Home
Geek Lifestyle
Tutorial
Writeups
Blog
Video
People
Cafelabs
Downloads

Title : **[writeups] CSAW 2015 - Crypto 50 - whiter0se**
Released : 2015-09-25 17:29:24 -0400
Viewed : 1072

Hi halo there, this is my first article that didn't use my native language. So if the language is less precise, please be advised.

This challenge is about cryptography. When i open it, i got this task

> *Note: The flag is the entire thing decrypted*
>
> *eps1.7_wh1ter0se_2b007cf0ba9881d954e85eb475d0d5e4.m4v*

I download the decrypted file from the link, and i got this hash:

> EOY XF, AY VMU M UKFNY TOY YF UFWHYKAXZ EAZZHN. UFWHYKAXZ ZNMXPHN. UFWHYKAXZ EHMOYACOI. VH'JH EHHX CFTOUHP FX VKMY IFFQAXZ MY VKMY'U MEFJH OU.

i try to decrypt this hash using some rotation but certainly not as easy as it :p

So I tried to figure it manually

The method I use is to consider "if there is one letter alone, surely it is a word suffix as an "A", and we get our first character subsitution.

M UKFNY = A UKFNY

first try, all hash looks like this

> EOY XF, AY VAU A UKFNY TOY YF UFWHYKAXZ EAZZHN. UFWHYKAXZ ZNAXPHN. UFWHYKAXZ EHAOYACOI. VH'JH EHHX CFTOUHP FX VKAY'U
> IFFQAXZ AY VKAY'U AEFJH OU.

but still not readable :p

Second charater. Now let's look at the word "EHHX", it could be "LOOK" "SEEN" or "DEEP" . But, let's assume it's a vowel. And for the secon

> EOY XF, AY VAU A UKFNY TOY YF UFWEYKAXZ EAZZEN. UFWEYKAXZ ZNAXPEN. UFWEYKAXZ EEAOYACOI. VE'JE EEEX CFTOUEP FX VKAY'U AX
> IFFQAXZ AY VKAY'U AEFJE OU.

still not readable :)

Now, let's looking for this word "VE'JE" and i am absolutely sure this word are "WE'VE" :)

so, lets substitute V to W, and J to V

> EOY XF, AY WAU A UKFNY TOY YF UFWEYKAXZ EAZZEN. UFWEYKAXZ ZNAXPEN. UFWEYKAXZ EEAOYACOI. WE'VE EEEX CFTOUEP FX WKAY'U
> IFFQAXZ AY WKAY'U AEFVE OU.

and the word "WAU" looks like "WAS", then substitute it again, U=S

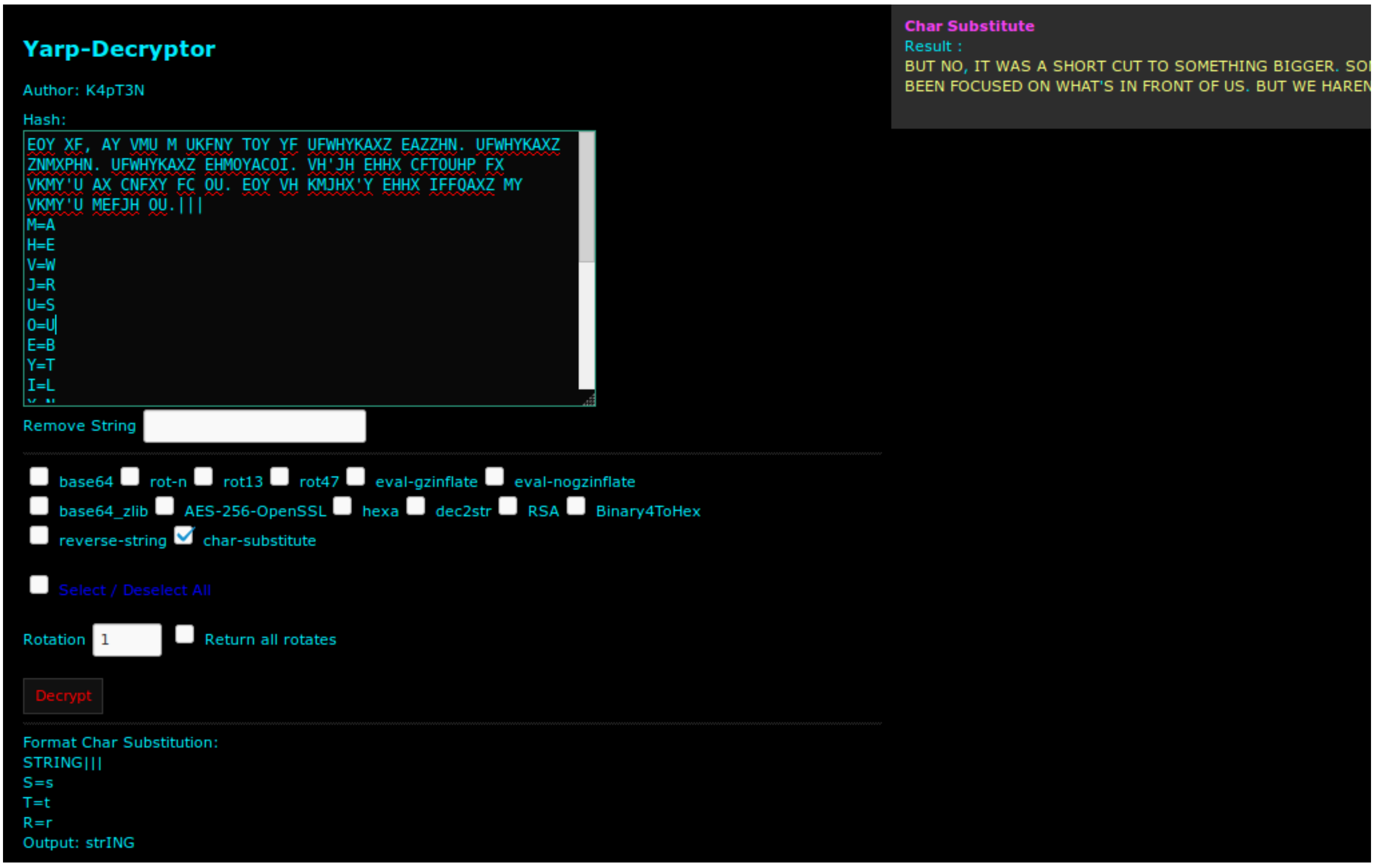
> EOY XF, AY WAS A SKFNY TOY YF SFWEYKAXZ EAZZEN. SFWEYKAXZ ZNAXPEN. SFWEYKAXZ EEAOYACOI. WE'VE EEEX CFTOSEP FX WKAY'S A
> IFFQAXZ AY WKAY'S AEFVE OS.

i think i;m on the right track. Next, i'll guess OS as US. So, O=U

> EUY XF, AY WAS A SKFNY TUY YF SFWEYKAXZ EAZZEN. SFWEYKAXZ ZNAXPEN. SFWEYKAXZ EEAUYACUI. WE'VE EEEX CFTUSEP FX WKAY'S A
> IFFQAXZ AY WKAY'S AEFVE US.

still, now looks at this word "EEAUYACUI" it's looks like "BEAUTIFUL". One more right track :)

But for this challenge, I do not really do it manually. Because it is really a waste of time. So, i coding it. Yarp. I made my own decryptor for th
Challenges.



Author: K4pT3N

Hash:

```
EOY XF, AY VMU M UKFNY TOY YF UFWHYKAXZ EAZZHN. UFWHYKAXZ
ZNMXPHN. UFWHYKAXZ EHMOYACOI. VH'JH EHHX CFTOUHP FX
VKMY'U AX CNFXY FC OU. EOY VH KMJHX'Y EHHX IFFQAXZ MY
VKMY'U MEFJH OU.|||
M=A
H=E
V=W
J=R
U=S
O=U
E=B
Y=T
I=L
```

Remove String

□ base64 □ rot-n □ rot13 □ rot47 □ eval-gzinflate □ eval-nogzinflate
□ base64_zlib □ AES-256-OpenSSL □ hexa □ dec2str □ RSA □ Binary4ToHex
□ reverse-string ☑ char-substitute

□ Select / Deselect All

Rotation 1 □ Return all rotates

```
Format Char Substitution:
STRING|||
S=s
T=t
R=r
Output: strING
```

Char Substitute

Result :

```
BUT NO, IT WAS A SHORT CUT TO SOMETHING BIGGER. SO
BEEN FOCUSED ON WHAT'S IN FRONT OF US. BUT WE HAREN
```

and after all, i got the flag

BUT NO, IT WAS A SHORT CUT TO SOMETHING BIGGER. SOMETHING GRANDER. SOMETHING BEAUTIFUL. WE'VE BEEN FOCUSED ON WHAT'S
BEEN LOOKING AT WHAT'S ABOVE US.

:)

**0 Comments** **Cafelinux**

♡ Recommend Share

Start the discussion…

Be the first to comment.

ALSO ON **CAFELINUX**

**Happy New Curl 2017**

1 comment • 5 months ago•

Mikazuki Augus — Pertamax..

**Mengatasi Error "The mbstring extension is missing." Setelah Upgrade ke PHP7 di Linux**

2 comments • 6 months ago•

Jamz D. Mozac — pesan errornya apa gan?

**Mengganti Port Default Ruby on Rails**

1 comment • 4 months ago•

Disk Jokey Adi — mantabs

**6 Alasan Kenapa Website Kamu Belum Perr**

6 comments • 2 months ago•

Ahmad Oriza — LOL

✉ Subscribe Add Disqus to your siteAdd DisqusAdd 🔒 Privacy