# “百度杯”CTF比赛 2017 二月场--web 爆破-3 writeup

原创

会下雪的晴天 于 2019-06-14 15:38:30 发布 404 收藏 1

分类专栏： CTF做题记录

会下雪的晴天

本文链接：https://blog.csdn.net/weixin_43578492/article/details/91979044





## 题目简介


## 解题思路

进入链接后得到

```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__);
?>
```

大概意思为：
Session中的num初始值为0，time为当前时间，whoami的初始值为ea。120秒之后销毁会话。用str_rands随机生成2个字母，whoami需要等于我们传递的value值的前两位，并且value的md5值的第5为开始，长度为4的字符串==0，这样num++，whoami=str_rands，循环10次后，输出flag。

代码审计得到关键部分：

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

由于`==`为弱判断类型，则可以用数组绕过，md5()==0；
因此，构造payload `?value[]=ea`

df <?php
error_reporting(0);
session_start();
require('./flag.php');

## 得到FLAG

接着构造payload `?value[]=df`,由于有120s，手工10次完全够
第十次得到flag

veflag{230e5ad9-f234-469f-8002-01c2be7b1978} <?php
```
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}
```