

## XOOPS SITE SECURITY GUIDE

First of all, you should keep this in mind - there is no such a thing as a 100% secured system. Everything is relative. Having said that, there are things you can do to make your system better secured.

This guide summarizes various steps to secure your site with tips from both this site and the official Xoops forums. Majority of the tips have already been listed on this site, but not in a structured way. We are hoping the structured presentation of all tips, old and new, will provide a better grasp of security issues.

### **Choosing a Host**

Many of us tend to diminish the importance of a good web hosting company and go with whoever offers the "best features" with minimum cost. You should put a lot of thoughts in selecting a host.

A good and reputable hosting company usually means good web security. As most of us do not have a budget for a dedicated server, you should pay special attention to the security of the whole server and other sites on the same server.

The securities of other sites and the server are just as important as the security of your site.

No matter how secure your site is, if the server has been compromised via other sites on the same server, all your efforts in the end may mean nothing in protecting your site.

One-man shop, resellers and small web hosting companies should be avoided if you can, as they generally don't have the resources or skills to properly manage and monitor your servers.

As web hosting increasingly being commoditized, web hosting is no longer a big expenditure. A good web host is worthy of the extra you paid.

The scarce part of web hosting is that nowadays, you could rent a server from large wholesalers such Everyone's Internet for \$200 or less a month and become a web host overnight. As long as the resellers pay their fees, the wholesalers don't give a damn to the server securities.

When you choose a reseller, ask yourself this question, "does the host have the skills to properly manage the server?"

If your hosting company is located in UK but its servers are located in Texas, what would happen if your server were to break down? You would have to call your host, and then your host would have to call its host to sort the problems out. Hopefully you got the idea.

When you select a host, keep this in mind, "What you paid, what you get". If your site is important to you, don't settle with a \$2 a month web host.

## **Installation - Choose a table prefix**

During the installation process, choose a not easily guessable table prefix. Don't use the stock "xoops" table prefix. It is too easily for crackers to guess.

If you have installed your site with "xoops" default table prefix, you can use GIJOE's Xoops protector module will change the prefix.

## **Post Installation**

Once you have successfully finished Xoops installation, do not forget to remove the install directory and chmod mainfile.php. Leaving your installation directory unremoved and mainfile unprotected, you are openly inviting others to overwrite your previous installation and take control of your site. If they were to do malicious things using your site, you would end up be liable for any damages done.

## **Install Xoops Protector Module**

Once you have finished the installation, the first module you should install is GIJOE's Xoops Protector module. If you are serious about the security of your Xoops site, the protector module is a must for your site.

Xoops system is perhaps one of the securest CMS systems around. However, its core does have weakness that could potentially allow crackers into your site. This has been demonstrated by GIJOE, by far the biggest contributor of Xoops security.

Xoops 2.0.10 will incorporate some of GIJOE's ideas. But the protector module is still highly recommended as it defends against attacks on both XOOPS core and modules.

The protector module can protect a various kind of attacks, such as DoS; bad crawlers or bot; SQL injection; XSS; system globals pollution; session hi-jacking; null-bytes; wrong file path specifications; CSRF (which is fatal in XOOPS <= 2.0.9.2).

For more information, please check GIJOE's website:

[www.peak.ne.jp/xoops/](http://www.peak.ne.jp/xoops/)

## **Move Username and Password out of Mainfile.php**

An additional consideration about your Xoops installation is moving database username and password out of the web tree. It is always a good practice keeping your sensitive information out of the web tree. This would prevent accidental disclosure of your sensitive information if your server were to mis-function, such as PHP stopped rendering. In this case, information in your mainfile.php is worldly readable by anyone.

For more information please check this TIP  
<http://xoops-tips.com/news-article.storyid-1.htm>  
(or see Appendices)

### **Protect Admin.php and System Module**

Xoops admin.php is accessible to anyone thus poses security problem if crackers do want to take a run of your systems. There are ways you can protect it. For more information check this TIP:

<http://xoops-tips.com/news-article.storyid-9.htm>  
(or see Appendices)

### **Protect Theme Directory**

You can protect your theme files from prying eyes. For more information check this TIP:

<http://xoops-tips.com/news-article.storyid-25.htm>  
(or see Appendices)

### **Disable Directory Listing**

If your host allows you to disable directory listing, turn it ON. If your host does not provide such a mechanism, create a simple index.html file with following  
<script>history.go(-1);</script>

Upload it to every directory of your Xoops site (except the root or module root directories).

Xoops stock distribution does provide this file in majority of the directories. Make sure every directory has it.

### **Protect Admin Email Address**

You should never ever reveal your Xoops admin email addresses to the world, except to your users. If you are using stock Xoopsheadline module, please consider this TIP to hide your admin email address:

<http://xoops-tips.com/news-article.storyid-51.htm>  
(or see Appendices)

## **Third-Party Modules**

Pay special attentions to third party modules. There may exist security risks that the developer(s) may have not been aware of.

If you are using modules from a third party, be sure to check for update and security fixes, and check Xoops forums regularly from other users.

Xoops protector module offers protection, but it might not be enough to protect you from serious security breaches.

## **Backing Up Your Site and Contents**

Backing up your contents should be considered as one of the most important aspect of protecting and securing your site. Regular backing up and downloading should become a routine.

If your contents change daily, you should do database backup daily. If your contents do not change on a daily basis, then a weekly database backup should be considered (**at least**).

As of the site files, a monthly backup should be sufficient. Or do an ad hoc backup whenever you have made major changes to your site.

## **Balance of Attracting Users and Security**

Some Xoopsers are attempted to open up their sites to anyone, crackers included, in a bid of attracting users to their sites. Our advice is "DON'T!!!"

Users will stay with you as long as you have unique contents or unique service offerings. They will NOT if you have little contents or service to offer, no matter what enticements you throw at them.

Running an un-moderated site is an open invitation for troubles. Sooner or later, you will regret of doing that.

## **Keep Your Xoops Core Up to Date**

You should keep your Xoops system up-to-date with new releases. Xoops Core developers are keen on security issues and bug fixes. With each new release, you eliminate potential bugs and security holes.

Don't have any illusions that the security holes will not exploited against your site. Securities holes had been and will be exploited if you don't plug them.

## **PHP and MySQL**

Since Xoops uses the combination of PHP and MySQL, it has also inherited a glaring weakness. MySQL requires PHP to send plain username and password. This, as you would guess, creates security headache. If your session got hijacked, then your database would be exposed. There is no easily devised mechanism to bypass this. We are mentioning this just to make you aware the problem.

If your host allows you to run PHP in cgi-wrap, you may consider using it. But be aware of using it on a busy site – you will incur speed penalties using it.

## **Cached Contents**

If you are selling contents, consider add the following to the header of your theme.html file.

```
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
```

This will stop people from stealing your contents. Even you had IP-banned them; they could still get a copy of your contents by clicking on cached version under Google (or other SE) search results. The cached versions are from the search engine's servers not yours, so you will have no control.

Be careful of using the tag, most of the search engines are particularly against URL cloaking. Unfortunately, the technique of cloaking is the use of noarchive tag. Your site may risk of being labeled by SEs as an offender of cloaking thus having the rank lowered.

## **Other Things to Make Your Xoops Site Secure**

If you have implemented all the suggested steps, your site should be fairly secure. As we have emphasized in the beginning, please don't be over-confident. A good practice is always skimming through your daily logs to spot potential problems and make correctional measures.

Hope this guide is helpful and secure Xoopsing to all!

## Appendices

### I. Move MySQL username/password out of mainfile.php

Xoops stores MySQL username and password combination in mainfile.php file. It is very insecure to store these in mainfile.php file, which is accessible by anonymous web site visitors.

Although the PHP code is interpreted at the server, and therefore a user name/password combination is unlikely to be shown in a web browser, it really not wise to store the combination in a publicly accessible place. Should the server stop interpreting PHP for some reasons, the combination would be available in plain view and readable by the world.

This tip will show how you can move the combination into a safe place, outside of your web site's document root. This way, it's not accessible by visitors, but it is available to Xoops.

**Precaution: This is a serious attempt and it may cause your web site stop working. You MUST know what you are doing and proceed at your own risk.**

#### Assumptions:

Your site root is /home/yoursite.com/

Your web root is /home/yoursite.com/public\_html

#### Create a folder outside your web root

Use FTP/SSH/Cpanel create a folder called /home/yoursite.com/securedata (you may want to name it to whatever you like)

**Create a php file** using your favorite editor (mine is notepad)

Fill in your mysql information in the file

```
<?php
$db_user = "db username"; //database username here
$db_passwd = "db password"; //database password here
$db_name = "db name"; //your database name here
?>
```

(Please take the slashes "\" out of the file, they are added by Xoops, are not part of the file.)

Save the file as xoops-auth.php and upload to /home/yoursite.com/securedata

**You may need to chmod 644 xoops-auth.php**

**WARNING: Please make sure there is NO white space after ?> Xoops is extremely sensitive to whitespace. You would either have a "blank page" or not able to log into your system, if there were a whitespace. So be warned.**

#### Modify mainfile.php

Please back up mainfile.php first, in case that something were to go wrong, you could simply replace the modified file with the original.

Chmod 777 mainfile.php

Add the following line in top of the mainfile.php file

```
include ("/home/yoursite.com/securedata/xoops-auth.php");
```

modify the following setting in mainfile.php

```
// Database Username
// Your database user account on the host
define('XOOPS_DB_USER', $db_user);

// Database Password
// Password for your database user account
define('XOOPS_DB_PASS', $db_passwd);

// Database Name
// The name of database on the host. ...
define('XOOPS_DB_NAME', $db_name);
```

**Please make sure that there are NO quotes around \$db\_user, \$db\_passwd, and \$db\_name. Just \$db\_user, ... as in the illustration**

Save the file and test. If your website continues to function, congratulations!

Don't forget, afterwards - chmod 444 mainfile.php

This tip will not stop crackers from getting the combination, if they can "read" your session.

### **Re: Move MySQL username/password out of mainfile.php Two alternative ways of doing it (suggested by Dave\_L)**

1. Replace the contents of mainfile.php with:

```
<?php require_once('/path/to/protected/dir/mainfile.php') ?>
```

The path specified above is your "real" mainfile.php. [copy the working real mainfile.php to the protected directory, then create a new mainfile.php file suggested by Dave. Be careful with whitespace. tl]

2. You could leave mainfile.php alone, and add an .htaccess file to the main Xoops directory:

```
<Files "mainfile.php">
Deny from all
</Files>
```

[First alternative is preferable, as it is not under the webtree. tl]

## II. Protecting Xoops Admin Login

Some people (count me as one of them 😊) are not very comfortable with admin.php located in the root directory. The location of the file does pose a security risk; and crackers could really take hack at it. Adding two .htaccess files will help you protect against misuses/crackes of your admin login and system module.

Web Server: Apache

Requirements:

Your hosting company allows .htaccess;

You have a static or semi-static IP address

Assumptions:

Webmaster A has a static IP 123.456.789.012

Webmaster B has a DSL line and a semi-static IP 456.789.123.456 (the last two sets change every time the DSL reconnects)

In the root .htaccess file, enter the following

```
<Files admin.php>
order deny,allow
deny from all
allow from 123.456.789.012
allow from 456.789
</Files>
```

In the /modules/system/.htaccess file, enter the following

```
AuthName "protected"
AuthType Basic
<Limit GET POST>
order deny,allow
deny from all
allow from 123.456.789.012
allow from 456.789
</Limit>
```

If you do xoops admin from multiple places, then just add the IP addresses into the allow from list. If it happens that you have to do urgent admin from someone else's computer, use FTP to download the .htaccess files, add the IP of the computer you are using, upload. Once you have finished your admin, delete the new IP from the files.

## III. Protecting Theme Files

Xoops Newsletter Editon 4 published DonXoop's tip protecting theme.html. You can create a .htaccess file either in your individual theme directory or in the theme root directory"

yoursite/themes/

Add the following in the file.

```
<Files ~ "theme.html">
Order allow,deny
Deny from all
</Files>
```

```
<FilesMatch "theme_blockcenter_?.html">
order deny,allow
deny from all
</FilesMatch>
```

The second section protects all of your 3 center blocks if you have them separated from the main theme.html

You can download the .htaccess sample file from the download section. Upload it and rename to .htaccess

Note: This tip applies only apache servers. Make sure there is no space after <  
Thanks to DonXoops for sharing this tip.

#### IV. Protect Admin Email Address – Backend.php

If you are using backend.php to syndicate your news, you should be aware that it might unwittingly expose too much information about your site. You would have to make some changes to backend.php file.

##### locate

```
if (is_array($sarray)) {
    $tpl->assign('channel_title',
xoops_utf8_encode(htmlspecialchars($xoopsConfig['sitename'], ENT_QUOTES)));
    $tpl->assign('channel_link', XOOPS_URL.'/');
    $tpl->assign('channel_desc',
xoops_utf8_encode(htmlspecialchars($xoopsConfig['slogan'], ENT_QUOTES)));
    $tpl->assign('channel_lastbuild', formatTimestamp(time(), 'rss'));
    $tpl->assign('channel_webmaster', $xoopsConfig['adminmail']);
    $tpl->assign('channel_editor', $xoopsConfig['adminmail']);
    $tpl->assign('channel_category', 'News');
    $tpl->assign('channel_generator', XOOPS_VERSION);
    $tpl->assign('channel_language', _LANGCODE);
    $tpl->assign('image_url', XOOPS_URL.'/images/logo.gif');
```

##### Make three changes (highlighted)

```
if (is_array($sarray)) {
```

```
$tpl->assign('channel_title',  
xoops_utf8_encode(htmlspecialchars($xoopsConfig['sitename'], ENT_QUOTES)));  
$tpl->assign('channel_link', XOOPS_URL.'/');  
$tpl->assign('channel_desc',  
xoops_utf8_encode(htmlspecialchars($xoopsConfig['slogan'], ENT_QUOTES)));  
$tpl->assign('channel_lastbuild', formatTimestamp(time(), 'rss'));  
$tpl->assign('channel_webmaster', XOOPS_URL.'/');  
$tpl->assign('channel_editor', XOOPS_URL.'/');  
$tpl->assign('channel_category', 'News');  
$tpl->assign('channel_generator', 'Xoops');  
$tpl->assign('channel_language', _LANGCODE);  
$tpl->assign('image_url', XOOPS_URL.'/images/logo.gif');
```

In doing so, you eliminate the risks of exposing your admin email address and the Xoops version. If left unprotected, your admin email might be harvested and ended up in spammers' database; and a cracker would have an easy time figuring out your system weakness if he/she knew your Xoops version.