

buuctf web [ACTF2020 新生赛]BackupFile

原创

0d@y 于 2020-07-18 21:55:56 发布 733 收藏 2

分类专栏: [buuctf web](#) 文章标签: [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/m0_46412682/article/details/107435701

版权



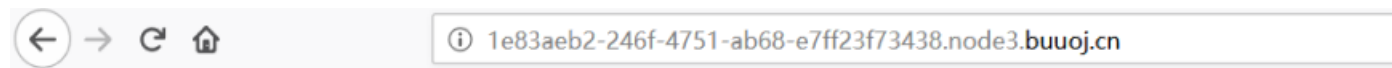
[buuctf web](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

buuctf web [ACTF2020 新生赛]BackupFile

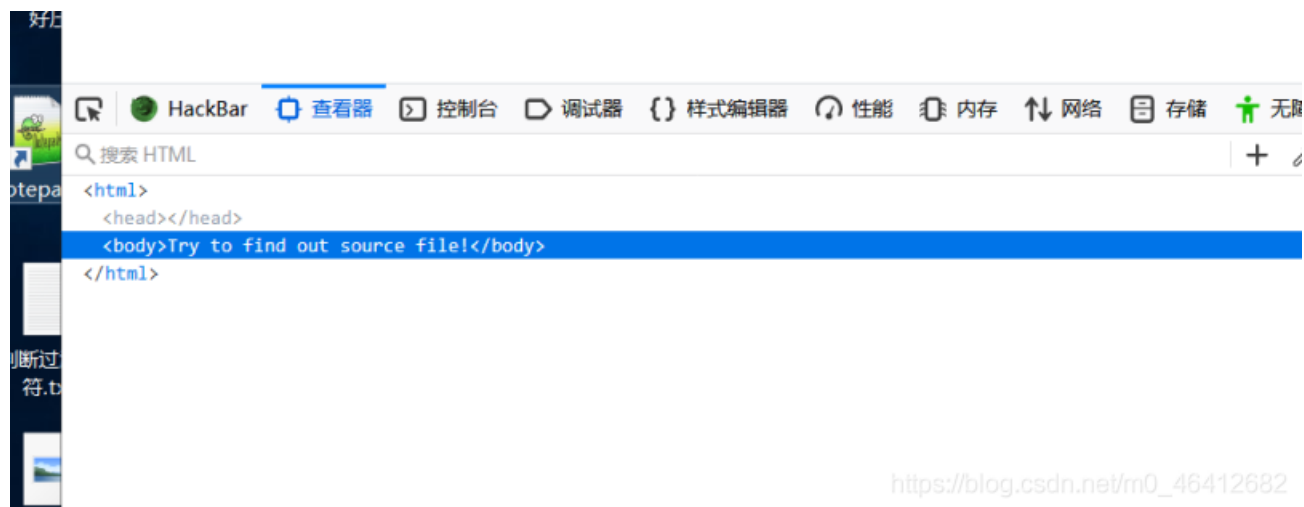
开始的页面



Try to find out source file!

https://blog.csdn.net/m0_46412682

先在源代码中查看有什么信息



https://blog.csdn.net/m0_46412682

啥信息都没有

题目的提示是backupFile备份文件

备份文件一般的后缀名为

.rar

.zip

.7z

.tar.gz

.bak

.swp

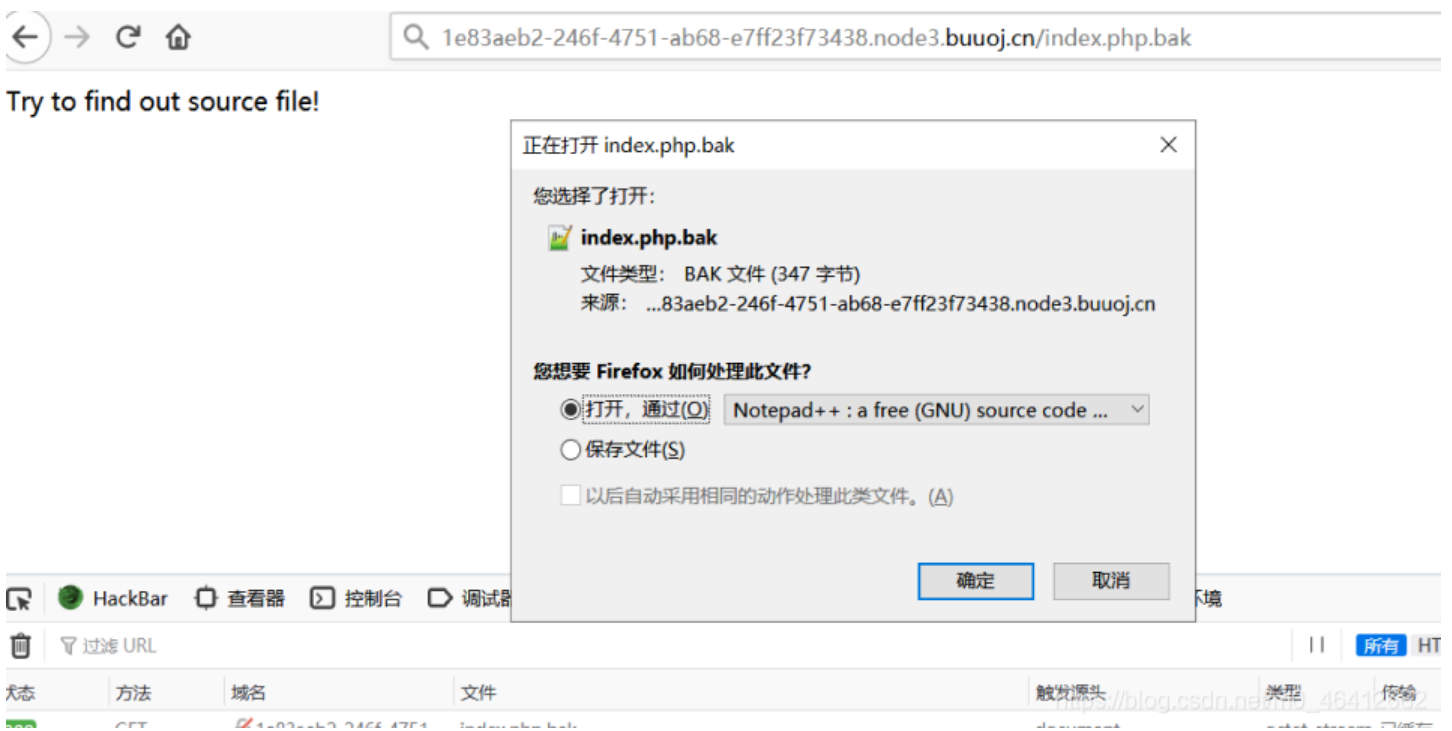
.txt

.html

.bak

这里的备份文件是index.php.bak,可以用dirsearch扫描

链接: [dirsearch](#).



正在打开 index.php.bak

您选择了打开:

index.php.bak
文件类型: BAK 文件 (347 字节)
来源: ...83aeb2-246f-4751-ab68-e7ff23f73438.node3.buuoj.cn

您想要 Firefox 如何处理此文件?

打开, 通过(O) Notepad++ : a free (GNU) source code ...

保存文件(S)

以后自动采用相同的动作处理此类文件。(A)

确定 取消

HackBar 查看器 控制台 调试器

过滤 URL

状态	方法	域名	文件	触发源	类型	传输
成功	GET	1e83aeb2-246f-4751-ab68-e7ff23f73438.node3.buuoj.cn	index.php.bak	document	46412892	已保存

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

PHP的弱类型特性，int和string是无法直接比较的，php会将string转换成int然后再进行比较，转换成int比较时只保留数字，第一个字符串之后的所有内容会被截掉

所以相当于key只要等于123就满足条件了

flag{186a264b-7106-487f-9ec1-4a770a38b080}