Challenge Name: Hackme_rox !

CATEGORY : FORENSICS

Level : Hard--

Flag: TamilCTF{this_is_SAFE?}

Author: Paul Jeremiah

Challenge	11 Solves	✕

Hack Me Da rox

597

Make sure you know the challenge format and it helps you.
Key length is 9

Author - 0xCyberPJ

link download

Flag	Submit

Description: Make sure to know the flag format of "Tamilctf" !

GIVEN:

hackmeda_rox.png

```
┌──(root💀kali)-[/tmp/hackme]
└─# ls &&  file hackme_rox.png
hackme_rox.png
hackme_rox.png: data
```

WALKTHROUGH

$file says, data!
Lets start with some basic things.

```
$ strings hackme_rox.png
wY*`
m}^{
B? C
u.ub
VuV8
n]Ex
s`UB
```

AS DESCRIPTION SAYS WE NEED TO CONCENTRATE ON FLAG FORMATS..

> Lets say
>
> - TamilCTF{
> - TamilCTF
> - TamilCTF{}
> - TamilCTF}
>   **So now we have some keys or password or something .**

You can also brute force

Rox is nothing but Xor!

// So what is the Key to decrypt?

They said Key length is 9

TamilCTF{ = 9

// YOU CAN USE CYBER CHEF AND XOR BRUTEFORCE OPTION AND TRY THESE KEYS TO GET ANY USEFUL PNG

→Here im going to use pwntools

```
pip3 install pwntools
```

```
>>> from pwn import xor
>>> png=open("hackme_rox.png","rb").read()
>>> new=open("new_image.png","wb").write(xor("TamilCTF{",png))
```

New image created successfully

```
┌──(kali㉿kali)-[/tmp/hackme]
└─$ ⚡ file new_image.png
new_image.png: PNG image data, 3840 x 2160, 8-bit/color RGB, non-interlaced
```

Final Hint : " 🐌 in stegano"

About 1,89,000 results (0.91 seconds)

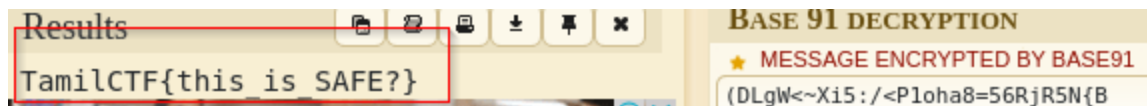https://pypi.org › project › stegano   ⋮

stegano - PyPI

Stegano, a pure **Python Steganography** module. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the ...

> Stegano, a pure Python Steganography module.

```
>>> from stegano import lsbset
>>> from stegano.lsbset import generators
>>> lsbset.reveal("new_image.png",generators.eratosthenes())
'(DLgW<~Xi5:/<Ploha8=56RjR5N{B'
```

hint is given for this (91)

base91 : Lets decode

Results   🖹 🖥 🖨 ± 📌 ✕   **BASE 91 DECRYPTION**

★ MESSAGE ENCRYPTED BY BASE91

TamilCTF{this_is_SAFE?}   (DLgW<~Xi5:/<Ploha8=56RjR5N{B

Flag: TamilCTF{this_is_SAFE?}

___

2. → // With Cyber chef!

After downloading
with zsteg

(These are basic kinds of stuff you should do with a png)

```
┌──(kali㉿kali)-[/tmp/mozilla_kali0]
└─$ ⚡file downloaded                                                    130 ✗
downloaded: PNG image data, 3840 x 2160, 8-bit/color RGB, non-interlaced


┌──(kali㉿kali)-[/tmp/mozilla_kali0]
└─$ ⚡zsteg -a downloaded
imagedata          .. text: "\n\n\n\t\t\t\n\n"
b1,r,lsb,xy        .. text: "PUEUETPUUTAUWGVss7www7"
b1,r,msb,xy        .. text: "wWWWUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU"
b1,g,lsb,xy        .. text: "QQWswv;~"
b1,g,msb,xy        .. text: "U_uUWU]]W]"
b1,b,lsb,xy        .. text: "UUUUUUWw"
es]
b1,r,lsb,xy,prime  .. text: "7zKR:Ores"
blah blahhh

b1,rgb,lsb,xy,prime .. text: "29:(DLgW<~Xi5:/<P1oha8=56RjR5N{B-$"
```
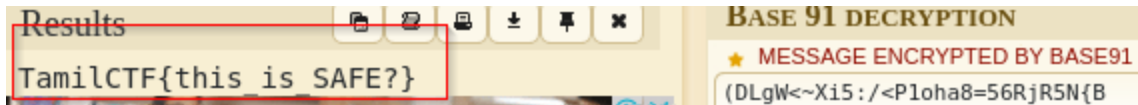
```
b2,r,lsb,xy,prime    .. text: "U@EUUUUUUUUUUUUUUUUUUUUYi"
b2,r,msb,xy,prime    .. text: "ifiUeYVUV"
b2,g,lsb,xy,prime    .. text: "DUUUUUUV"
```
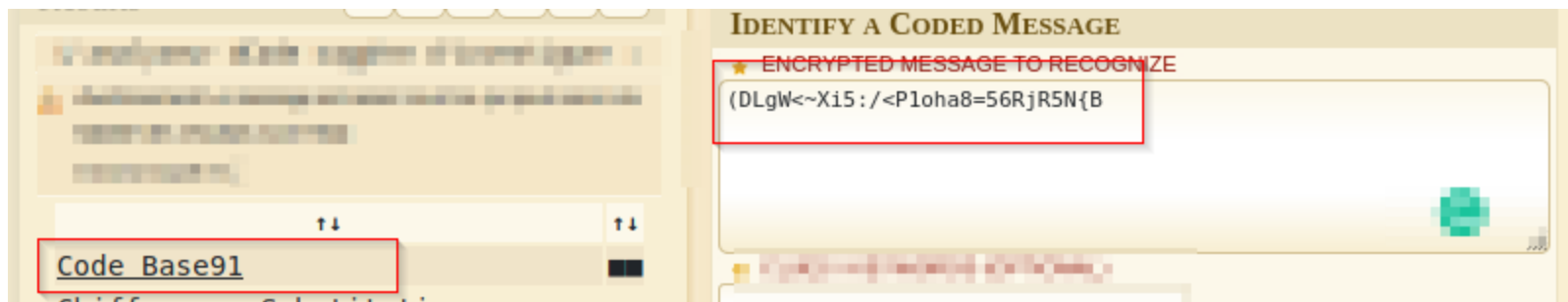
Here too, we got this :

```
(DLgW<~Xi5:/<Ploha8=56RjR5N{B
```
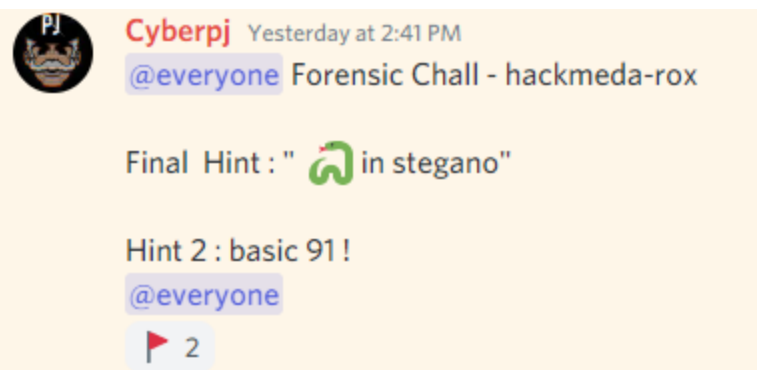
- decode it and get the flag

Thats all

(DLgW<~Xi5:/<Ploha8=56RjR5N{B

Hits Given :

python stegano
and base91 from lsb

THANK YOU - @cyberpj