

Web源码泄露的漏洞：

- git源码泄露
 - svn源码泄露
 - hg源码泄露
 - CVS泄露
 - Bazaar/bzr泄露
 - 网站备份压缩文件
 - WEB-INF/web.xml 泄露
 - DS_Store 文件泄露
 - SWP 文件泄露
 - GitHub源码泄露
-

1、git 源码泄露

Git是一个开源的分布式版本控制系统，在执行 `git init` 初始化目录的时候，会在当前目录下自动创建一个 `.git` 目录，用来记录代码的变更记录等。发布代码的时候，如果没有把 `.git` 这个目录删除，就直接发布到了服务器上，攻击者就可以通过它来恢复源代码。

漏洞利用工具：GitHack

github项目地址：<https://github.com/lijiejie/GitHack>

用法示例：

```
GitHack.py http://www.openssl.org/.git/
```

修复建议：删除.git目录或者修改中间件配置进行对.git隐藏文件夹的访问。

2、SVN 源码泄露

SVN是一个开放源代码的版本控制系统。在使用SVN管理本地代码过程中，会自动生成一个名为.svn的隐藏文件夹，其中包含重要的源代码信息。网站管理员在发布代码时，没有使用‘导出’功能，而是直接复制代码文件夹到WEB服务器上，这就使.svn隐藏文件夹被暴露于外网环境，可以利用.svn/entries文件，获取到服务器源码。

漏洞利用工具：Seay SVN漏洞利用工具



修复建议：删除web目录中所有.svn隐藏文件夹，开发人员在使用SVN时，严格使用导出功能，禁止直接复制代码。

3、hg源码泄漏

Mercurial 是一种轻量级分布式版本控制系统，使用 `hg init` 的时候会生成.hg。

漏洞利用工具：dvcs-ripper

github项目地址：<https://github.com/kost/dvcs-ripper>

用法示例：

```
rip-hg.pl -v -u http://www.example.com/.hg/
```

4、CVS泄露

CVS是一个C/S系统，多个开发人员通过一个中心版本控制系统来记录文件版本，从而达到保证文件同步的目的。主要是针对 CVS/Root以及CVS/Entries目录，直接就可以看到泄露的信息。

```
http://url/CVS/Root 返回根信息
http://url/CVS/Entries 返回所有文件的结构
```

漏洞利用工具：dvcs-ripper

github项目地址：<https://github.com/kost/dvcs-ripper.git>

运行示例:

```
rip-cvs.pl -v -u http://www.example.com/CVS/
```

5、Bazaar/bzr泄露

运行示例：

6、网站备份压缩文件

常见的备份文件后缀：

- 漏洞利用工具：御剑



WEB-INF 是Java的WEB应用的安全目录，如果想在页面中直接访问其中的文件，必须通过web.xml文件对要访问的文件进行相应映射才能访问。

WEB-INF 主要包含一下文件或目录：

```
WEB-INF/web.xml : Web应用程序配置文件，描述了servlet和其他的应用组件配置及命名规则。  
WEB-INF/database.properties : 数据库配置文件  
WEB-INF/classes/ : 一般用来存放Java类文件(.class)  
WEB-INF/lib/ : 用来存放打包好的库(.jar)  
WEB-INF/src/ : 用来放源代码(.asp和.php等)
```

通过找到 web.xml 文件，推断 class 文件的路径，最后直接 class 文件，再通过反编译 class 文件，得到网站源码。

8、DS_Store 文件泄露

.DS_Store是Mac下Finder用来保存如何展示 文件/文件夹 的数据文件，每个文件夹下对应一个。如果将.DS_Store上传部署到服务器，可能造成文件目录结构泄露，特别是备份文件、源代码文件。

漏洞利用工具：

github项目地址：https://github.com/lijiejie/ds_store_exp

用法示例：

```
ds_store_exp.py http://hd.zj.qq.com/themes/galaxyw/.DS_Store
```

9、SWP 文件泄露

swp即swap文件，在编辑文件时产生的临时文件，它是隐藏文件，如果程序正常退出，临时文件自动删除，如果意外退出就会保留，文件名为 .filename.swp。

漏洞利用：直接访问.swp文件，下载回来后删掉末尾的.swp，获得源码文件。

10、GitHub源码泄漏

GitHub是一个面向开源及私有软件项目的托管平台。很多人喜欢把自己的代码上传到平台托管，通过关键词进行搜索，可以找到关于目标站点的敏感信息，甚至可以下载网站源码。

类似的代码托管平台还有很多，人才是最大的漏洞。

```
https://github.com/search?q=smt+user+@qq.com&type=code
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

