1. Challenge Overview

There's a `secretdoor.zip` containing:

Item	Purpose
`secret.png`	Image that hides the flag
`secretbox.py`	Encoder script (our blueprint for decoding)
`__MACOSX/…`	Mac metadata; ignorable

Goal: extract the hidden message (flag) from `secret.png`.

2. Reverse-engineering `secretbox.py`

```
import sys
from PIL import Image

def prob(s_img, msg, d_img):
    im  = Image.open(s_img).convert("RGBA")
    p   = im.load()
    c   = 0
    msg = map(lambda x: ord(x) ^ len(d_img), msg[::-1])  # (1)
    for i in range(0, len(msg)):
        enc = msg[i]
        p[c, 0] = (p[c, 0][0], p[c, 0][1], p[c, 0][2], enc)  # (2)
        c += 1
    im.save(d_img)
```

Key observations

Line	Meaning
(1)	The plaintext message is **reversed**, then each byte is **XOR-ed** with `len(d_img)` (the length of the output file's name).
(2)	Encoded bytes are written into the **alpha channel** of consecutive pixels along the first row. Unused pixels keep alpha = 255 (fully opaque).

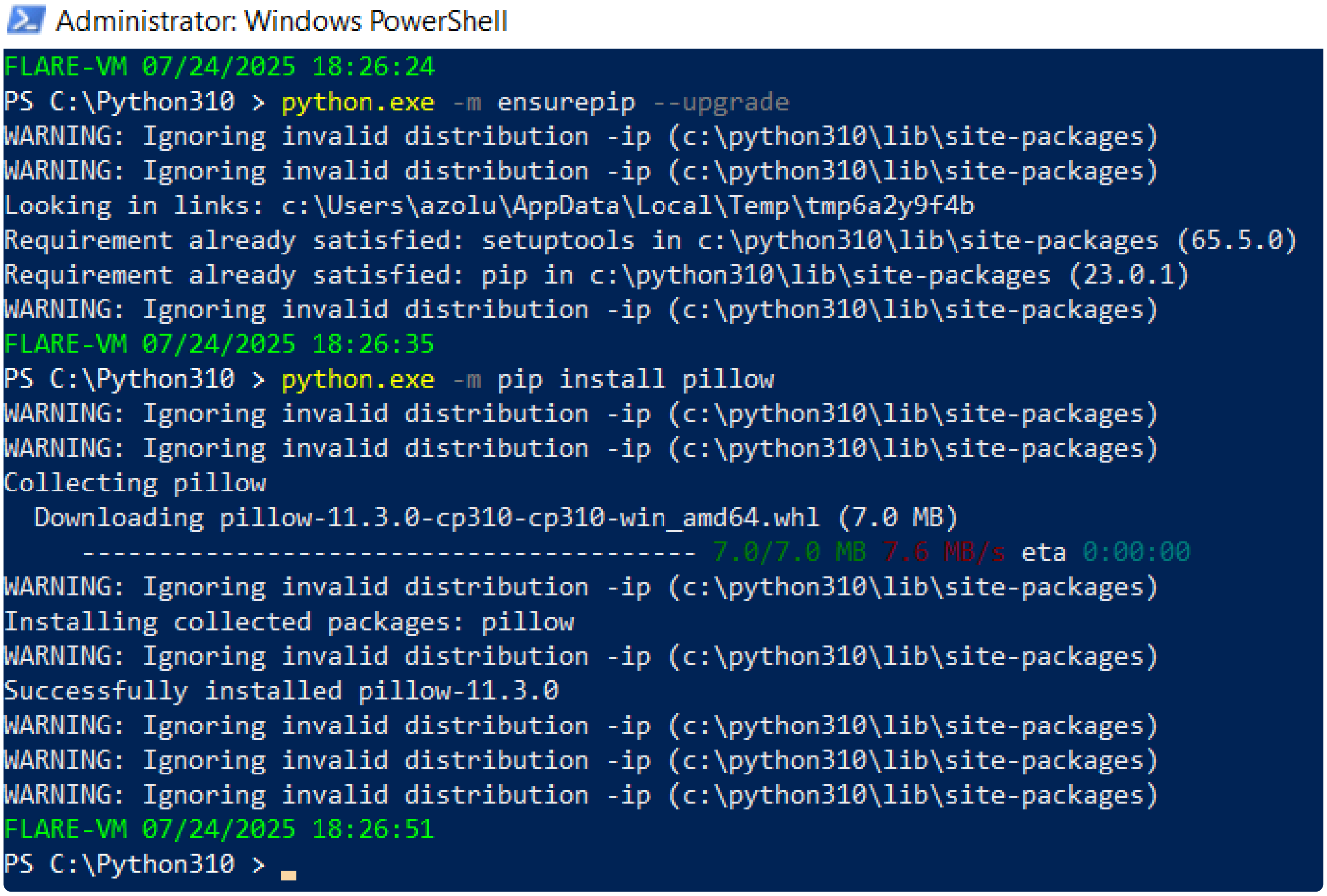
During the original run, the output file was `secret.png` (`len = 10`).
Therefore decoding requires:

1. Read α-values pixel-by-pixel until you hit `255` (terminator).
2. XOR each byte with **10**.
3. Reverse the resulting byte string.

3. Decoder Script (`decode.py`)

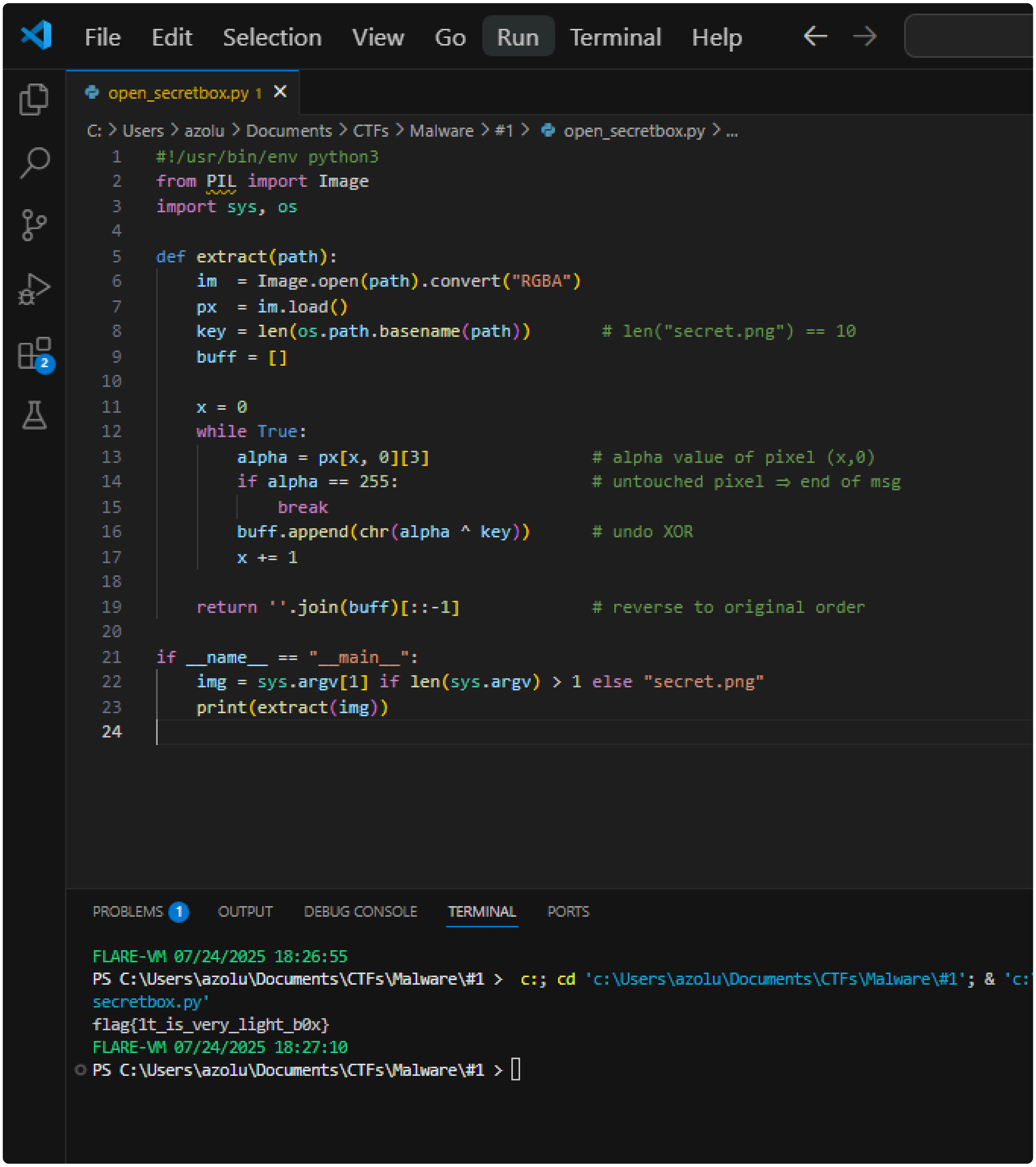
```
#!/usr/bin/env python3
from PIL import Image
import os, sys

def extract(path="secret.png"):
    im  = Image.open(path).convert("RGBA")
    px  = im.load()
    key = len(os.path.basename(path))          # 10
    buf = []

    x = 0
    while True:
        alpha = px[x, 0][3]                   # α of pixel (x,0)
        if alpha == 255:                      # marks end of payload
            break
        buf.append(chr(alpha ^ key))          # undo XOR
        x += 1

    return ''.join(buf)[::-1]                 # restore original order

if __name__ == "__main__":
    target = sys.argv[1] if len(sys.argv) > 1 else "secret.png"
    print(extract(target))
```

4. Install `pip` and `pillow`



Administrator: Windows PowerShell

```
FLARE-VM 07/24/2025 18:26:24
PS C:\Python310 > python.exe -m ensurepip --upgrade
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
Looking in links: c:\Users\azolu\AppData\Local\Temp\tmp6a2y9f4b
Requirement already satisfied: setuptools in c:\python310\lib\site-packages (65.5.0)
Requirement already satisfied: pip in c:\python310\lib\site-packages (23.0.1)
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
FLARE-VM 07/24/2025 18:26:35
PS C:\Python310 > python.exe -m pip install pillow
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
Collecting pillow
  Downloading pillow-11.3.0-cp310-cp310-win_amd64.whl (7.0 MB)
     ---------------------------------------- 7.0/7.0 MB 7.6 MB/s eta 0:00:00
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
Installing collected packages: pillow
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
Successfully installed pillow-11.3.0
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
WARNING: Ignoring invalid distribution -ip (c:\python310\lib\site-packages)
FLARE-VM 07/24/2025 18:26:51
PS C:\Python310 >
```



```python
#!/usr/bin/env python3
from PIL import Image
import sys, os

def extract(path):
    im  = Image.open(path).convert("RGBA")
    px  = im.load()
    key = len(os.path.basename(path))       # len("secret.png") == 10
    buff = []

    x = 0
    while True:
        alpha = px[x, 0][3]                # alpha value of pixel (x,0)
        if alpha == 255:                   # untouched pixel ⇒ end of msg
            break
        buff.append(chr(alpha ^ key))      # undo XOR
        x += 1

    return ''.join(buff)[::-1]             # reverse to original order

if __name__ == "__main__":
    img = sys.argv[1] if len(sys.argv) > 1 else "secret.png"
    print(extract(img))

```

```
FLARE-VM 07/24/2025 18:26:55
PS C:\Users\azolu\Documents\CTFs\Malware\#1 >  c:; cd 'c:\Users\azolu\Documents\CTFs\Malware\#1'; & 'c:
secretbox.py'
flag{1t_is_very_light_b0x}
FLARE-VM 07/24/2025 18:27:10
PS C:\Users\azolu\Documents\CTFs\Malware\#1 >
```

```
flag{1t_is_very_light_b0x}
```