

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！)

```
% cat flag.dat
??????????????????????%
```

ASCIIではなさそうなので、hexdump(16進数で見てみる)

```
% hexdump -C ./flag.dat
00000000  e8 f4 f0 ad e3 f4 e6 fb  c1 e8 df ce e1 f4 f3 f5  |.....|
00000010  f9 e1 f3 f5 ed e9 fd      |.....|
00000017
```

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。

```
babyblue0@babyblue0-ctf ~/Desktop/htpctf/IS_THIS_ASCII
% hexdump -C test.row
00000000  41 42 43 44 45 0a                |ABCDE.|
00000006

babyblue0@babyblue0-ctf ~/Desktop/htpctf/IS_THIS_ASCII
% hexdump -C test.dat
00000000  c1 c2 c3 c4 c5                |.....|
00000005
```

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い表示が出てしまう。。！

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）

```
babyblue0@babyblue0-ctf ~/Desktop/httpctf/IS_THIS_ASCII
% ./dec.py
babyblue0@babyblue0-ctf ~/Desktop/httpctf/IS_THIS_ASCII
% cat result.dat
http-ctf{Ah_Natsuyasumi}%
babyblue0@babyblue0-ctf ~/Desktop/httpctf/IS_THIS_ASCII
% hexdump -C ./flag.dat
00000000 e8 f4 f0 ad e3 f4 e6 fb c1 e8 df ce e1 f4 f3 f5 |.....|
00000010 f9 e1 f3 f5 ed e9 fd |.....|
00000017
babyblue0@babyblue0-ctf ~/Desktop/httpctf/IS_THIS_ASCII
% hexdump -C ./result.dat
00000000 68 74 70 2d 63 74 66 7b 41 68 5f 4e 61 74 73 75 |http-ctf{Ah_Natsu|
00000010 79 61 73 75 6d 69 7d |yasumi}|
00000017
```


3. Writeup

flag: http-ctf{Ah_Natsuyasumi}

flag元ネタ:

TUBE「あー夏休み」(<https://youtu.be/aFrFLgz2IV4>)

もうすぐ夏休みですね(他意はないです)

