A Guide to Make your XOOPS Installation even more secure - Security

NEWS_PDF_AUTHOR: anderssk

NEWS_PDF_DATE: 2008/9/13 20:30:00

The reason for writing this guide is **NOT** because XOOPS CMS-system isn’t secure enough.

It’s written to give new XOOPS'ers a chance to make, with a few changes, a secure installation even more secure. We believe, that existing users also can use the guide, for securing an already installed XOOP website.

This guide is written for XOOPS version 2.3.3RC as Core-version.

Initial steps

First initial step is to create a support ticket. There are some default settings, that have to be changed.
If you are using another hosting company, make sure that;

'register_globals' is set to OFF. That can be done in PHP.ini but also in the .htaccess file adding **php_flag register_globals off**
'allow_url_fopen' is set to OFF. That can only be change in PHP.ini or in Apache httpd.conf
'session.use_trans_sid' is set to OFF. That can be done in PHP.ini but also in the .htaccess file adding **php_flag session.use_trans_sid of**

Next, [Download XOOPS]() and unzip it.

Now you have 4 folders. These are htdocs, docs, extras and upgrade.

Create a fifth folder and name it **temp.**
Inside the **htdocs** folder you will find 2 folders named **xoops_data** and **xoops_lib**.
Move them from **htdocs** to the temp folder.
Create a new folder in the same directory level as **xoops_data** and **xoops_lib**
Name it anything you want. It’s for keeping the database credentials later on.
You can also rename the **xoops_data** and **xoops_lib** folders to something else.

As you can see beneath, we have used the original **htdocs** and a folder named **temp**
In the **temp** folder we have 3 sub-folders names:

mainsite_xoopsdata
mainsite_xoopslib
mainsite_secure

That’s because later on, we want to install one or two subdomains, and we can’t have the same folder names for

different sites.
Beyond that, it decreases security, when sensitive data is stored in folders with default names.

Click on the image to enlarge

Prepare installation of Protector module

Delete **mainfile.dist** in **htdocs** folder
Copy **mainfile.dist.php.protector** from **extras** to **htdocs**.
Rename **mainfile.dist.php.protector** to **mainfile.dist.php**

Uploading content

Now you have to upload the content to the web-host.

The first thing to upload are the 3 special-folders from the temp folder.

Do **not** upload them in **public_html** or **www**
You have to upload them within Your home-directory ***/***

Click on the image to enlarge

Now you can upload the content of **htdocs** in to **public_html**

Preparing e-mail

We always like to keep our personal mails and our webmaster mails separated.
Therefore you should create a mailaccount for webmaster-use at the site.

Login to your Cpanel at http://www.*yoursite.com*/cpanel , and select **email accounts**

Click on the image to enlarge

Type in **webmaster** in the email formula and click **generate password**
The password there is generated is absolutely strong, and you don’t have to remember it for pop3 access, so why choose an easy password..
Finish up by clicking **create**.

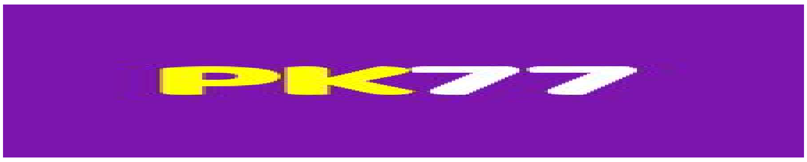
Click on the image to enlarge

Preparing database

Login to your Cpanel at http://www.*yoursite.com*/cpanel and select **email accounts**
If you’re already signed in, just click at the **home**icon at the top left corner.
Scroll down and locate the databases, and click on **MySQL Databases**

Click on the image to enlarge

Enter a name for your database and finish by clicking **Create Database**



Click on the image to enlarge

Go back and create a MySQL user for the database
Type in a name for the user in the user name formula and click **generate password**
The password there is generated is absolutely strong, and you don’t have to remember it for daily database access , only when installing XOOPS.

Finish up by clicking **Create User**

Click on the image to enlarge

Just two more steps:
Go back and scroll down to **Add User To Database**
Select the user and database you created
Click **Add**
Mark **All Privileges** and click **Make Changes**

Click on the image to enlarge

Finally Install

Open your site at http://www*.yoursite.com*

You will see the first step of the installation wizard.

Click on the image to enlarge

Second step tells you about the requirements and some initial steps.
Step 5 and 6 is made, but take notice on step 7. They have to be writeable!

Click on the image to enlarge

Third step shows you server configuration.
The extensions are default at Danordesign.com. On other hosting companies the results may be different.

Click on the image to enlarge

Fourth step checks the paths settings, and now you should see two errors.
Change the **datafiles directory** and **library directory** to the name you gave them.
Remember to remove the **public_html** in the paths

Click on the image to enlarge

Fifth step is the Database settings.
Just put in the userrname and the password that was autogenerated.
Keep **localhost** as server hostname.

Click on the image to enlarge

Next step: You only have to type the database name that you created earlier

Click on the image to enlarge

Step seven and eight are just next-pictures.
In step nine I’ve added the webmaster account/password, and webmaster email.

Click on the image to enlarge

Step eleven.
You can change the default settings for your site at this point. If you don't want to do it now, it can be done later in your sites system settings preferences.

Click on the image to enlarge

Step thirteen. Now it's time to install some of the default modules.
In this guide we only choose to install Protector.

Click on the image to enlarge

Step fifteen is the last step.

Remember to delete the install_remove_xxxxx folder after install!

Click on the image to enlarge

Customizing

First step is to logon with the webmaster-account.

Now you have to work locally.
Create a txt-file with the following content.:(replace with your own user, password and database name)

Click on the image to enlarge

Save the file with the extension .php.
The name is up to you.
Upload the file into the third folder you created

Click on the image to enlarge

Now download mainfile.php located at **/public_html**

Open mainfile.php in a text-editor (notepad is fine)
Insert the line:

```
include ("/home/xxxxxxx/mysecurefolder/mainsite_db_credentials.php");
```

In the beginning of mainfile.php

Click on the image to enlarge

Scroll down and change the settings for the 3 settings for database connections

Click on the image to enlarge

Save the file and upload it again.

Final step

Login to You Cpanel at http://www*.yoursite.com*/cpanel and select **File Manager**

Click on the image to enlarge

In the window that shows up, select **Web Root (public_html/www)** and click **go**

Click on the image to enlarge

In the file manager locate **mainfile.php** and click on the permissions (the value are 0644) at the right.
change the value to 0444 and click OK.

Click on the image to enlarge

Now open your site and click on **Administration menu.**
Click on **Protector** and select **Security Advisory** to check that everything looks good!

Click on the image to enlarge

Other things.

If You install the backup module (strongly recommended)
https://xoops.org/modules/repository/singlefile.php?cid=17&lid=1115

The cronjob in Cpanel should be
/usr/bin/GET http://yourwebsite/modules/backup/admin/backup.php

The reason for writing this guide is **NOT** because XOOPS CMS-system isn’t secure enough.

It’s written to give new XOOPS'ers a chance to make, with a few changes, a secure installation even more secure. We believe, that existing users also can use the guide, for securing an already installed XOOP website.

This guide is written for XOOPS version 2.3.3RC as Core-version.

Initial steps

First initial step is to create a support ticket. There are some default settings, that have to be changed.
If you are using another hosting company, make sure that;

'register_globals' is set to OFF. That can be done in PHP.ini but also in the .htaccess file adding **php_flag register_globals off**
'allow_url_fopen' is set to OFF. That can only be change in PHP.ini or in Apache httpd.conf
'session.use_trans_sid' is set to OFF. That can be done in PHP.ini but also in the .htaccess file adding **php_flag session.use_trans_sid of**

Next, Download XOOPS and unzip it.

Now you have 4 folders. These are htdocs, docs, extras and upgrade.

Create a fifth folder and name it **temp.**
Inside the **htdocs** folder you will find 2 folders named **xoops_data** and **xoops_lib**.
Move them from **htdocs** to the temp folder.
Create a new folder in the same directory level as **xoops_data** and **xoops_lib**
Name it anything you want. It’s for keeping the database credentials later on.
You can also rename the **xoops_data** and **xoops_lib** folders to something else.

As you can see beneath, we have used the original **htdocs** and a folder named **temp**
In the **temp** folder we have 3 sub-folders names:

mainsite_xoopsdata
mainsite_xoopslib
mainsite_secure

That’s because later on, we want to install one or two subdomains, and we can’t have the same folder names for different sites.
Beyond that, it decreases security, when sensitive data is stored in folders with default names.

Click on the image to enlarge

Prepare installation of Protector module

Delete **mainfile.dist** in **htdocs** folder
Copy **mainfile.dist.php.protector** from **extras** to **htdocs**.
Rename **mainfile.dist.php.protector** to **mainfile.dist.php**

Uploading content

Now you have to upload the content to the web-host.

The first thing to upload are the 3 special-folders from the temp folder.

Do **not** upload them in **public_html** or **www**
You have to upload them within Your home-directory ***/***

Click on the image to enlarge

Now you can upload the content of **htdocs** in to **public_html**

Preparing e-mail

We always like to keep our personal mails and our webmaster mails separated.
Therefore you should create a mailaccount for webmaster-use at the site.

Login to your Cpanel at http://www.*yoursite.com*/cpanel , and select **email accounts**

Click on the image to enlarge

Type in **webmaster** in the email formula and click **generate password**
The password there is generated is absolutely strong, and you don’t have to remember it for pop3 access, so why choose an easy password..
Finish up by clicking **create**.

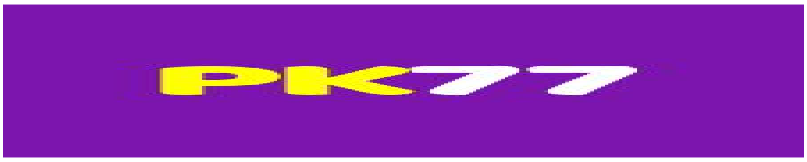
Click on the image to enlarge

Preparing database

Login to your Cpanel at http://www.*yoursite.com*/cpanel and select **email accounts**
If you’re already signed in, just click at the **home**icon at the top left corner.
Scroll down and locate the databases, and click on **MySQL Databases**

Click on the image to enlarge

Enter a name for your database and finish by clicking **Create Database**



Click on the image to enlarge

Go back and create a MySQL user for the database
Type in a name for the user in the user name formula and click **generate password**
The password there is generated is absolutely strong, and you don’t have to remember it for daily database access , only when installing XOOPS.

Finish up by clicking **Create User**

Click on the image to enlarge

Just two more steps:
Go back and scroll down to **Add User To Database**
Select the user and database you created
Click **Add**
Mark **All Privileges** and click **Make Changes**

Click on the image to enlarge

Finally Install

Open your site at http://www.*yoursite.com*

You will see the first step of the installation wizard.

Click on the image to enlarge

Second step tells you about the requirements and some initial steps.
Step 5 and 6 is made, but take notice on step 7. They have to be writeable!

Click on the image to enlarge

Third step shows you server configuration.
The extensions are default at Danordesign.com. On other hosting companies the results may be different.

Click on the image to enlarge

Fourth step checks the paths settings, and now you should see two errors.
Change the **datafiles directory** and **library directory** to the name you gave them.
Remember to remove the **public_html** in the paths

Click on the image to enlarge

Fifth step is the Database settings.
Just put in the userrname and the password that was autogenerated.
Keep **localhost** as server hostname.

Click on the image to enlarge

Next step: You only have to type the database name that you created earlier

Click on the image to enlarge

Step seven and eight are just next-pictures.
In step nine I've added the webmaster account/password, and webmaster email.

Click on the image to enlarge

Step eleven.
You can change the default settings for your site at this point. If you don't want to do it now, it can be done later in your sites system settings preferences.

Click on the image to enlarge

Step thirteen. Now it's time to install some of the default modules.
In this guide we only choose to install Protector.

Click on the image to enlarge

Step fifteen is the last step.

Remember to delete the install_remove_xxxxx folder after install!

Click on the image to enlarge

Customizing

First step is to logon with the webmaster-account.

Now you have to work locally.
Create a txt-file with the following content.:(replace with your own user, password and database name)

Click on the image to enlarge

Save the file with the extension .php.
The name is up to you.
Upload the file into the third folder you created

Click on the image to enlarge

Now download mainfile.php located at **/public_html**

Open mainfile.php in a text-editor (notepad is fine)
Insert the line:

```
include ("/home/xxxxxxx/mysecurefolder/mainsite_db_credentials.php");
```

In the beginning of mainfile.php

Click on the image to enlarge

Scroll down and change the settings for the 3 settings for database connections

Click on the image to enlarge

Save the file and upload it again.

Final step

Login to You Cpanel at http://www.*yoursite.com*/cpanel and select **File Manager**

Click on the image to enlarge

In the window that shows up, select **Web Root (public_html/www)** and click **go**

Click on the image to enlarge

In the file manager locate **mainfile.php** and click on the permissions (the value are 0644) at the right.
change the value to 0444 and click OK.

Click on the image to enlarge

Now open your site and click on **Administration menu.**
Click on **Protector** and select **Security Advisory** to check that everything looks good!

Click on the image to enlarge

Other things.

If You install the backup module (strongly recommended)
https://xoops.org/modules/repository/singlefile.php?cid=17&lid=1115

The cronjob in Cpanel should be
/usr/bin/GET http://yourwebsite/modules/backup/admin/backup.php