated