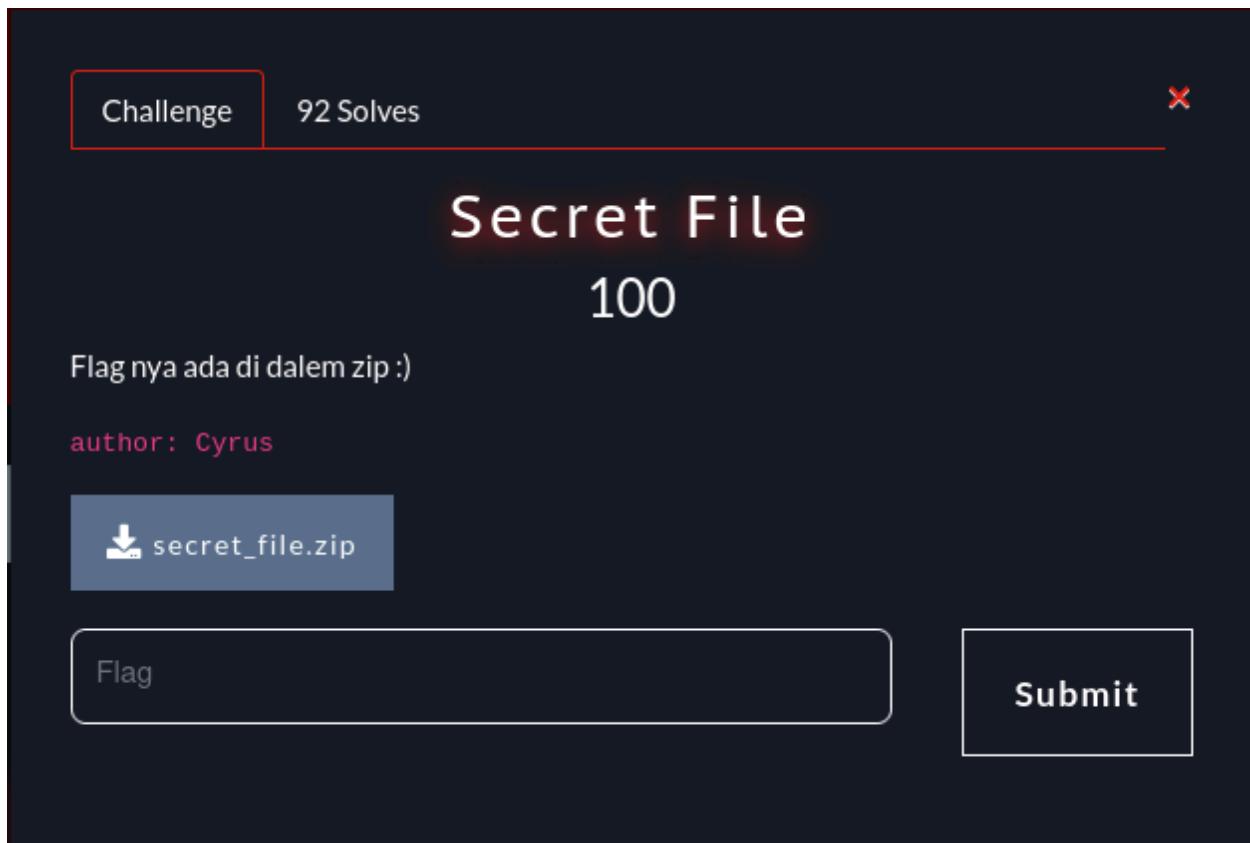


CTF Write-Up: Secretfile

Player: Constantine

Category: Forensics

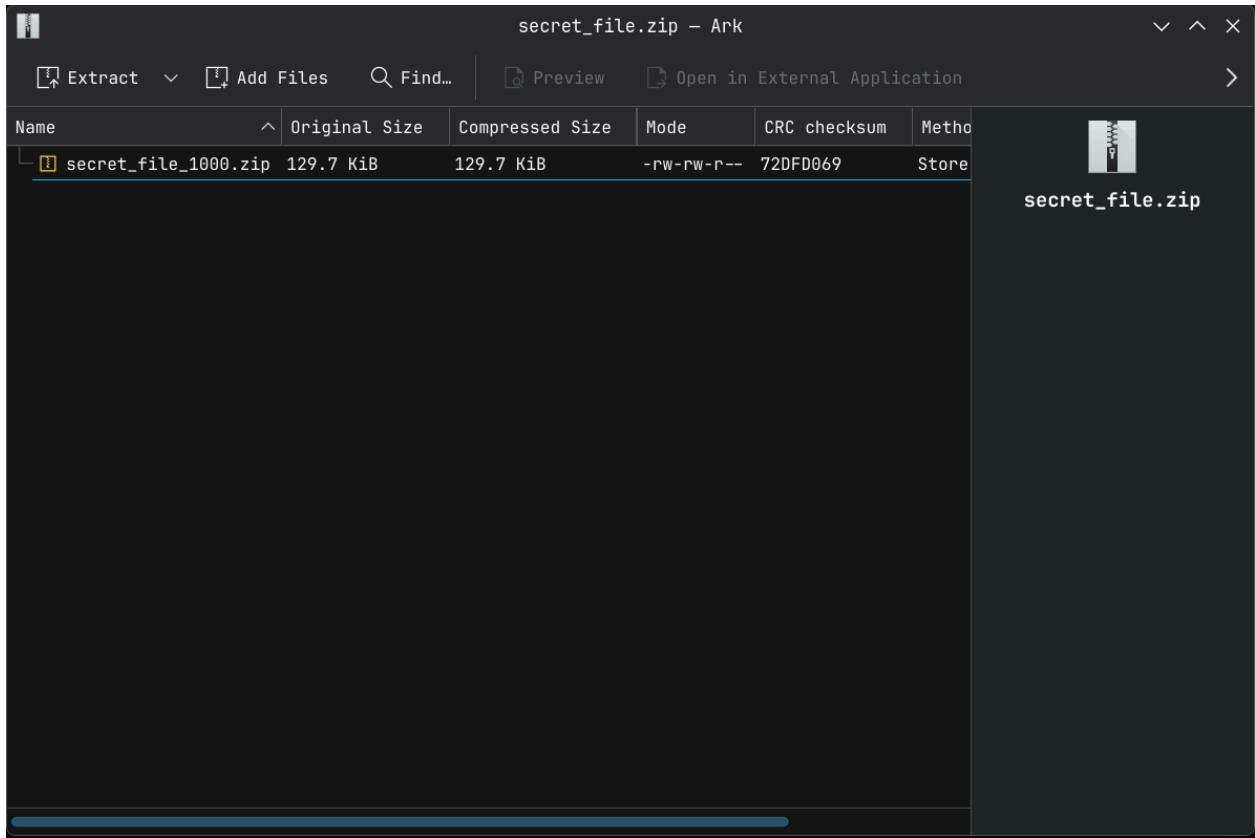


Konteks Dikit

Challengenya tipe klasik Matryoshka doll (boneka Rusia yang bisa tumpuk-tumpuk), di mana sebuah file .zip menyembunyikan file .zip lain di dalamnya secara rekursif. Melakukan ekstraksi manual itu buang buang waktu. Solusi yang aku pakai adalah otomatisasi menggunakan bash scripting untuk ngelakuin looping proses dekompresi sampai mencapai core file yakni flag kita nanti.

1. Initial Reconnaissance & Analysis

Langkah pertama adalah mengunduh artefak `secret_file.zip`. Aku buka menggunakan Ark untuk melihat struktur isinya.



Tampilan awal di Ark. Kelihatan indikasi nesting dengan penamaan file yang berurutan (1000).

Analisis awal menunjukkan pola yang jelas:

- secret_file.zip → berisi secret_file_1000.zip
- Kemungkinan besar secret_file_1000.zip → berisi secret_file_999.zip
- Pola ini akan berlanjut hingga 0 atau sampai file Flag ditemukan.

Melakukan klik kanan Extract sebanyak 1000 kali bukanlah opsi. Jadi kita pakai [Python](#)

2. Automation via Python

Alih-alih menggunakan native shell command yang aku sendiri lupa caranya, aku pakai [Python](#) aja. Saya minta Gemini untuk buat scriptnya dan ini hasil dari scriptnya:

```

39 import zipfile
38 import os
37 import glob
36
35 # Cari file zip pertama
34 initial_zips = glob.glob("*.zip")
33
32 if not initial_zips:
31 | print("Tidak ada file zip awal.")
30 | exit()
29
28 current_zip = initial_zips[0]
27
26 while True:
25 | print(f"Mengekstrak: {current_zip}")
24 | try:
23 | | with zipfile.ZipFile(current_zip, 'r') as zip_ref:
22 | | | zip_ref.extractall(".")
21 | | | extracted_files = zip_ref.namelist()
20 | |
19 | | # Hapus zip lama untuk kebersihan
18 | | os.remove(current_zip)
17 | |
16 | | # Cari zip berikutnya dari file yang baru diekstrak
15 | | next_zip = None
14 | | for f in extracted_files:
13 | | | if f.endswith('.zip'):
12 | | | | next_zip = f
11 | | | break
10 | |
9 | | if next_zip:
8 | | | current_zip = next_zip
7 | | else:
6 | | | print("Rantai zip berakhir. Cek file berikut:")
5 | | | print(extracted_files)
4 | | | break
3 | |
2 | | except zipfile.BadZipFile:
1 | | | print("File rusak atau bukan zip valid.")
40 | | break

```

Setelah script solver.py siap, aku execute lewat terminal di direktori yang sama dengan secret_file.zip.

```

Mengekstrak: secret_file_006.zip
Mengekstrak: secret_file_005.zip
Mengekstrak: secret_file_004.zip
Mengekstrak: secret_file_003.zip
Mengekstrak: secret_file_002.zip
Mengekstrak: secret_file_001.zip
Rantai zip berakhir. Cek file berikut:
['flag.txt']

```

A terminal window showing the execution of the solver.py script. The output shows the script extracting files from multiple zip files in sequence until it reaches the end of the chain, at which point it prints the contents of the final file, 'flag.txt'.

3. Flag Retrieval

File terakhir yang tersisa adalah flag.txt. Baca isinya cukup dengan perintah cat:

```
constantine ~/OprecForesty/secretfile (solved) v3.13.7 08:16 > cat flag.txt  
FORESTY{kamu_gak_solve_challenge_ini_dengan_manual_kan_???
```

Flagnya adalah **FORESTY{kamu_gak_solve_challenge_ini_dengan_manual_kan_???**