BugkuCTF web16_备份是个好习惯 writeup

原创

Mitch311 于 2021-01-10 21:21:55 发布 254 收藏
分类专栏： CTF 文章标签： unctf

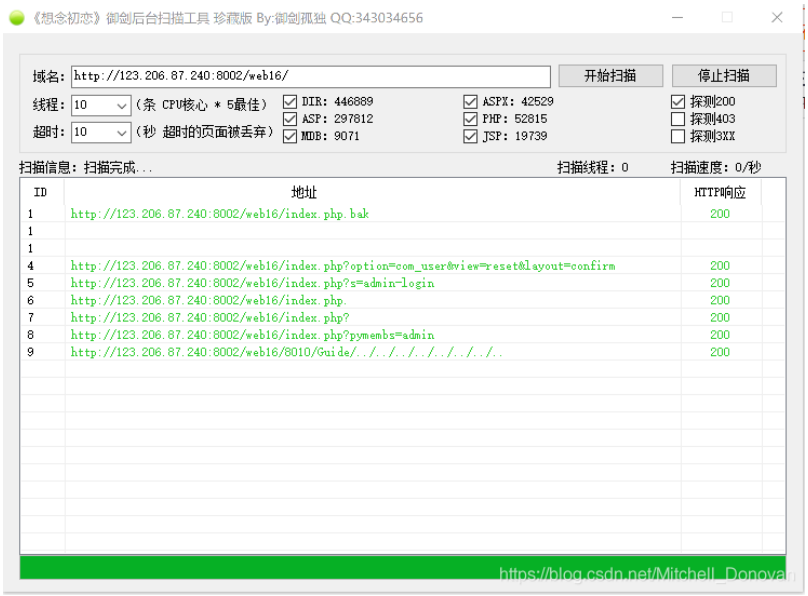
web16_备份是个好习惯

原题链接

key:备份文件访问+php绕过

①场景打开后啥也没有，只有一串神秘代码（MD5加密后的字符串，大佬说的）

根据题目提示，应该是有备份文件存在的，所以用御剑扫描一下吧



成功发现备份文件index.php.bak

②在地址栏后加上/index.php.bak，把备份文件下载到本地

打开备份文件后，发现这是php代码

进行代码审计和资料搜集，给代码加上注释

```php
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";//包含flag.php

ini_set("display_errors", 0);//设置危险等级为0的会报错

$str = strstr($_SERVER['REQUEST_URI'], '?');//设变量str的值为url中?后面的字符串

$str = substr($str,1);//设str为str中第一位开始后的字符串

$str = str_replace('key','',$str);//把str中的key替换成空

parse_str($str);//把str中的字符串解析为变量

echo md5($key1);//输出md5加密的key1

echo md5($key2);//输出md5加密的key2

if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```

③我们的最终目的肯定是**让$key1和$key2的md5值相同但内容不相同**，从而得到flag

> **典型md5函数绕过问题**
>
> 参考链接
>
> **思路有两个：**
>
> **1.传md5值是0e开头的字符串，比如QNKCDZO 和 s214587387a（网上能搜到好多payload）**
>
> **因为php在处理哈希字符串时，会利用”!=”或”==”来对哈希值进行比较，它把每一个以”0E”开头的哈希值都解释为0**
>
> **2.传递数组**
>
> **因为向md5函数传递数组会返回NULL**

至此我们知道了最后一步的绕过方法，这只是问题的一部分

因为$str的值为url中?后面的字符串,所以我们会用类似GET传参的方法传参

还有一个问题就是字符“key”会被过滤掉

不过我们可以让变量名是kkeyey1和kkeyey2，过滤后就变成key1和key2

④传参**?kkeyey1[]=1&kkeyey2[]=2**

或?kkeyey1=QNKCDZO&kkeyey2[]=s214587387a

得到flag

Bugku{OH_YOU_FIND_MY_MOMY}鍙栧緱flag

⑤最后看看开始的那段神秘代码是什么意思

拿到MD5解密试一下

结果为NULL，也就是说这是NULL的MD5值

因为默认是没有传入key1和key2的，这两个值也就是NULL