

# [ACTF2020 新生赛] BackupFile

原创

[\[已注销\]](#) 于 2021-04-19 13:57:48 发布 34 收藏

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/weixin\\_55776335/article/details/115829801](https://blog.csdn.net/weixin_55776335/article/details/115829801)

版权

1.打开后提示我们找源码，打开F12发现什么都没有，根据题目提示应该是备份文件泄露



2.用dirsearch进行目录扫描发现index.php.bak打开看一下。

```
[15:06:54] Starting:
[15:07:01] 503 - 596B - /www.tar
[15:07:01] 503 - 596B - /web.7z
[15:07:01] 503 - 596B - /web.zip
[15:07:01] 503 - 596B - /web.rar
[15:07:01] 503 - 596B - /index.php
[15:07:01] 503 - 596B - /index.php.~
[15:07:01] 503 - 596B - /web.tar.gz
[15:07:01] 200 - 347B - /index.php.bak
[15:07:01] 503 - 596B - http://blog.csdn.net/weixin_55776335
```

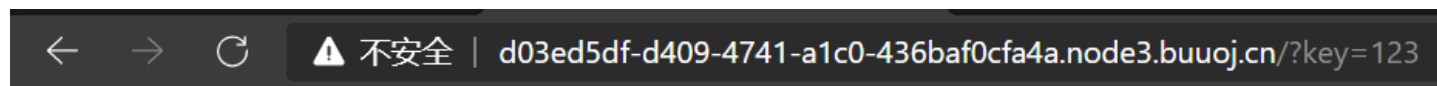
3.发现是个php代码。

```
<?php
include_once "flag.php"; // 包含flag文件

if(isset($_GET['key'])) // 检测变量是否设置
    $key = $_GET['key']; // 获取key
    if(!is_numeric($key)) // 判断key是否为数值或数字字符串
        exit("Just num!"); // 不是则退出脚本
    }
    $key = intval($key); // 获取变量整数数值
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) // 判断key与str的值是否相等
        echo $flag; // 条件成立输出flag
    }
}
else {
    echo "Try to find out source file!";
}
?>
```

4.int和string无法直接比较，php会将string转换成int，然后再进行比较，转换会自动将第一个字符串出现之后的内容除去，即将str转换成了123。

5.传参url/?key=123获得flag。



flag{cade7d95-6d47-4548-8b46-4a5d50669b22}