

buu web: [ACTF2020 新生赛]BackupFile (源码泄漏+PHP弱类型)

原创

[m0_55378150](#) 已于 2022-04-18 14:23:01 修改 1042 收藏

分类专栏: [buuctf](#) 文章标签: [web安全](#)

于 2022-04-18 14:18:03 首次发布

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/m0_55378150/article/details/124247695

版权



[buuctf](#) 专栏收录该内容

20 篇文章 0 订阅

订阅专栏

打开靶场



93c6fb2b-f451-438b-80c1-e820349a74c7.node4.buuoj.cn:81

Try to find out source file!

CSDN @m0_55378150

让我们找源文件, 右键源代码里啥都没有, 那就拿扫描器扫一下 (但是buu有防扫机制, 我线程开多低都扫不出来, 只能去看看别人的扫描结果), 扫到一个index.php.bak, 下载下来将后缀改成txt看一下, 发现是index.php的源码

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

可以看到，传入的key参数值需要通过两个函数

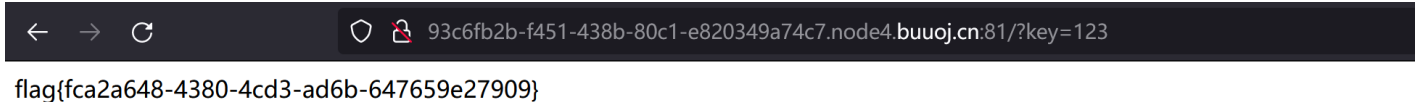
is_numeric(): 用于检测变量是否为数字或数字字符串

intval(): 函数用于获取变量的整数值

所以我们只能传入数字并且会被转换成整数值，然后拿去和str变量做比较，如果相等，就输出flag

这里的比较是一个弱类型（不知道的可以先去百度一下），所以我们key的值只要为123就行了

payload为?key=123



CSDN @m0_55378150

成功!