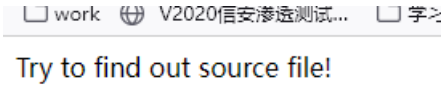
[ACTF2020 新生赛]BackupFile1 writeup

原创

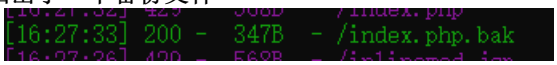
咸鱼一方 于 2022-04-20 19:26:02 发布 7 收藏
文章标签： php

本文链接：https://blog.csdn.net/dlccom/article/details/124305101

- 打开靶机后看见



- 估计还是查找备份文件的题
- 继续拿出dirsearch扫网站根目录，扫出了一个备份文件‘



- 打开之后发现

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

- 我们看到想要拿到flag 需要 get传的参数等于”123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3“
- 由于是两个==，我们知道在php里面两个等号意思是，在执行关系运算”==“时要求运算符两边的数据类型必须一致，所以如果有一方是int类型，一方是字符串类型的话，字符串类型会被强制转换为整型
- 那么具体怎么转换呢
  - 1.当字符串中 以 数字开头 +字符串+数字或字符(字符串)+... 格式与数字进行 == 判断时，
  - 会取第一次出现字符(字符串)前的数字作为转换值。
  - 2.当字符串中 以 字符(字符串)开头 +数字+数字或字符(字符串)+... 格式与数字进行 == 判断时，
  - 不能转换为数字，被强制转换为0
- 所以我们只需要把key=123传给get方法就可以拿到flag啦
- payload：xxxxxxx:xx?key=123
- 成功拿到flag

flag{77e25844-ef81-4748-9895-efadf30c5254}

-