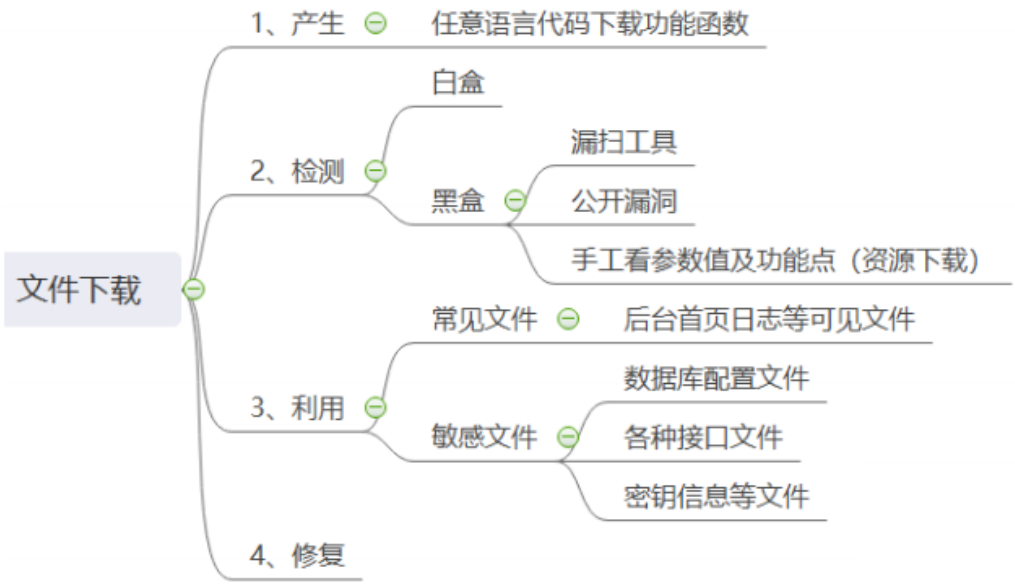
# Day32　WEB漏洞–文件操作之文件下载读取全解




## 32.1 文件下载的作用

下载文件，凡是存在文件下载的地方都可能存在文件下载漏洞

---

## 32.2 判断文件下载漏洞

1. 文件被解析，则是文件包含漏洞
2. 显示源代码，则是文件读取漏洞
3. 提示文件下载，则是文件下载漏洞，凡是有下载功能的地方都可能有下载漏洞

```
#文件名，参数值，目录符号
read.xxx?filename=
down.xxx?filename=
readfile.xxx?file=
downfile.xxx?file=
../ ..\ .\ ./等
%00 ? %23 %20 .等
&readpath=、&filepath=、&path=、&inputfile=、&url=、&data=、&readfile=、&menu=、META-INF= 、WEB-INF
```

## 32.3 获取下载文件

当我们发现文件下载漏洞时，如何获取想要下载的常规文件和敏感文件?

- 扫描工具爬行或扫描地址
- 下载好的文件代码中去分析路径（可见文件）和包含文件获取

数据库配置文件下载或读取后续

接口密匙信息文件下载或读取后续

## 32.4 常见的重要文件

**Windows:**

```
C:\boot.ini //查看系统版本
C:\Windows\System32\inetsrv\MetaBase.xml //IIS 配置文件
C:\Windows\repair\sam //存储系统初次安装的密码
C:\Program Files\mysql\my.ini //Mysql 配置
C:\Program Files\mysql\data\mysql\user.MYD //Mysql root
C:\Windows\php.ini //php 配置信息
C:\Windows\my.ini //Mysql 配置信息
C:\Windows\win.ini //Windows 系统的一个基本系统配置文件
```

**Linux:**

```
/root/.ssh/authorized_keys
/root/.ssh/id_rsa
/root/.ssh/id_ras.keystore
/root/.ssh/known_hosts //记录每个访问计算机用户的公钥
/etc/passwd
/etc/shadow
/usr/local/app/php5/lib/php.ini //PHP 配置文件
/etc/my.cnf //mysql 配置文件
/etc/httpd/conf/httpd.conf //apache 配置文件
/root/.bash_history //用户历史命令记录文件
/root/.mysql_history //mysql 历史命令记录文件
/proc/mounts //记录系统挂载设备
/porc/config.gz //内核配置文件
/var/lib/mlocate/mlocate.db //全文件路径
/porc/self/cmdline //当前进程的 cmdline 参数
都可以尝试下载
```

## 资源：

```
https://www.seebug.org/vuldb/ssvid-98122
https://www.ichunqiu.com/battalion?t=1&r=57475
https://blog.csdn.net/Cheng_May/article/details/78600833
https://buuoj.cn/challenges#%5BRoarCTF%202019%5DEasy%20Java
```