Website Security: What do I need to know? What do I need to do?

This document describes some of the emerging security issues for and threats to websites as well as some of the options to address them. The information is first in a series of articles that will discuss how to make a website more secure. We will provide

This target audience is owners and managers of websites. The contents reflect a high level perspective of how websites get infected with malware code, why this happens and some best practices to prevent infection(s). We have tried to balance providing enough detailed information so that website owners can take concrete steps, at the same time avoid providing a level of detail that would only be useful for experienced security professionals.

1. How are most websites built

Websites today are built quickly, using mostly off the shelf software and easily available reusable components. Think of it as building a car with parts that are easily sourced, free, and widely used. Building a website by integrating together parts like these, i.e. existing frameworks, content management systems and third party plugins has many benefits.

- Quick turn around time for the web-designer/programmer, allowing them to design and launch more sites
- Customer gets to launch the website quicker, allowing them to address their target audience faster

Take away: Find out what software is being used to power you website. Identify the version numbers and deduce if you need to upgrade.

Example: If your website is running a blog, and is powered by WordPress, you should navigate to the admin area. Usually something like mywebsite.com/wp-login.php . Log in and see if there is a message on your dashboard under "WordPress Blog" about a new version. Click on that piece of information to see how you can upgrade.

2. Why are websites insecure

2.1. Lack of communication

Website owners/admins, who maintain websites after they have been handed over by a designer/developer, do not necessarily understand the complex nature of the software used to put a website together. This occurs due to a lack of communication and information transfer between the two main parties: (1) The web designer/programmer (WD) and (2) The website owner/maintenance person (WO).

It is imperative to understand the basics of what is actually powering a website. If there is any Content Management System (such as WordPress, Typo3), a bulletin board (such as vBulletin), ad server system (such as OpenX), these must be communicated, at least at a high level to the WO by the WD.

Handing over basic information like this puts the onus of keeping all these pieces of software current, patched and updated on the WO. With most software like WordPress, whenever a new update/version is made available by the developers of the software, a message is highlighted on the main dashboard letting the WO know about this update and instructions about what to do.

Without this basic information about what software is powering the website, many a time WOs are left in the lurch with no idea as to what is outdated, and can cause security issues, that will be expensive to handle later on.

It is very important for WOs to understand at least what are the main components of software that a WD is using to build and power a website, so that the WO can make sure they can take the right steps.

Take away: Ask your web designer/developer if your site is running any ad servers, blogs, bulletin boards. Make a list of all third party plugins (like timthumb, any image gallery plugins, jquery scripts). Find out which of these need to be updated by you, the website owner/admin, and what tools you can use to keep these pieces of software updated.

Example: If your website is running a blog, and is powered by WordPress, you can try to find out of your website is using a third party software called "timthumb". This software is used for resizing images while being uploaded to your blog/website. To find out if you are running an outdated, vulnerable version of this software, simply install the timthumb vulnerability scanner, available via the wordpress site. Once installed, navigate to Tools-> Timthumb Scanner. A scan will ensue and highlight the fixes that are needed. All you need to do is click on the "Fix" buttons. This scanner checks for instances of timthumb that are older than version 2.0

2.2. Lack of maintenance processes

Often times owners of websites (WOs), do not have a formal process for maintenance and review of the websites they rely on to do business and interact with the world. This is one of the primary causes for websites to get compromised. We shall now detail what kind of maintenance processes could be considered as a good rule of thumb:

1. Change FTP and Access passwords every 60 days.
2. Scan the computers being used to upload files to the hosting account, everyday, with multiple anti viruses.
3. Check for updates to software powering your website every 7 days.
4. Conduct a web-malware detection scan on your website everyday.
5. Check your SEO ranking to detect any fluctuations.
6. Check the reputation of your website on different blacklists to detect if your website is being used by spammers, phishers, malware distributors or not.
7. Check your .htaccess files every 7 days.

Take away: Maintain constant vigilance, follow maintenance processes religiously.

Example: Get hold of Avira, Avast and ClamAV anti viruses. They all have free editions and set them up on your PC to do scans every night. This will prevent hackers from stealing your username and password to get administrative rights to your website and thereby inject malicious code on your site.

2.3. Vulnerabilities in website software

Website software, or the computer code powering a website is often termed as "Web app" (short for website application code). This web app software often accepts input from users visiting a site in the form of blog comments, usernames, date of birth, and other information. It is good practice on part of web developers to cleanse the input data to prevent any malicious computer code from causing harm during analysis of the input. Unfortunately, web developers are often not trained to write secure code, or do not test their code sufficiently because of time constraints. Unsafe web apps often allow malicious hackers to break in and inject websites with malware. The good news is that if your website is powered by well known software like WordPress, Typo3, vBulletin and such, the developers of these software package release patches and updates to fix vulnerabilities in their software pretty regularly. You can even analyze the vulnerabilities on your website using vulnerability assessment scans that can point out flaws like SQL injection, Cross Site Scripting and more.

Take away: Determine if your website is powered by vulnerable software. If you are running an old outdated versions of popular software, you are most definitely putting your website at risk. You can also investigate the option of getting a vulnerability scan for your website to identify any issues, before the malicious hackers break in.

Example: You can get hold of free tools like XSSme, SQLinjectme and such to test whether your website has the most common web application vulnerabilities or not. Remember though, interpreting the report data may not be easy for most website owners.

2.4. Vulnerabilities in server software

Computer software that powers the actual server (machine) that is hosting your website is termed as server software. A prime example of this kind of software is the FTP server that allows you to log in and update/upload webpages in your hosting account. Sometimes hosting companies will provide default packages as a convenience to their customers, such as mailman scripts, these help with setting up email related functionality and such. These server level software can cause security issues too. A vulnerable FTP server can allow an attacker to break into a website, so can misconfigurations on part of the hoster.

Take away: Find out what default packages if any are installed on your hosting account and if they are up to date. If you are not using these packages, remove them. If they cannot be removed make sure you understand who is in charge of keeping them up to date.

Example: You can simply log into your hosting account and see if you have mailman scripts enabled or not. You can also find the version of your FTP server from your control panel. A good tutorial on using FTP from a windows machine can be found at http://www.textheavy.com/tutorials/winftp.html

2.5. Insecure website access

Insecure website access is one of the primary reasons of website compromise. A prime example would be easy to guess passwords. There some basic steps that can followed to help make the management of a website more secure. We list these below:

- Try to not use FTP for uploading website related files to your hosting account. FTP connections can be sniffed by trojans/viruses installed on PCs while a website owner connects to his/her hosting account. Once these trojans/viruses detect a successful login via FTP, the account username, password and ftp location are sent out to a botnet network that proceeds to pump in malware into the hosting account. This process of infecting the hosting account via compromised FTP credentials is extremely prevalent and somewhat hard to detect, since it seems as if a legitimate user has logged into the account and is uploading/modifying some files. Also, do not store your FTP credentials in your FTP client. Instead of FTP consider using SFTP/SCP.

- Try to use passwords that are 10 to 12 characters or more, with numbers, upper and lower case letters and special symbols.

- Try to make sure that permissions for all files are set appropriately. A permission of 777 would provide a read, write and execute access to everyone, this is highly undesirable. try to set permissions to 644 for most files.

Take away: Have secure passwords. Try to move away from FTP, use SCP/SFTP.

Example: You can WinSCP, and use it to connect to your website and transfer/update files on your hosting account.

3. What can happen if a website is not secured

Insecure sites can be compromised by malicious hackers. Once compromised these sites can be used to spread malware and spew spam. More than 6,600 websites get blacklisted by Google alone, on a daily basis. Some of the consequences of not protecting your website are listed below:

3.1. Compromised website is infected with web-malware, in turn infecting all visitors to the website. This leads to the website getting blacklisted by search engines and security watchdogs in the Internet. Once a site is blacklisted, all modern browsers like Internet Explorer, Safari, Firefox will block access to your website. On average it takes about 7 days for a website to get itself cleaned and off the blacklists.

3.2. (3.2) Compromised website is infected with spam-shells. Spam shells use the hosting account as a staging ground for sending out spam to users in the Internet. This can cause your website to get blacklisted and emails from your domain may be blocked or dropped completely.

3.3. (3.3) Customer confidence can drop greatly if a website is blacklisted. Moreover it takes hours worth of effort to find the web-malware causing issues on a site. This leads to loss in sales as well as expending money ant time on fixing a problem that could have been avoided.

3.4. (3.4) Customer data such as credit card information, customer addresses and other personal information can be stolen and distributed on underground networks.

Take away: Protect your website, do not take security lightly if you value your reputation and visitors.

Example: On average is takes 7-10 days for a website to recover from a hacking incident. More information can be found on the StopTheHacker blog.

4. What can I do to protect my website

There are two primary product categories that can help you secure your website:

Website Vulnerability Assessment: On a PC, Microsoft will act as the vulnerability assessment tool and tell you where you're vulnerable and what you can do about it. Unfortunately, such a service is not available on web sites. But there are tools available that will scan your website and tell you if you're vulnerable and what you can do about it. If you understand security issues on a website well and have the time and money to keep your site up to date, this is an excellent tool to reduce the risk of being infected by hackers.

Website Malware Scans: As with PCs, most website owners and administrators realize they can't keep up with all vulnerabilities and that sooner or later they will get infected. As a minimum, they therefore subscribe to a service that scans their website daily and alerts them when a hacker has injected malicious code so they can take immediate action before their users get infected or they get blacklisted. Because the attacks can be more complicated on web sites, signature based virus engines are not enough. An effective scan engine will check for both known viruses and unknown web malware.

Several vendors offer solutions like this. We have teamed up with StopTheHacker, and is offering their services through our dashboard. Our top priority is the security of your website and you're of course free to use any service out there.

This article has described some good practices that when put in practice can dramatically reduce the chances of getting hacked and blacklisted.

Please feel free to provide feedback about your experiences and comments at info@stopthehacker.com.