广东省强网杯CTF Web部分详解

转载

普通网友 于 2017-09-26 15:43:48 发布 2266 收藏
分类专栏： CTF


CTF 专栏收录该内容
10 篇文章 0 订阅
订阅专栏

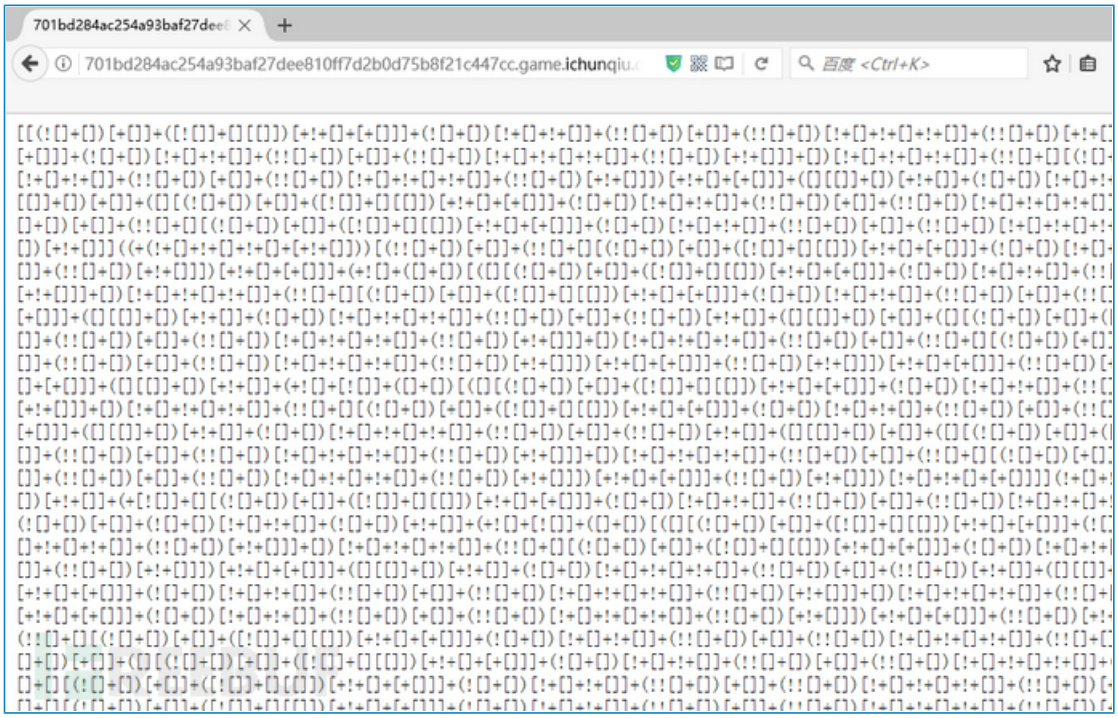
0×00 前言

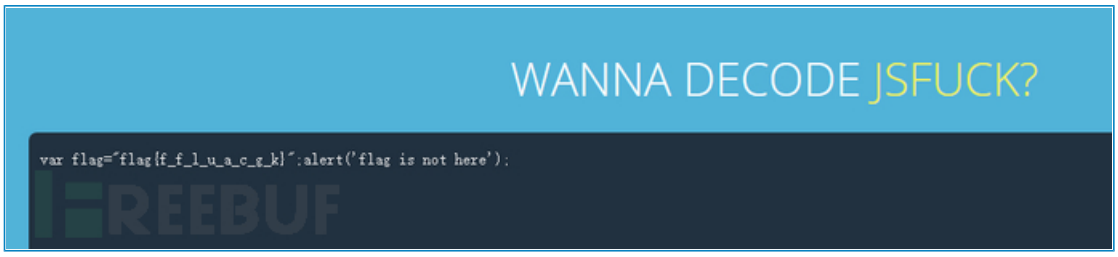
周末打了一场CTF，只做了Web部分，学到不少东西，不过Web题量太少了，两天才4题。下面是具体解题思路。

0×01 WP正文

第一题

题目给了一个损坏的jsfuck，修复一下解密即可，将开头[[改成[][，然后转换成代码即可看到flag。注意这里不要将代码直接放在控制台运行，因为flag被赋值给一个变量了。

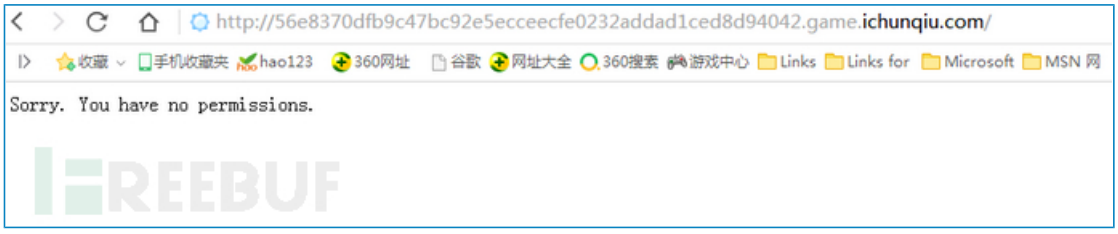


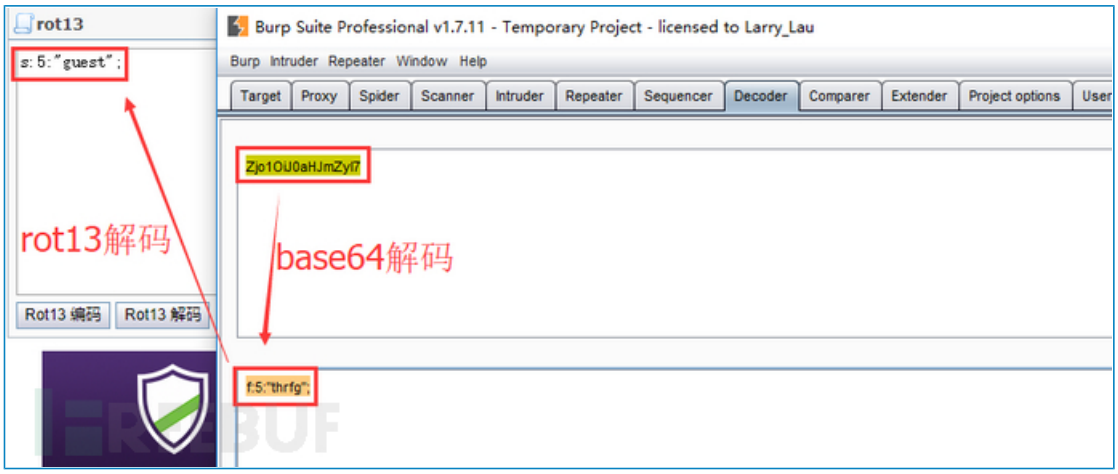


解密地址：https://enkhee-osiris.github.io/Decoder-JSFuck/

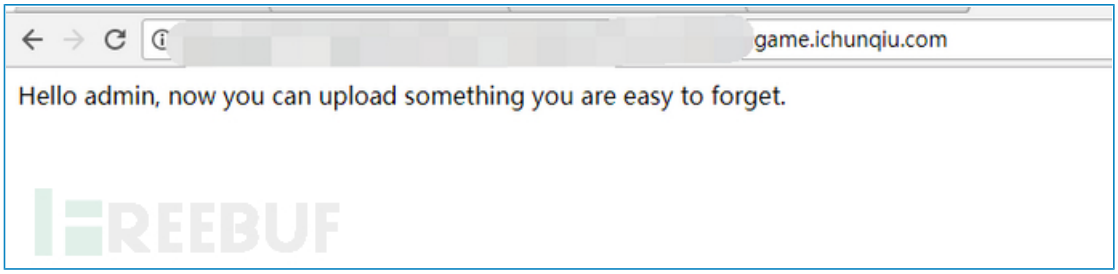
第二题

访问链接，发现被禁止访问，抓包发现，role参数有点奇怪role=Zjo1OiJ0aHJmZyI7





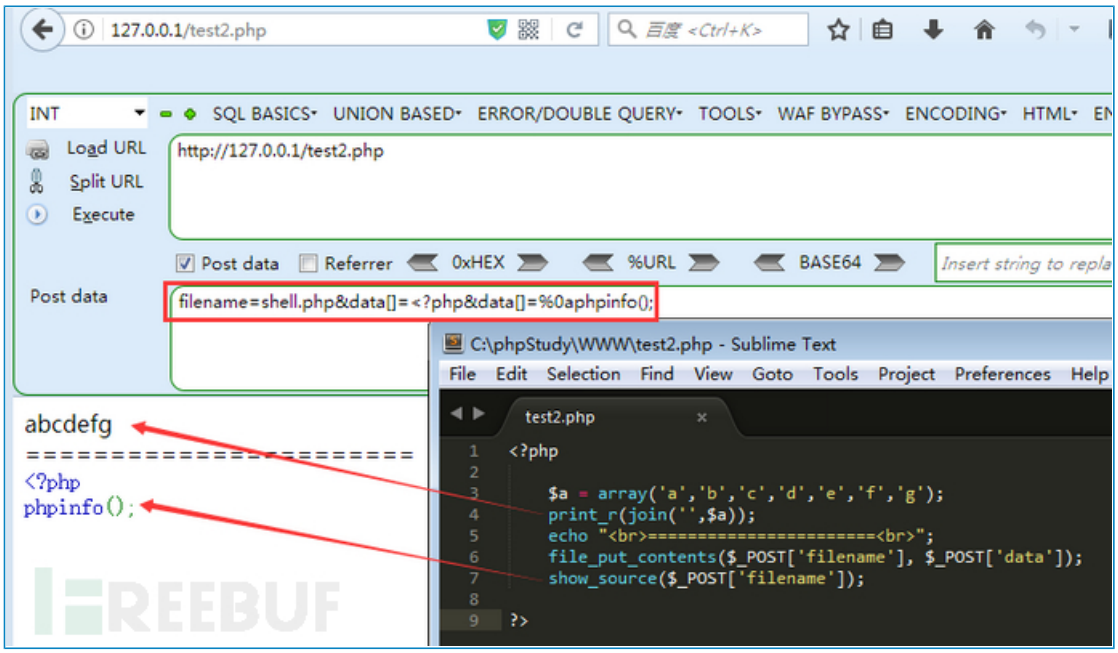
根据题目提示我是谁？我在哪？我要干什么？将s:5”admin”进行rot13加密再base64加密发送数据包，就以admin身份登录进来了。



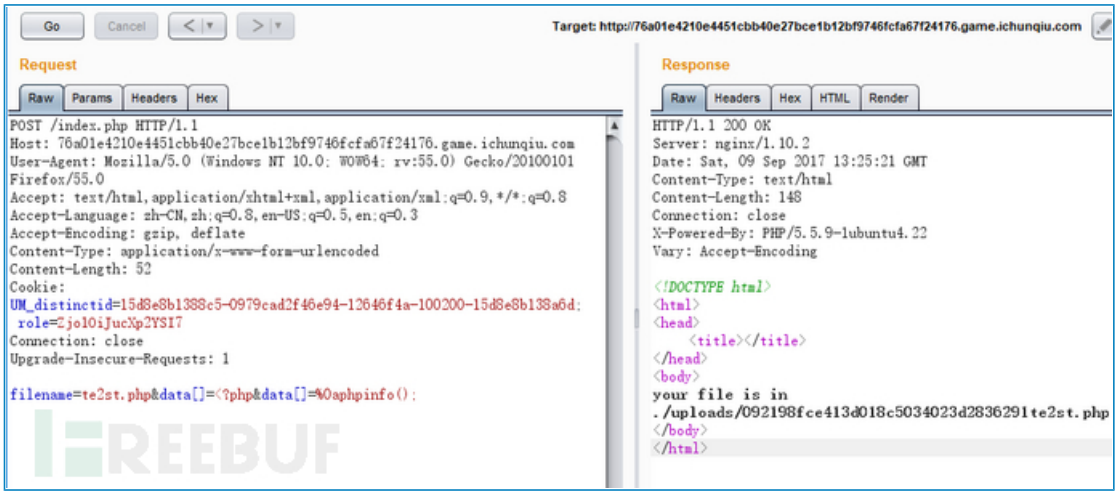
查看网页源代码发现需要POST数据给服务器

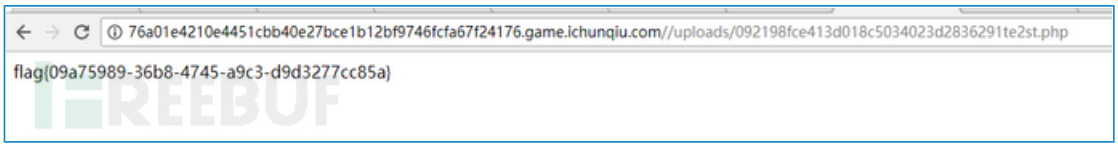
那就随便POST数据filename=test1.php&data=<?php phpinfo(); ?>发现被拦截，但是POST数据filename=test1.txt&data=<?php phpinfo(); ?>可以，而且给出了路径，也可以访问到。这里应该是做了限制。可以猜测后台代码使用了file_put_contents()函数，于是根据PHP手册介绍，第二个参数可以是数组

如果第二个参数传入的是数组，则会将他们以字符串的形式拼接起来，测试如下：



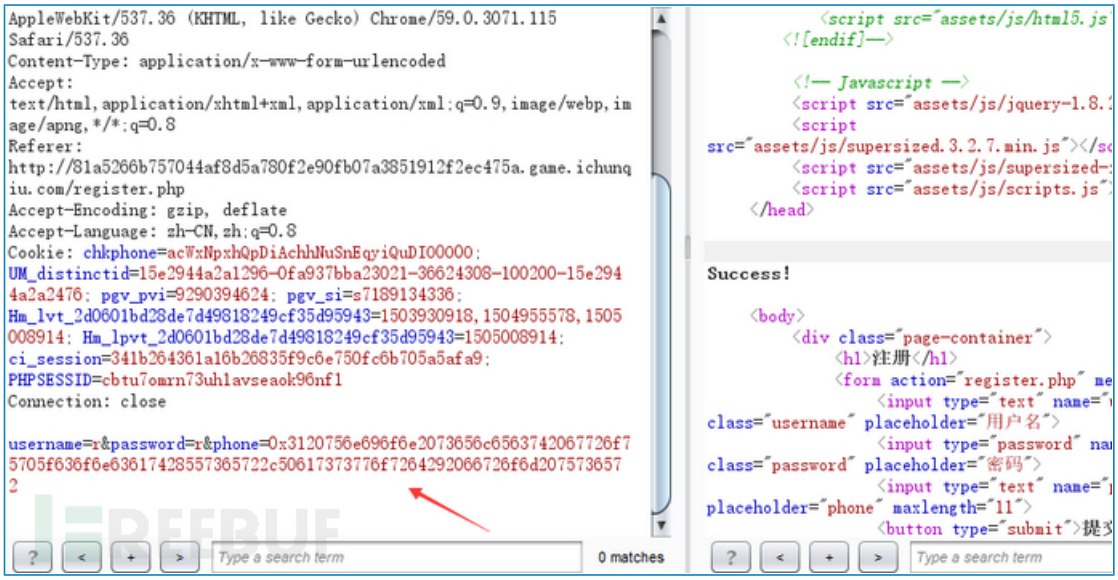
获取路径后访问既得flag

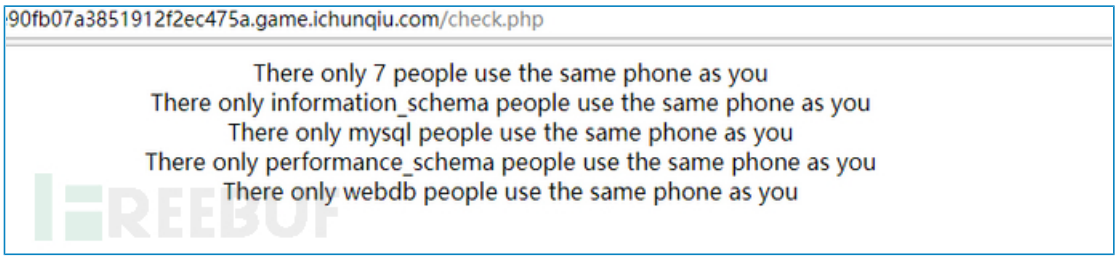


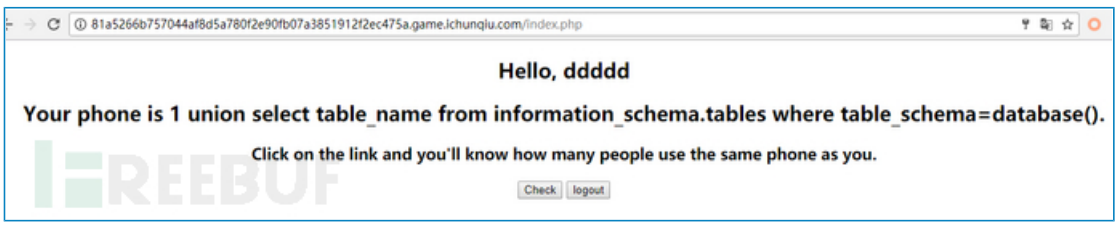


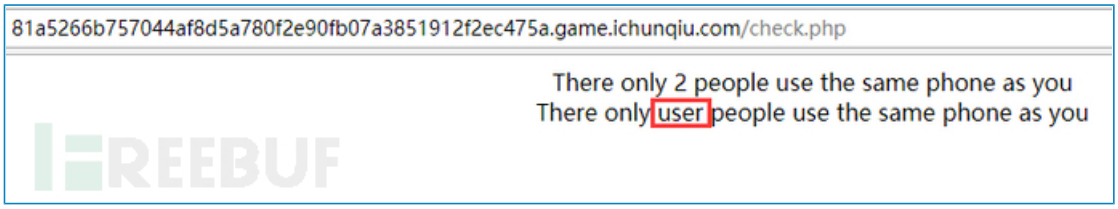
第三题

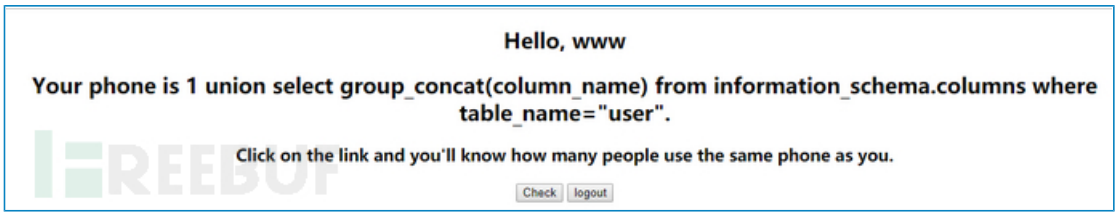
考察sql二次注入，随便注册即可登录，登录后发现有个check按键可以查询有多少人的号码和你一样，这样必定要用到电话号码，并查询数据库，而电话号码只能是数字。所以，思路就是将sql语句转换成16进制进行注册，这样在查询的时候就会执行我们构造的sql语句

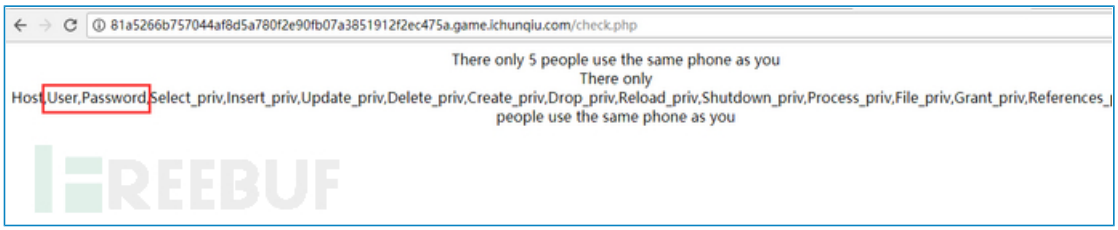


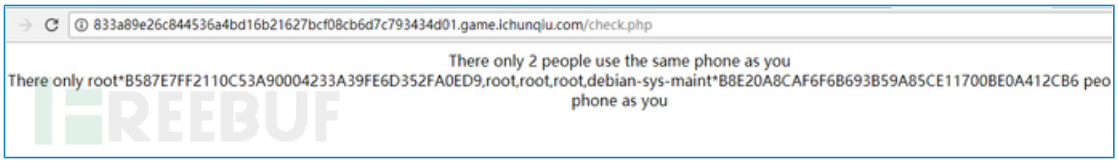


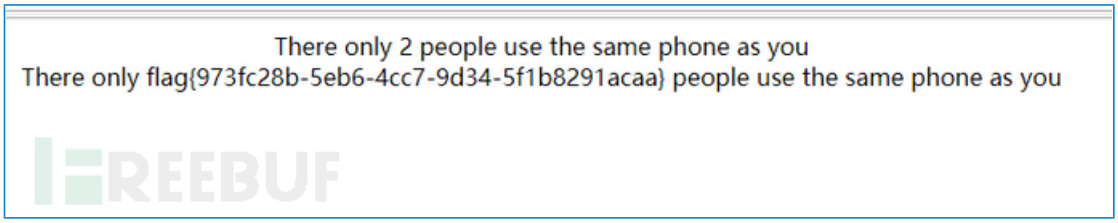








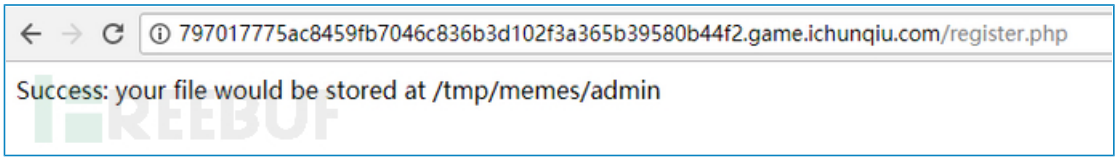




第四题

考察jinjia2模板注入

注册完后，在donate.php处可以填写图片url，以及用户名。随便填报错，发现使用后台了jinja2模板。

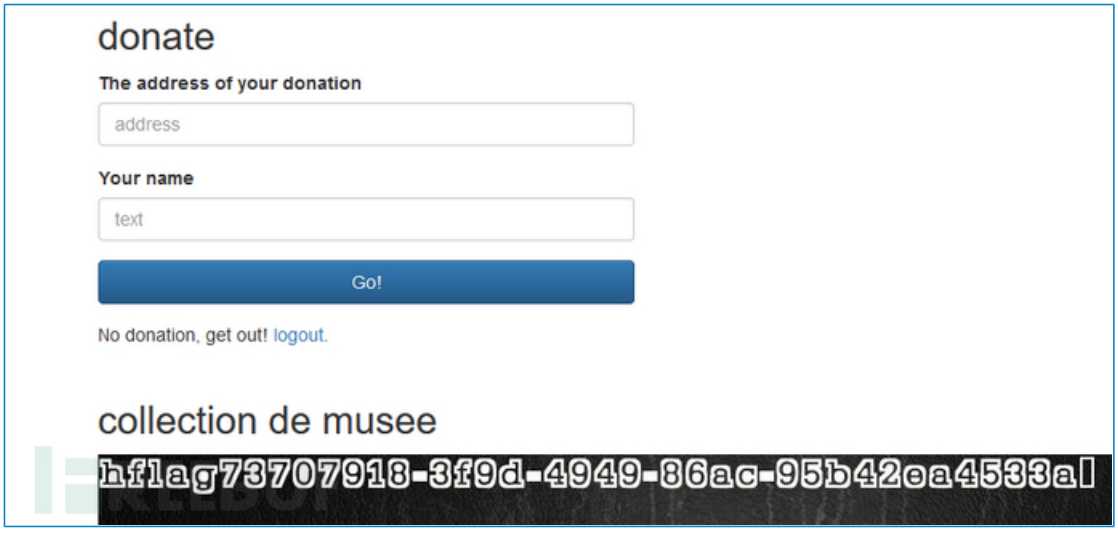


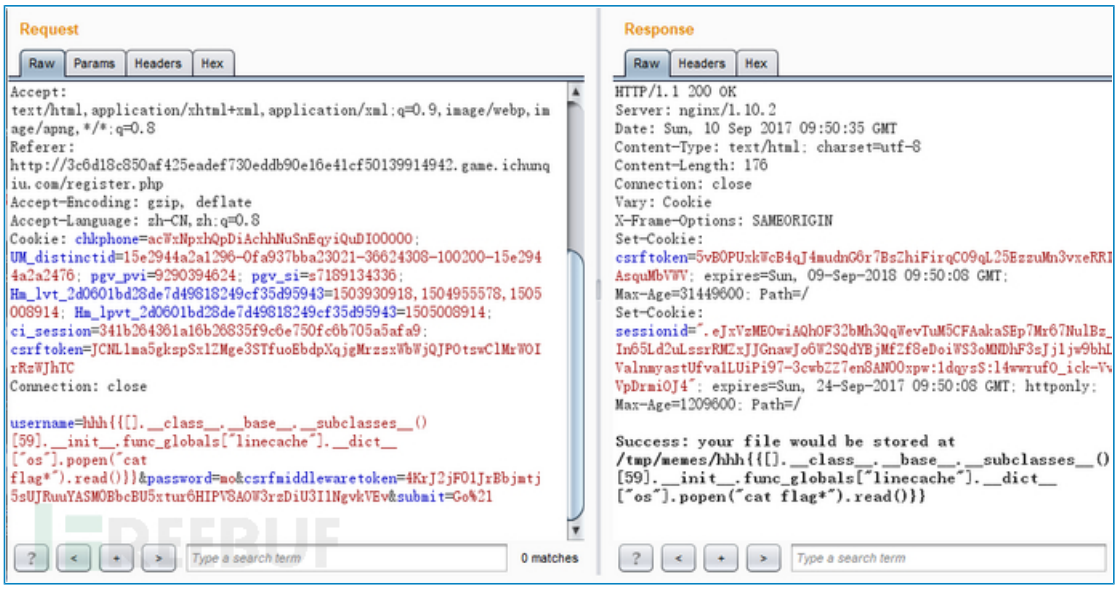
```
TEMPLATES                       [{'APP_DIRS': True,
                                  'BACKEND': 'django.template.backends.jinja2.Jinja2',
                                  'DIRS': ['/var/www/html/templates'],
                                  'OPTIONS': {'environment': 'museum.myjinja2.environment'}},
                                 {'APP_DIRS': True,
                                  'BACKEND': 'django.template.backends.django.DjangoTemplates',
                                  'DIRS': ['/var/www/html/templates'],
                                  'OPTIONS': {'context_processors': ['django.template.context_processors.de
                                                                     'django.template.context_processors.re
                                                                     'django.contrib.auth.context_processor
                                                                     'django.contrib.messages.context_proce
```

google一下，get姿势，具体看这篇文章：CSAW-CTF Python sandbox write-up

```
C:\Users\Mochazz>python
Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:53:40) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> [].__class__.__base__.__subclasses__()[59].__init__.func_globals['linecache'].__dict__["os"].popen("whoami").read()
'desktop-sej9981\\mochazz\n'
>>>
```

下面思路就是用python语句进行命令执行，当然后台过滤了一些关键词





jinjia2注入参考文章：

CSAW-CTF Python sandbox write-up

利用 Python 特性在 Jinja2 模板中执行任意代码

*本文作者：Mochazz，转载请注明来自 FreeBuf.COM

Mochazz 3 篇文章 等级： 2级

- 上一篇：如何制作基础认证钓鱼页面
- 下一篇： ACHE：一款功能强大的聚焦型网络爬虫

发表评论

已有 3 条评论

- 111 2017-09-20 回复 1楼
  请问楼主是哪只队伍的哪位呢？嘻嘻，要是被发现代打，那就是被扣除成绩了哦

  亮了(2)
- 路人 2017-09-20 回复 2楼
  我 代打 第一名队伍

  亮了(0)
- 213 2017-09-20 回复 3楼
  我 代打 第一名队伍