CTF中常见信息搜集学习总结

原创

等灬 于 2021-11-28 20:16:50 发布
分类专栏： ctf线上解题学习总结 文章标签： web安全

信息搜集的必要性：在线上解题时，信息搜集可以帮助我们建立解题思路，发现解题方向。

0.题目描述

其实最主要的还是题目描述里的信息，不然没法做题，用心读题才能把题做好。

1.页面源代码

这个就不用多说了，现在基本上打开题目就是习惯性地按F12，抓包看源码。

源码里面可能会发现一些JS脚本代码、注释掉的标签信息、在图片标签的src属性里可能会发现网站后台的路径等等。

2.敏感文件泄露

①robots.txt

当我们在搜索引擎上打上内容点击搜索的时候，搜索引擎靠一个叫robot的程序去互联网中访问并获取网页信息。

robots.txt文件是存放在网站根目录下的文本文件，是robot访问网站时第一个要检查有无的文件，如果存在的话，那robots.txt文件会告诉robot我这个网站里的哪些页面是可以访问哪些是不能访问的。

做题时就可以先尝试一下/robots.txt看看有没有这个文件如果有的话，里面的那些disallow的文件就是我们重点访问的文件[手动狗头]。

②.phps文件

PHP是服务端语言，在前端页面用户是无法看到的，如果需要让用户查看php源码呢？就是这个xx.phps文件里面是xx页面的php源码。当然.phps文件不是哪个网站都有，做题的时候怎么说呢基本碰不到吧，一些入门题，题目描述到.phps文件，打开题目链接就直接/index.phps就可以了如果不是index.phps也可以用御剑扫一下。。

③www.zip文件

网站的所有文件都在www文件中，可能是怕网站文件丢失，所以将www文件压缩成www.zip备份，这时候访问/www.zip(也可能不在根目录下)可能会有惊喜。www.zip/rar/tar.gz往往是网站的源码备份。

④vim缓存文件泄露

在使用vim编辑过程中如果异常退出编辑，比如不小心碰到了电源键。但是你编辑的东西不会丢失而是系统帮你生成一个.swp的缓存文件(格式为.文件名.swp)第二次意外退出时为.swo，第三次为.swn，所以根据题目描述就可以访问.xx.swp的文件(注意最前面多个.)。

恢复文件内容的方法，执行“vim 文件名”命令的目录下创建一个名字相同的文件夹“touch 文件名”“cat 文件名（此时为空）”再使用“vim -r 文件名”命令。然后"cat 文件名"就能看见被缓存的内容了

⑤mdb文件泄露

mdb文件是早期asp+access构架的数据库文件，文件泄露相当于数据库被脱裤了

文件路径：URL/db/db.mdb

3.敏感目录泄露

目录扫描工具：http://github.com/maurosoria/dirsearch

使用方法：

-u 指定网址

-e 指定网站语言

-w 指定字典

-r 递归目录（跑出目录后，继续跑目录下面的目录）

--random-agents 使用随机UA

例如：python dirsearch.py -u 网址 -e*

我在win10 系统中总是出问题，把文件拖到kali里，使用命令

python3 dirsearch.py -u www.baidu.com -e*

成功。

①git泄露

根本原因是因为开发人员忘记了自动生成的.git隐藏文件，导致攻击者可以通过,git文件夹中的信息获取开发者提交过的所有源码。

工具：GitHack（以下是 在win系统中操作）

(1)常规git泄露

直接运行工具:在GitHack-master目录打开命令行，输入命令：python GitHack.py http://xxxx/.git/

然后会在dist文件里生成一个文件，里面是.git文件夹

(2)git分支

flag等关键信息可能不在当前版本中，所以直接利用工具可能搜集不到。

在dist目录下生成的文件下使用cmd命令行执行：

git log 查看历史记录

git reset --hard HEAD^/切换到上一版本

git diff HEAD^或git diff xxxx，比较当前版本与上一版本或其他版本的修改

②SVN泄露

造成svn源代码漏洞的主要原因是管理员操作不规范将SVN隐藏文件夹暴露于外网环境，利用.svn/entries或wc.db获取服务器源码等信息。

工具：dvcs-ripper

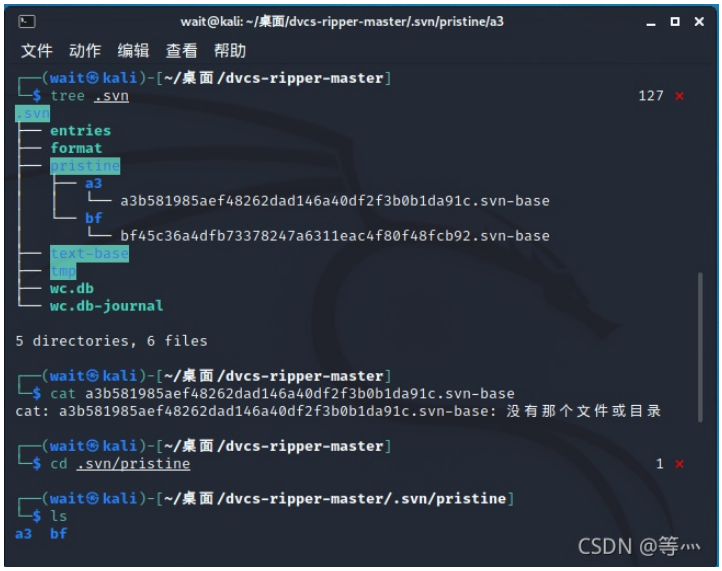
在win系统中感觉使用起来有太多的问题，所以就把dvcs-ripper-master文件拖到了kali里面，右击文件打开终端，

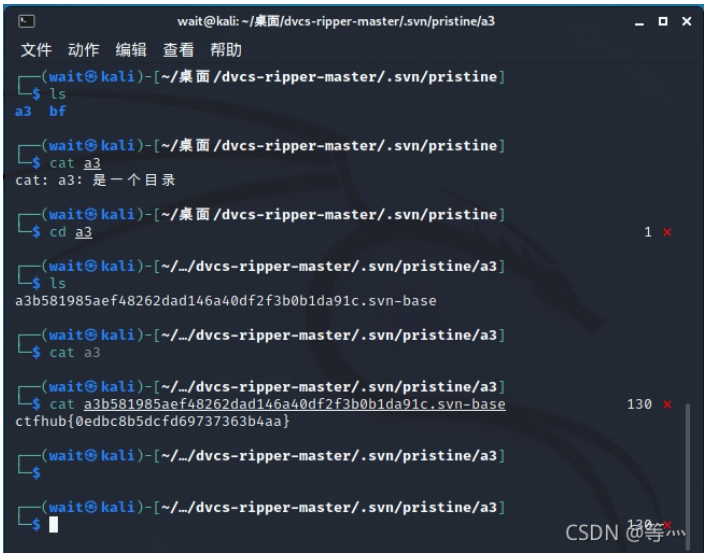
命令：./rip-svn.pl -u http://xxx/.svn/

第一次使用也是出现了问题所以在网上搜了一波要配置相关的组件： sudo apt-get install perl libio-socket-ssl-perl libdbd-sqlite3-perl libclass-dbi-perl libio-all-lwp-perl

配置完之后就可以了，下面是我的解题过程(有点捞),因为.svn是隐藏文件，如果用Linux的话必须要用ls -al 才能看得到。

代码的历史版本会存储在pristin文件里。





③HG泄露

工具：dvcs-ripper

在初始化项目时，HG会在当前文件夹下创建一个.hg隐藏文件夹，其中包含代码和分支修改记录等信息。

ctfhub技能书HG泄露解题过程：

打开题目环境复制网址进入kali执行命令：

./rip-hg.pl -v -u http://challenge-c25ca39ef9614244.sandbox.ctfhub:10800.com/.hg/

```
文件  动作  编辑  查看  帮助

┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master]
└─$ ./rip-hg.pl -v -u http://challenge-c25ca39ef9614244.sandbox.ctfhub.com:10
800/.hg/
[i] Downloading hg files from http://challenge-c25ca39ef9614244.sandbox.ctfhu
b.com:10800/.hg/
[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.

┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master]
└─$ ls -al                                                          2 ×
总用量 104
drwxrwxrwx 4 wait wait  4096 11月 28 19:27 .
drwxr-xr-x 3 wait wait  4096 11月 28 18:54 ..
-rwxrw-rw- 1 wait wait   149  8月 18  2020 .gitignore
drwxr-xr-x 3 wait wait  4096 11月 28 19:27 .hg
-rwxrw-rw- 1 wait wait  3855  8月 18  2020 hg-decode.pl
-rw-r--r-- 1 wait wait   221 11月 28 19:07 index.html
-rwxrw-rw- 1 wait wait 18027  8月 18  2020 LICENSE
-rwxrw-rw- 1 wait wait  5597  8月 18  2020 README.md
-rwxrw-rw- 1 wait wait  6401  8月 18  2020 rip-bzr.pl
-rwxrw-rw- 1 wait wait  4717  8月 18  2020 rip-cvs.pl
-rwxrw-rw- 1 wait wait 15114  8月 18  2020 rip-git.pl
-rwxrw-rw- 1 wait wait  6102  8月 18  2020 rip-hg.pl
-rwxrw-rw- 1 wait wait  6157  8月 18  2020 rip-svn.pl
drwxrwxrwx 5 wait wait  4096 11月 28 19:07 .svn
                                                    CSDN @等灬
```

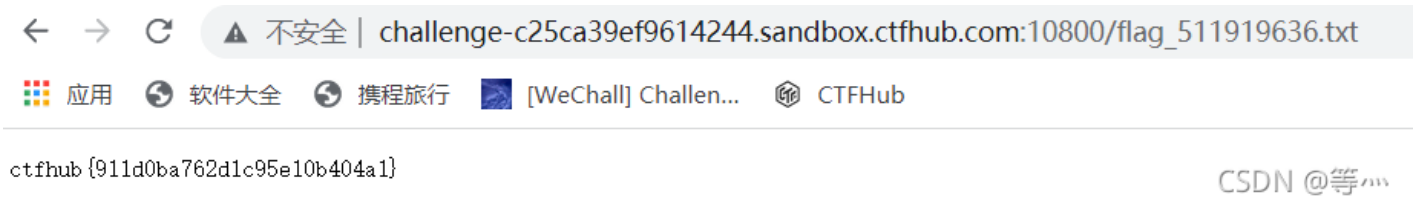
```
┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master/.hg/store]
└─$ ls -al
总用量 28
drwxr-xr-x 3 wait wait 4096 11月 28 19:27 .
drwxr-xr-x 3 wait wait 4096 11月 28 19:27 ..
-rw-r--r-- 1 wait wait  352 11月 28 19:27 00changelog.i
-rw-r--r-- 1 wait wait  289 11月 28 19:27 00manifest.i
drwxr-xr-x 2 wait wait 4096 11月 28 19:27 data
-rw-r--r-- 1 wait wait   60 11月 28 19:27 fncache
-rw-r--r-- 1 wait wait   63 11月 28 19:27 undo

┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master/.hg/store]
└─$ cat fncache
data/index.html.i
data/50x.html.i
data/flag_511919636.txt.i

┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master/.hg/store]
└─$ cat data/flag_511919636.txt.i
cat: data/flag_511919636.txt.i: 没有那个文件或目录

┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master/.hg/store]
└─$ cat data/flag_511919636.txt
cat: data/flag_511919636.txt: 没有那个文件或目录

┌──(wait㉿kali)-[~/桌面/dvcs-ripper-master/.hg/store]
└─$
                                                    CSDN @等灬
```



ctfhub{911d0ba762d1c95e10b404a1}

CSDN @等灬

4.PHP探针

有时候一些关键信息比如flag有可能会在phpinfo里(我发现FLAG总在phpinfo的Environment里)。

php探针是用来探测空间、服务器运行状况和PHP信息用的，探针可以实时查看服务器硬盘资源、内存占用、网卡 流量、系统负载、服务器时间等信息。 url后缀名添加/tz.php 版本是雅黑PHP探针。

5.编辑器默认配置泄露网站根目录

0day:某编辑器最新版默认配置下，如果目录不存在，则会遍历服务器根目录.

做过一个题，使用编辑器上传照片的时候，可以在网站根目录里找