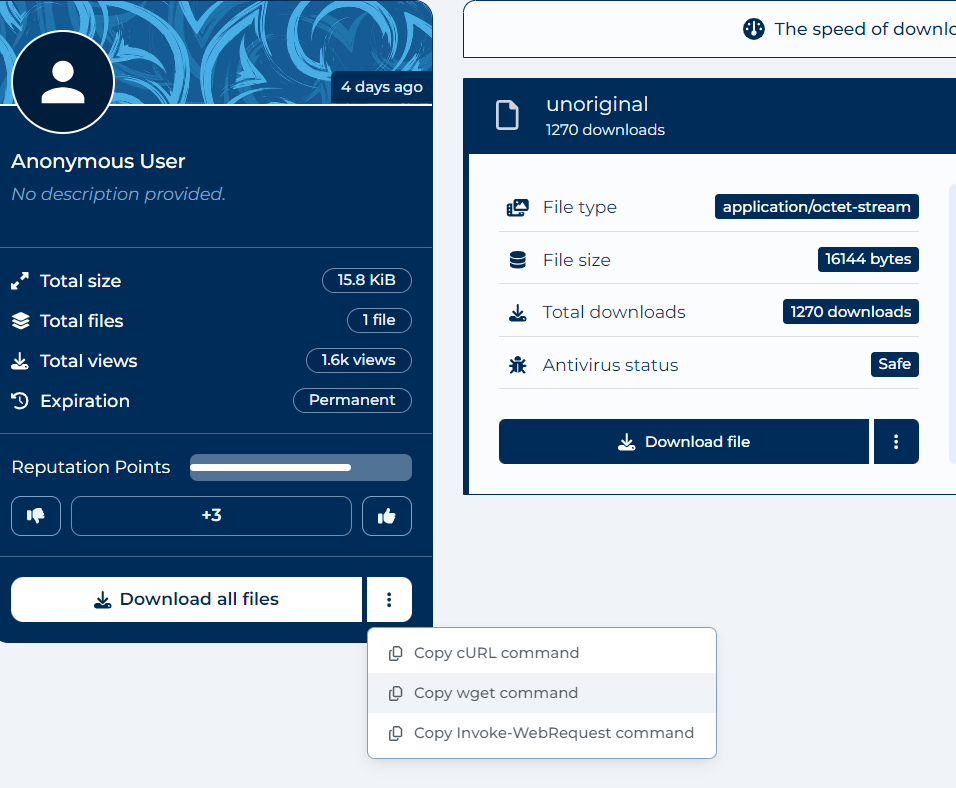
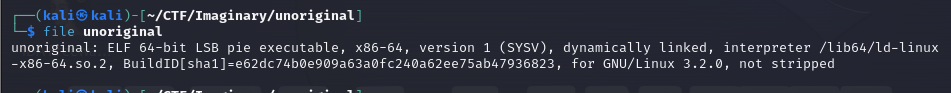


First click the link



Press the copy wget command

Then open kali linux VM and download it

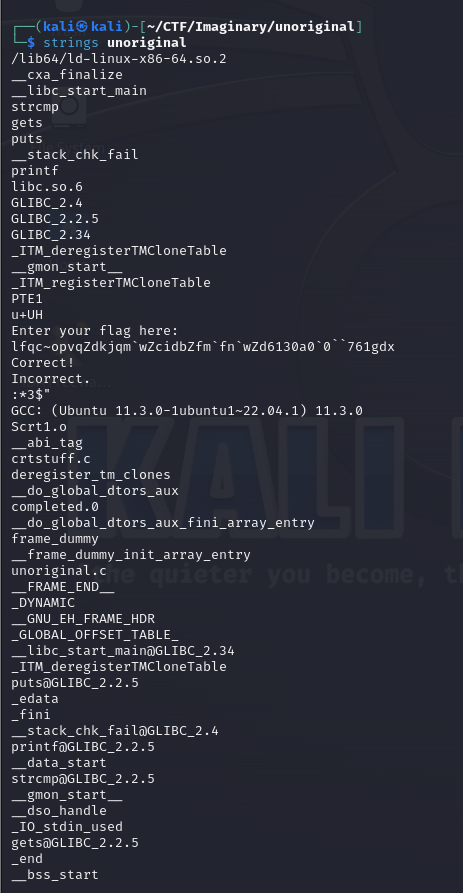


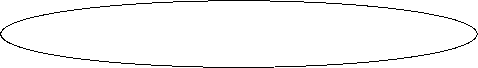
Use file command to look the file type.

From the command we know it is a ELF file, 64 bit , x86-64 and not Stripped.



Next we can use Strings commands to find strings inside the file and try to grep the flag by using the format ictf{ . Unfortunately it not exist . Nevermind we direct Strings the file .





We can find some important message through Strings commands

“ lfqc~opvqZdkjqm`wZcidbZfm`fn`wZd6130a0`0``761gdx “ this Strings probably will be our flag .



Make the file executable and start run it .



We enter smtg and see the output .



It is wrong and nevermind let us start with static analysis . Open the ida and disassemble the file .

A screenshot of a computer

Description automatically generated

We will jump to this page .

A screenshot of a computer

Description automatically generated

Next press shift+F12 to open the Strings

A screenshot of a computer

Description automatically generated



We found the important message .

Let start with input Enter the flag to see what the heck inside

A screenshot of a computer

Description automatically generated



Double click here

A screenshot of a computer

Description automatically generated

You will jump to this page

A screenshot of a computer

Description automatically generated



Press the list cross references to and press ok .

A screenshot of a computer

Description automatically generated

You will jump to this page and let us scroll down a little bit .

A screenshot of a computer

Description automatically generated



Throughout the assembly code I found that it will call a strcmp function.

Strcmp – String compare function if equal return 0 else return 1

Then it will jump to loc\_1264 if it is not equal to zero .

Let see what happen in loc\_1264 .

Loc\_1264 is the the function that will call out Incorrect thus we need to make sure it will return 0 during the strcmp function so we can get the correct .

A screenshot of a computer

Description automatically generated

Next we press f5 to look into the C code . Throughout the code , I found that s1 is the input and lets us change the variable name .

A screenshot of a computer

Description automatically generated

It looks lile our input will undergo the bitwise XOR with 5 and then compare with the Strings “ lfqc~opvqZdkjqm`wZcidbZfm`fn`wZd6130a0`0``761gdx “ and if equal it will call out correct .

Let reverse it with some simple coding .

A screen shot of a computer program

Description automatically generated

The main idea :

A ^ B = B ^A

By following the formula we just take each of the character and XOR by 5 .



Lastly we get the flag.