

Nama : Gayu Gumelar  
Team : bangjono  
TUCTF\_2018

---

## Welcome

### Welcome (1)

Challenge

178 Solves

×

Welcome  
1

Difficulty: Dream Crushing Welcome to TUCTF!  
Stop and smell the exploits.

The flag is located in the **welcome** chat under *Challenge Categories* on our [Discord Server](#)

Flag

Submit

saya masuk ke Link yang sudah di berikan, dan saya mencari kategori welcome.

Flag : TUCTF{my\_f1r57\_fl46}

## Reversing

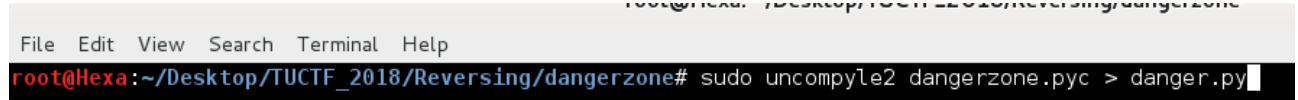
### Dangerzone (63)

Diberikan file dangerzone.pyc

Hint : what is a .pyc file and can you convert it?

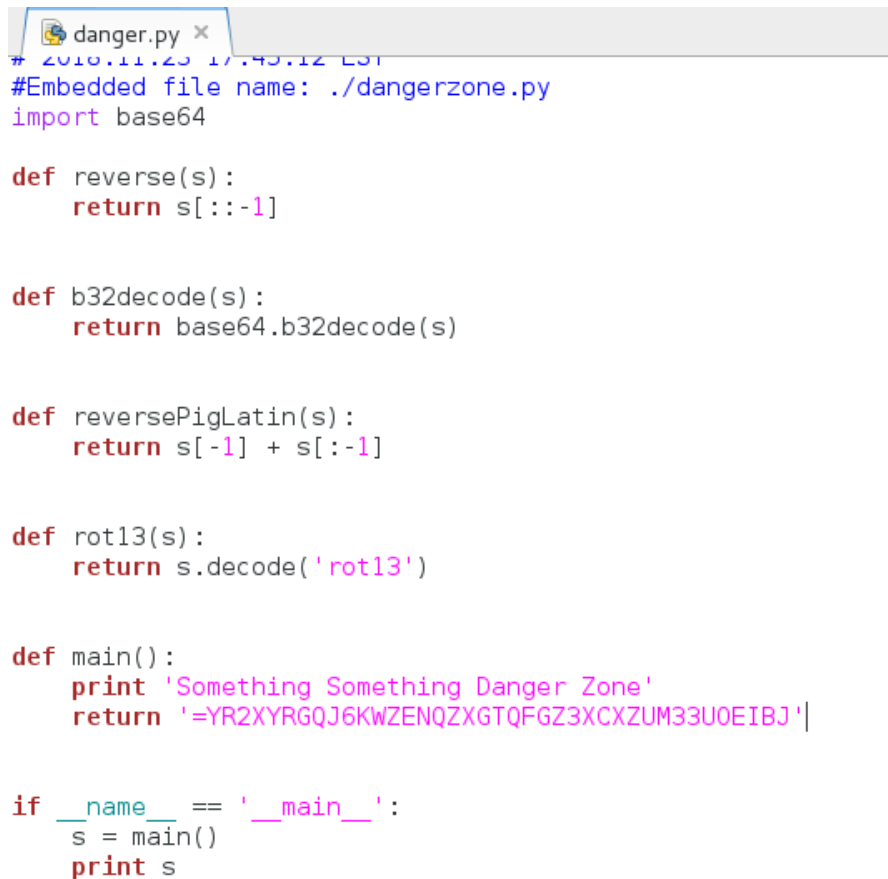
Kemudian saya masuk ke terminal dan mengetikan perintah untuk convert file pyc itu ke py

sudo uncompile2 dangerzone.pyc > danger.py



```
File Edit View Search Terminal Help
root@Hexa:~/Desktop/TUCTF_2018/Reversing/dangerzone# sudo uncompile2 dangerzone.pyc > danger.py
```

kemudian saya buka file hasil convert tadi dan muncul clue,



```
danger.py x
# 2018.11.23 17:43:12 EST
#Embedded file name: ./dangerzone.py
import base64

def reverse(s):
    return s[::-1]

def b32decode(s):
    return base64.b32decode(s)

def reversePigLatin(s):
    return s[-1] + s[:-1]

def rot13(s):
    return s.decode('rot13')

def main():
    print 'Something Something Danger Zone'
    return '=YR2XYRGQJ6KWZENQZXGTQFGZ3XCXZUM33U0EIBJ|'

if __name__ == '__main__':
    s = main()
    print s
```

kemudian saya buka file hasil convert tadi dan muncul clue : reverse, b32decode, rot13

jadi saya simpulkan hasil membalik, kemudian saya decode ke base32, dan hasil decode base32 saya decode lagi ke rot13

berikut scriptnya

script untuk decode ke base32

```
cobadecode.py x
import base64

|
dcd = "JBIE0U33MUZX3ZGFQTGXZQNEZWK6JQGRYX2RY="
ecd2 = dcd
dcd2 = base64.b32decode(ecd2)
print dcd2
```

hasil decode dari base32 saya masukan ke script di bawah ini untuk memunculkan flag hasil dari rot13

```
caesar.py x

for l in plaintext.lower():
    try:
        i = (key.index(l) + n) % 26
        result += key[i]
    except ValueError:
        result += l

return result.lower()

def decrypt(n, ciphertext):
    """Decrypt the string and return the plaintext"""
    result = ''

    for l in ciphertext:
        try:
            i = (key.index(l) - n) % 26
            result += key[i]
        except ValueError:
            result += l

    return result

for i in range(27):
    print i, decrypt(i, "HPGS{e3q_y1a3_0i3ey04q}G")

|
```

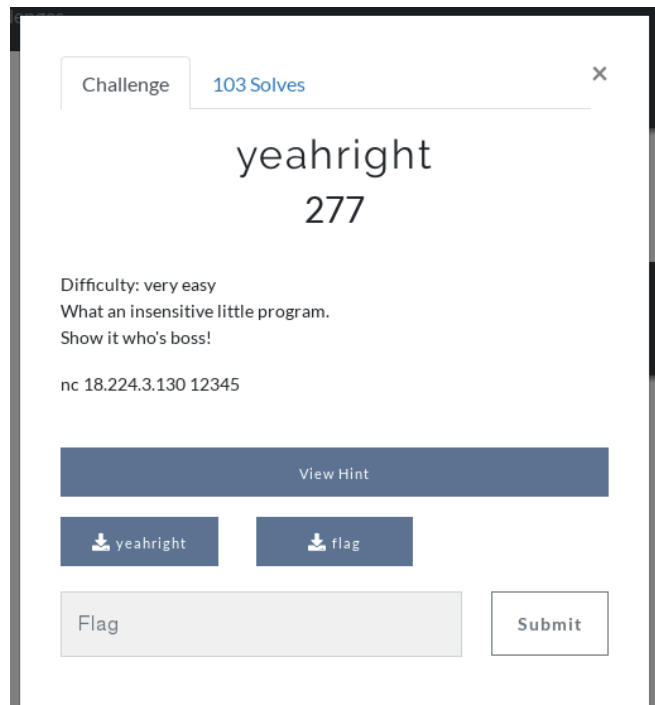
```
File Edit View Search Terminal Help
root@Hexa:~/Desktop# python cobadecode.py
HPGS{e3q_y1a3_0i3ey04q}G
root@Hexa:~/Desktop# python caesar.py
0 HPGS{e3q_y1a3_0i3ey04q}G
1 HPGS{d3p_x1z3_0h3dx04p}G
2 HPGS{c3o_w1y3_0g3cw04o}G
3 HPGS{b3n_v1x3_0f3bv04n}G
4 HPGS{a3m_u1w3_0e3au04m}G
5 HPGS{z3l_t1v3_0d3zt04l}G
6 HPGS{y3k_s1u3_0c3ys04k}G
7 HPGS{x3j_r1t3_0b3xr04j}G
8 HPGS{w3i_q1s3_0a3wq04i}G
9 HPGS{v3h_p1r3_0z3vp04h}G
10 HPGS{u3g_o1q3_0y3uo04g}G
11 HPGS{t3f_n1p3_0x3tn04f}G
12 HPGS{s3e_m1o3_0w3sm04e}G
13 HPGS{r3d_l1n3_0v3rl04d}G
14 HPGS{q3c_k1m3_0u3qk04c}G
15 HPGS{p3b_j1l3_0t3pj04b}G
16 HPGS{o3a_i1k3_0s3oi04a}G
17 HPGS{n3z_h1j3_0r3nh04z}G
18 HPGS{m3y_g1i3_0q3mg04y}G
19 HPGS{l3x_f1h3_0p3lf04x}G
20 HPGS{k3w_e1g3_0o3ke04w}G
21 HPGS{j3v_d1f3_0n3jd04v}G
22 HPGS{i3u_c1e3_0m3ic04u}G
23 HPGS{h3t_b1d3_0l3hb04t}G
24 HPGS{g3s_a1c3_0k3ga04s}G
25 HPGS{f3r_z1b3_0j3fz04r}G
26 HPGS{e3q_y1a3_0i3ey04q}G
```

kemudian saya running kedua script tersebut, dan muncul

Flag : TUCTF{r3d\_l1n3\_0v3rl04d}

## yeahright (149)

Diberikan nc 18.224.3.130 12345 dan dua buah file yeahright dan flag



kemudian saya buka file flag dan muncul clue flag{test-flag-here} kemudian saya membuka file yeahright, namun file itu tidak dapat di buka. Jadi saya coba buka di terminal (cek string) dan mengetikan perintah strings yeahright

```
[ ]A\A]A^A_
7h3_m057_53cr37357_p455w0rd_y0u_3v3r_54w
*Ahem*... password?
yeahright!
/bin/cat ./flag
;*3$"
root@Hexa:~/Desktop/TUCTF_2018/Reversing/yeahright#
```

dan benar saja muncul password untuk membuka nc 18.224.3.130 12345

```
root@Hexa:~/Desktop/TUCTF_2018/Reversing/yeahright# nc 18.224.3.130 12345
*Ahem*... password? 7h3_m057_53cr37357_p455w0rd_y0u_3v3r_54w
TUCTF{n07_my_fl46_n07_my_pr0bl3m}
root@Hexa:~/Desktop/TUCTF_2018/Reversing/yeahright#
```

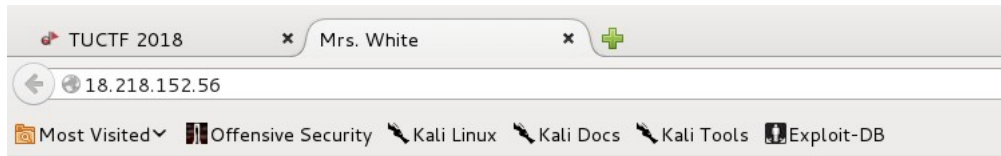
setelah saya masukan password dari hasil strings tadi, kemudian saya mendapatkan

Flag : TUCTF{n07\_my\_fl46\_n07\_my\_pr0bl3m}

## Web

### Mrs. White's Messy Maids (25)

Diberikan link berikut ini <http://18.218.152.56/>



## Welcome to Mrs. White's Maid Service



kemudian saya ctrl+u dan muncul pesan Boddy

```
Source of: http://18.218.152.56/ - Iceweasel
File Edit View Help
1 <html>
2   <head>
3     <title>Mrs. White</title>
4     <link rel="stylesheet" href="styles.css">
5   </head>
6
7   <body>
8     <h1>Welcome to Mrs. White's Maid Service</h1>
9     
10    <p>We offer only the best maids for all your cleaning needs
11    <br>
12    To learn more about our services, call 275-317-3581
13    <!-- I might kill if I could find him. Stupid Mr. /Boddy --></p>
14  </body>
15 </html>
```

kemudian saya tambahnya Boddy pada link tadi <http://18.218.152.56/Boddy>  
dan muncullah

Flag : TUCTF{1\_4ccu53\_Mr5.\_Wh173\_w17h\_7h3\_c4ndl3571ck\_1n\_7h3\_c0mm3n75}