

# i春秋 第二届春秋欢乐赛 Hello World

原创

witwitwiter 于 2021-05-07 21:37:01 发布 57 收藏

分类专栏: [CTF](#) 文章标签: [信息安全](#)

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/witwitwiter/article/details/116503260>

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

## i春秋 第二届春秋欢乐赛 Hello World

先使用dirmap扫描

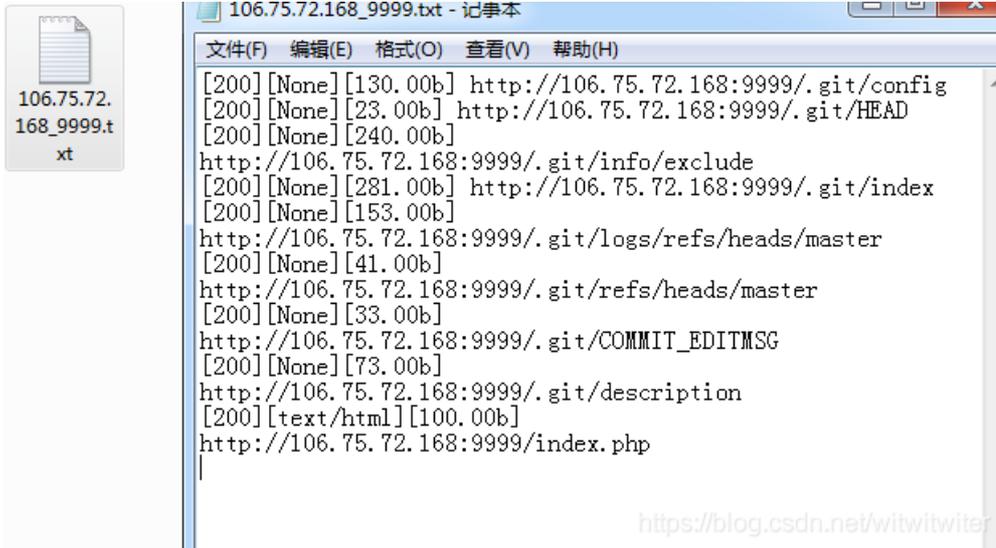
```
C:\Windows\System32\cmd.exe - python3 dirmap.py -lcf -i http://106.75.72.168:9999/
dirmap.py: error: argument -i: expected one argument

C:\Users\Administrator\Downloads\dirmap-master\dirmap-master>python3 dirmap.py -lcf -i http://106.75.72.168:9999/

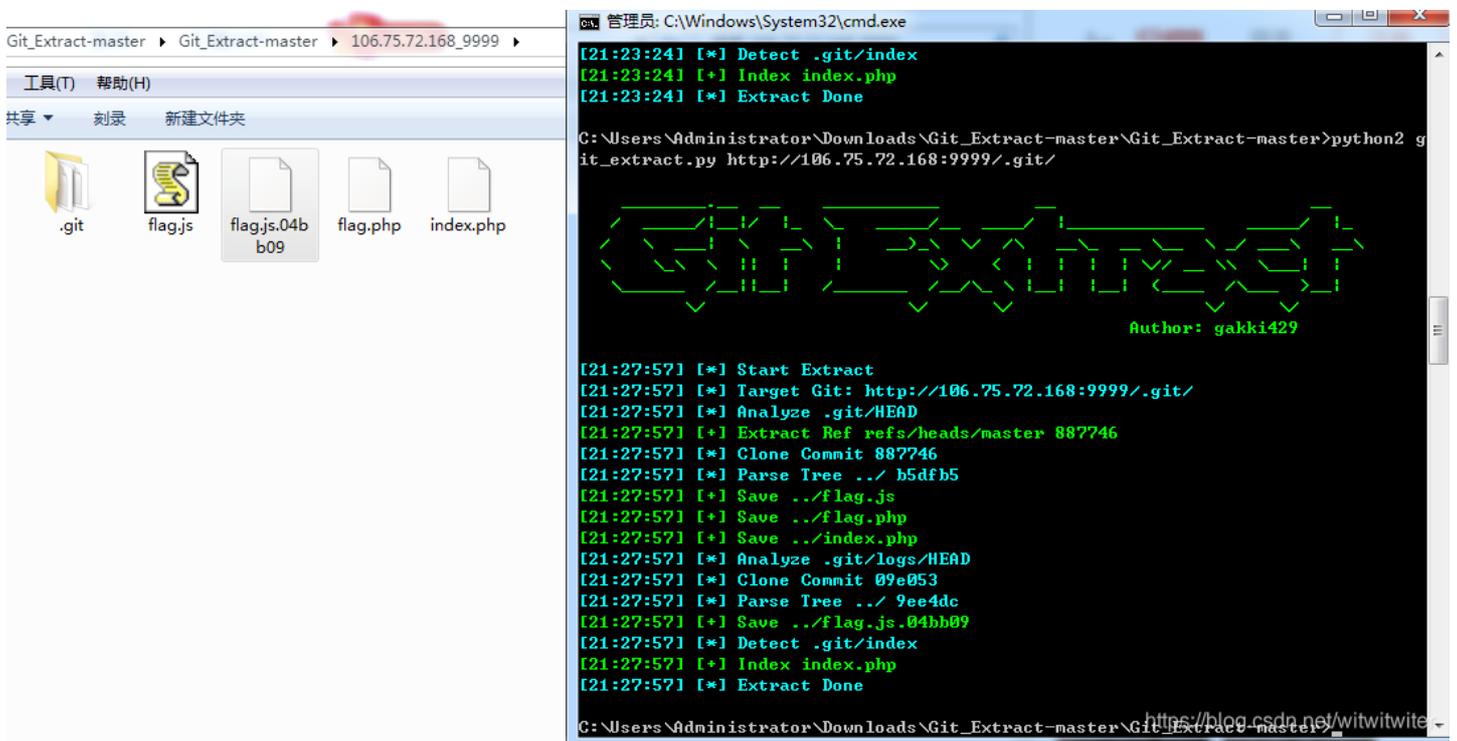
##### # ##### # # ## #####
# # # # # ## ## # # # #
# # # # # # # # # # # # #
# # # ##### # # ##### #####
# # # # # # # # # # # #
##### # # # # # # # # v1.0

[*] 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/eoivedsgteiaadrthqvehkuwgqixsghmgdunrqwic
[*] Use recursive scan: No
[*] Use dict mode
[+] Load dict:C:\Users\Administrator\Downloads\dirmap-master\dirmap-master\data\dict_mode_dict.txt
[*] Use crawl mode
[200][None][130.00b] http://106.75.72.168:9999/.git/config
[200][None][23.00b] http://106.75.72.168:9999/.git/HEAD
[200][None][240.00b] http://106.75.72.168:9999/.git/info/exclude
[200][None][281.00b] http://106.75.72.168:9999/.git/index
[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][None][33.00b] http://106.75.72.168:9999/.git/COMMIT_EDITMSG
[200][None][73.00b] http://106.75.72.168:9999/.git/description
20% <1181 of 5768> !#### ! Elapsed Time: 0:00:45 ETA: 0:02:48

https://blog.csdn.net/witwitwiter
```



发现git源码泄露，故使用Git\_Extract-master将泄露的文件下载下来



发现两个flag.js文件，将其放在一起对比

在kali中使用diff命令进行对比

```
(root@kali)-[~]
└─# diff flag.js flag.js.04bb09
220c220
<     BufferedBlockAlgorithm=o
---
>     BufferedBlockAlgorithm=f
256c256
<     c=n/(4*o),c=e           ?t.ceil(c):
---
>     c=n/(4*o),c=e           ?t.cell(c):
297c297
<     _append                 (t)
---
>     _ppend                  (t)
334c334
<     }; return r             }(Math);(
---
>     }; return g             }(Math);(
377c377
<     (n)                     ,-1≠n    86      (r=n
---
>     (n)                     ,-1≠n    86      {r=n
410c410
<     (t)                     ,e,
---
>     (t)                     ,8,
431c431
<     return(t <<             o|t >>>32-o    )+e}
---
>     return(t <<             o|t >>>3-o    )+e}
454c454
<     ,s=0                    .algo    ,f=    [],
---
https://blog.csdn.net/witwitwiter
```

字符选取的规则:

- 1.不同的字符按下面的（比如第一个o和f，就选择下面的f）
- 2.两行中多出的字符（比如第三处不同，第一个append比下面的ppend多一个a，就选择a）

得到的flag为

flag{82efc37f1cd5d4636ea7cadcd5a814a2}

## 总结

先用dirmap扫描，得到是git泄露之后使用Git\_Extract-master将文件下载下来进行分析，对比两个不同的flag.js得出flag。