MacroHard WeakEdge

Description

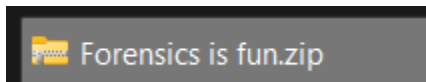I've hidden a flag in this file. Can you find it? Forensics is fun.pptm

I went through all the given questions to check if any seemed doable. This was the first one that seemed easy to attempt to me. I encountered a similar problem at a cryptic hunt a few days ago.

The given file has the extension .pptm

A file with the PPTM file extension is a Microsoft PowerPoint Open XML macro-enabled presentation file. They're comprised of pages/slides that hold text, media files like images and videos, graphs, and other things pertinent to a presentation. 13-Jun-2023

So, In simple terms, a .pptm file is not exactly a ppt. It's more like a zip file.
I was taught this back during the cryptic hunt by a friend.

So if I first rename this file with a .zip extension :

Forensics is fun.zip

Then If I open it with winrar, I can see what's inside :

When traversing through it, I found an interesting file in ppt/slideslayout/

Opened it and found this:

ZmxhZzogcGljb0NURntEMWRfdV9rbjB3X3BwdHNfcl96MXA1fQ

Encoded bengali bs lesgoo.
Pasted it into cyber chef to decode it

(Cyber chef is this site i came across out of pure desperacy of finding an xor decrypter online during that cryptic hunt I mentioned. It's literally a swiss army knife whoa : https://gchq.github.io/CyberChef/#input=Wm14aFp6b2djR2xqYjBOVVJudEVNV1JmZFY5cmJqQjNYM0J3ZEhOfcl96MXA1fZlE)

Tried rot13-ing first, out of pure guesswork

Recipe

ROT13

☑ Rotate lower case chars   ☑ Rotate upper case chars

☐ Rotate numbers

Amount
13

Input

ZmxhZzogcGljb0NURntEMWRfdV9rbjB3X3BwdHNfcl96MXA1fQ

ᴬᴮᶜ 50   ☰ 1   📍 50

Output

MzkuMmbtpTywo0AHEagRZJEsqI9eowO3K3OjqUAspy96ZKN1sD

Bro cooked nothing

Tried base64 after that

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars   ☐ Strict mode

Input

ZmxhZzogcGljb0NURntEMWRfdV9rbjB3X3BwdHNfcl96MXA1fQ

ᴬᴮᶜ 50   ☰ 1

Output

flag: picoCTF{D1d_u_kn0w_ppts_r_z1p5}

picoCTF{D1d_u_kn0w_ppts_r_z1p5}

Ez dub.