Features Business Explore Pricing This repository Search Sign in or Sign up

team-bitskrieg / CTF-writeups

Watch 3 Star 3 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Pulse Graphs

Branch: master CTF-writeups / tuctf / Magic Image / Create new file Find file History

illustris . Latest commit a693225 on 16 May 2016

..

files	Added Magic Image	10 months ago
README.md	.	10 months ago

README.md

#TUCTF 2016 : Magic Image

##Challenge A zip file is given, wiith an encrypted image and the python script used to encrypt it 100 points

##Solution Contents of encrypt.py:

```
#!/usr/bin/env python

def xor(s1, s2):
    res = [chr(0)]*12
    for i in range(len(res)):
        q = ord(s1[i])
        d = ord(s2[i])
        k = q ^ d
        res[i] = chr(k)
    res = ''.join(res)
    return res

def add_pad(msg):
    l = 12 - len(msg)%12
    msg += chr(l)*l
    return msg

with open('flag.png') as f:
    data = f.read()

data = add_pad(data)

with open('key') as f:
    key = f.read()

enc_data = ''
for i in range(0, len(data), 12):
    enc = xor(data[i:i+12], key)
    enc_data += enc

with open('encrypted.png', 'wb') as f:
    f.write(enc_data)
```

The script is XORing the image with a 12 byte long key. That's convenient. The first few bytes of any PNG are the same. I spent a good 5 minutes searching for a PNG file that i can use for that and found this one in my screenshots folder. Then i used the python interpretter to get the key and decrypt the image

```
>>> with open('encrypted.png') as f:
...     data = f.read()
...
>>> with open('ctfflag.png') as f:
...     data2 = f.read()
...
>>> print data2[0:11]
```

```
¦PNG


>>> print data[0:11]
¦o+R{¦?¦*?
>>> def xor(s1, s2):
...     res = [chr(0)]*12
...     for i in range(len(res)):
...             q = ord(s1[i])
...             d = ord(s2[i])
...             k = q ^ d
...             res[i] = chr(k)
...     res = ''.join(res)
...     return res
...
>>> xor(data[0:12],data2[0:12])
'\x03?e\x15v\xea%\xbc*\xd3\xb5\r'
>>> print xor(data[0:12],data2[0:12])
?ev¦%¦*?
>>> key = xor(data[0:12],data2[0:12])
>>> enc_data = ''
>>> for i in range(0, len(data), 12):
...     enc = xor(data[i:i+12], key)
...     enc_data += enc
...
>>> with open('decrypted.png', 'wb') as f:
...     f.write(enc_data)
...
>>> exit()
```

This gives us this image: with the flag

> TUCTF{st@llowning_xOR_5ince_Apollo}