

CTFhub——信息泄露

原创

[Be_immortal](#)  于 2022-03-13 22:19:38 发布  1121  收藏

文章标签: [php](#) [linux](#) [vim](#)

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/qq_62540010/article/details/123467684

版权

CTFHUB——信息泄露

1.目标遍历

这个没什么好讲的一个一个点就可以了

2.PHPINFO

这个也一样ctrl+f搜索一下就行

3.备份文件下载

3.1 网站源码

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

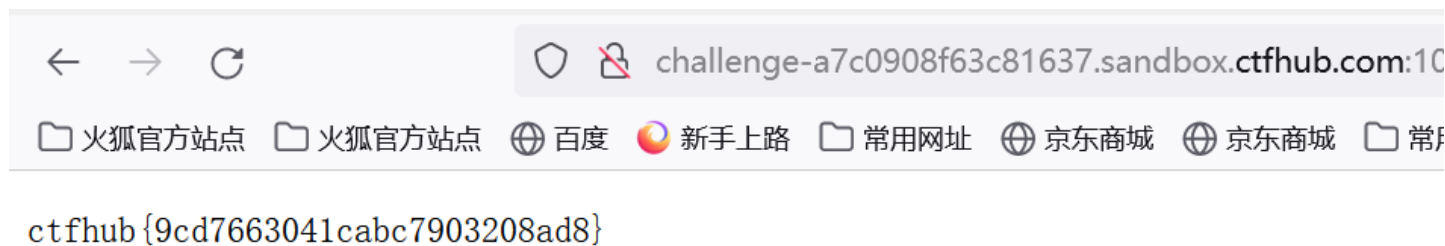
CSDN @Be_immortal

我们可以一个一个试，但有些麻烦，我们可以用burp抓包用clusterbomb模块来尝试，最后试出来为www.zip,我们下载下来为

where is flag ??

CSDN @Be_immortal

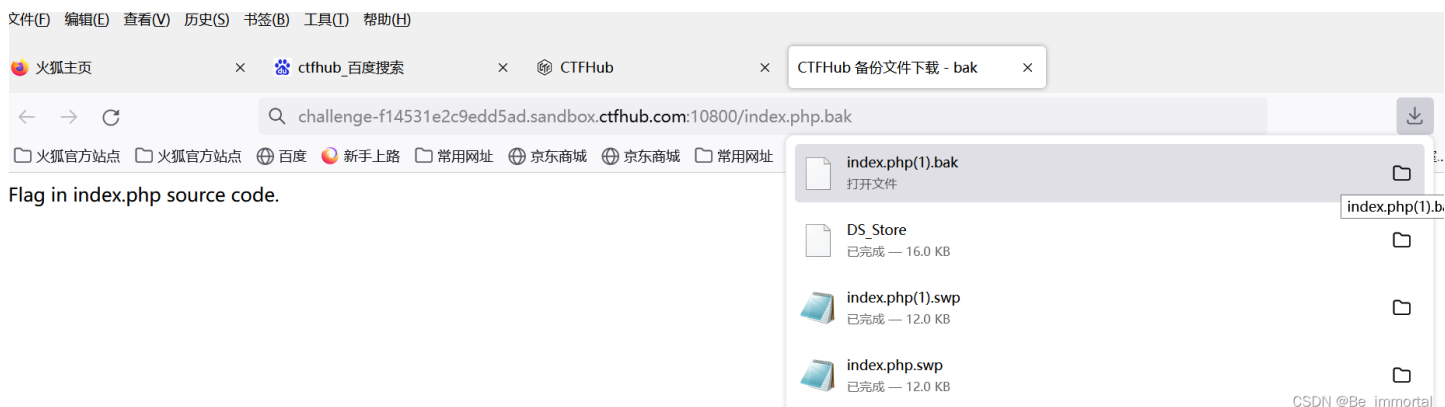
我们发现单独打开没有flag，但php开发的网站通常以www目录下的文件为访问路径，所以我们通过url来打开



CSDN @Be_immortal

3.2 bak文件

我们进入后发现它提示我们flag在index.php中，但我们看页面的源代码并没有发现，题目为bak文件，所以我们访问一下index.php.bak文件



下载该文件得到flag

CSDN @Be_immortal

```
<!DOCTYPE html>
<html>
<head>
  <title>CTFHub 备份文件下载 - bak</title>
</head>
<body>
<?php

// FLAG: ctfhub{0bdde6e3f13abd66f271ba91}

echo "Flag in index.php source code.";
?>
</body>
</html>
```

3.3 vim缓存

在创建vim时回产生缓存文件，退出时就会删除，若异常退出，会产生.swp,.swo,.swn等缓存文件

以 index.php 为例：

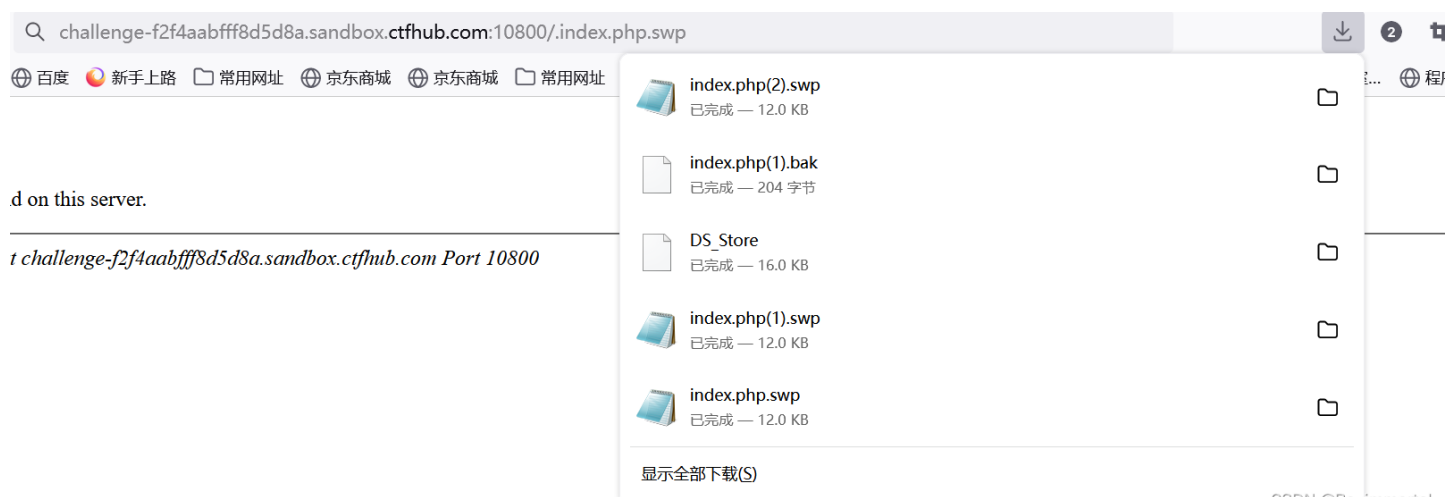
第一次产生的交换文件名为 .index.php.swp

当index.php.swp意外退出时，将会产生名为 .index.php.swo 的交换文件

第三次意外退出时产生的交换文件则为 .index.php.swn

所以这关考的是我们对vim缓存文件名称的认识

我们访问index.php.swp文件



发现是not found,我们在index前面加个点（访问隐藏文件的方法）

得到文件后我们用记事本打开



```
index.php(2).swp - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

</html> </body> <p>flag 鏹?index.php 婧悛熾涓?/p> <br/> <h1>漚囡
緼緼囡欢涓嬩浇 - vim</h1> <body> </head> <title>CTFHub BackUp Vim</title> <meta
harset="UTF-8" /> <head> <html> ?> // ctfhub{b5e2c9f28fb2d961408a75a4} <?php

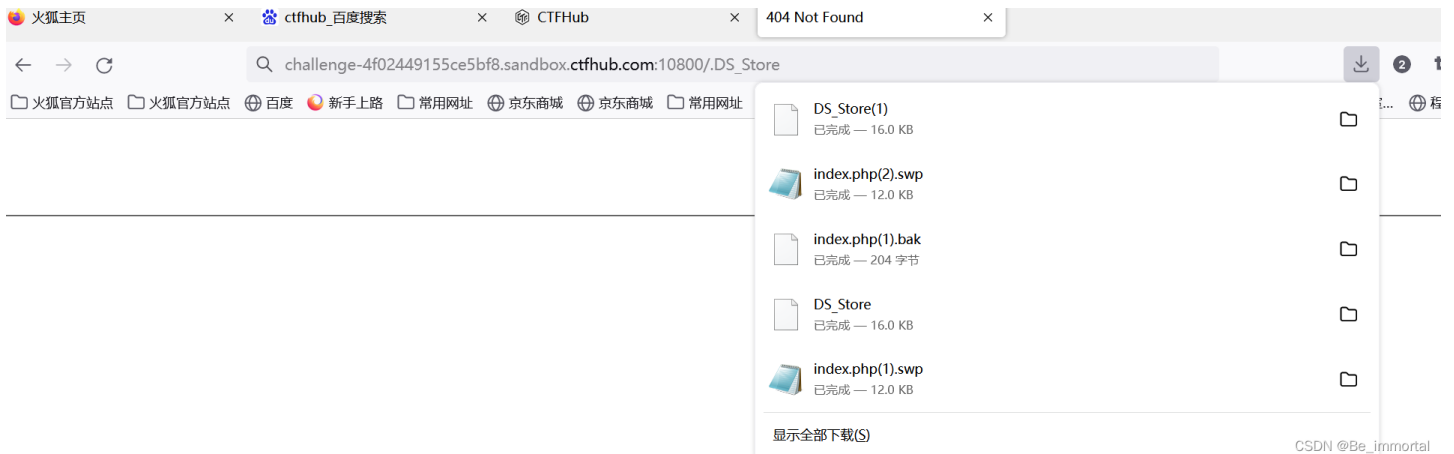
第 3 行, 第 11250 列 100% Unix (LF) CSDN@Be_immortal...
```

成功拿到flag

3.4

.DS_Store是Mac OS保存文件夹的自定义属性的隐藏文件，如文件的图标位置或背景色，相当于Windows的desktop.ini。

和前几关相同，我们在url上补充.DS_Store



打开文件后，得到flag



4 git泄露

这一大关开始之前，先下载一个工具，在ctfhub就有叫githack，详细的解释马上补充(我还有一些没搞懂)

5.SVN泄露 (liunx)

这关需要用到 `dvcs-ripper` 这个工具

步骤

安装dvcs-ripper

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

安装依赖包

```
apt-get install perl libio-socket-ssl-perl libdbd-sqlite3-perl libclass-dbi-perl libio-all-lwp-perl
```

安装失败，先执行下面的命令，再重新执行

```
apt-get update
```

dvcs-ripper工具用法:

```
./rip-svn.pl -v -u http://challenge-563ffc1ab84bbca7.sandbox.ctfhub.com:10800/.svn/ (url不固定)
```

```
root@kali: ~/dvcs-ripper
# ./rip-svn.pl -v -u http://challenge-4bb7762c559de00b.sandbox.ctfhub.com:10800/.svn/
[i] Found new SVN client storage format!
install_driver(SQLite) failed: Can't locate DBD/SQLite.pm in @INC (you may need to install the DBD::SQLite module) (/usr/x86_64-linux-gnu/perl/5.32.1 /usr/local/share/perl/5.32.1 /usr/lib/x86_64-linux-gnu/perl5/5.32 /usr/share/perl5 /usr/lib/x86_64-linux-gnu/perl/5.32 /usr/share/perl/5.32 /usr/local/lib/site_perl) at (eval 38) line 3.
Perhaps the DBD::SQLite perl module hasn't been fully installed,
or perhaps the capitalisation of 'SQLite' isn't right.
Available drivers: DBM, ExampleP, File, Gofer, MariaDB, Mem, Proxy, Sponge.
at ./rip-svn.pl line 85.

root@kali: ~/dvcs-ripper
# sSSs
```

我们在用ls查看并用tree .svn查看它的树结构

```
root@kali: ~/dvcs-ripper
-rw-r--r-- 1 root root 3855 3月 13 19:02 hg-decode.pl
-rw-r--r-- 1 root root 18027 3月 13 19:02 LICENSE
-rw-r--r-- 1 root root 5597 3月 13 19:02 README.md
-rwxr-xr-x 1 root root 6401 3月 13 19:02 rip-bzr.pl
-rwxr-xr-x 1 root root 4717 3月 13 19:02 rip-cvs.pl
-rwxr-xr-x 1 root root 15114 3月 13 19:02 rip-git.pl
-rwxr-xr-x 1 root root 6102 3月 13 19:02 rip-hg.pl
-rwxr-xr-x 1 root root 6157 3月 13 19:02 rip-svn.pl
drwxr-xr-x 5 root root 4096 3月 13 19:10 .svn

root@kali: ~/dvcs-ripper
# tree ,svn
,svn [error opening dir]

0 directories, 0 files

root@kali: ~/dvcs-ripper
# tree .svn
.svn
├── entries
├── format
├── pristine
├── text-base
├── tmp
└── wc.db
```

cd到pristine里就可以得到flag了

5.hg泄露

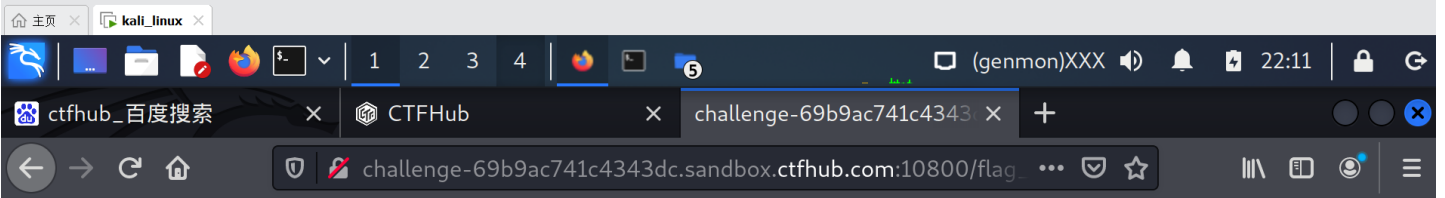
这一关和上一关解决方式一样

```
root@kali: ~/dvcs-ripper
文件 动作 编辑 查看 帮助
[i] Auto-detecting 404 as 200 with 3 requests
[i] Getting correct 404 responses
[d] found 00changelog.i
[d] found dirstate
[d] found requires
[!] Not found for branch: 404 Not Found
[!] Not found for branchheads.cache: 404 Not Found
[d] found last-message.txt
[!] Not found for tags.cache: 404 Not Found
[d] found undo.branch
[d] found undo.desc
[d] found undo.dirstate
[d] found store/00changelog.i
[!] Not found for store/00changelog.d: 404 Not Found
[d] found store/00manifest.i
[!] Not found for store/00manifest.d: 404 Not Found
[d] found store/fncache
[d] found store/undo
[!] Not found for .hgignore: 404 Not Found
[i] Running hg status to check for missing items
cannot find hg: No such file or directory at ./rip-hg.pl line 140.

(root@kali)-[~/dvcs-ripper]
#
```

```
root@kali: ~/dvcs-ripper/.hg/store
应用程序
文件 动作 编辑 查看 帮助
(root@kali)-[~/dvcs-ripper/.hg/store]
# cd data
(root@kali)-[~/dvcs-ripper/.hg/store/data]
# ls -al
总用量 8
drwxr-xr-x 2 root root 4096 3月 13 19:46 .
drwxr-xr-x 3 root root 4096 3月 13 19:47 ..
(root@kali)-[~/dvcs-ripper/.hg/store/data]
# cd ~/dvcs-ripper/.hg/store
(root@kali)-[~/dvcs-ripper/.hg/store]
# cd fncache
cd: 不是目录: fncache
(root@kali)-[~/dvcs-ripper/.hg/store]
# cat fncache
data/index.html.i
data/50x.html.i
data/flag_636428943.txt.i
(root@kali)-[~/dvcs-ripper/.hg/store]
# ss
```

然后我们发现flag文件，我们将它复制在网站中打开



ctfhub{eb7d4e34955d8fa2a468e5da}

得到flag