CTFHub信息泄露WriteUP

原创

TaibaiXX1 于 2021-05-28 12:07:00 发布 139 收藏
文章标签： git github css svn 编程语言

本文链接：https://blog.csdn.net/tangshuangsss/article/details/117377122

点击"仙网攻城狮”关注我们哦~

不当想研发的渗透人不是好运维 

让我们每天进步一点点

简介

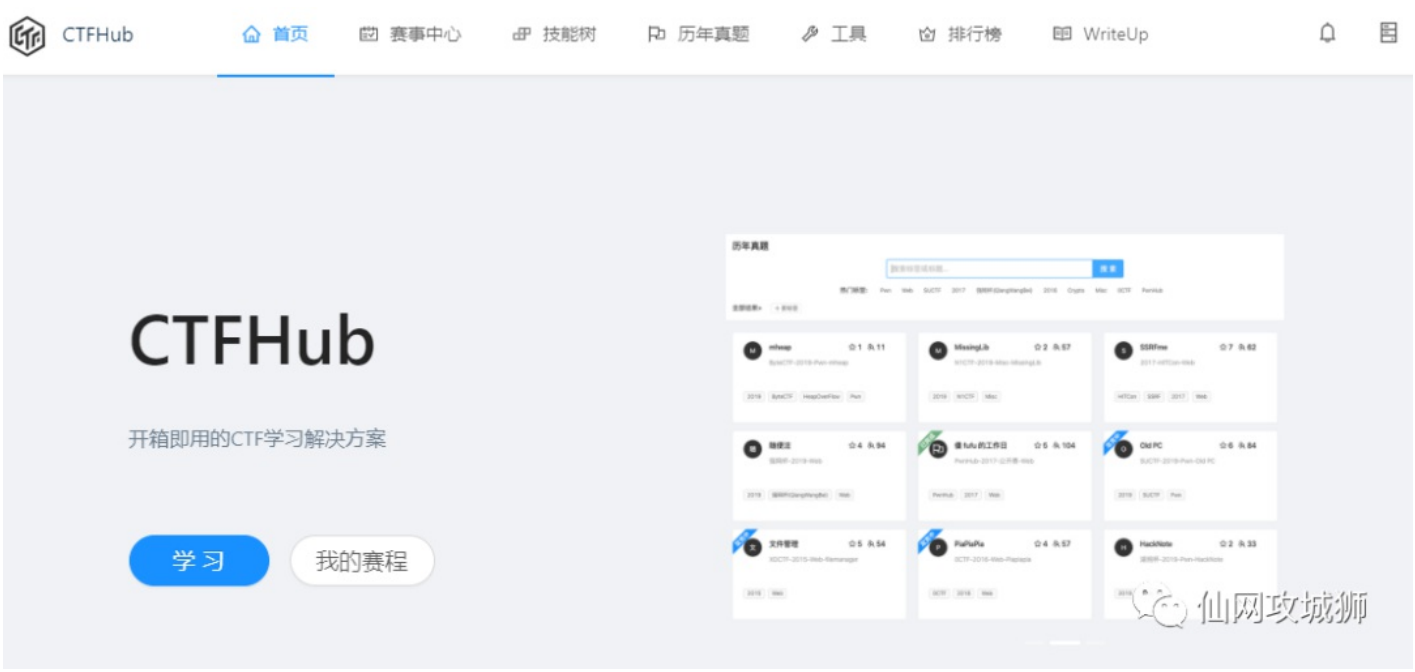
CTFHub 为网络安全工程师提供网络安全攻防技能培训、实战、技能提升等服务。

「赛事中心」提供全网最全最新的 CTF 赛事信息，关注赛事定制自己专属的比赛日历吧。

「技能树」提供清晰的 CTF 学习路线，想要变强就加点，哪里不会点哪里。

「历年真题」提供无限次赛后复盘，边学边练。

「工具」提供各类常用工具，打仗没有一把趁手的武器怎么行。



实战

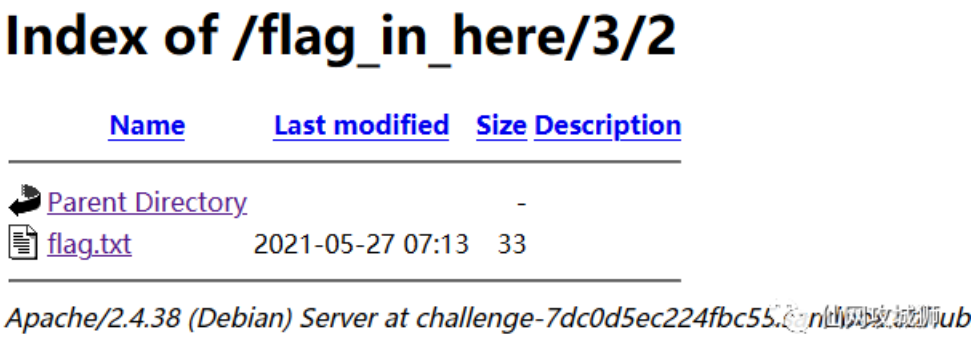
下面内容将为大家讲解信息泄露常见的六种类型

一、目录遍历

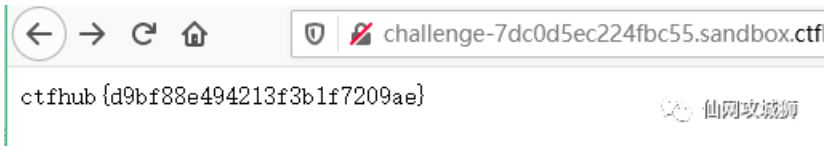
1.点击目录遍历题目后会给一个连接，点开连接就是下面界面，

2.点击开始寻找后出现4个目录，注意每个目录下面还有4个目录。

3.挨个点击后找到flag.txt



4.点击flag.txt后出现flag。

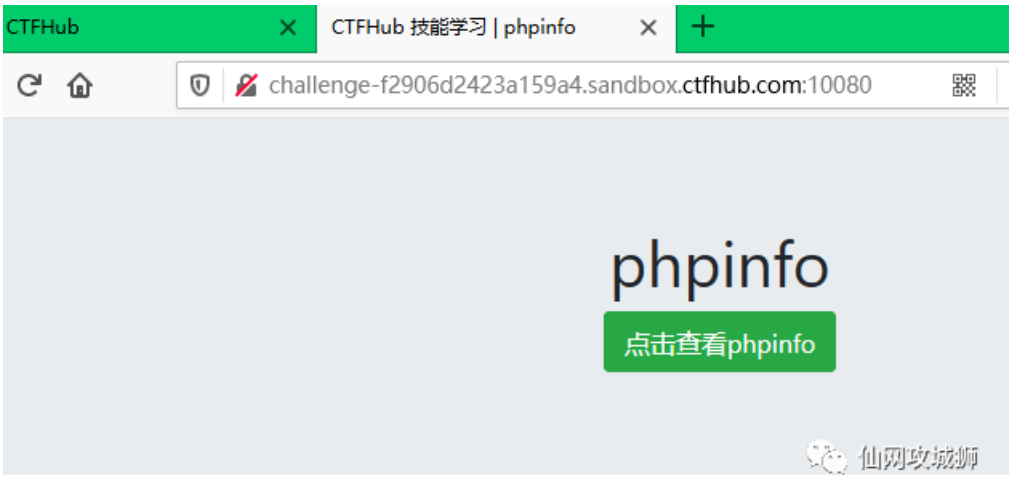


5.把上面flag复制提交完成。

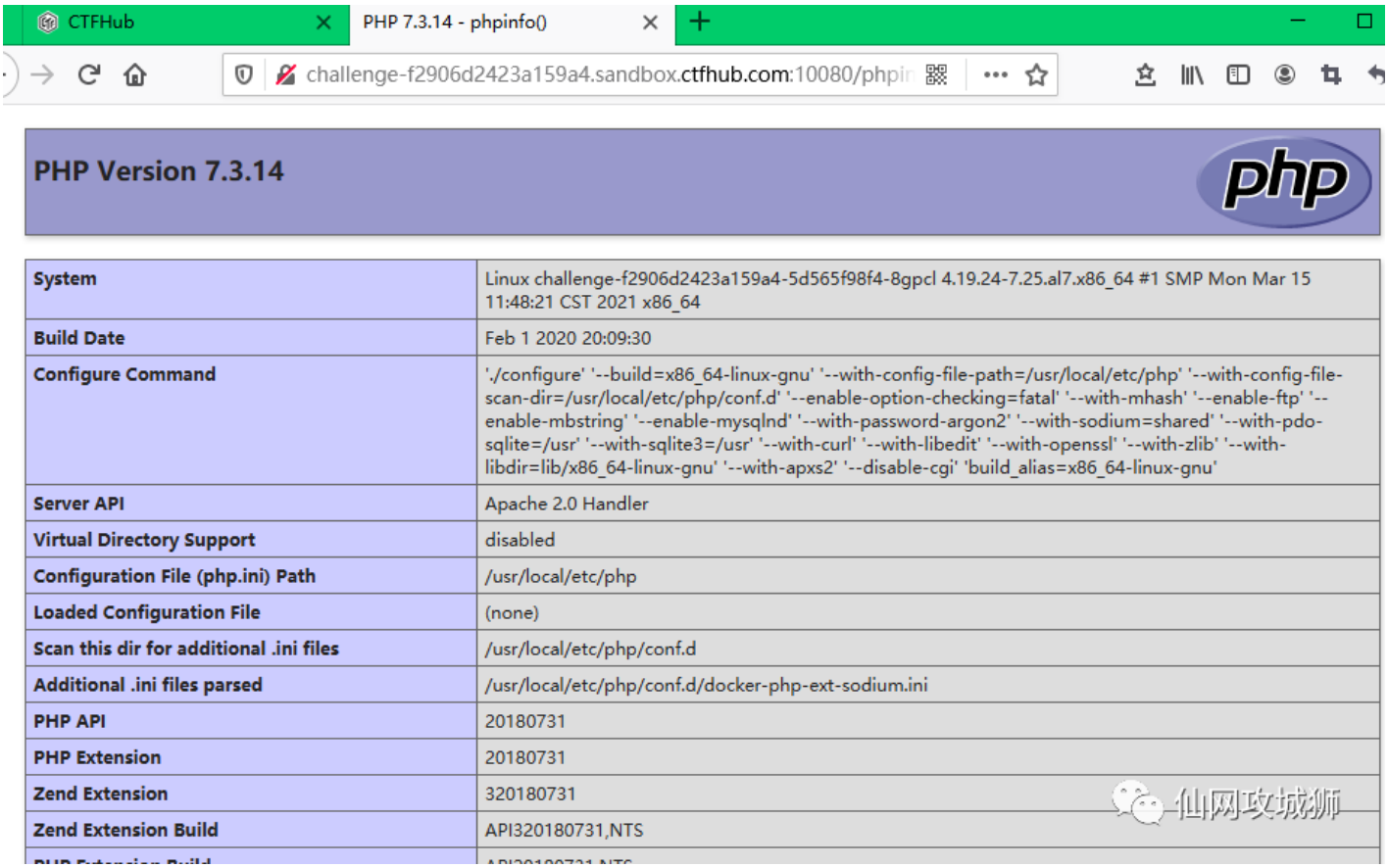
二、PHPINFO

1.点击启动

2.访问url



3.点击查看



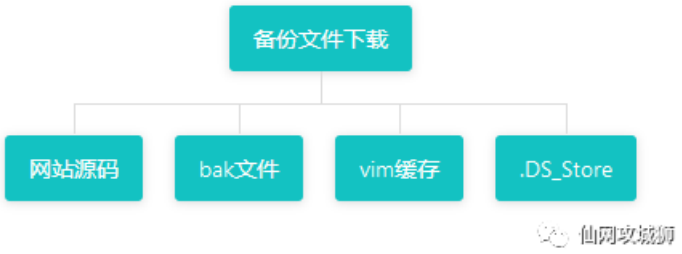
4.接着往下翻啊翻就找到了flag

Environment

Variable	Value
APACHE_RUN_DIR	/var/run/apache2
APACHE_PID_FILE	/var/run/apache2/apache2.pid
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
APACHE_LOCK_DIR	/var/lock/apache2
LANG	C
APACHE_RUN_USER	www-data
APACHE_RUN_GROUP	www-data
APACHE_LOG_DIR	/var/log/apache2
PWD	/
FLAG	ctfhub{2806d0770b0e5e195eb8e71f}

5.复制提交完成

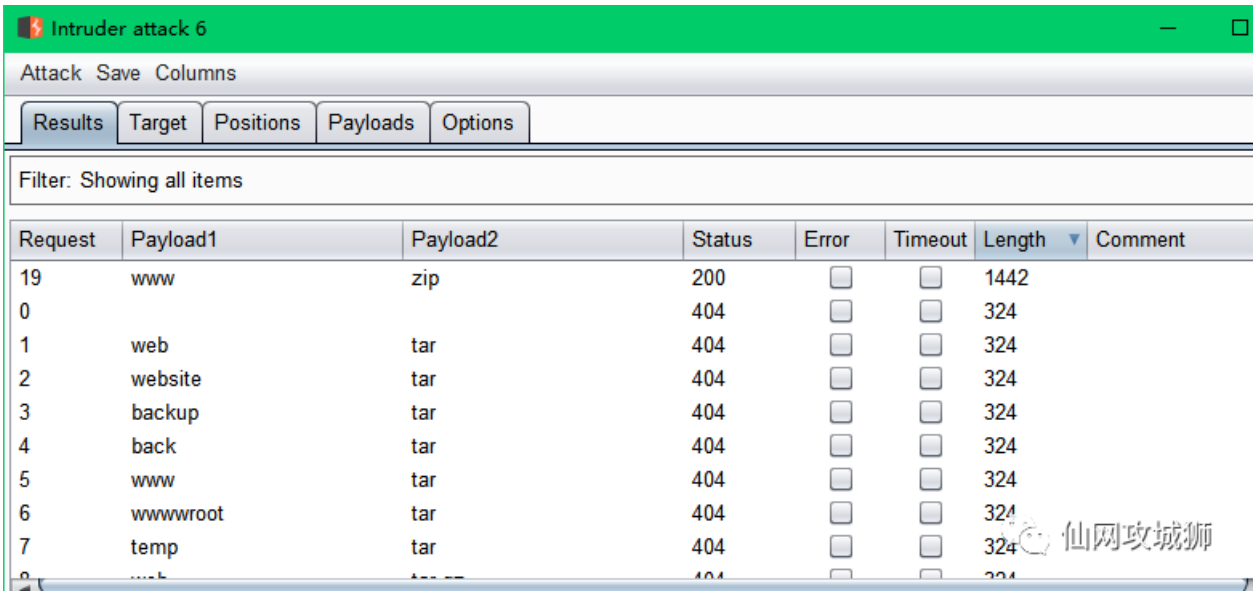
三、备份文件下载



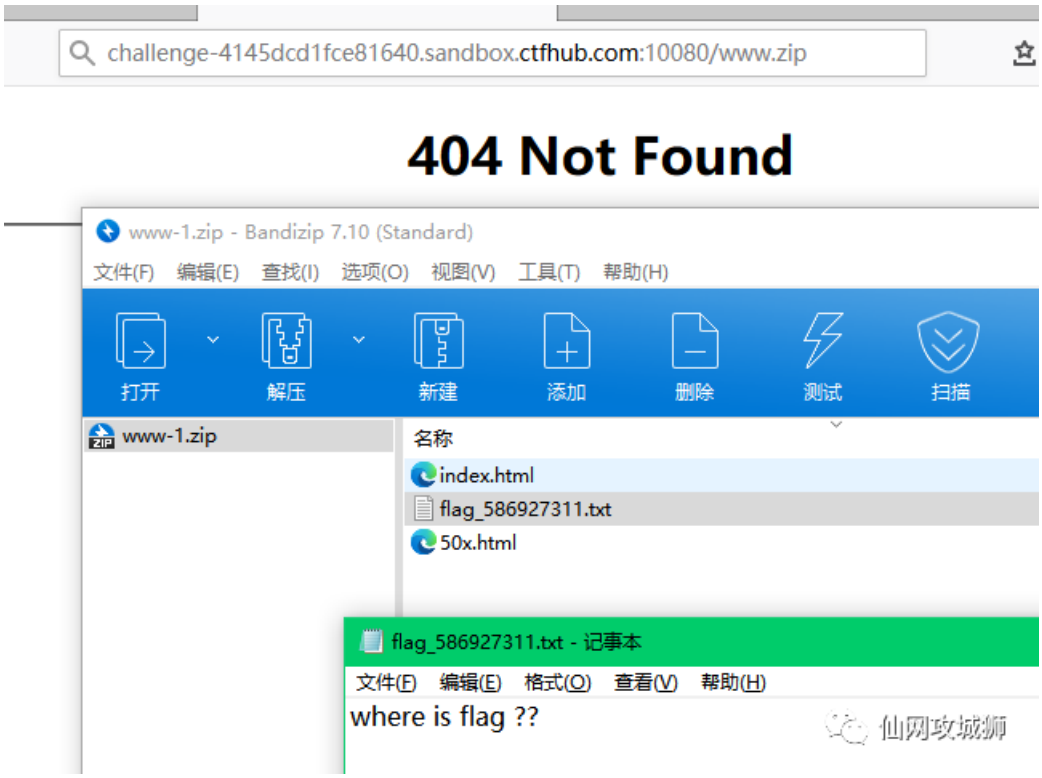
1..就写一个吧，大同小异，开启

2.点击连接后出现说明，只需在url后面构造即可。

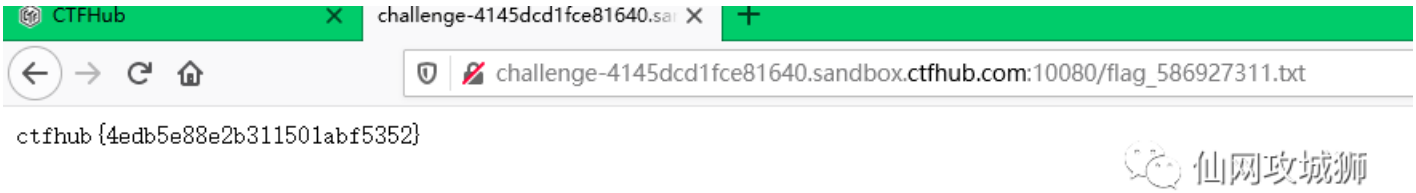
3.如果觉得麻烦就用burpsutie跑一波。



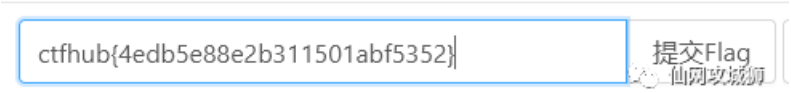
4.右键复制访问获取zip源码找到flag.txt 这里作者有点皮啊，居然是个假的



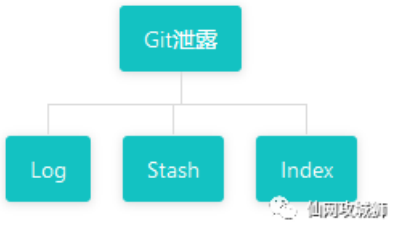
5.直接访问flag_586927311.txt获得flag，想不开的可能会在这卡一会。



6.复制提交flag



四、Git泄露



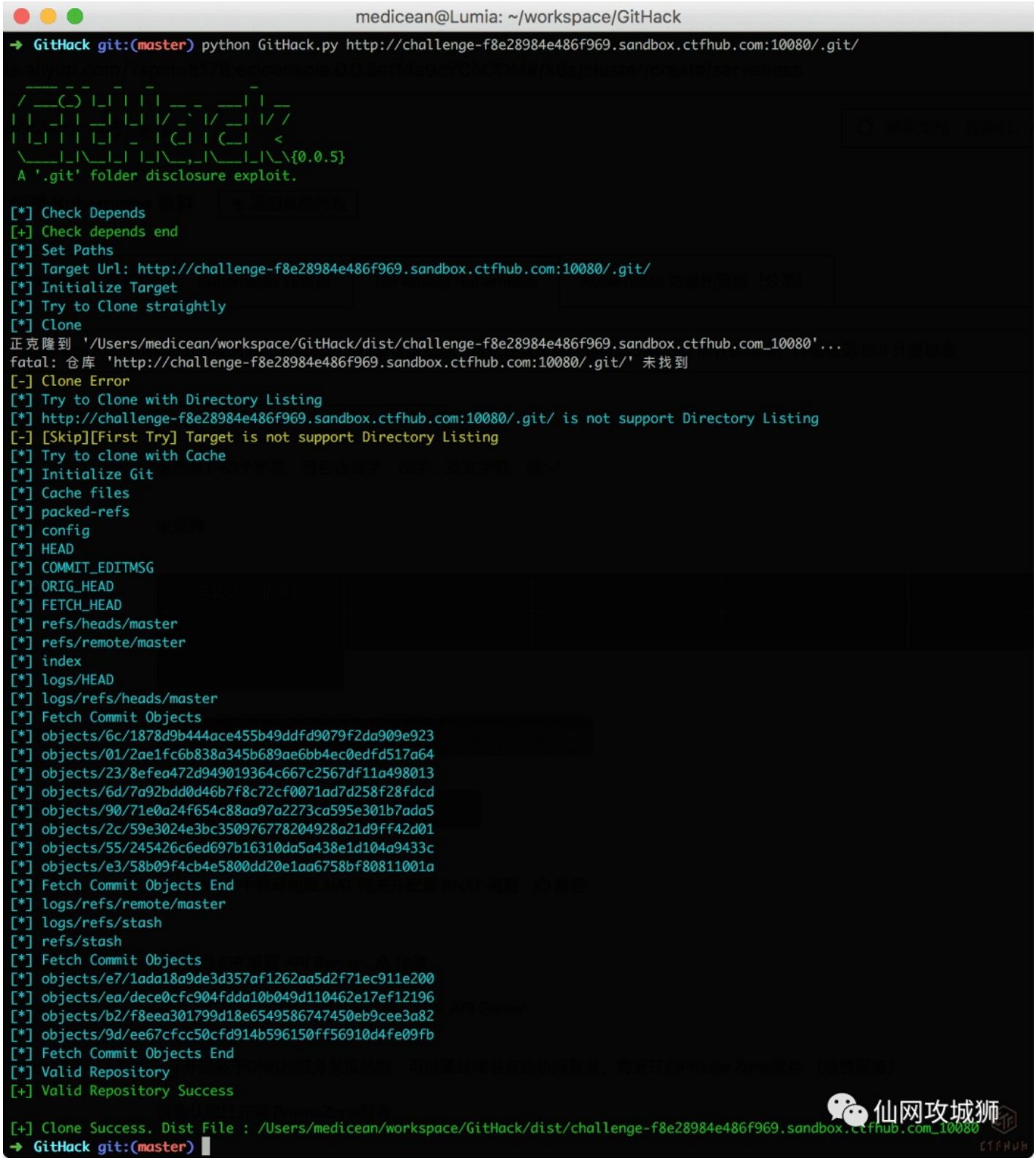
1.stash走一波，这个难度高一点。

2.尝试访问敏感目录发现有

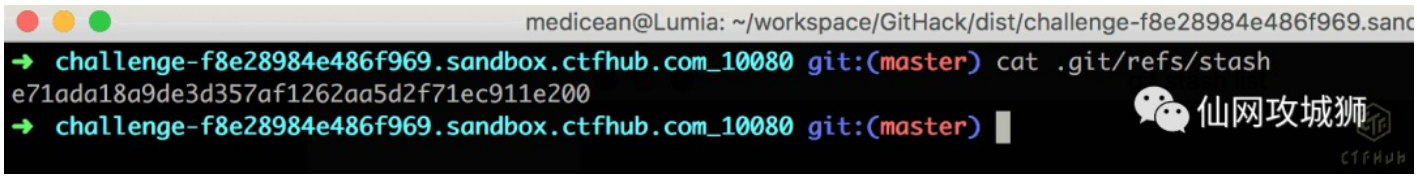
3.工具下载

```
git clone https://github.com/lijiejie/GitHack.git
```

4.利用 GitHack 工具将网站源代码 clone 到本地



5.查看 .git/refs/stash 找到 stash 对应的 hash



6.git diff e71ada 即可看到 flag

7.复制提交flag

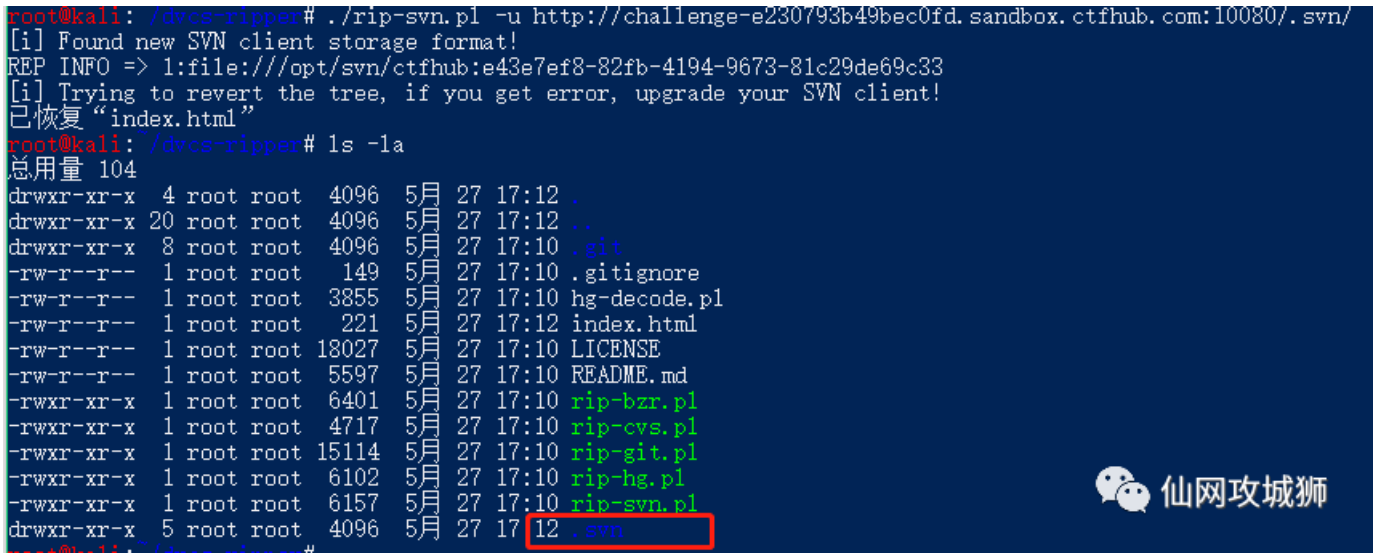
五、SVN泄露

1.点击开启

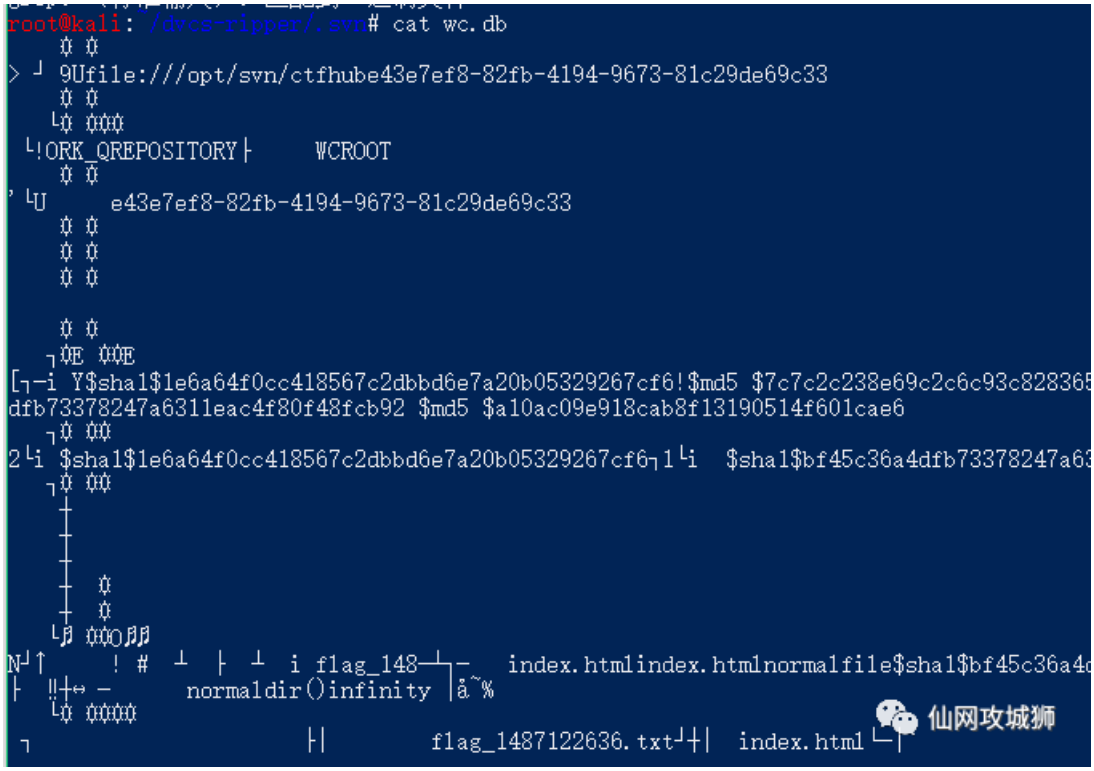
2.工具下载

```
git clone https://github.com/kost/dvcs-ripper.git
```

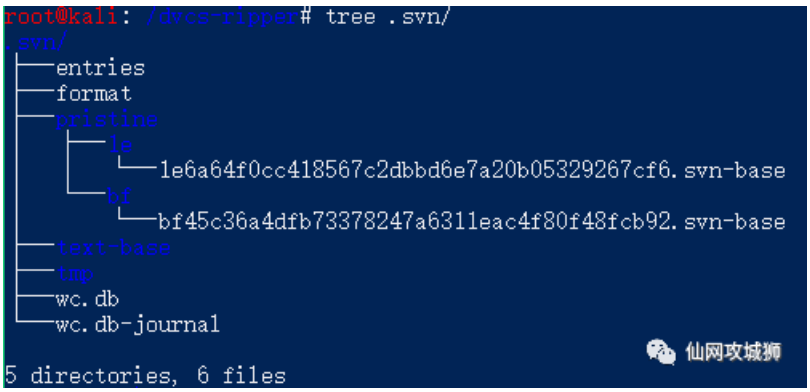
3.使用 dvcs-ripper 工具中的 rip-svn.pl 脚本进行 clone.

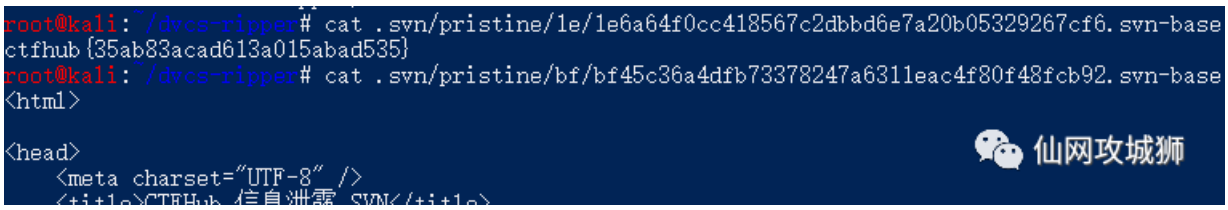


4.从 wc.db 中找到 flag 的文件的文件名, 尝试访问结果发现被删除了。皮

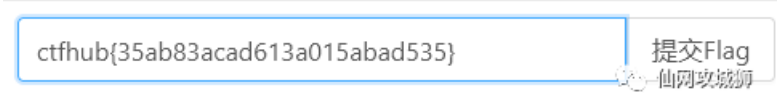


5.查找转而寻找 .svn/pristine/ 中的文件，找到 flag





6.复制提交flag



六、HG泄露

1.点击开启

2.扫描发现有 .hg/ 目录，确认是 .hg 泄露。使用 dvcs-ripper 工具中的 rip-hg.pl 脚本进行 clone.

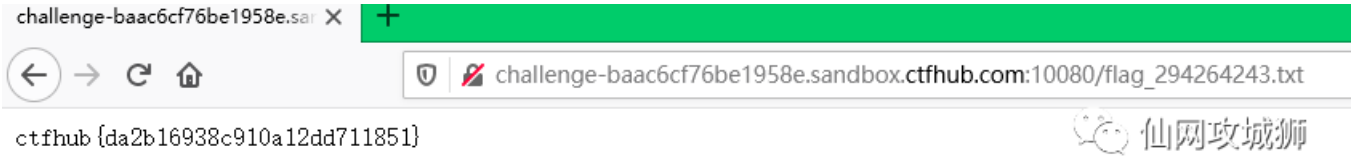
```
root@kali: /dvcs-ripper# ls
hg-decode.pl  index.html  LICENSE  README.md  rip-bzr.pl  rip-cvs.pl  rip-git.pl  rip-hg.pl  rip-svn.pl
root@kali: /dvcs-ripper# ./rip-hg.pl -u -v http://challenge-baac6cf76be1958e.sandbox.ctfhub.com:10080/.hg/
[i] Getting correct 404 responses
[i] Finished (0 of 42)
root@kali:~/dvcs-ripper# ls -la
总用量 108
drwxr-xr-x  5 root root  4096  5月 28 09:32 .
drwxr-xr-x 20 root root  4096  5月 27 17:12 ..
drwxr-xr-x  8 root root  4096  5月 27 17:10 .git
-rw-r--r--  1 root root   149  5月 27 17:10 .gitignore
drwxr-xr-x  4 root root  4096  5月 28 09:32 .hg
-rw-r--r--  1 root root  3855  5月 27 17:10 hg-decode.pl
-rw-r--r--  1 root root   221  5月 27 17:12 index.html
-rw-r--r--  1 root root 18027  5月 27 17:10 LICENSE
-rw-r--r--  1 root root  5597  5月 27 17:10 README.md
-rwxr-xr-x  1 root root  6401  5月 27 17:10 rip-bzr.pl
-rwxr-xr-x  1 root root  4717  5月 27 17:10 rip-cvs.pl
-rwxr-xr-x  1 root root 15114  5月 27 17:10 rip-git.pl
-rwxr-xr-x  1 root root  6102  5月 27 17:10 rip-hg.pl
-rwxr-xr-x  1 root root  6157  5月 27 17:10 rip-svn.pl
drwxr-xr-x  5 root root  4096  5月 27 17:12 .svn
root@kali:~/dvcs-ripper#
```


3.查找flag，tree和find命令进行搜索，发现flag_txt。

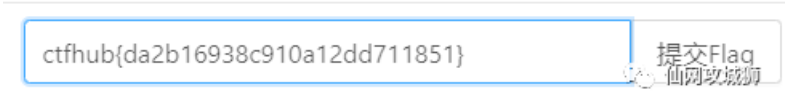
```
root@kali:~/dvcs-ripper# tree .hg
.hg
├── 00changelog.i
├── cache
│   ├── checkisexec
│   ├── checklink -> checklink-target
│   ├── checklink-target
│   └── checknoexec
├── dirstate
├── last-message.txt
├── requires
├── store
│   ├── 00changelog.i
│   ├── 00manifest.i
│   ├── data
│   │   ├── 50x.html.i
│   │   └── index.html.i
│   ├── fncache
│   └── undo
├── undo.branch
├── undo.desc
└── undo.dirstate

3 directories, 17 files
root@kali:~/dvcs-ripper# find .hg -type f -name "*"|xargs grep flag
grep: .hg/store/undo: 匹配到二进制文件
.hg/store/fncache:data/flag_294264243.txt.i
grep: .hg/store/00manifest.i: 匹配到二进制文件
grep: .hg/dirstate: 匹配到二进制文件
grep: .hg/undo.dirstate: 匹配到二进制文件
.hg/last-message.txt:add flag
root@kali:~/dvcs-ripper#
```

4.访问获取flag，注意把.i去掉。



5.复制提交，



往期内容

CTF学习和比赛平台简介

ATT&CK实战-红队评估之二

简单讲解一下什么是ATT&CK框架

更多资讯长按二维码 关注我们

觉得不错点个“赞”呗