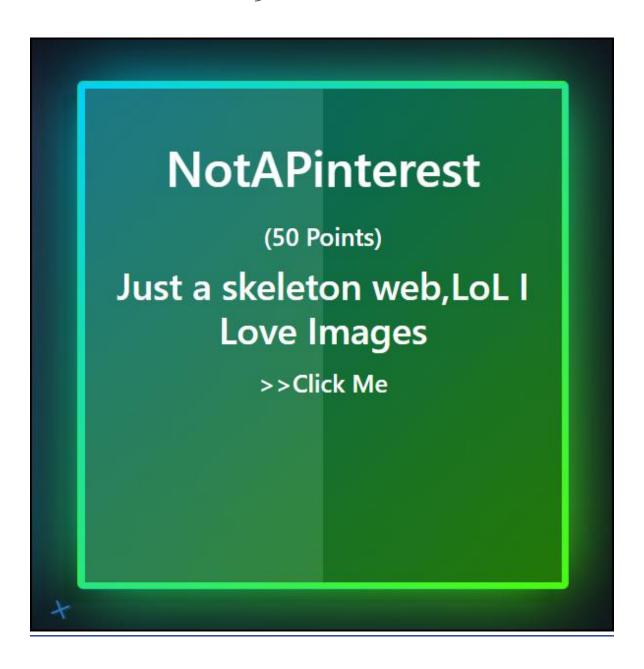
CTF Walkthrough

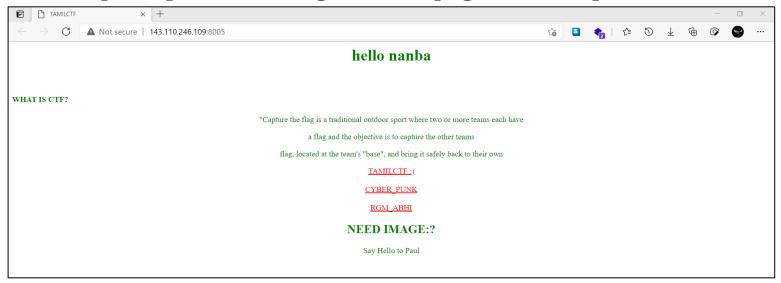
WEB Challenge

NotAPinterest

50 Points



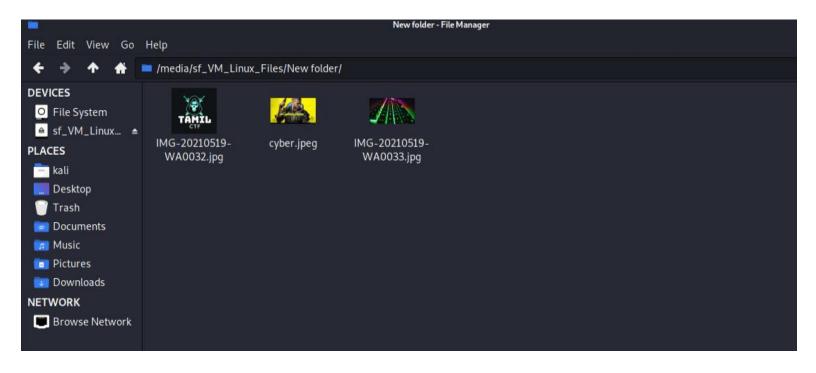
First open up the challenge. A web page will be opened.



Let's have a look at the source code.

```
TAMILCTF
                                        □ view-source:143.110.246.109:800 ×
                     ▲ Not secure | view-source:143.110.246.109:8005
Line wrap 🗌
    <html>
    <head><title>TAMILCTF</title></head>
    <center><h1>hello nanba</h1></center>
    <body>
  5 <br>
    <h4> WHAT IS CTF? </h4>
    <center> "Capture the flag is a traditional outdoor sport where two or more teams each have
    a flag and the objective is to capture the other teams
     flag, located at the team's "base", and bring it safely back to their own 
    <a href="https://mega.nz/file/ThgHhKSb#EsLACyQoRaKrstZabgHs-5kcILOnawc_3tzay0WyP60" class="name">TAMILCTF :)</a>
    (br)
 15
    <br>
    <style>
    .name{
        color:red;}
    <a href="https://mega.nz/file/21hlFAAQ#htnROQopo6zUjFQv4WtMNuuiJIL-DUJSrH3VEqcxstM" class="name">CYBER_PUNK</a>
    (br)
    <br>
    <a href="https://mega.nz/file/bwgRAABa#W5Dopn7UnU_BHQbjfCM0mXVu7b17jbG9IpLgWof_sik" class="name">RGM_ABHI</a>
    <br>
    <h2> NEED IMAGE: ?</h2>
    </body>
    </html>
   Say Hello to Paul
```

Nothing here. We can see just the link to the images. So, download the 3 images.



Just use **exiftool** to view the metadata of the image. In metadata of the "**cyber.jpeg**" image I found a base64 encoded text in a comment.

```
(kali⊗ kali) - [/media/sf_VM_Linux_Files/New folder]
 -$ exiftool cyber.jpeg
ExifTool Version Number
                                 : 12.16
File Name
                                   cyber.jpeg
Directory
File Size
                                   11 KiB
File Modification Date/Time
                                   2021:05:22 10:12:14-04:00
File Access Date/Time
                                   2021:05:24 12:58:40-04:00
File Inode Change Date/Time
                                   2021:05:22 10:12:59-04:00
File Permissions
                                   rwxrwxrwx
File Type
                                   JPEG
File Type Extension
                                   jpg
MIME Type
                                   image/jpeg
JFIF Version
                                   1.01
Resolution Unit
                                   None
X Resolution
Y Resolution
                                 : L2FzZGYvY3liZXJfZXJhL2RHRnRhV3hqZEdZSy9mbGFnLnR4dAo=
Comment
Image Width
Image Height
                                   170
                                   Baseline DCT, Huffman coding
Encoding Process
Bits Per Sample
Color Components
Y Cb Cr Sub Sampling
                                   YCbCr4:2:0 (2 2)
Image Size
                                   297×170
                                   0.050
Megapixels
```

Let's decode it.

(kali% kali) - [/media/sf_VM_Linux_Files/New folder]
\$ echo "L2FzZGYvY3liZXJfZXJhL2RHRnRhV3hqZEdZSy9mbGFnLnR4dAo=" |base64 -d/asdf/cyber_era/dGFtaWxjdGYK/flag.txt

It shows the path to the Flag. Let's open it up in the browser.



THE END