

Writeup: Pick up flag

HACK THE PODS CTF 第2回
作問者：嶋田壮志

1. 説明文

あ`あ`あ`あ`ああ、、、やっちまったああああ`あ`あ`あ`

フラグを記述したファイルの編集集中にキーボードが押されぱなしになってて、フラグの前後に余計な文字を入力してしまった

どうかフラグの文字列を探してはもらえないだろうか

2. 共有されるファイル

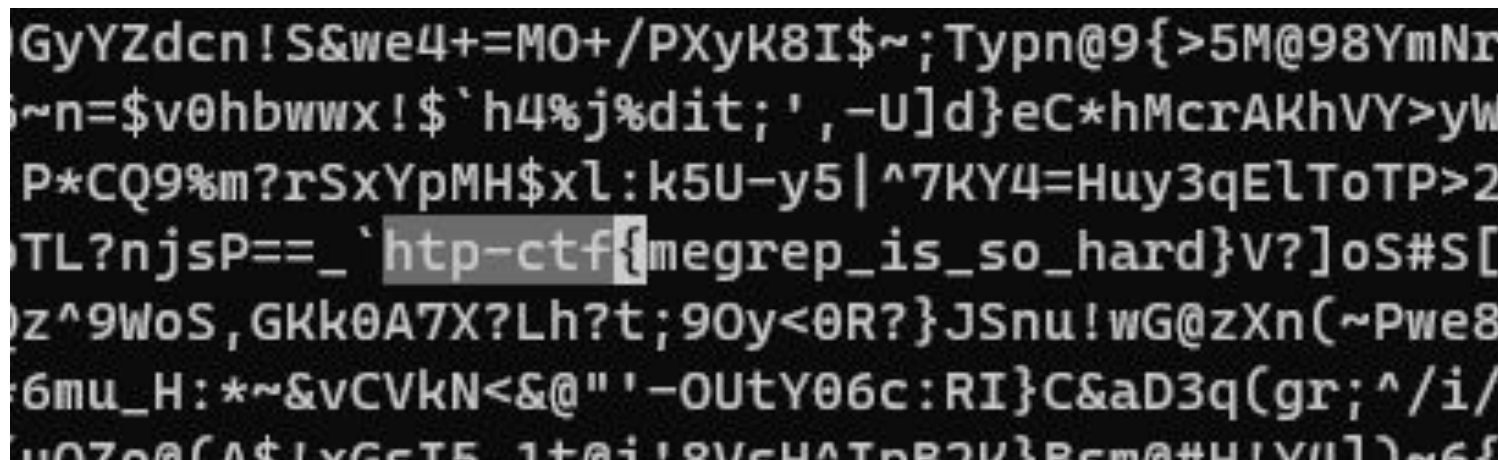
- data.dat
 - 問題のテキストファイル
 - すべてASCIIテキストで書かれている

[illegible]

3. Writeup

フラグ発見！

flag: `http-ctf{megrep_is_so_hard}`



```
GyYZdcn!S&we4+=MO+/PXyK8I$~;Typn@9{>5M@98YmNr  
~n=$v0hbwwwx!$`h4%j%dit;' , -U]d}eC*hMcrAKhVY>yw  
P*CQ9%m?rSxYpMH$x1:k5U-y5|^7KY4=Huy3qELToTP>2  
TL?njsP==_`http-ctf{megrep_is_so_hard}V?]oS#S[  
z^9WoS,GKk0A7X?Lh?t;90y<0R?}JSnu!wG@zXn(~Pwe8  
6mu_H:*~&vCVkN<&@"'-OUtY06c:RI}C&aD3q(gr;^/i/  
u07o0(A$1xG5T5_1t0j!8V6H^TpB?K}B5m0#H1YU1)~6f
```

4. おまけ

grepで文字検索してみると、

```
% cat data.dat | grep http-ctf
Y9C0.m|]l~YDVJ:U(XIW!31/cU>"Y`~P8)iw,S>y-s(+.NO73j#zJ,SMYS[U2G16M+42^07!:(:}'YqlE2H[,):g~U:/:
kwb:kCF6_UJ[14n#wR:I1HobJ!mtZ5|1'ueUu(PT%3~A@[1xW|M7JDE"! ]mSo$c3f`oUvoe[5>}VOJ/6Hxno]VpTBm<)<]
cMf=ytg]=E-Fygia|j'P&dF]Ti[z]JJ4p!en}e_uX%TG":$=g2YlKc^{:B@UZ^vyls9b8V2>aE%J|j[qIv@la@iIFUPb:
`%I]s>=$X?kDk^jZ0x&H)C{Mbyb@s?+_ :E:GstC*9yN4>bL2)jBbQ[r|X<Duto^pLQziB5rf}G%Z>88C*L-_XKyV/lzz&
KuF>Rcyv_joj35a-OwqzVS1!:dZK1T`MYL2&(Z0S67Ago_I'fe35GWYI_D!A9ScQt~LN|Z*%_x7q>^|gG|WT{K?_30Pha
%RP?5;OqQe%#: .q$#wwd8^|h9$tE8r`r`xowz*.p%dJ;(~'F7GF1%6Yhu{7~->~dn~"=Ht5ra};h&RSHRDDjCj|r(5!D
E6&]Rg[?=<{px/Rk<N6*A)aJDD`/P^"BPvy+qB-nzj]ieVnZ[(X&7ZMI)]ooU|wIZk(m:9Ee-Vcr`WoGn-(&.mRY2rG"-
&>Z7v3g,EUM?)58BSM^}$`xKK)[sHC`UDqVJ#$;<7ugLBddrg$U^b*oFvJvn!tBj<TK.=(9;&wR_<*nd70%Yh"PQMTui
JlGn5hh,vJM>`[q59v6loxw""k&I[k^ijFGP@V=bh79N;OW31NC~I"!m>)]Aq#?R;8NUe{AXt9_kk6F'm6+F`ESKk(~
~yfmlP^9EjOq+oPOXoO<.0;!%KRHLExmnf{ej`L`X^`VXe$Q3W9"c(yUEMjRifV`3nu@u)&BtFLC#Hh~kkC6BS%icbN5I
,i{Hr(Zh6}uh*'7I+[~7oib.sF*Z2m93l%(,nvN1:*[yky}8>Ltc(pLff&c.bc-O'kX9Mcfhd^=?dL{dsLm*4!9Q/P>L
4pthZ<p!qtV;w/)k[L:u5!RI>7D00muybQ^/us{2@?1LtCZF4p;w`YX|lN5aA0(Q1i[*c|!~X'i}ll:xaC~>26$,qtXC
```

全文字列が出力されてしまう

grepは検索にマッチした「**行**」を出力する

4. おまけ

正規表現で検索したい場合、
awkコマンドやsedコマンドを使えば良さそう
(私は普段使っていないので分かりません。)

他にも、「私はこの解法で解いたよ～」って人がいたら教えて下さい！

4. おまけ

ちなみに、flag文字列の**megrep**(= 目grep)とは、
コマンドやツールを使わずに、
人力で目的の文字列(今回はflag文字列)を見つけ出すことです。

またそこから発展してバイナリエディタで16進数を眺めて、
ファイルの種類を特定したりするらしい(意味わからん)

あー、みんなでバイナリかるたしたいなあ(願望)

