CTF

|  |  |  |
| --- | --- | --- |
| Tomas |  | Hernandez Trillo |

## Image, Audio, Video

1. **Open image** -> content may be the flag
2. **file img.jpg** -> check if it’s a image
3. **strings img.jpg** -> check if there are hidden strings
4. **exiftool img.jpg** -> check the metadata
   1. **Identify –verbose img.jpg** -> another way
5. **hexedit** -> check the hex code looking for hidden strings
6. **binwalk img.jpg** -> check for hidden files/foulders inside the img
   1. **-e** to extract the content

## File

1. **cat file** -> try reading it
2. **strings file** -> find strings
   1. If there’s ‘IHDR’ at the start, the file it’s an image
3. **chmod +x file** ->file becomes executable
4. **./file** -> execute file

## Zip File

1. **unzip file.zip -****d .** -> unzip in current directory

## Site/Link

1. **Click** -> take a look at the site
2. **Inspect**-> check all the HTML, CSS and JS code
3. **wget link** -> download site content
4. **Cookie editor** -> check cookies and try changing the values
5. **Change URL ending** -> ex: Robots.txt to find non-indexed files
6. **--header=’ ‘** -> change the header properties (wget --help)
   1. User-agent: user -> change user
   2. Referer -> visit from the same site
   3. Date -> view site in that date
   4. DNT: dnt -> don’t be tracked
   5. X-Forwarded-For: 255.255.255.255 -> change country IP
   6. Accept-language: it -> accept italian language

## Python

1. **python file.py** -> open file
2. **cat file.py** -> read file

## Server (GET e POST)

1. **cat file.html** -> check if methods exist other than GET and POST
2. **curl –I GET –i link.php** -> execute method

## SQL injections

1. **‘admin’ or 1=1--**

## Encodings

1. **ROT13**
2. **Base64 –** usually the string ends with ==
3. **G-Code** – G0Z0, G1X1... -> 3d printing code