Beefest2 (Final): Snekription

Deskripsi: Dapatkah anda menemukan kata kunci rahasia?

Writeup:

Pertama kita menggunakan file:

```
nacl@ubuntu:~$ file beefest2.pyc
beefest2.pyc: python 2.7 byte-compiled
```

Setelah itu kita mencoba menjalankan program:

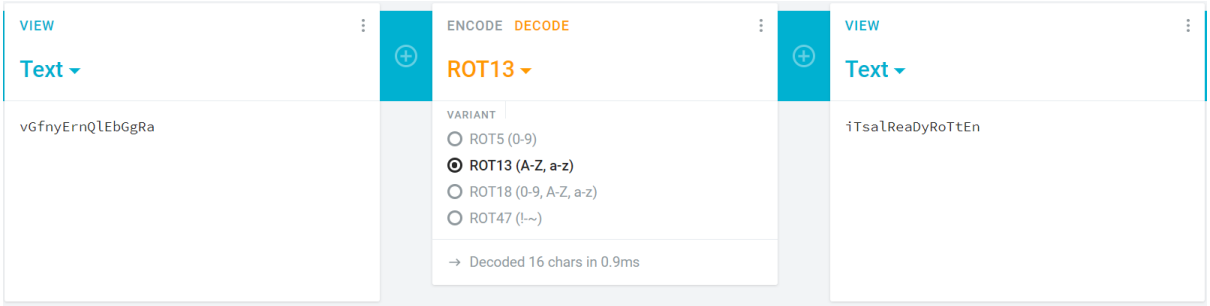
```
nacl@ubuntu:~$ python beefest2.pyc
Kopi kembung tidak bikin luwak passwordnya?:
```

Terlihat bahwa program meminta sebuah password. Karena file merupakan python yang telah decompile, kita dapat menggunakan tool uncompyle6 untuk mendapatkan source codenya:

```
nacl@ubuntu:~$ uncompyle6 beefest2.pyc
# uncompyle6 version 3.2.0
# Python bytecode 2.7 (62211)
# Decompiled from: Python 2.7.14 (default, Sep 23 2017, 22:06:14)
# [GCC 7.2.0]
# Embedded file name: ./beefest2.py
# Compiled at: 2018-05-24 11:15:09
s = raw_input('Kopi kembung tidak bikin luwak passwordnya?: ')

def encrypt(str):
    result = ''
    for i in str:
        c = ord(i)
        if c >= ord('a') and c <= ord('z'):
            if c > ord('m'):
                c -= 13
            else:
                c += 13
        else:
            if c >= ord('A') and c <= ord('Z'):
                if c > ord('M'):
                    c -= 13
                else:
                    c += 13
        result += chr(c)

    return result


flag = encrypt('vGfnyErnQlEbGgRa')
if encrypt(s) == 'vGfnyErnQlEbGgRa':
    print 'DUA JUTA RUPIAH!!!'
    print 'flag: BeeFest{%s}' % flag
else:
    print 'Silahkan dicoba kembali'
# okay decompiling beefest2.pyc
```

Disini terlihat bahwa ada function encrypt yang mengenkripsi flag kita. Pertama function melakukan loop sebanyak jumlah karakter string, kemudian mengubahnya menjadi nilai ASCII karakter tersebut. Function mengecek apabila karakter termasuk dalam huruf kapital dan non-kapital. Jika karakter merupakan huruf antara n-z, huruf tersebut akan mundur sebanyak 13 huruf (nilai ASCII dikurangi). Sedangkan jika termasuk dalam huruf antara a-m, huruf tersebut akan maju sebanyak 13 huruf (nilai ASCII ditambahkan.)

Sepertinya ini merupakan enkripsi ROT13. Dengan menggunakan tool online, kita dapat mendekripsi flag 'vGfnyErnQlEbGgRa'.



Setelah itu kita dapat mengecek dengan memasukkan hasil dekripsi kedalam program:

```
nacl@ubuntu:~$ python beefest2.pyc
Kopi kembung tidak bikin luwak passwordnya?: iTsalReaDyRoTtEn
DUA JUTA RUPIAH!!!
flag: BeeFest{iTsalReaDyRoTtEn}
```

Flag: BeeFest{iTsalReaDyRoTtEn}