love CTF

CTF never makes me tired …

23/09/2013

[CSAW CTF 2013] CSAWpad (Crypto100)

> *CSAWpad – 100 Points*
>
> *Solved by 141 teams.*
>
> *csawpad.py*

File backup:

- https://db.tt/p6zWhqXR

main content

In this article, we provided encrypt and decrypt functions 2, with a few lines of text have been encrypted. Tasks from the well known saying, that encode them.

I do not try to understand the algorithm, they try to see it do something was:

```
print encrypt('thisismypadpadpad', 'thisismytext').encode('hex')
print encrypt('thisismypadpadpad', 'ahisismytext').encode('hex')
print encrypt('thisismypadpadpad', 'thisismytex').encode('hex')
```

for the output:

```
746c52985298381d86116b86
6f6c52985298381d86116b86
746c52985298381d86116b
```

Thus, it is like a swap byte-to-byte so, should resolve to make no matter what.

We did not know any information about the value of the **pad** , however it **should** bring an important characteristic, that is after decrypt with it, the data returned must be in plain text consisting of only those characters **printable** . In this direction, we will look for each byte of the pad, looking to satisfy the condition byte. Where to find only 1 byte, then simply select it, and if there are more, it will need a bit of English competency

```
ciphers = [
'794d630169441dbdb788337d40fe245daa63c30e6c80151d4b055c18499a8ac
'14a60bb3afbca7da0e8e337de5a3a47ae763a20e8e18695f39450353a2c6a26
'250d83a7ed103faaca9d786f23a82e8e4473a5938eabd9bd03c3393b812643e
'68a90beb191f13b621747ab46321a491e71c536b71800b8f5f08996bb433838
'0fc30404846913 7d0e2f3a71885a5a78e749145510cf2d56157939548bfd5dd
'254c0bb31453badaca9d060ce5faa45fa66378a6716915473579d3743e315db
'41cd1c01c62883b2ca71e671dce57e5f96b1610e29507b6c03c382116532845
'68c50bd5197bfdbdfa887883783d2455a673a685436915bd72d1af74dffdd2b
```

RECENT COMMENTS

health care on [CSAW CTF 2013] Impossible (Re500)
Ngọc Au on [Plaid CTF 2016] quite quixotic quest (Re300)
xss on [Plaid CTF 2016] quite quixotic quest (Re300)
yeuchimse on [Plaid CTF 2016] quite quixotic quest (Re300)
Ta Quang Khanh on [Plaid CTF 2016] quite quixotic quest (Re300)

RECENT POSTS

- [Plaid CTF 2016] quite quixotic quest (Re300) 19/04/2016
- [Plaid CTF 2016] quick (Re175) 19/04/2016
- New Post, New Year ^_^ 19/02/2015
- Repost: RE Driver Checker v2.7.4 by P.E Onimusha & Unregistered ! 06/08/2014
- byectf 04/02/2014

CATEGORIES

- CTF Events (15)
  - 30C3 CTF 2013 (1)
  - CSAW CTF 2013 (5)
  - No Name cON Facebook which ones should CTF 2013 (1)
  - Plaid CTF 2016 (2)
  - Sharif University which ones should CTF 2013 (2)
  - SVATTT CTF 2013 (2)
  - WarGameVN CTF (1)
  - WhiteHat CTF 2013 (1)
- CTF Sites (50)
  - CodeEngn (19)

- OverTheWire (24)
- WarGame (7)
- OEP (2)
- Uncategorized (1)

```

def test_decrypt(pad):
    for cipher in ciphers:
        cipher_part = cipher[:len(pad)]
        print decrypt(pad, cipher_part)

pad = ''
index = len(pad)
for i in range(index, index + 1):
    for c in [chr(j) for j in range(1, 256)]:
        valid = True
        for cipher in ciphers:
            cipher_char = cipher[i]
            plain_char = decrypt(c, cipher_char)

            if (len(plain_char) == 0):
                continue

            if (ord(plain_char) not in range(0x20, 0x7E)):
                valid = False
                break

        if (valid):
            print 'nndecrypt with next char = 0x' + c.encode('hex
            test_decrypt(pad + c)
```

After some three minutes painstakingly, we find:

```
pad = 'xdfx47x28x8bxd4xeax6fx68x39xa4xe4x86x71x2bxbex9bx8fx61x7fx4
```

though not enough to get the entire contents of the text, but the need is the flag they appeared:

```
decrypt with next char = 0xe5
The difference between stupidity and genius is that
Go to Heaven for the climate, Hell for the company-
I am not a member of any organized political party.
My definition of an intellectual is someone who can
Republicans want less government for the same reason
If there are no stupid questions, then what kind of
And now, in the interest of equal time, here is a me
MY key for you is {And yes the nsa can read this to}
```

flag = **And yes the nsa can read this to**

This entry was posted in CSAW CTF 2013, CTF Events and tagged crypto.

Bookmark the permalink.

Leave a comment

← PREVIOUS NEXT →

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

COMMENT

THE NAME *

EMAIL *

WEBSITE

Post Comment

□ NOTIFY ME OF FOLLOW-UP COMMENTS BY EMAIL.

□ NOTIFY ME OF NEW POSTS BY EMAIL.