Title: Securing Your Website

Subtitle: Web Technologies

Author: SKenow http://xoopsinfo.com/modules/smartsection/item.php?item
Date: 2007/8/20
URL: https://www.christianwebresources.net/modules/article/view.article.

Keywords: security, php, mysql, apache

Summary: Being responsible for at least one web site, if not more, there
much thought because they seem beyond your control, of little interest, c
Security usually falls in this category.

In spite of all that, anyone who maintains a site has the task of taking th
security. If you don't, your visitors may find one day a new version of yo
your host may suspend your account because a script on your site is cau
you have to do something.

Where do you start? Most of us will need guidance when it comes to secu
and optimization. There is good news - help is readily available, if you a
reviewing the security notes for the different aspects of running a web si
people to get some useful tips to protect your investments of time and ef

First, let's take a look at the major components of your web site - the we
server, the scripting language and your application. Each of those compo
'hardened' for use on the public Internet.

Web Server

This is really 2 components - the operating system (Windows and Linux a
the web server software (Apache and IIS)

You will need a good relationship with your web host for securing these c
about -

- Which version of web server are they running?
- What operating system are they running?
- What backups do they run and how often?
- What security programs and modules to they run? (mod_security for Apa
- Can you block IP addresses?
- Can you turn of indexes? Anonymous FTP access?
- How can you learn about network outages?
- What kind of control panel access do they provide?
- Can you provide overrides for the server? (htaccess files)

The more easily and openly they answer those questions, the better chan
relationship with your provider and being able to secure your web site.

The Database Server - MySql

Your content, your users' information and your entire site is based on a
access to that, you can lose everything!

Again, your hosting provider will be instrumental in this area. Be sure ge
version of the MySql server they are running and it is properly secured.
'anonymous' user, be sure they don't expose your database to unnecessa

The Script - PHP

This is what pulls everything together and presents your content to your
access to the database and the files on your server, it has to have suffic
them, which means there can be malicious use of the script to damage yo
You need to be aware of how to prevent this.

There are different configurations of PHP - suExec is the most secure op
version of PHP is used by your host and how it is configured. Learn if yo
for their default settings.

Again - your hosting provider needs to be a good resource for this. If the
another host.

The Application - XOOPS and Modules

Be sure you are using the latest version of XOOPS on your site (2.0.16,
followed the installation instructions for setting permissions on files and
directory once you have finished your install.

The Protector module provides additional assistance in preventing malici
sure to install the latest version (3.04, as of August 2007) and read the

For more insight into the server and Protector settings, I went to JMorris
admin for XOOPS.org and currently maintains several other sites - here i
discussions -

CXR: James, as an experience server administrator, would you offer som
sites?

James: I can provide some security info in general, but I'm not a securit
"overall" web master. You know, "jack of all trades, master of none."

In a nutshell, most hacks are at the server level and not the XOOPS leve
malicious users behind proxy servers. Server configuration and permissio
defense. If your application is properly coded, everything else is bubble
server configuration, permissions and installation of Protector has kept
some time now.

CXR: What can the average web master do to be sure his server is secur

James: Too many users are caught up in features and do not take the tim
what the risks are with features. If people want to be a "web master" of
students of the risks present online or they will most certainly fall victim
in time. It's not a matter of if, it's a matter of when.

CXR: Where should we start?

James:

1. Turn off Indexes

2. Deny access to folders that should not be directly accessed using an

3. Insist on suExec on their servers (shared accounts will have a tough t

4. chmod 777 is a bad idea - suExec fixes that. templates_c/ cache/ and
chmod 755 with suExec, mainfile.php can be run at chmod 400.

5. Move your DB details out of mainfile.php and out of the web root.

6. chmod 444 any file that does not need written to.

7. chmod 755 all folders. (some modules will stop working if you use chm

8. Turn off anonymous ftp access.

9. Be sure all mysql users have a secure password (like: P4s5.w0_rD).

10. Be sure SSH (if enabled) has properly configured permissions and th

11. Research security threats on any module before installing it.

12. In addition to the PHP tweaks suggested by Protector, have your hos
Fork Bomb protection.

13. Never give admin rights to anyone, especially to the XOOPS blocks a

14. Never assume you are safe. Regularly audit your site for suspicious

15. Backups, Backups, Backups, Backups, Backups!

CXR: That's a lot to be considered!

James: I don't know nearly as much as I want to know about the topic. It
And, it's constantly changing. That's why it is important be proactive and

CXR: After the server is secured, then what?

James: Where XOOPS is most vulnerable is modules - many modules do n
strings and therefore can be exploited to reveal DB details. That's where

CXR: Are the default settings in Protector what you use?

James: I set Protector to the most restrictive settings possible, then bac
Remember, I'm p@r@n0!D and for a darn good reason! "If you're not p@
attention."

Banning an attacker's IP is only a temporary fix. Banning their IP will slo
much. Eventually, the attackers will find another proxy with another set o
continue their attacks. The real issue is closing the hole in the applicati

One last thing to **Yocounrsiudseerr.s**

Sorry, but that's the truth. XOOPS has a great permissions system, but i
permissions, your users can get access to areas of your site that can cau

In future articles, we will look more closely at the individual components
your web site running smoothly.

Here are some additional resources -

- Xoops-tips : Protecting DB information
- Xoops-tips: Protect Admin Login
- XOOPS FAQ: Protecting your site
- Xoops-tips: Webmaster Security Guide
- Starting a New XOOPS Site: Day 21 - Security Checkpoint