Subject **DailyDealFind.com, Is Your WordPress Blog Secure?**
Sender Daily Blog Tips <daniel@dailyblogtips.com>
Recipient DailyDealFind.com <hello@dailydealfind.com>
Date 01.03.2011 05:07

Hi DailyDealFind.com,

Daniel Scocco here, and this is the Daily Blog Tips newsletter.

Today I want to share with you some must-apply security tips for WordPress blogs.

Securing your blog is one of the most important things you could do. Producing content is essential, and so is promoting it, but if your blog is not secure, you could lose everything overnight (literally!).

In this email I will share some security tips that you should apply in your blog.

1. Backup, Backup and Backup!

In security circles people always say that if someone wants to break into your site, with enough time and determination eventually he will. In other words, no website can be made 100% secure.

If that is the case, your first line of defense are your backups.

With functional backups someone could erase everything in your server and you would be back online in a matter of hours.

So remember to backup your blog often (preferable daily), and to have backups in at least two different physical locations (else a theft or fire could take both your site and the backup...).

2. Change The "Admin" User

One of the most common methods to break into a website is the brute force one. That is, the malicious person will try to guess the name of the admin and, once he finds that out, he will use scripts to try thousands of password combinations with that user name.

If the admin user in your blog is called "admin", well, you just facilitated things a lot.

Luckily changing that is quite easy. Simply create a new user for your blog, and give it "Administrator" privileges. Then login with that user, and delete the "admin" user. If you have posts published with "admin" WordPress will ask you if you want to move those posts under a new user.

3. Obscure Your WordPress Version

Another common saying among security geeks is "security through obscurity." This is related to the fact that the fewer things a malicious person knows about your blog or server, the harder it will be to break into it.

By default WordPress broadcasts to the world the version that you are running, and this information can be used against you, because hackers know the security holes on each WordPress version.

Hiding that information is not difficult though. First of all you want to disable the "generator" meta tag. You can do that by adding the following code to the functions.php file of your theme:

```
function hide_wp_vers()
{
return '';
}
add_filter('the_generator','hide_wp_vers');
```

There is another place where hackers can find the version of your WordPress, and most people forget to deal with that. It is the readme file that comes with all WordPress installs. Simply access your server via FTP to delete that file.

4. Disable Folder Browsing

Another thing that you should obscure in your site is the content of your folders. If people can browser your folders, they will be able to collect a lot of information, including what plugins you are running, what themes you have installed and so on. Needless to say that such information can be used to find security holes in your site.

If your web hosting is based on Linux, you can easily disable folder browser with a .htaccess file placed at the root of your server. Either create that file or open the existing one and add the following line:

```
Options -Indexes
```

That is it. If your hosting is not based on Linux, you can still protect the content of your folders by uploading a blank index.html page inside each folder.

5. Always Update

WordPress is an open source software, so its source code is public, and anyone can have access to it. This means that hackers can scrutinize the code looking for security holes.

Sometimes they find them, but the WordPress community usually responds quickly and releases an updated version protected against the new threats.

If you always run the latest WordPress version, therefore, you will be minimizing the chances of having problems.

Want more WordPress tips? Check the "WordPress" category I have on http://www.dailyblogtips.com , I am sure you'll like it.

Talk to you next week,
Daniel Scocco
