有效防御PHP木马攻击的技巧Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E6_9C_89_E6_95_88_E9_98_B2_E5_c103_645294.htm 1、防止跳出web目录 首先修改httpd.conf，如果你只允许你的php脚本程序在web目录里操作，还可以修改httpd.conf文件限制php的操作路径。比如你的web目录是/usr/local/apache/htdocs，那么在httpd.conf里加上这么几行： php_admin_value open_basedir /usr/local/apache /htdocs 这样，如果脚本要读取/usr/local/apache/htdocs以外的文件将不会被允许，如果错误显示打开的话会提示这样的错误： Warning: open_basedir restriction in effect. File is in wrong directory in /usr/local/apache/htdocs/open.php on line 4 等等。 2、防止php木马执行webshell 打开safe_mode， 在，php.ini中设置 disable_functions= passthru，exec，shell_exec，system 二者选一即可，也可都选 3、防止php木马读写文件目录 在php.ini中的 disable_functions= passthru，exec，shell_exec，system 后面加上php处理文件的函数 主要有 fopen，mkdir，rmdir，chmod，unlink，dir fopen，fread，fclose，fwrite，file_exists closedir，is_dir，readdir.opendir fileperms.copy，unlink，delfile 即成为 disable_functions= passthru，exec，shell_exec，system，fopen，mkdir，rmdir，chmod，unlink，dir，fopen，fread，fclose，fwrite，file_exists，closedir，is_dir，readdir.opendir，fileperms.copy，unlink，delfile ok，大功告成，php木马拿我们没辙了，遗憾的是这样的话，利用文本数据库的那些东西就都不能用了。 如果是在windos平台下搭建的apache我们还

需要注意一点，apache默认运行是system权限，这很恐怖，这让人感觉很不爽.那我们就给apache降降权限吧。 net user apache fuckmicrosoft /add net localgroup users apache /del ok.我们建立了一个不属于任何组的用户apche。 我们打开计算机管理器，选服务，点apache服务的属性，我们选择log on，选择this account，我们填入上面所建立的账户和密码，重启apache服务，ok，apache运行在低权限下了。 实际上我们还可以通过设置各个文件夹的权限，来让apache用户只能执行我们想让它能干的事情，给每一个目录建立一个单独能读写的用户。这也是当前很多虚拟主机提供商的流行配置方法哦，不过这种方法用于防止这里就显的有点大材小用了。 