

[ACTF2020 新生赛]BackupFile 1

原创

菜菜zhao 于 2022-04-07 00:25:38 发布 50 收藏

分类专栏: [CTF-web](#) 文章标签: [php](#)

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_53146913/article/details/124003772

版权



[CTF-web 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

知识点1: 备份文件

常见的备份文件后缀名有 .git .svn .swp .~ .bak .bash_history

于是用dirsearch扫描目录

```
10:40:10] 200 - 347B - /index.php.bak
10:40:10] 429 - 568B - /install.htm
```

看到bak的后缀(或者一个一个试一试),

下载后出现源码:

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

```
?>
```

CSDN @菜菜zhao

知识点二: php弱比较

php中 “==” 两个等于号就是弱比较。

弱比较：如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换成数值并且比较按照数值来进行，在比较时该字符串的开始部分决定了它的值，如果该字符串以合法的数值开始，则使用该数值，否则其值为0。所以直接传入key=123就行。

参考链接：[php 弱类型总结 - Mrsm1th - 博客园](#)