

buuctf—[ACTF2020 新生赛]BackupFile

原创

小常吃不了了 于 2021-11-02 19:16:29 发布 14 收藏

分类专栏: BUUCTF 文章标签: 目录扫描

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_52620919/article/details/121106950

版权

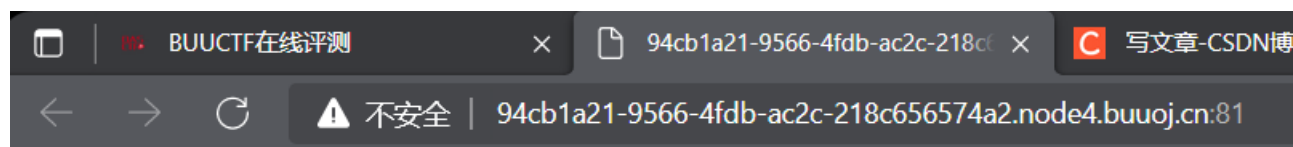


[BUUCTF 专栏收录该内容](#)

37 篇文章 0 订阅

订阅专栏

根据提示, 是备份文件泄露



Try to find out source file!

查找大佬文章, 知道用一个新工具

dirsearch

目录扫描

使用方法:

在dirsearch目录下cmd

然后命令

```
py dirsearch.py -u url地址 -e*
```

```
429 - 568B - /index.old
429 - 568B - /index.orig
429 - 568B - /index.php
429 - 568B - /index.php-bak
429 - 568B - /index.php.bak
```

然后找到index.php.bak文件

删去bak, 打开index.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!";
}
```

得到payload

?key=123

然后得到flag

