Writeup: IS THIS ASCII?

HACK THE PODS CTF 第2回

作問者 : 嶋田壮志

1. 説明文

FLAGを転送してもらったが通信線が破損していてデータがおかしくなってしまったんだ。

頼む、どうか正しいデータを取り出してくれないか！

P.S. 適当なデータをこの回線を使って受信してみた、解析の参考にしてくれ。

2. 共有されるファイル

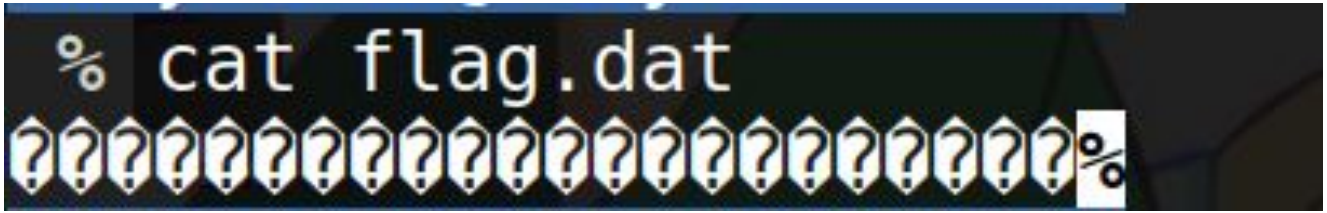
- flag.dat
  - 問題のファイル

テストデータ

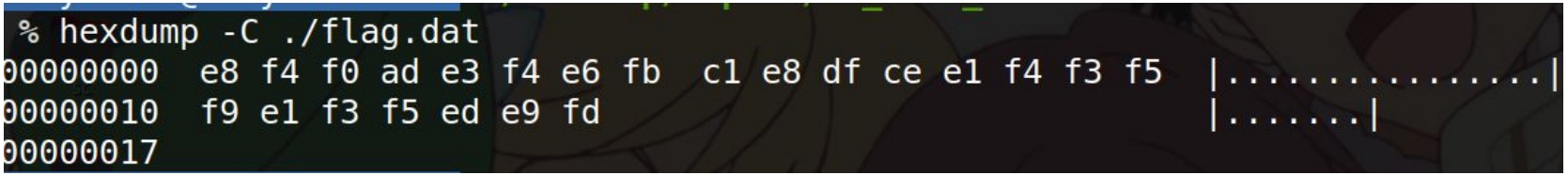
- test.row（これ、rawですね。。名前直そうとして忘れてました。。）
  - テストデータ（ソース）
- test.dat
  - テストデータ（エンコード後）

3. Writeup

まずはflag.datを見てみる（終端の%はプロンプトです。ゴメンね！）

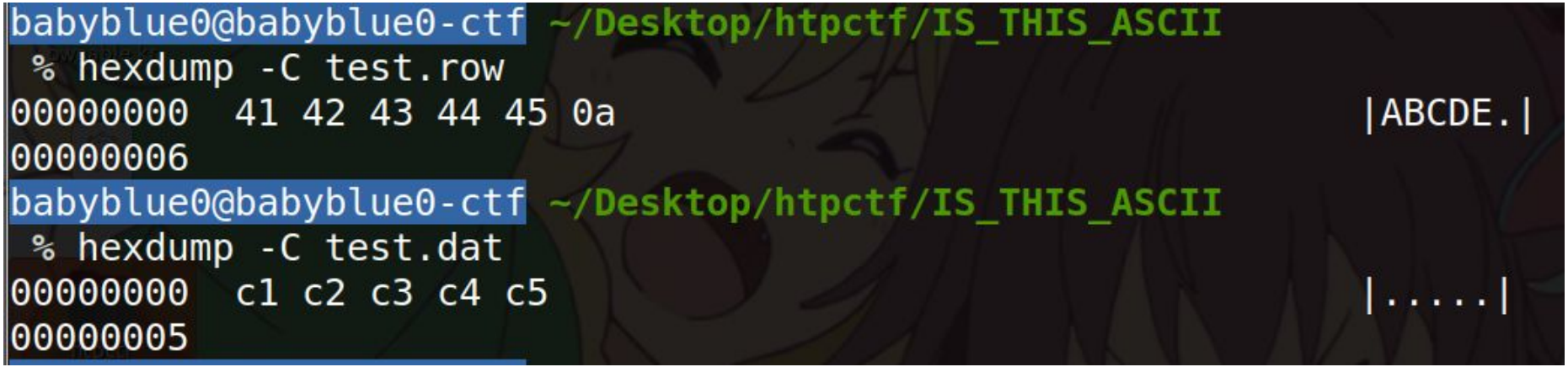


ASCIIではなさそうなので、hexdump（16進数で見てみる）



3. Writeup

テストデータのデコードに挑戦してみる
まずは16進で比較。



3. Writeup

どうやら規則性がありそう。
2進で比較してみる

41	42	43	44	45
0100 0001	0100 0010	0100 0011	0100 0100	0100 0101
c1	c2	c3	c4	c5
1100 0001	1100 0010	1100 0011	1100 0100	1100 0101

最上位ビットに1が立ってる！
本来、ASCIIは、0x00 ~ 0x7cの間でしか定義されてないため、
エンコードされたものを表示しようにもおかしな表示が出てしまう。。！

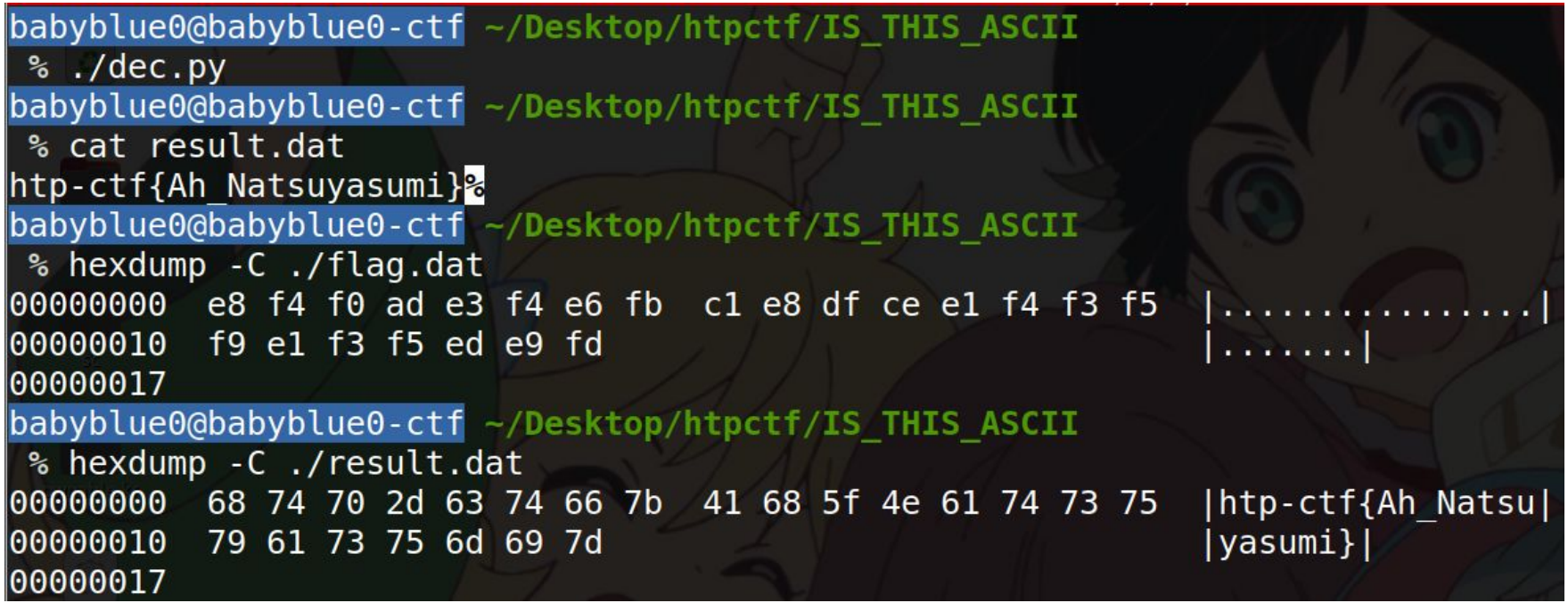
3. Writeup

ということで、flag.datの最上位ビットを削除するスクリプトを書いてみる

```
1   #!python3
  1 import sys
  2
  3 with open("./flag.dat", mode="rb" ) as f:
  4     row_flag = f.read()
  5
  6 with open( "./result.dat", mode="wb" ) as f:
  7     for c in row_flag:
  8         f.write( bytes([c^0x80]) )
~
```

3. Writeup

フンガー！（実行）



3. Writeup

flag: htp-ctf{Ah_Natsuyasumi}

flag元ネタ:
TUBE「あー夏休み」(https://youtu.be/aFrFLgz2lV4)

もうすぐ夏休みですね(他意はないです)