A Guide to Securing Your Moodle Server

Simple Measures

- The best security strategy is a good backup!
    - Backup! Backup! Backup!
    - If you have your server on the Internet long enough you will eventually face a security breach of some sort. Normally this is just someone looking to steal your bandwidth, but you should always be prepared for the worst, even while you hope for the best.
- Don't load software or services you are not going to use
- Perform regular updates

Run regular security updates on your operating system and software

- Windows: Windows Update
    - Install versions of php that have security patches
        - subscribe to the php security alert list.
    - Install updated versions of mysql that have security patches
        - subscribe to the mysql security alert list.
- Linux
    - Red Hat Based (CentOS/Whitebox, etc)
        - up2date and yum
    - Debian Based
        - apt-get upgrade; apt-get upgrade
    - Consider automating updates with a schedule scripted via cron
        - Note that is you use the up2date or apt systems to install your mysql and php software than this method updates not only your basic OS files, but also your php and mysql software
        - Note that update systems often do not upgrade the kernel by default.
- Consider subscribing to a security alert mailing list for your OS, or a generic one such as Cern's

Firewalls

- Security experts recommend a dual firewall system using two different types of firewalls between the public Internet and your server.
    - Differing hardware/software combinations decrease the likelihood of one bug compromising system security
    - Dual Firewalls are not always practical
- Not installing unused software and or disabling unused services is often as effective (more so) than the way most firewalls are deployed.
- Firewalls are not the end all be all of security, esp for web specific exploits that are commonly used against off the shelf web applications.

- Model your security after the layers of clothing you wear on a cold winter day. No single layer by itself stops you from freezing, but multiple layers acting together keep you warm, and secure!

Be prepared for the worst

- If you operate a public server long enough your security will eventually be compromised.
    - Have backups ready
    - Practice recovery procedures ahead of time
    - Learn how to use a rootkit detector and run it on a regular basis
        - Linux/MacOSX: http://www.chkrootkit.org/
        - Windows: http://www.sysinternals.com/Utilities/RootkitRevealer.html

Moodle Specific Measures

Moodle Security Alerts

- Register your site on Moodle.org and you will automatically receive security emails for the email address you used to register with.
- http://security.moodle.org/
- Subscribe to the moodle security list
    - RSS feed (http://security.moodle.org/rss/file.php/1/1/forum/1/rss.xml)

Commercial vs open source security, forum post
http://moodle.org/mod/forum/discuss.php?d=36387

Hosting multiple sites with a single moodle install. Easing upgrading of Moodle.
http://moodle.org/mod/forum/discuss.php?d=36875#171276

There is a setting to make profiles searchable and indexable by Google. In admin settings. OpentoGoogle is the setting name. Consider not allowing this, esp for sites with K12 students.

Consider using SSL for at least authentication. Note that SSL increases server loade, but encrypts data between server and sender.

Have a site guideline for how course access is limited. Consider placing enrollment keys on all courses and restricting access from guest users if not needed.

The site is only as good as the passwords used. Use good password selection criteria. Require passwords to change on a regular basis. If using an external

authentication source then this may already be managed for you by someone else.

Secure forms setting? Are there security implications to this setting?

Most secure file permissions posts
http://moodle.org/mod/forum/discuss.php?d=36185
http://moodle.org/mod/forum/discuss.php?d=38428

MySQL Specific
Make sure you have set the MySQL root user password. Many installers and packages set this to blank by default. MySQL may also be setup to not allow access from the network. This is the best policy for security. This is the current default on most new mysql installers, but don't assume. Setup to allow no network access or only to listen two connections from 127.0.0.1. If you need to have access from several remote machines than use mysql user permissions to restrict access to specific hosts.