

BUUCTF-[ACTF2020 新生赛]BackupFile1

原创

[Monica](#) 于 2021-10-05 23:22:11 发布 699 收藏 1

分类专栏: [BUUCTF](#) 文章标签: [安全漏洞](#) [网络安全](#) [信息安全](#)

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/qq_46918279/article/details/120619373

版权



[BUUCTF 专栏收录该内容](#)

20 篇文章 1 订阅

订阅专栏

目录

题目

分析

知识点

方法

题目

Try to find out source file!

CSDN @_Monica_

分析

除了题目说尝试找到源文件外找不到其他的提示, 猜测应该是找子目录

用dirsearch扫描目录

扫出来/index.php.bak

bak是备份文件的扩展名

访问url/index.php.bak,并下载

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!";
}
```

知识点

[is_numeric\(\)](#) 检测变量是否为数字或数字字符串

[intval\(\)](#):获取变量的整数值

[PHP: intval - Manual](#)

[PHP intval\(\) 函数 | 菜鸟教程](#)

[PHP弱比较](#)

简单的代码审计

要求我们GET传入key，key只能为数字否则会执行exit("Just num!"), 截取key的整数部分，如果==\$str那么就会输出\$flag

注意这里使用的是==而不是===，那么就是一个简单的弱比较问题

所以我们只需要传入key=123即可。

方法

flag{210d317f-956f-434a-94b1-688490d21638}

DevTools is now available in Chinese! [Always match Chrome's language](#) [Switch DevTools to Chinese](#) [Don't show again](#)

Elements Console Sources Network Performance Memory Application Security Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASH

URL
<http://250ed8c3-8d1a-4cae-827e-03f16a189632.node4.buuoj.cn:81/?key=123>