[ACTF2020 新生赛]BackupFile

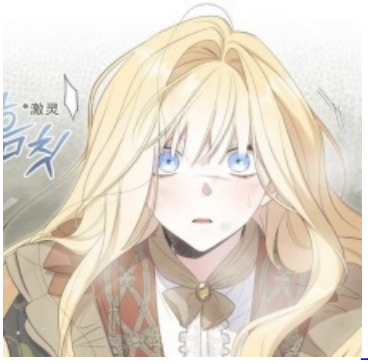
原创

没事就逛博客 已于 2022-04-17 22:15:15 修改 283 收藏

分类专栏： CTF题目笔记 文章标签： web安全

于 2022-04-16 16:07:06 首次发布

本文链接：https://blog.csdn.net/weixin_52116519/article/details/124214994



CTF题目笔记 专栏收录该内容

34 篇文章 0 订阅

订阅专栏

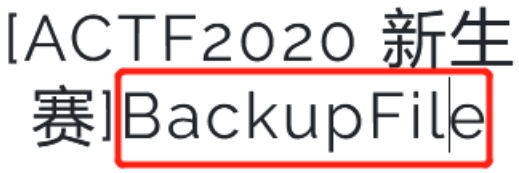
1、找源码，啥也无。

Try to find out source file!

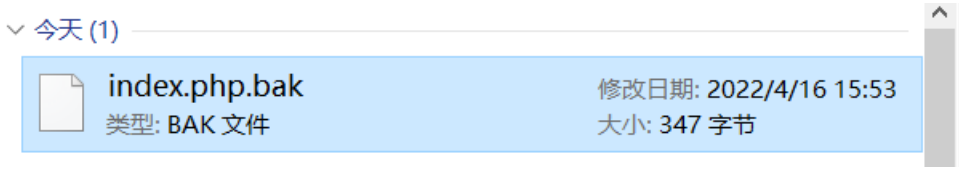
2、扫它，有点慢。

```
[+] Load dict:D:\software\CTFtools\dirmap-master\data\dict_mode_dict.txt
[*] Use crawl mode
[200][application/octet-stream][347.00b] http://1952ea7a-3a40-4a29-a6fe-3f961a507e3d.node4.buuoj.cn:81/index.php.bak
 94% (5418 of 5716) |############################################################    | Elapsed Time: 0:04:24 ETA:   0:00:36
```

3、我看到题目是备份，我也想到了`/index.php.bak`



4、还真有，下载看源码。



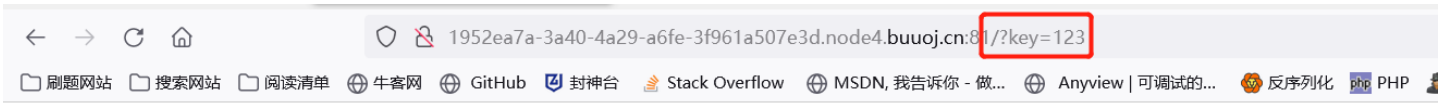
5、传入key，首先判断key是否为数字或者数字字符。然后对key取整。最后判断key和str是否相等。这里存在弱比较漏洞。
原理：如果key为数字时，在做==比较时，str字符串自动变为数字，即str=123。

> is_numeric () 函数用于检测变量是否为数字或数字字符串。
> intval() 函数用于获取变量的整数值。

```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!";
}
```


6、得到flag



flag{2accf77a-cb41-40c5-90dd-fdd86e5c2d34}