BUUCTF之[ACTF2020 新生赛]BackupFile 解题过程

原创

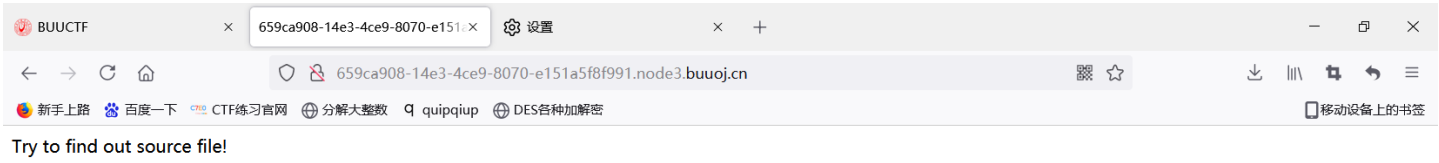
若丶时光破灭 于 2021-06-18 11:53:45 发布 120 收藏

分类专栏： CTF-WEB 文章标签： php web 安全

本文链接：https://blog.csdn.net/weixin_44632787/article/details/118021053

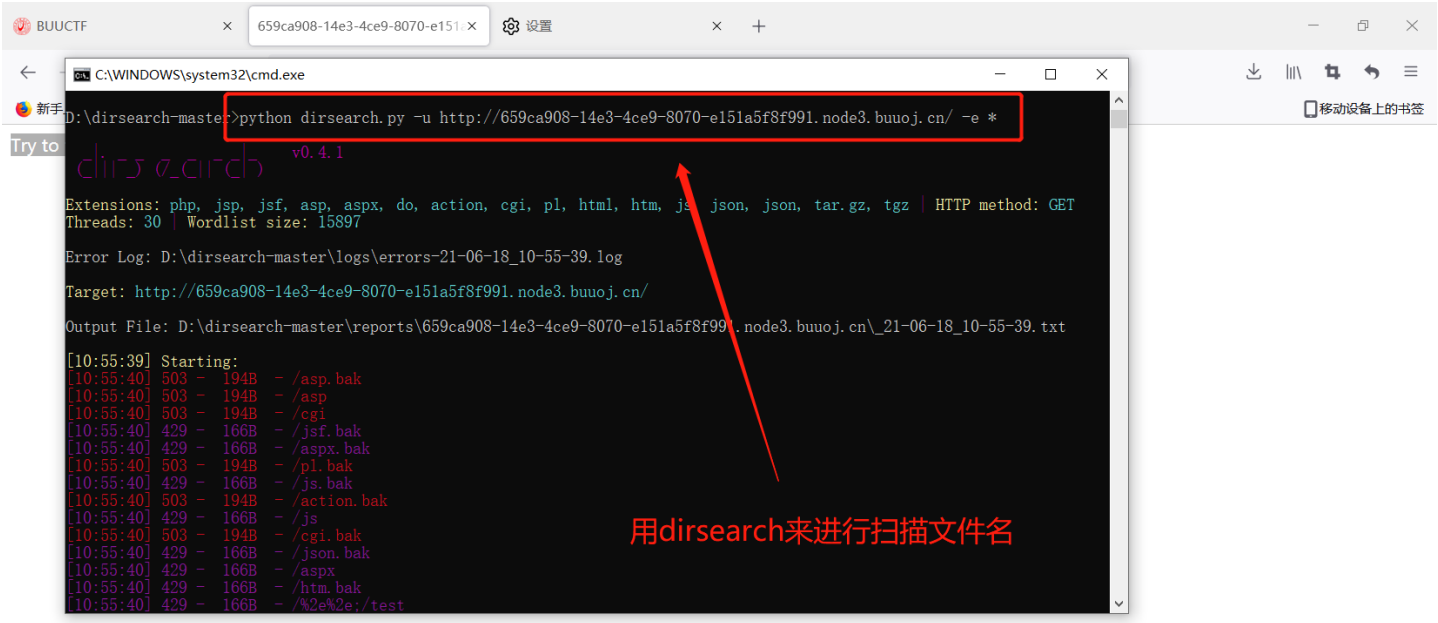
CTF中的BUUCTF之[ACTF2020 新生赛]BackupFile 解题过程

启动我们的挑战项目，发现上面什么都没有。只有一段话：Try to find out source file!

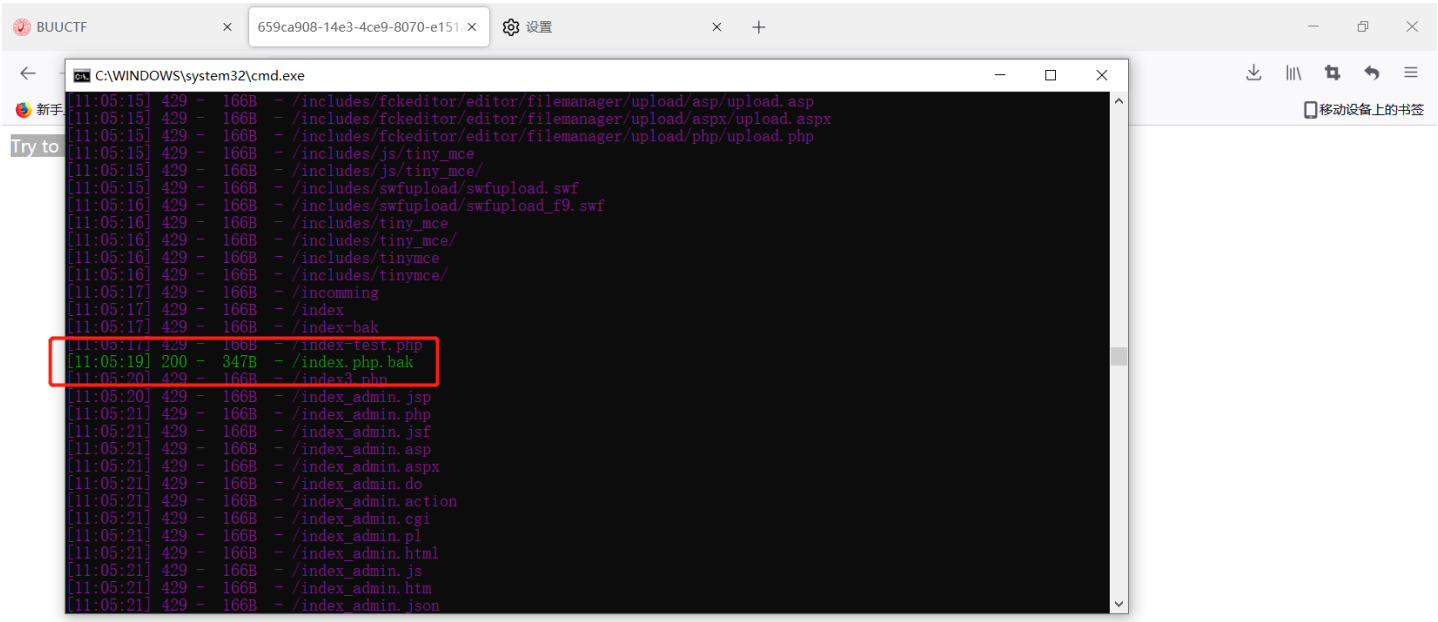


但是，题目有给我们提示说：Backup file，翻译成中文就是备份文件的意思

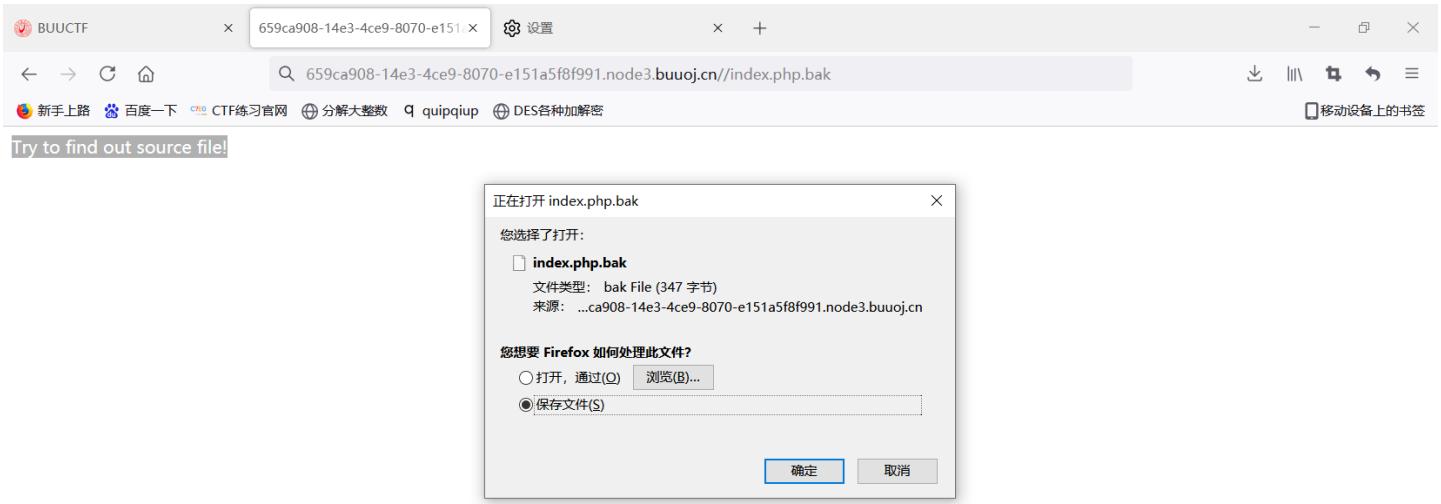
根据做题经验我了解到备份文件名有www.zip还有名为.bak .swp等等。但是因为懒，我就直接用dirsearch来进行扫描了（虽然扫描的时候要花很多时间...）



最终扫描到一个文件名为：/index.php.bak的文件



然后访问这个连接，然后把备份文件下载下来。发现是一个PHP的代码审计



用记事本这样的工具打开便可以看到里面的PHP代码

```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!";
}
```

emmmmmm感觉是弱类型的比较题。主要代码是：

```php
$str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
```

在PHP中：

= = 为弱相等，即当整数和字符串类型相比较时。会先将字符串转化为整数然后再进行比较。比如a=123和b=123admin456进行= =比较时。则b只会截取前面的整数部分。即b转化成123。

所以，这里的a = = b是返回True。

所以这里我们只需要提供一个参数?key=123就可以拿到flag了

flag值