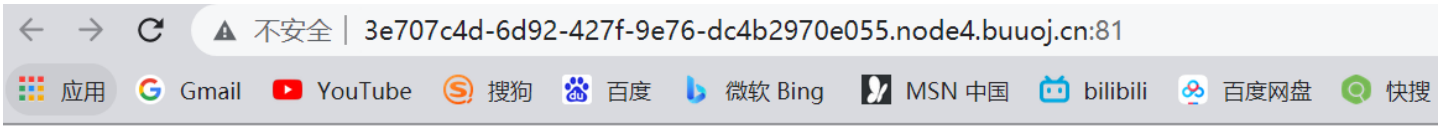
2021-08-06关于[ACTF2020 新生赛]BackupFile 1

原创

1431880277 于 2021-08-08 20:10:54 发布 33 收藏

题目



Try to find out source file!

根据提示，查看网页源码，里面什么都没有

自动换行

```
1 Try to find out source file!
```

应该是备份文件的问题，抓包什么都没发现，看别人的笔记是使用dirsearch（至于为什么使用dirsearch，我不清楚）

```
[17:40:32] 429 -  568B  - /includes/fckeditor/editor/filemanager/upload/asp/upload.asp
[17:40:32] 429 -  568B  - /includes/fckeditor/editor/filemanager/upload/php/upload.php
[17:40:33] 503 -  596B  - /includes/tinymce/
[17:40:40] 200 -  347B  - /index.php.bak
[17:40:44] 503 -  596B  - /install.pgsql.txt
[17:40:44] 429 -  568B  - /install_manifest.txt
[17:40:44] 429 -  568B  - /installation
```

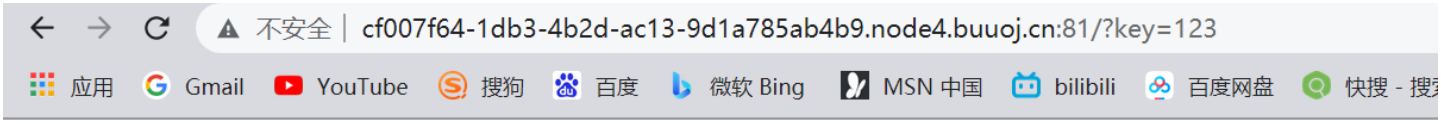
发现index.php.bak文件，下载源码

```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!";
}
```


大概意思就是有一个变量key，如果key=str，就可以输出flag。
=== 是强等于，会先比较变量类型， ==是弱等于，不会比较变量类型。当比较的一方是字符串时，会先把其转换为数字，不能转换为数字的字符串被转换为0。
这里会强制把str转换成int再进行比较，转换后即为123。然后GET请求传参



flag{c46bee89-15cf-416e-8eec-1a7853caaa0b}

得到flag。

补充：

1. 常见的备份文件后缀名有 .git .svn .swp .~ .bak .bash_history .rar .zip .7z .txt .html .tar.gz .old .temp
2. 浅谈“备份文件泄漏”
3. Dirsearch探测Web目录