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

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

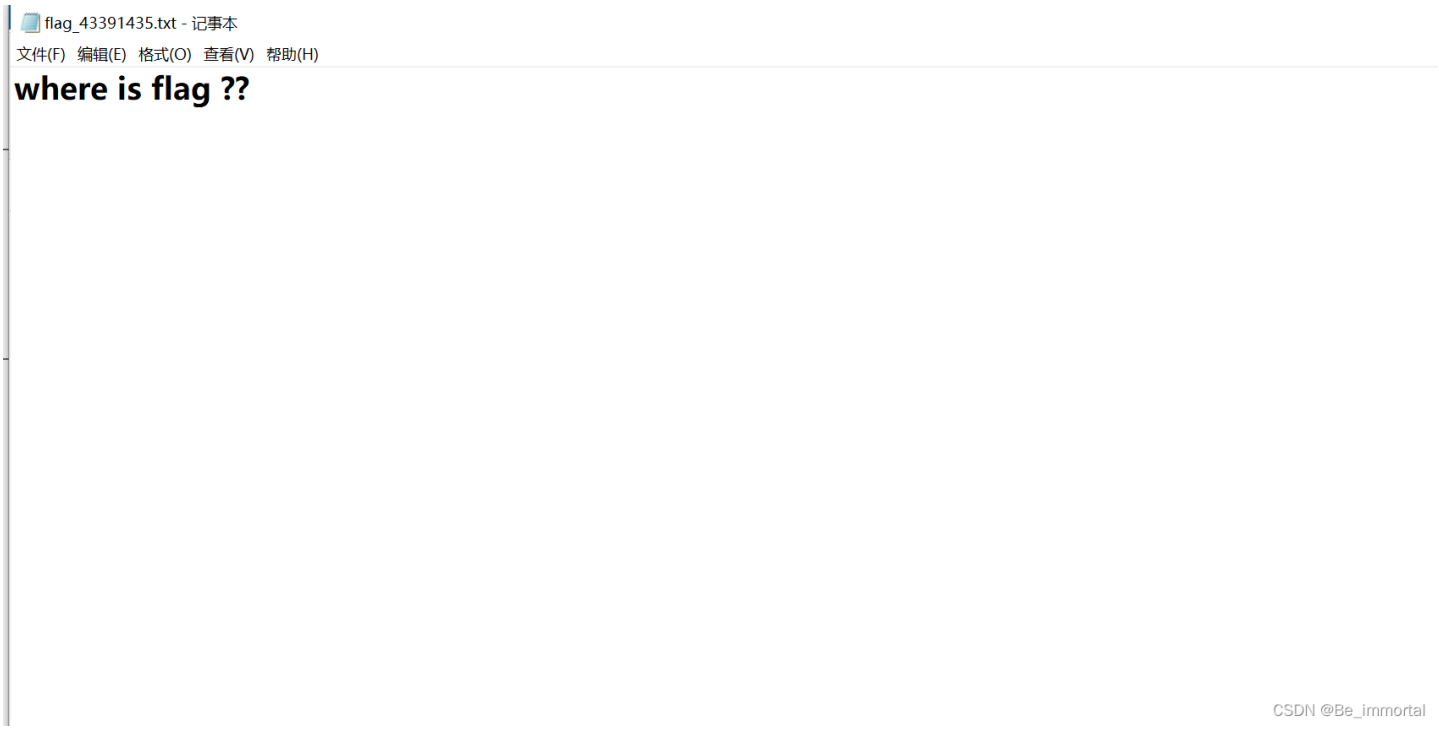
常见的网站源码备份文件后缀

- tar
- tar.gz
- zip
- rar

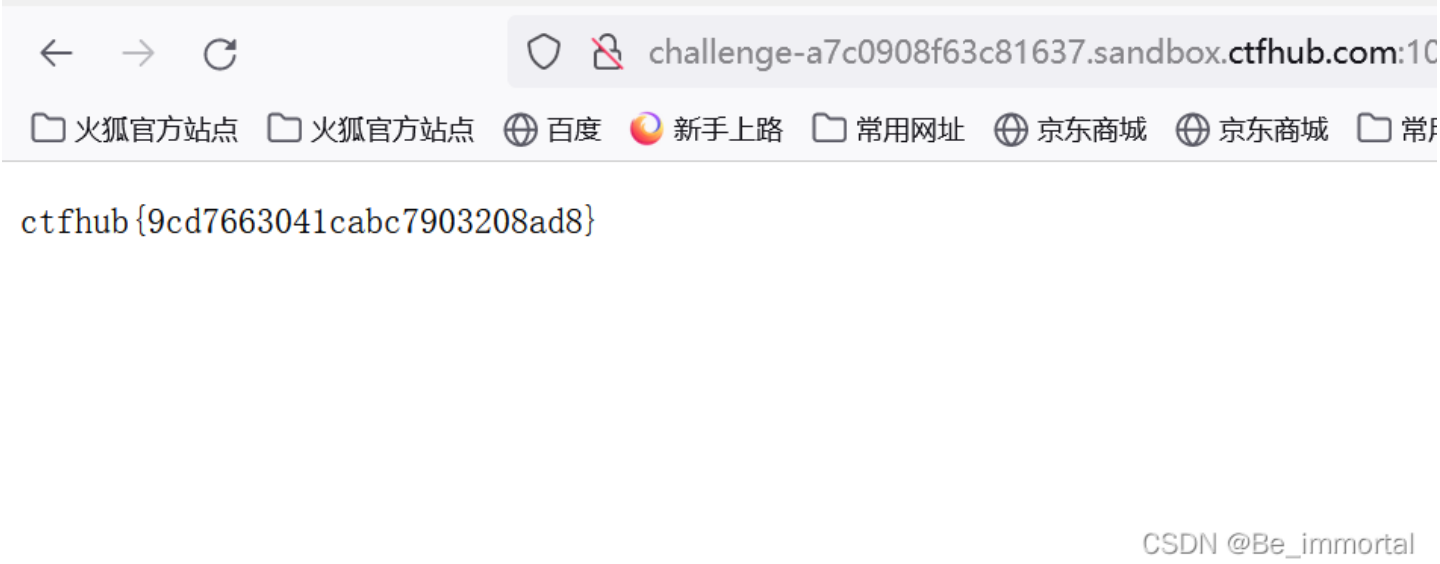
常见的网站源码备份文件名

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

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

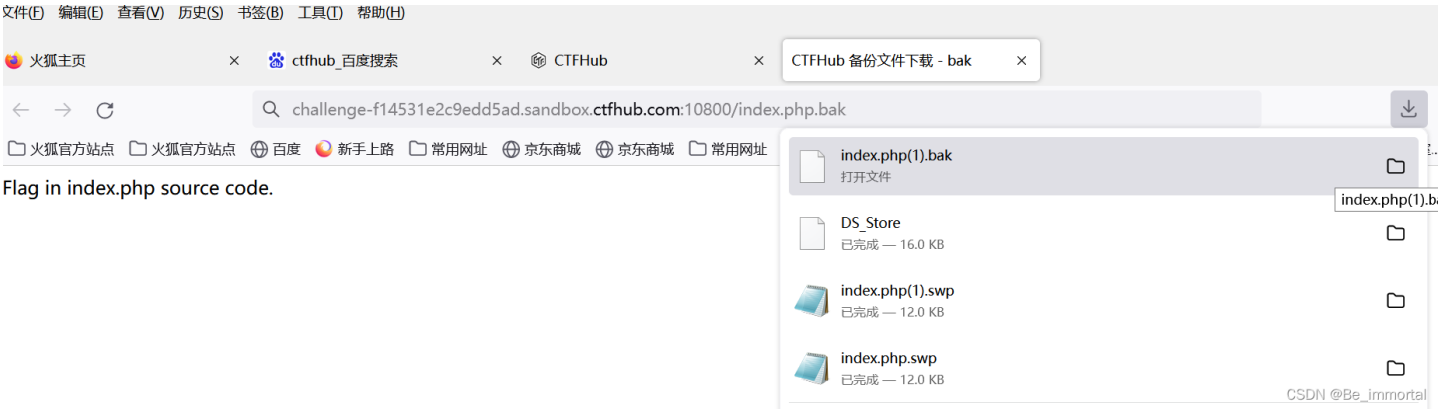


我们发现单独打开没有flag，但php开发的网站通常以www目录下的文件为访问路径，所以我们通过url来打开



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

index.php(1).bak - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<!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>
```


第 9 行，第 4

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

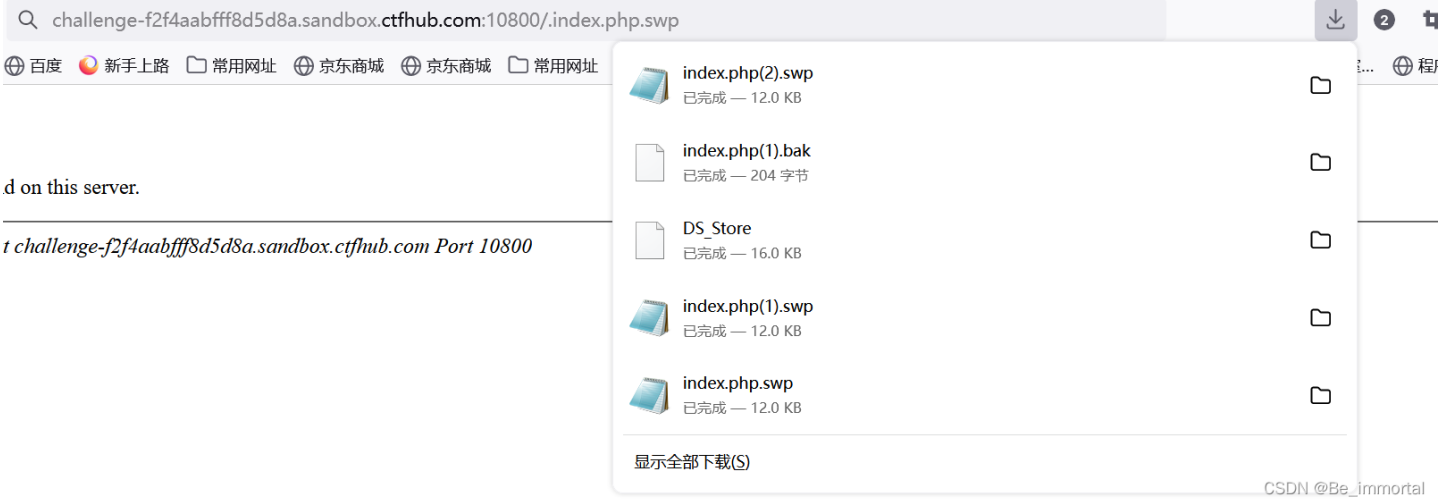
以 index.php 为例：
第一次产生的交换文件名为 .index.php.swp

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）

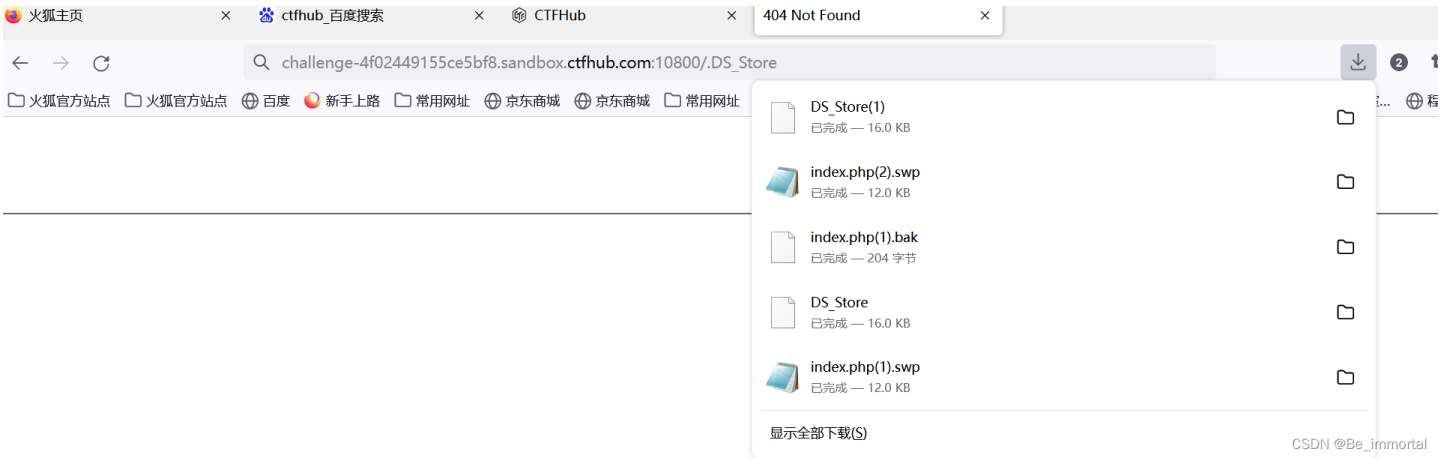
得到文件后我们用记事本打开

成功拿到flag

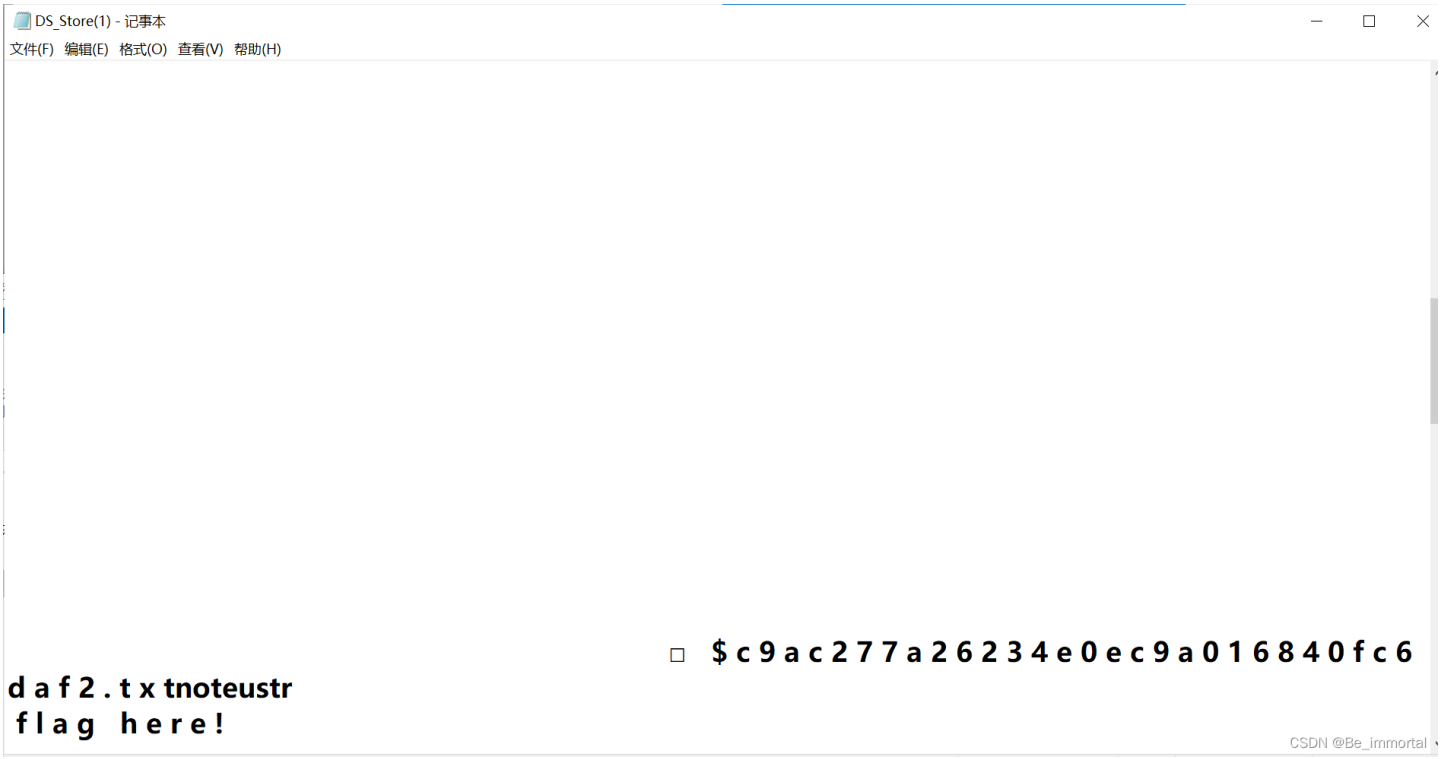
3.4

.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

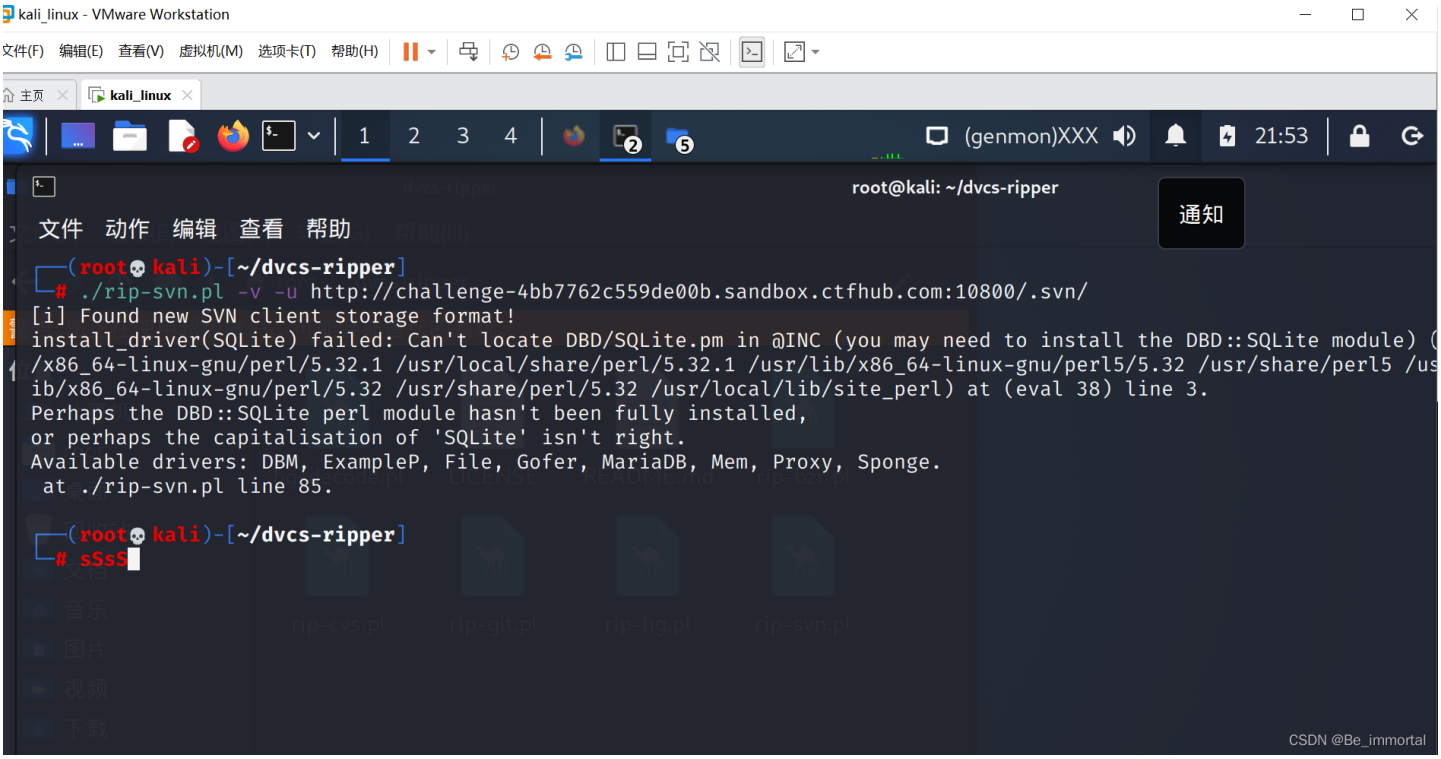
```
apt-get install perl libio-socket-ssl-perl libdbd-sqlite3-perl libclass-dbi-perl libio-all-lwp-perl
```

安装失败，先执行下面的命令，再重新执行

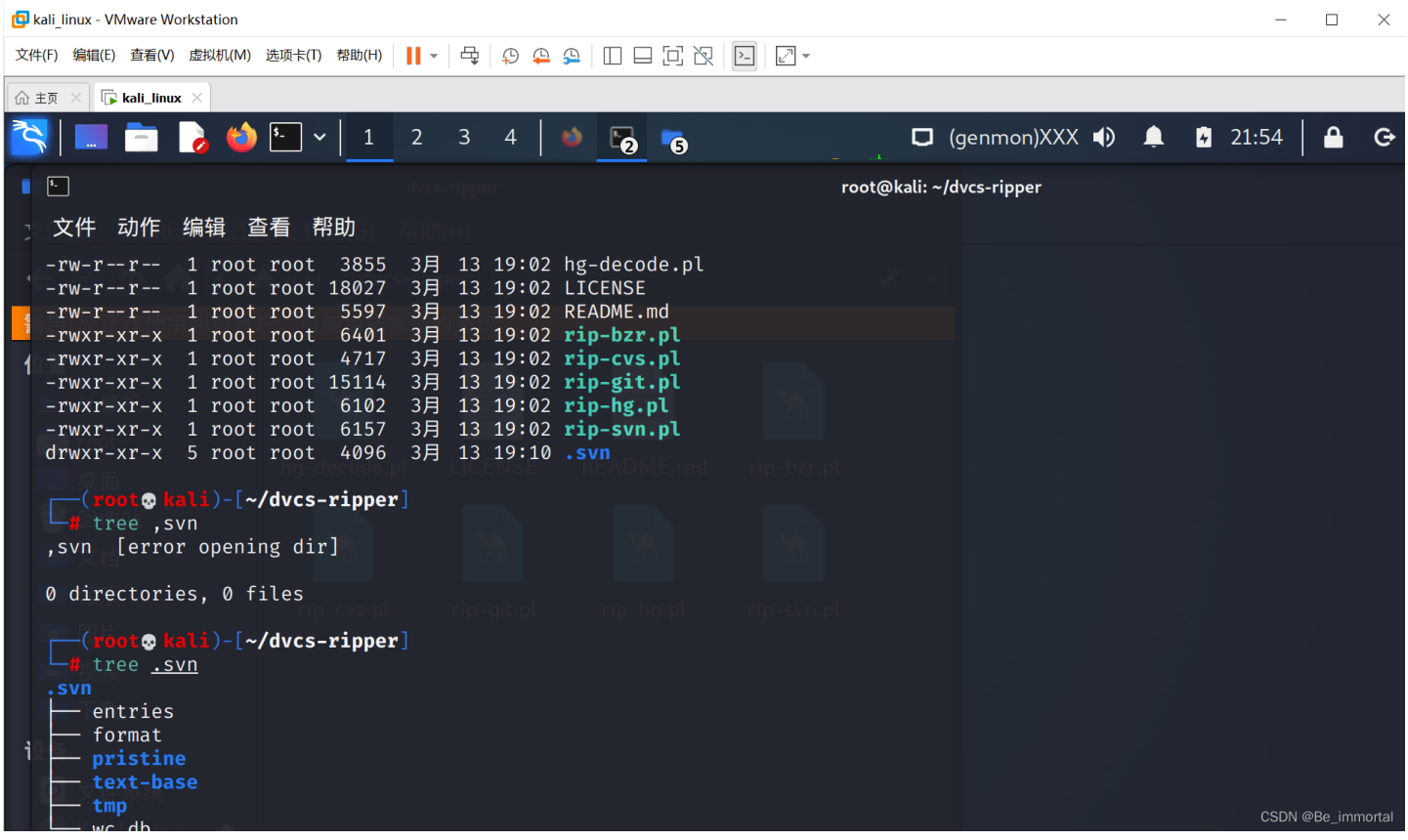
```
apt-get update
```

dvcs-ripper工具用法：

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



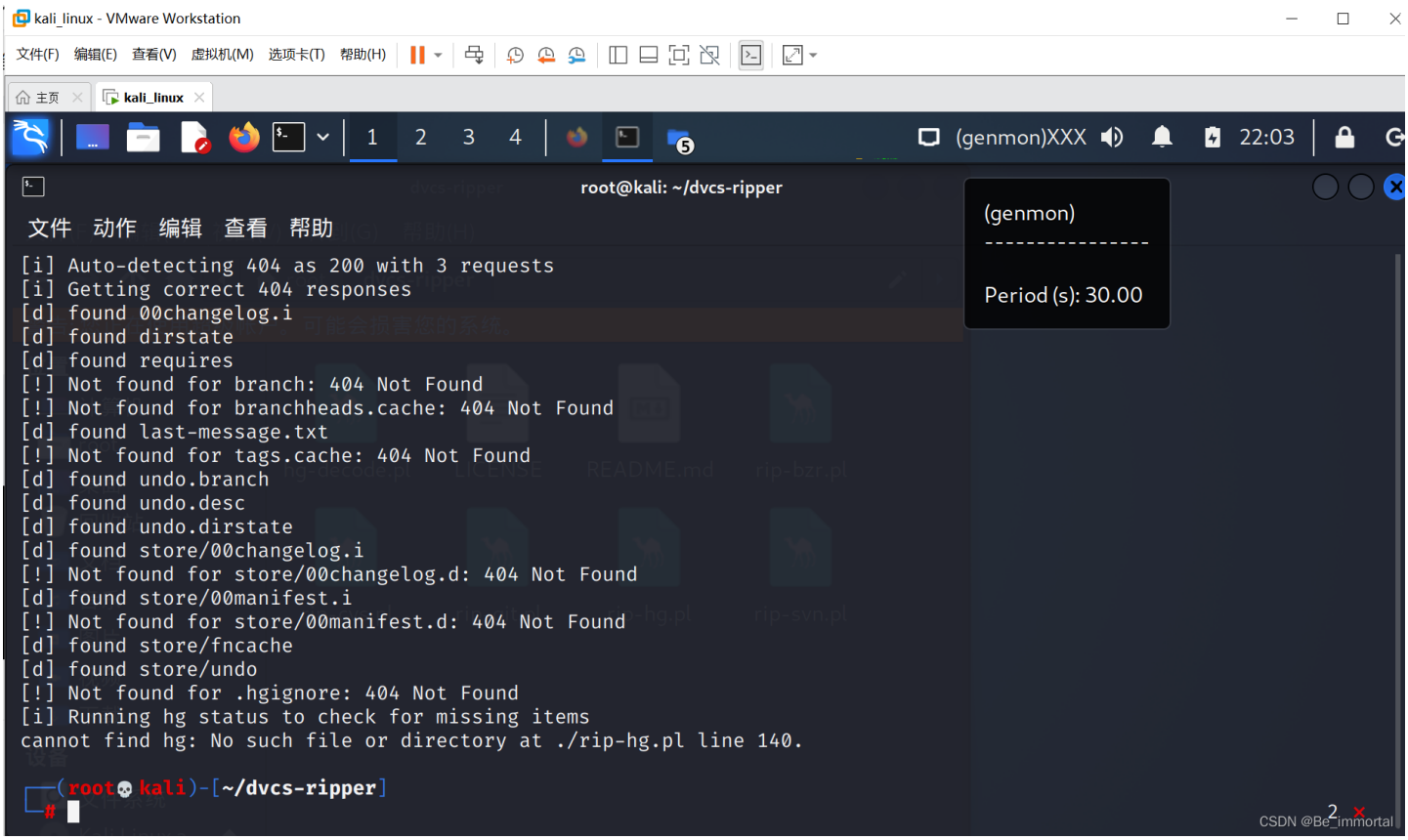
我们在用ls查看并用tree .svn查看它的树结构

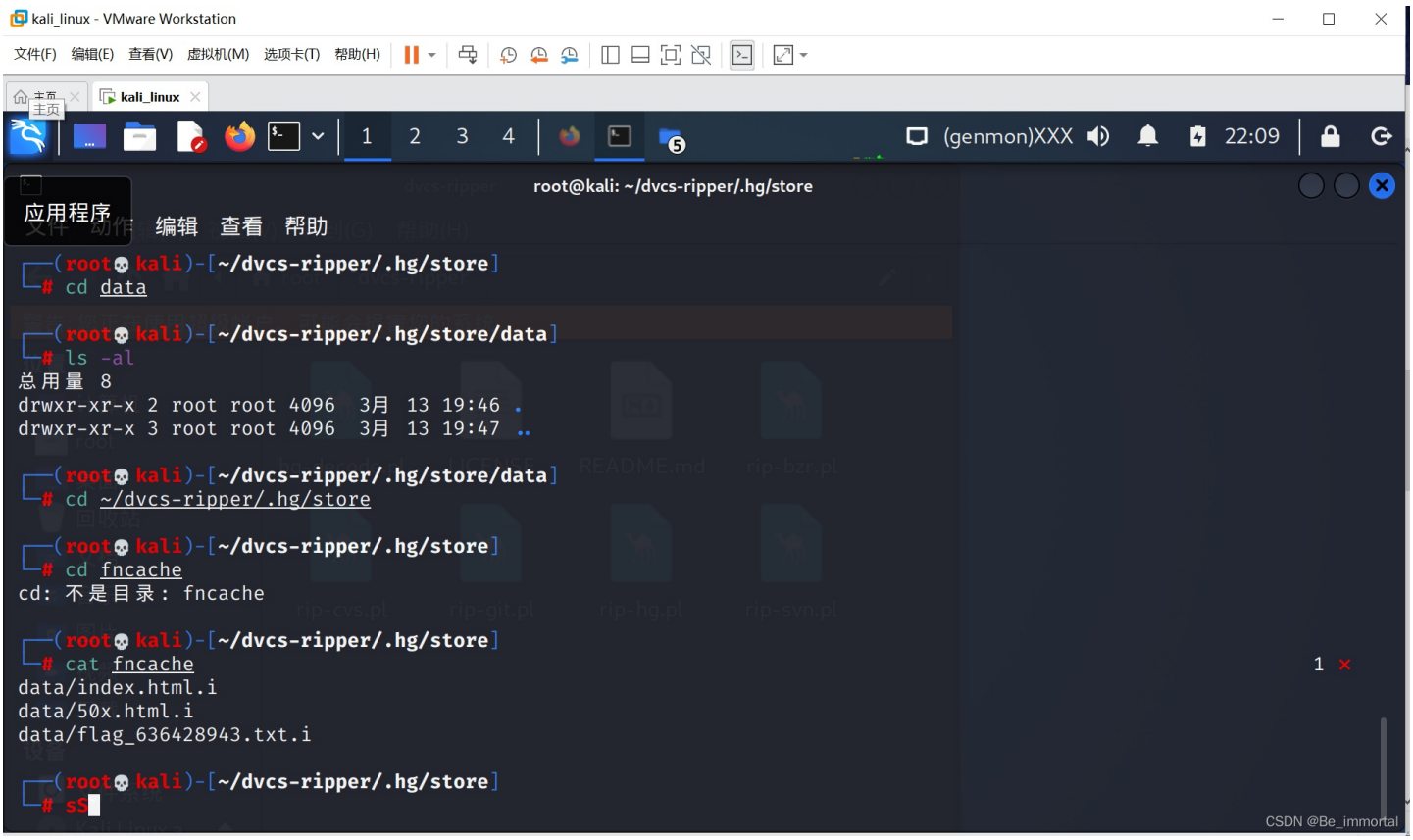


cd到pristine里就可以得到flag了

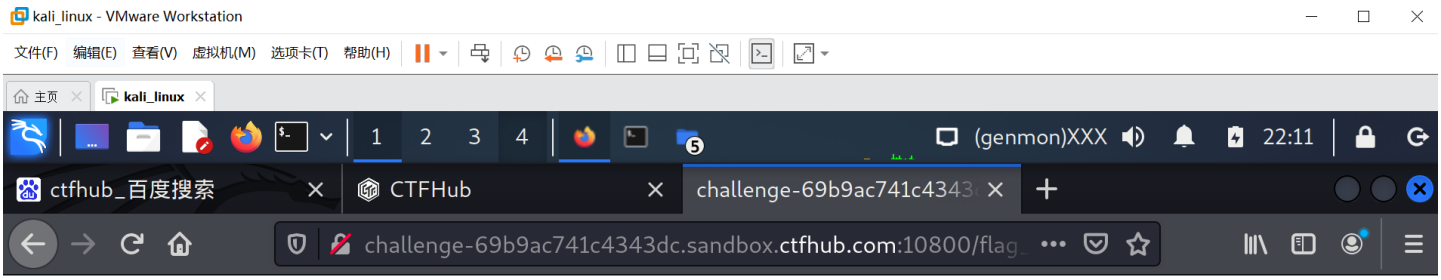
5.hg泄露

这一关和上一关解决方式一样





然后我们发现有flag文件，我们将它复制在网站中打开




```
ctfhub{eb7d4e34955d8fa2a468e5da}
```


得到flag