13 better security tips for Joomla CMS

TipsMake.com - With the current popularity of Joomla, it is not surprising if many hackers take it as the main goal. However, you don't need to worry. There are a number of things you can do to increase the security of your website, this article will offer those solutions.

TipsMake.com - **With the current popularity of Joomla, it is not surprising if many hackers take it as the main goal. However, you don't need to worry. There are a number of things you can do to increase the security of your website, this article will offer those solutions.**

Joomla is popularly developed as an open source CMS, which is increasingly being used by many individuals and businesses as the foundation for their online products and services. In fact, more than 2.5% of websites run Joomla CMS - this is a good goal for hackers to attack.

Joomla is free and has more than 8,600 extended settings (*extensions*) that allow you to do most of what you want on CMS. Add to that a strong development community that helps you see that this is an attractive product and also attractive to hackers. For that reason, you need to do a few things when using this platform to prevent attacks and increase the security of your CMS.

The platform for installing this platform is just one of the weaknesses of the system, most of its security issues relate to Joomla's code. Most problems arise from the old version, are not updated regularly or sometimes due to the expansion settings (third party *extension*).

1. Server and Host

There are no important decisions by selecting the appropriate host or host. Many problems may arise because the server / host has not been patched, some ports are open or the shared security is poor. Even if the server is set up correctly, the system can still be attacked by another website hosted on that server with poor security. If you're using a poor host, think about switching providers or it's best to replace it with a separate server so you don't have shared security issues.

Currently there are some famous and quite secure Hosting providers like Brinkster or Godaddy.

Store your website on a server running PHP 5.2 or better in CGI mode with Su_PHP. Su_PHP basically allows script execution under a specific user account, as opposed to Apache's default account. This makes it easy to identify and track security areas.

Make sure you are using the latest version of Apache and configuring Apache does not allow *browsing / indexing* (*browsing / indexing*). IT managers also need to ensure that there are appropriate settings for the location of the *.htaccess , serverconfig* and *php.ini files* .

2. Activate and use htaccess file

By default, htaccess files are not used. Make sure you rename it from *.htaccess.txt* to **.htaccess** , then it needs to be placed in the root directory of the website. You can also add some rewrite rules for it to prevent the possibility of being exploited. You can find more instructions on editing htaccess files for additional protection for the system.

3. Use accounts and Permission

Joomla works well from the beginning after properly installing on the server. You need to set all CHMOD files to 644 and folders to 755. There are some exceptions to this rule as the **configuration.php** file will convert CHMOD to **640** . Make sure nothing is set to 777.

The default administrator account name is usually " **admin** ", you must immediately change this account name. It will make it a little more difficult for hackers to find account name details.

4. Backup and troubleshooting

Take the time to consider a troubleshooting plan first, not after your website is visited by hackers. Advance the outline of what will happen if you become a victim. Must remember: " **Backup early and often** ". If this step works well, the biggest pressure when the website is hacked is gone, because the data is the most important, you've always backed up. Perform daily backups or even - *if possible* - for hours to ensure that when you restore, your website has no downtime or data loss. Once a backup is available, the only thing to worry about when a problem occurs is to look for a vulnerability on the website.

5. Carefully manage the extension settings (extension)

Third-party extensions are what make Joomla so popular, but it is many times the way to get into your website. Each different extension is an object that you need to update patches on a regular basis. This is also the reason you need to consider installing only really necessary extensions. You should be sure to take the following steps:

1. Implement the review code for any extension used.
2. Run a test set (there are many on-line) and review the results.
3. Update and patch the extension as needed.

Remember, an unsafe extension can harm your entire website.

6. Delete the version number of the extended installation

Typically, exploits typically specify a specific version of the extension, which is why you should delete the version number information of any installed extensions. Removing version numbers can prevent an attack before it happens.

You can edit the extension so that it only displays the name using a tool like Dreamweaver. Do a global search and replace all the necessary information in the file extension folder.

7. Remove unused files

You install a lot of extensions but don't use it? This is not only a weakness but also garbage for your server. Please remove them completely to avoid possible inconvenience.

8. Password protection

Common attacks often target weak passwords. Make a good habit: ***Regularly change your password and it must ensure 4 elements: uppercase, lowercase, special characters and numbers*** .

Your database (CSDL) is very important. A SQL injection attack or any other type of attack on the database can make your whole month of work disappear. Make sure your database access is a password protected at MySQL level. Try using tools like Nikto or Nmap to scan the system, look for open exploits and weaknesses.

Password protection in Joomla administration section is at the directory level. This password adds an additional layer of security. It is usually a different username and password.

9. Change the Prefix to the default table

Most SQL injection attacks often try to access the **jos_users** database table. Once hackers can access this file, they get the corresponding user name and password - including the senior administrator. Using a short, random name to replace this default name helps prevent most database attacks.

If you are using Joomla 1.5, you can use DB administration components to do this. If you're using version 1.6 and don't make changes during the installation, this process can still be done but it's a bit more complicated.

In other versions of Joomla, including 1.7, random table names are used during the installation process to combat these types of attacks.

10. Use SSL certificate

Use SSL on your website for all member login. Note that you must have a properly configured SSL certificate for your website domain (SSL certificate sharing will not work).

11. Disable Joomla FTP Layer

Disable the FTP Layer of Joomla and make sure it does not save your login information.

12. Turn off Register_globals

Turn off Register_globals, but you must know that this can disable some PHP working scripts, and may affect other programs that your website is using. To do this, simply edit the php.ini file of the website in the root of the domain name.

13. Friendly URL for search engine

Always use search engine friendly URLs. This not only improves Google's website rankings but also prevents hackers from exploiting Google's search results.

References:

1. http://www.joomla.org
2. http://secunia.com/advisories/product/5788/
3. http://trends.builtwith.com/cms
4. http://www.opensourcevarsity.com/joomla1-7/joomla17install
5. http://blog.rochenhost.com/2008/09/joomla-security-ever-been-hacked-sorting-fact-from-fiction-some-useful-joomla-hosting-tips-including-some-you-might- now-know /
6. http://www.siteground.com/tutorials/joomla15/joomla_security.htm
7. http://docs.joomla.org/Vulnerable_Extensions_List
8. http://docs.joomla.org/Category:Security_Checklist
9. http://en.wikipedia.org/wiki/Joomla
10. http://www.securelive.net/
11. http://www.howtojoomla.net/how-tos/security/joomla-security-primer