Zippy - Writeup

Nice and easy, we start by unzipping the file we're given

```
┌──(kali㉿kali)-[~/Desktop]
└─$ unzip stuff.zip
Archive:  stuff.zip
  inflating: a file
  inflating: another file
```

Checking the files we have, we have one which tells us to remove important and another that is some kind of 7zip archive with "flag.rar" inside

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat a\ file
REMEMBER TO REMOVE BEFORE RELEASE, DATA HIDDEN IN FILE.

┌──(kali㉿kali)-[~/Desktop]
└─$ cat another\ file
♦I♦♦'F7♦3pj♦/♦7ⁿJ+♦
  ]s♦u♦♦♦♦♦*1♦^♦XN♦♦♦♦7♦♦H?}♦L<gg♦D♦♦SG♦♦♦r♦H♁♦♦♦F♦-Z♦e♦♦♦       ♦ä       kG♦♦T"+♦♦#♦\M♦e`♦♦`9♦DG♦♦♦       p
                                                                                                        $♦
S,♦♦♦2♦♦♦!!
           lh
d*♦/    flag.rar
2Z8x♦ ♦♦♦

┌──(kali㉿kali)-[~/Desktop]
└─$ file another\ file
another file: 7-zip archive data, version 0.4

┌──(kali㉿kali)-[~/Desktop]
└─$ stegsnow -C a\ file
TWVnYVNlY3VyaXR5MTIzISLCowo=
```

Similar to Stegosaurus, we use stegsnow to get some base64 encoded data which when we decode it, we get a password.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "TWVnYVNlY3VyaXR5MTIzISLCowo=" | base64 -d
MegaSecurity123!"£
```

Here comes our research, we have to try and figure out the file extension. We can make it quite easy and just rename it to .7z since we know its a 7 zip archive and it should work, but LZH is what it was originally compiled as.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ 7z e a.lzh

7-Zip 24.07 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-06-19
 64-bit locale=en_US.UTF-8 Threads:32 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 250 bytes (1 KiB)

Extracting archive: a.lzh
WARNING:
a.lzh
Cannot open the file as [Lzh] archive
The file is open as [7z] archive

--
Path = a.lzh
Open WARNING: Cannot open the file as [Lzh] archive
Type = 7z
Physical Size = 250
Headers Size = 138
Method = LZMA2:12 7zAES
Solid = -
Blocks = 1


Enter password (will not be echoed):
Everything is Ok

Archives with Warnings: 1
Size:       104
Compressed: 250
```

We put our password in and get flag.rar extracted, we could either then extract flag.rar or just cat the file and find our flag!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat flag.rar
◆7zXZ◆F!t/◆◆-HACKSOC_CTF{ec42b30dafe47a8bba906fe97324f76d}
◆◆◆L◆◆NF.gPsZ◆◆}YZ
```