[ACTF2020 新生赛]BackupFile 1

原创

狼王7号 于 2021-07-30 00:06:23 发布 80 收藏

过程

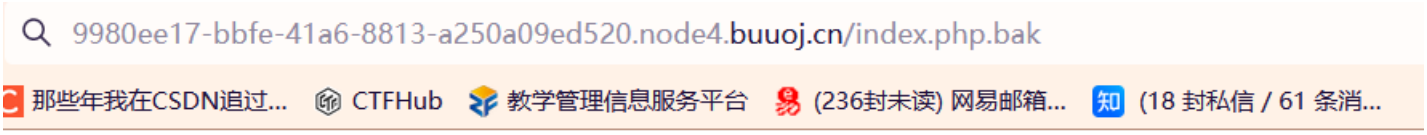
常见的备份文件后缀名有 .git .svn .swp .~ .bak .bash_history

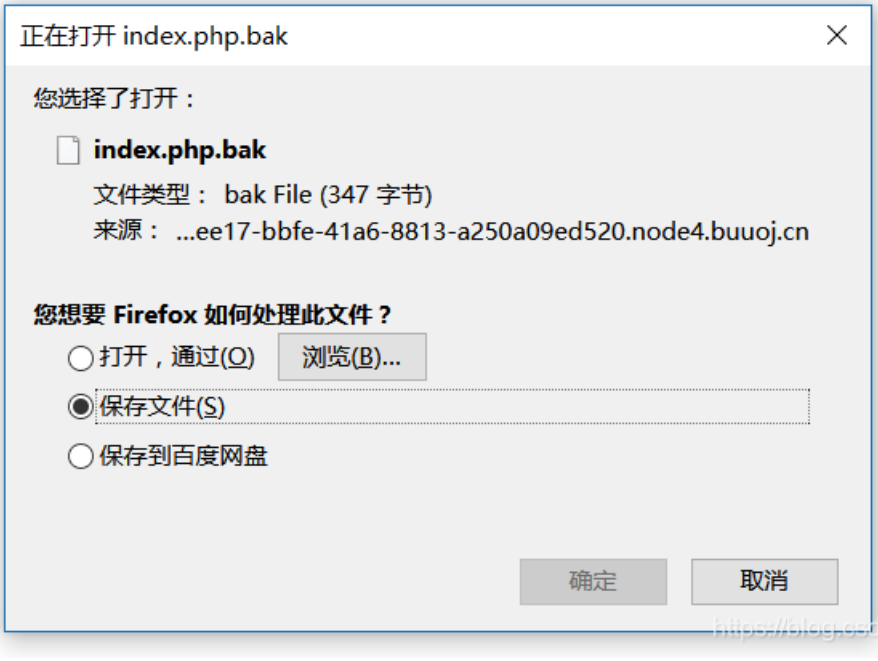
于是用dirsearch扫描目录

```
E:\信息安全\CTF\工具\dirsearch-master>python .\dirsearch.py -u http://9980ee17-bbfe-41a6-8813-a250a09ed520.node4.buuoj.cn/ -e php
E:\信息安全\CTF\工具\dirsearch-master\thirdparty\requests\__init__.py:91: RequestsDependencyWarning: urllib3 (1.26.6) or chardet (4.0.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "

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

Extensions: php | HTTP method: GET | Threads: 20 | Wordlist size: 7085

Error Log: E:\信息安全\CTF\工具\dirsearch-master\logs\errors-21-07-29_22-58-36.log

Target: http://9980ee17-bbfe-41a6-8813-a250a09ed520.node4.buuoj.cn/

Output File: E:\信息安全\CTF\工具\dirsearch-master\reports\9980ee17-bbfe-41a6-8813-a250a09ed520.node4.buuoj.cn\_21-07-29_22-58-37.txt

[22:58:37] Starting:
[22:58:37] 503 -  596B  - /php.tgz
[22:58:37] 503 -  596B  - /%ff
[22:58:37] 200 -   28B  - /php
[22:58:37] 503 -  596B  - /php.tar
[22:58:37] 500 -  576B  - /.LSOverride
[22:58:37] 429 -  568B  - /.aliases
[22:58:37] 429 -  568B  - /.agilekeychain
[22:58:37] 429 -  568B  - /.agilekeychain.zip
[22:58:37] 429 -  568B  - /.angular-cli.json
搜狗拼音输入法 全 :68B  - /.all-contributorsrc
```


发现index.php.bak文件

```
[22:58:51] 429 -  568B  - /index.old
[22:58:51] 429 -  568B  - /index.php.bak
```





下载后发现源码：

```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!";
}
```

简单的弱类型绕过

php中两个等于号是弱等于

取str的123与key进行比较，（弱比较：如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换成数值并且比较按照数值来进行，在比较时该字符串的开始部分决定了它的值，如果该字符串以合法的数值开始，则使用该数值，否则其值为0。所以直接传入key=123就行）

flag{c4f38507-afd7-4c0c-81d3-0dd58636af90}

总结

学习了有关PHP弱类型绕过，网站备份文件的类型与查找，网站敏感信息的查找，Dirsearch工具探测Web目录的方法

链接

【tool】如何使用Dirsearch探测Web目录
php 弱类型总结
[ACTF2020 新生赛]BackupFile 1
白帽子黑客教你：通过dirsearch脚本扫描和收集网站敏感文件实战