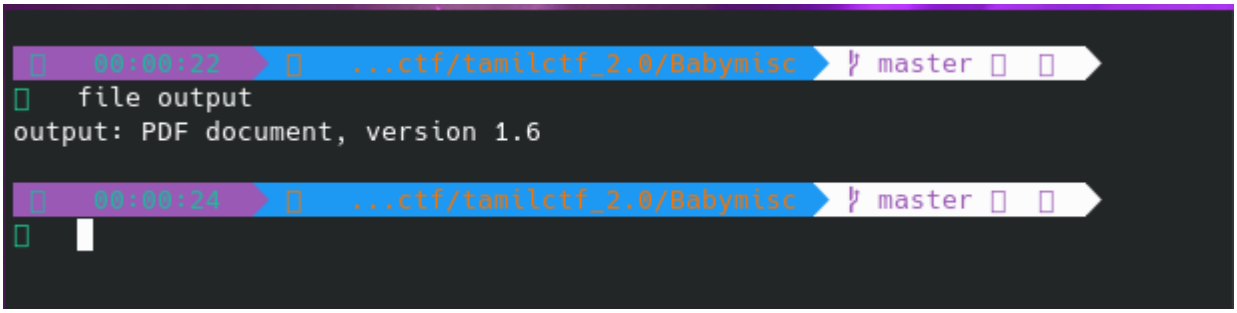
BabyMisc

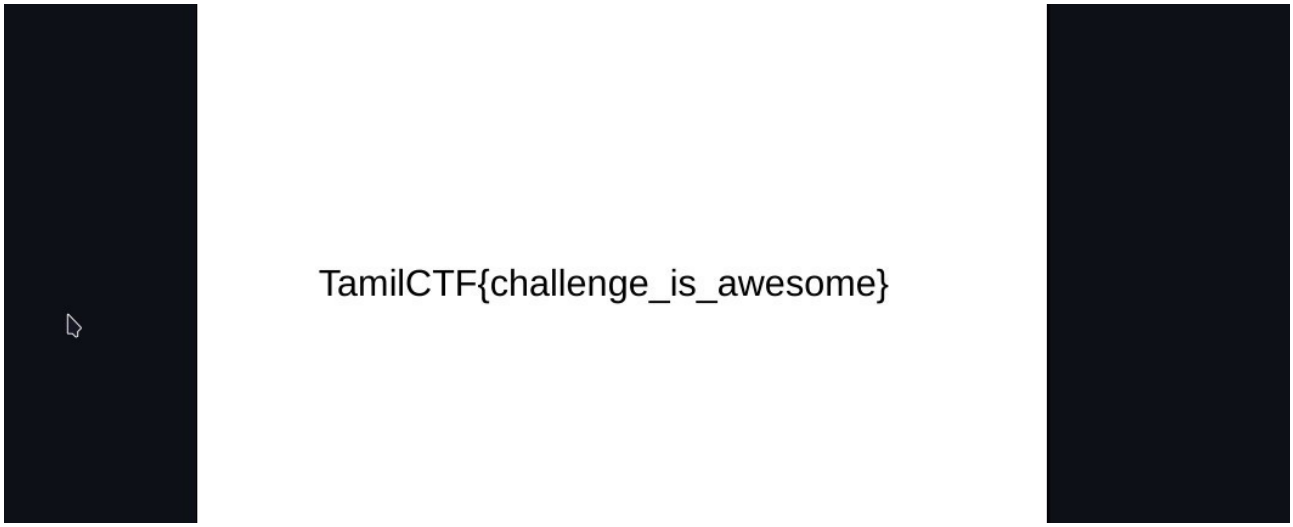
Description : See the file structure.
Author : 0xRakesh Kumar.

Given:

There are only one file . ***BabyMisc*** . It has no extension, so find the file type with file command .



It is **PDF** document file, open in any document viewer.



It has the flag. First time, I think was the flag. But it was the ***fake flag***. :(
Lets investigate the file.

Open in HexViewer:

I am using **GHEX** . Open the file in GHEX Editor.

```
00000000  25 50 44 46 2D 31 2E 36 0A 25 E2 E3 CF D3 0A 31 20 30 20 6F 62 6A 0A 3C 3C 0A 2F 46 69 6C 74  %PDF-1.6.%.....1 0 obj.<<./Filt
0000001F  65 72 20 2F 46 6C 61 74 65 44 65 63 6F 64 65 0A 2F 4C 65 6E 67 74 68 20 31 31 36 38 0A 3E 3E  er /FlateDecode./Length 1168.>>
0000003E  0A 73 74 72 65 61 6D 0A 50 4B 03 04 0A 00 00 00 00 00 23 BF 19 53 A8 22 58 9C 21 00 00 00 21  .stream.PK........#..S."X.!...!
0000005D  00 00 00 0A 00 1C 00 31 30 2E 70 64 66 2E 74 78 74 55 54 09 00 03 7A 8B 26 61 CD 8A 26 61 75  .......10.pdf.txtUT...z.&a..&au
0000007C  78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 61 72 65 20 73 6F 6C 76 65 20 72 65 6D 61 69 6E 20  x.............are solve remain
0000009B  6D 69 73 63 20 63 68 61 6C 6C 65 6E 67 65 73 0A 50 4B 03 04 0A 00 00 00 00 00 29 BF 19 53 E3  misc challenges.PK........)..S.
000000BA  35 B8 A3 14 00 00 00 14 00 00 00 0A 00 1C 00 31 31 2E 70 64 66 2E 74 78 74 55 54 09 00 03 85  5.............11.pdf.txtUT....
000000D9  8B 26 61 DD 8A 26 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 61 72 65 20 69 6E 74 65 72  .&a..&aux.............are inter
000000F8  65 73 74 20 69 6E 20 70 77 6E 0A 50 4B 03 04 0A 00 00 00 00 00 34 BF 19 53 49 22 CC DB 23 00  est in pwn.PK........4..SI"..#.
00000117  00 00 23 00 00 00 0A 00 1C 00 31 32 2E 70 64 66 2E 74 78 74 55 54 09 00 03 9C 8B 26 61 E1 8A  ..#.......12.pdf.txtUT.....&a..
00000136  26 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 6F 75 72 20 74 65 61 6D 20 6D 61 74 65 73  &aux.............our team mates
00000155  20 61 72 65 20 61 77 65 73 6F 6D 65 20 70 65 6F 70 6C 65 73 0A 50 4B 03 04 0A 00 00 00 00 00  are awesome peoples.PK........
00000174  51 BE 19 53 78 BC 67 A5 09 00 00 00 09 00 00 00 0A 00 1C 00 31 33 2E 70 64 66 2E 74 78 74 55  Q..Sx.g.............13.pdf.txtU
00000193  54 09 00 03 F1 89 26 61 F1 89 26 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 54 54 46 7A  T.....&a..&aux.............TTFz
000001B2  51 33 30 4B 0A 50 4B 03 04 0A 00 00 00 00 00 26 BE 19 53 9A 47 A6 F7 0D 00 00 00 0D 00 00 00  Q30K.PK........&..S.G..........
000001D1  09 00 1C 00 31 2E 70 64 66 2E 74 78 74 55 54 09 00 03 9F 89 26 61 B6 87 26 61 75 78 0B 00 01  ....1.pdf.txtUT.....&a..&aux...
000001F0  04 E8 03 00 00 04 E8 03 00 00 56 47 46 74 61 57 78 44 56 45 59 4B 0A 50 4B 03 04 0A 00 00 00  ..........VGFtaWxDVEYK.PK......
0000020F  00 00 E9 BE 19 53 8C 2E 44 A9 0F 00 00 00 0F 00 00 00 09 00 1C 00 32 2E 70 64 66 2E 74 78 74  .....S..D.............2.pdf.txt
0000022E  55 54 09 00 03 0E 8B 26 61 8E 8A 26 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 68 65 6C  UT.....&a..&aux.............hel
0000024D  6C 6F 20 65 76 65 72 79 6F 6E 65 0A 50 4B 03 04 0A 00 00 00 00 00 F4 BE 19 53 96 EE 9B 2C 18  lo everyone.PK..........S.....
```

Did you notice that , the file has a two extension **PDF (PDF)** and **ZIP (.PK)** It is polyglots file. Lets unzip the file and look up the unzipped files.

```
 00:05:08    ...ctf/tamilctf_2.0/Babymisc  master
 unzip something.zip -d something
Archive:  something.zip
 extracting: something/10.pdf.txt
 extracting: something/11.pdf.txt
 extracting: something/12.pdf.txt
 extracting: something/13.pdf.txt
 extracting: something/1.pdf.txt
 extracting: something/2.pdf.txt
 extracting: something/3.pdf.txt
 extracting: something/4.pdf.txt
 extracting: something/5.pdf.txt
 extracting: something/6.pdf.txt
 extracting: something/7.pdf.txt
 extracting: something/8.pdf.txt
 extracting: something/9.pdf.txt

 00:05:11    ...ctf/tamilctf_2.0/Babymisc  master
```

It has **many text files** . Cat all the files.

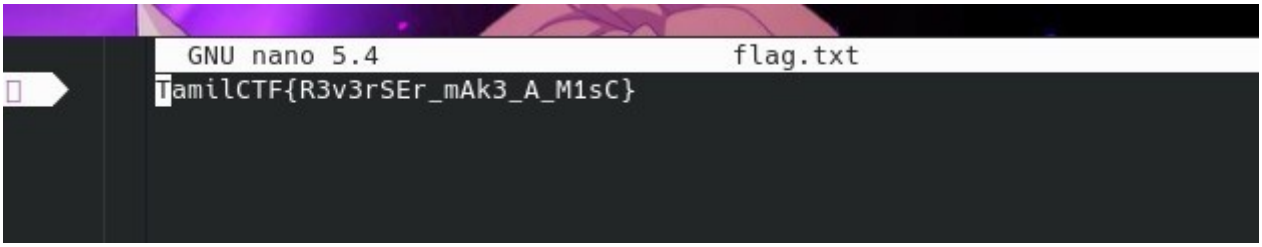
```
 00:05:52    ..tamilctf_2.0/Babymisc/something  master
 cat *
are solve remain misc challenges
are interest in pwn
our team mates are awesome peoples
TTFzQ30K
VGFtaWxDVEYK
hello everyone
are you join in discord
are follow us in twitter
e1IzdjNyU0VyCg==
did enjoy our ctf challenges

waste of time

are you solve reverse engineering challenge
X21BazNfQQo=

 00:05:53    ..tamilctf_2.0/Babymisc/something  master
```

It has some human readable strings and encoded strings. Quickly I find that some strings are encoded in ***Base64***. Decode it .



Yeah , The correct flag is
TamilCTF{R3v3rSEr_mAk3_AM1sC}