LNMP服务器安全及优化指南

作者：杨树海

QQ：130775

博客：www.4wei.cn

目录

[Linux权限配置 2](#_Toc289336162)

[PHP安全配置 3](#_Toc289336163)

[NginX安全配置 4](#_Toc289336164)

[Mysql安全配置 5](#_Toc289336165)

[其它优化建议 6](#_Toc289336166)

# Linux权限配置

1. 合理分配SSH管理及用户间的权限，记录登陆日志，如果可能，可以配置防火墙，只开放某些IP进行管理
2. 合理分配FTP权限，如果可能，可以关闭FTP 功能
3. 所有网站统一放置于某一WEB目录，设置适当目录权限（根据网站程序，分配不同网站不同目录的读写权限，除需要写入文件的目录授予777权限以外，其它目录均可以考虑只给555权限）
4. 定期扫描或者记录网站目录下，新建、修改过的PHP文件，认真进行记录分析
5. 定期扫描或者记录网站目录下大小超过100KB或小于1KB的PHP文件，这类文件通常都是木马

# PHP安全配置

1. 禁用高危函数  
   disable\_functions= exec,passthru,shell\_exec,system,popen,proc\_open,proc\_close,curl\_exec,curl\_multi\_exec,parse\_ini\_file,show\_source,dl,passthru,escapeshellarg,escapeshellcmd
2. 禁用高位类库  
   disable\_classes = "com"
3. Php.ini中，请将open\_basedir限制为网站所在Web目录，禁止跨目录请求
4. PHP6以下的版本，请设置register\_globals = Off

# NginX安全配置

1. 禁用Nginx文件类型错误解析漏洞  
   参考：http://www.80sec.com/nginx-securit.html
2. 启用网站目录隔离，不同网站配置不同对应权限，防止跨站  
   参考：<http://www.xpb.cn/blog/665.html>
3. Nginx配置虚拟主机的功能尚不完善，网站权限控制比较复杂，建议认真分配网站各目录的读、写、执行权限
4. 文件上传所在的存放目录，一定要禁止PHP程序运行
5. 记录PHP运行日志和错误日志，认真分析异常访问请求

# Mysql安全配置

1. 关闭除跳转服务器以外的其它远程链接
2. 每个网站设置不同的数据库管理账号并分配最低权限
3. 禁用Mysql 除Root账户以外其它用户的以下权限：  
   FILE、PROCESS、GRANT、SUPER、SHUTDOWN

# 其它优化建议

1. 开启Memcache
2. 开启eAccelerator
3. 开启Mysqli扩展