

# [ACTF2020 新生赛] web题-BackupFile

原创

BROTHERYY 于 2020-07-08 15:46:09 发布 158 收藏 1

分类专栏: [CTF练习](#)

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/BROTHERYY/article/details/107207494>

版权



[CTF练习](#) 专栏收录该内容

53 篇文章 3 订阅

订阅专栏

复现环境: buuoj.cn



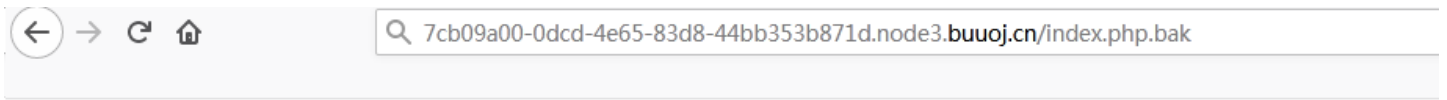
7cb09a00-0dcd-4e65-83d8-44bb353b871d.node3.buojj.cn

Try to find out source file!

提示说需要找到源码

扫了一把没扫到, 最开始没看到扫描的结果, 后面手动输入的时候就发现了, 回头去看结果发现没扫出来, 可能哪里出问题了。

```
[03:34:36] 429 - 568B - /index.PHP
[03:34:36] 429 - 568B - /index.php-bak
[03:34:36] 429 - 568B - /index.php.bak
[03:34:36] 429 - 568B - /index.php/login/
[03:34:36] 429 - 568B - /index.php3
[03:34:36] 429 - 568B - /index.php4
[03:34:36] 429 - 568B - /index.php5
[03:34:36] 429 - 568B - /index.php~
[03:34:36] 429 - 568B - /index.rar
[03:34:37] 429 - 568B - /index.save
[03:34:37] 429 - 568B - /index.shtml
[03:34:37] 429 - 568B - /index.tar.bz2
```



Try to find out source file!



分析一下源码

```
<?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!";
}
```

key的值需要等于str的值，有两个等于号，php弱类型绕过，输入123得flag



7cb09a00-0dcd-4e65-83d8-44bb353b871d.node3.buuoj.cn/?key=123

flag{adb0bae7-6a58-4298-ad62-06481487fe22}