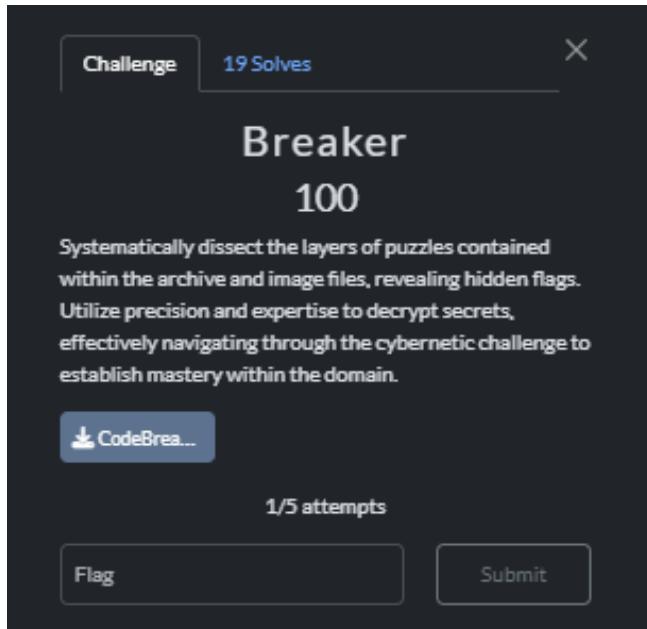




Challenge Name: Breaker (100 points) (Reversing)



We got a zip file called CodeBreakerX.zip. I grabbed it using wget:

```
(kali㉿kali)-[~/Desktop]
$ wget https://cybersecure-x.ctfd.io/files/dce13ea2f44939de04961fd4207957f5/CodeBreakerX.zip?token=eyJcI2vyX2lkIjoyMTIsInRlYw1faWQiojEwNSw1ZmlsZV9pZCI6Mj19.aEarqg.10BxnBaXpxPSWc9lGDIlvx8ih0 -O CodeBreaker.zip
--2025-06-09 05:59:02-- https://cybersecure-x.ctfd.io/files/dce13ea2f44939de04961fd4207957f5/CodeBreakerX.zip?token=eyJcI2vyX2lkIjoyMTIsInRlYw1faWQiojEwNSw1ZmlsZV9pZCI6Mj19.aEarqg.10BxnBaXpxPSWc9lGDIlvx8ih0
Resolving cybersecure-x.ctfd.io (cybersecure-x.ctfd.io)... 45.55.122.20, 138.197.58.222
Connecting to cybersecure-x.ctfd.io (cybersecure-x.ctfd.io)|45.55.122.20|:1443... connected.
HTTP request sent, awaiting response... 302 FOUND
Location: https://29832a894184429780dc1139b5658a4e.s3.amazonaws.com/dce13ea2f44939de04961fd4207957f5/CodeBreakerX.zip?token=eyJcI2vyX2lkIjoyMTIsInRlYw1faWQiojEwNSw1ZmlsZV9pZCI6Mj19.aEarqg.10BxnBaXpxPSWc9lGDIlvx8ih0
Certificates:94184d85d077de819c9120ebfbcc862798ecbc7bf1e772f143157e27278c [following]
--2025-06-09 05:59:03-- https://29832a894184429789dc1139b5658a4e.s3.amazonaws.com/dce13ea2f44939de04961fd4207957f5/CodeBreakerX.zip?token=eyJcI2vyX2lkIjoyMTIsInRlYw1faWQiojEwNSw1ZmlsZV9pZCI6Mj19.aEarqg.10BxnBaXpxPSWc9lGDIlvx8ih0
Resolving 29832a894184429789dc1139b5658a4e.s3.amazonaws.com (29832a894184429789dc1139b5658a4e.s3.amazonaws.com)... 3.5.28.21, 3.5.25.28, 16.182.99.9, ...
Connecting to 29832a894184429789dc1139b5658a4e.s3.amazonaws.com (29832a894184429789dc1139b5658a4e.s3.amazonaws.com)|3.5.28.21|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4387363 (4.2M) [binary/octet-stream]
Saving to: 'CodeBreaker.zip'

CodeBreaker.zip                                     [ <=> ] 4.18M 81.0KB/s   in 89s

2025-06-09 06:00:33 (48.4 KB/s) - 'CodeBreaker.zip' saved [4387363/4387363]
```

Unzipped it:

```
(kali㉿kali)-[~/Desktop]
$ unzip CodeBreaker.zip
Archive:  CodeBreaker.zip
  creating: Mis5/
  inflating: Mis5/AndroidBackup.ab

(kali㉿kali)-[~/Desktop]
$
```

Inside it had a directory and in that had one file:

```
(kali㉿kali)-[~/Desktop]
$ cd Mis5
$ ls
AndroidBackup.ab

(kali㉿kali)-[~/Desktop/Mis5]$
```

Let's checked it:

```
(kali㉿kali)-[~/Desktop/Mis5]
└─$ file AndroidBackup.ab
AndroidBackup.ab: Android Backup, version 1, Compressed, Not-Encrypted
(kali㉿kali)-[~/Desktop/Mis5] break...
```

It said it's an Android backup (not encrypted, compressed). I converted it to .tar like usual:

```
(kali㉿kali)-[~/Desktop/Mis5]
└─$ dd if=AndroidBackup.ab bs=1 skip=24 | openssl zlib -d > backup.tar
4386473+0 records in
4386473+0 records out
4386473 bytes (4.4 MB, 4.2 MiB) copied, 9.02552 s, 486 kB/s
(kali㉿kali)-[~/Desktop/Mis5]
└─$ ls
AndroidBackup.ab  backup.tar
(kali㉿kali)-[~/Desktop/Mis5] break...
```

Tried extracting it:

```
(kali㉿kali)-[~/Desktop/Mis5]
└─$ tar -xvf backup.tar
tar: This does not look like a tar archive
tar: Skipping to next header
tar: Exiting with failure status due to previous errors
(kali㉿kali)-[~/Desktop/Mis5] break...
```

Boom. Error.

Checked file type again:

```
(kali㉿kali)-[~/Desktop/Mis5]
└─$ file backup.tar
backup.tar: RAR archive data, v5
```

Turns out it's a **RAR archive** (not tar at all 🤦):

```
(kali㉿kali)-[~/Desktop/Mis5]
$ unrar x backup.tar

UNRAR 7.10 freeware      Copyright (c) 1993-2025 Alexander Roshal
File System    breaker    banner.php... GhostPay

Extracting from backup.tar

Creating  AndroidBackup                               OK
Creating  AndroidBackup/shared                           OK
Creating  AndroidBackup/shared/0                         OK
Creating  AndroidBackup/shared/0/Pictures               OK
Extracting  AndroidBackup/shared/0/Pictures/IMAG0002.jpg   OK
Extracting  AndroidBackup/shared/0/Pictures/IMAG0003.jpg   OK
Extracting  AndroidBackup/shared/0/Pictures/IMG_20231118_231022676.jpg   OK
Extracting  AndroidBackup/shared/0/Pictures/IMAG0001.jpg   OK
Extracting  AndroidBackup/shared/0/Pictures/IMAG0006.jpg   OK
Extracting  AndroidBackup/shared/0/Pictures/IMAG0005.jpg   OK
Creating  AndroidBackup/apps                            OK
Creating  AndroidBackup/apps/com.android.wallpaperbackup  OK
Creating  AndroidBackup/apps/com.android.wallpaperbackup/f  OK
Extracting  AndroidBackup/apps/com.android.wallpaperbackup/f/empty  OK
Extracting  AndroidBackup/apps/com.android.wallpaperbackup/f/wallpaper-info-stage  OK
Extracting  AndroidBackup/apps/com.android.wallpaperbackup/_manifest  OK
Creating  AndroidBackup/apps/com.android.proxyhandler    OK
Extracting  AndroidBackup/apps/com.android.proxyhandler/_manifest  OK
Creating  AndroidBackup/apps/com.android.settings.intelligence  OK
Creating  AndroidBackup/apps/com.android.settings.intelligence/sp  OK
Extracting  AndroidBackup/apps/com.android.settings.intelligence/sp/SuggestionEventStore.xml  OK
Extracting  AndroidBackup/apps/com.android.settings.intelligence/sp/suggestions.xml  OK
Extracting  AndroidBackup/apps/com.android.settings.intelligence/_manifest  OK
Creating  AndroidBackup/apps/com.android.providers.partnerbookmarks  OK
Extracting  AndroidBackup/apps/com.android.providers.partnerbookmarks/_manifest  OK
Creating  AndroidBackup/apps/com.android.dialer           OK
Creating  AndroidBackup/apps/com.android.dialer/sp        OK
Extracting  AndroidBackup/apps/com.android.dialer/sp/com.android.dialer_preferences.xml  OK
Extracting  AndroidBackup/apps/com.android.dialer/_manifest  OK
Creating  AndroidBackup/apps/com.android.wallpaper.livepicker  OK
Extracting  AndroidBackup/apps/com.android.wallpaper.livepicker/_manifest  OK
Creating  AndroidBackup/apps/com.android.gallery3d        OK
Creating  AndroidBackup/apps/com.android.gallery3d/sp      OK
Extracting  AndroidBackup/apps/com.android.gallery3d/sp/com.android.gallery3d_preferences.xml  OK
Extracting  AndroidBackup/apps/com.android.gallery3d/_manifest  OK
Creating  AndroidBackup/apps/com.android.cts.priv.ctsshim  OK
Extracting  AndroidBackup/apps/com.android.cts.priv.ctsshim/_manifest  OK
Creating  AndroidBackup/apps/com.android.traceur         OK
Extracting  AndroidBackup/apps/com.android.traceur/_manifest  OK
```

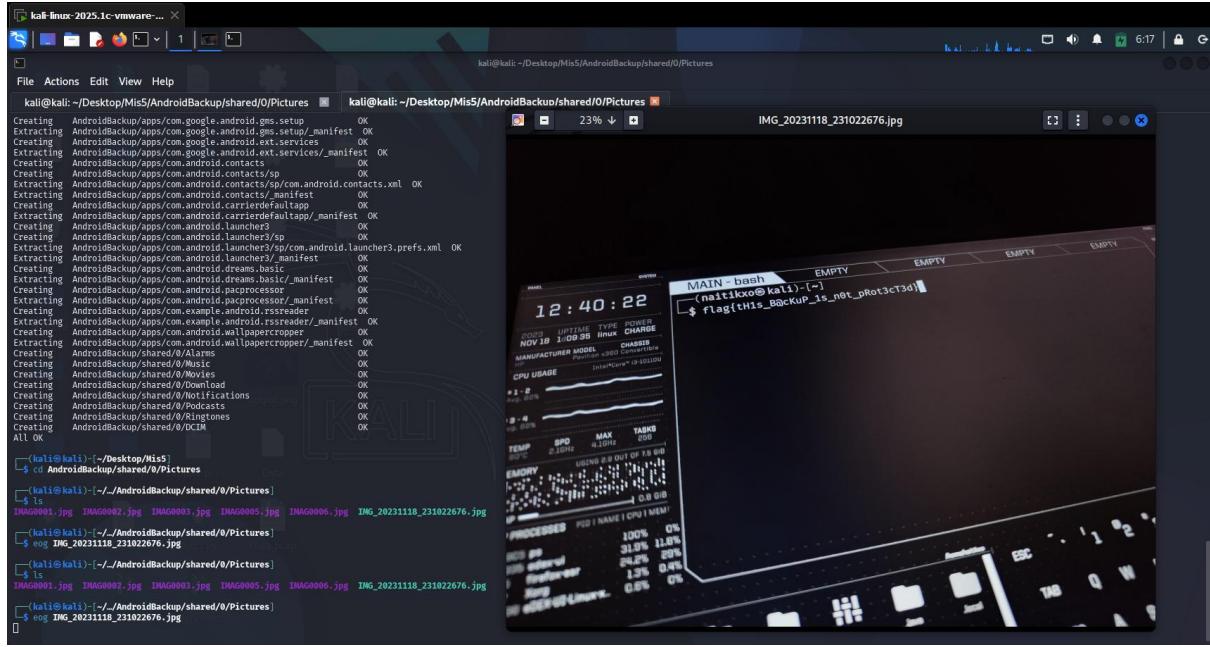
It extracted everything into a folder called **AndroidBackup**. Went in:

```
(kali㉿kali)-[~/Desktop/Mis5]
$ cd AndroidBackup/shared/0/Pictures

(kali㉿kali)-[~/.../AndroidBackup/shared/0/Pictures]
$ ls
IMAG0001.jpg  IMAG0002.jpg  IMAG0003.jpg  IMAG0005.jpg  IMAG0006.jpg  IMG_20231118_231022676.jpg

(kali㉿kali)-[~/.../AndroidBackup/shared/0/Pictures]
$
```

There were a bunch of .jpg images. I just started opening them with **eog**:



✓ The flag was **inside that image**, just written there.

FLAG: flag{tH1s_B@cKuP_1s_n0t_pRoT3cT3d}

~By Team justahacker