How to evaluate and improve security for a website

Security is an important aspect of any website - especially e-commerce. So what are the ways to protect a website and how to reduce the chance of a website being hacked or altered for nefarious purposes?

Security is an important aspect of any website - especially e-commerce.

There have been times when people and companies almost completely abandoned their fate and only hoped that no one would hack the content or install malware on their website.

But that has been a thing of the past, because the number and frequency of attacks, which means it is a constant threat, is growing rapidly. The more successful a website is, the higher the risk of being attacked.

So what are the ways to protect the website and how to reduce the possibility of a website being hacked or altered for nefarious purposes?

However, before learning that, readers need to understand the most basic level of security, which is the level at which many websites are attacked - even those websites that are hosted on secure servers.

Ensuring security for a website

1. First line of defense
2. Security check
3. General concern
4. Weakness in design

5. Have appropriate protection

First line of defense

Although some companies still insist on hosting their own websites, most websites of businesses are located on secure servers from web hosting services.

When choosing a hosting service provider, the user must determine the operating system the system is running on (Windows Server, Linux or Unix) and that indicates the security protocols required.

Only webmasters responsible for admin can change the file structure on it.

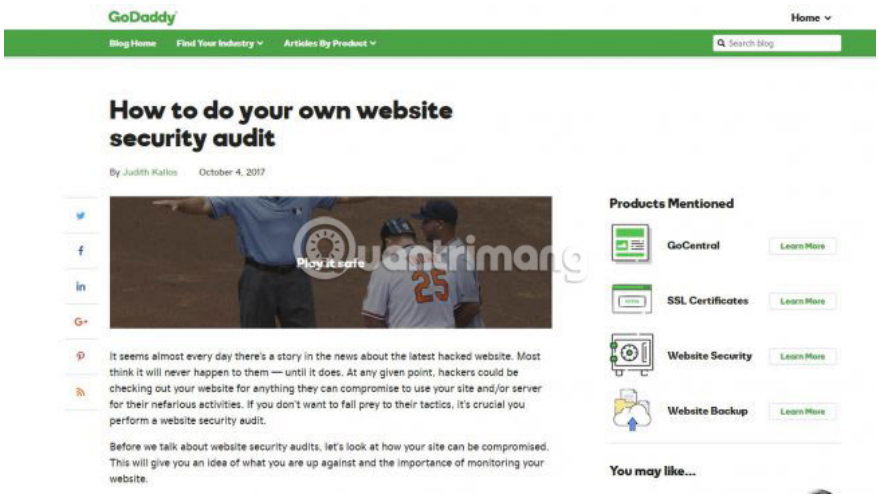
In case there are too many people who know admin account details and passwords do not change very often, just a keylogger is installed on one of the machines used by the admin, the login password will be revealed.

But to be honest, remembering passwords by writing notes is very common in offices.

Securing these passwords is the first 'defensive product'. Without that, anything done could easily be undone by bad guys.

Therefore, there are two lessons to keep in mind about site security first:

1. The network where the website is built should be well secured.
2. Security issues cannot be improved by recording passwords and placing them in easily visible places.



Security check

Performing a security check on a website is a relatively simple exercise that can be done by IT staff, using the appropriate software tools. In addition, it is possible to sign a contract with a third party to perform a scan of the entire website and to provide potential weaknesses to note.

If you are using a web hosting service, your provider may also suggest a security tool to ensure that the site is safe from the start.

In addition, many vendors also offer site security packages, promising to respond quickly to threats and minimize denial of service attacks. This is the right investment, unless you have only a small personal blog.

The price of these services is not too high, considering the excessively high money lost when the site collapsed in any time period, especially for e-commerce services.

Whichever method is used, it is important that security scanning procedures be performed on a regular basis, to identify new threats that may occur, as soon as they appear and process them immediately. News.

General concern

The most common attacks that websites encounter are:

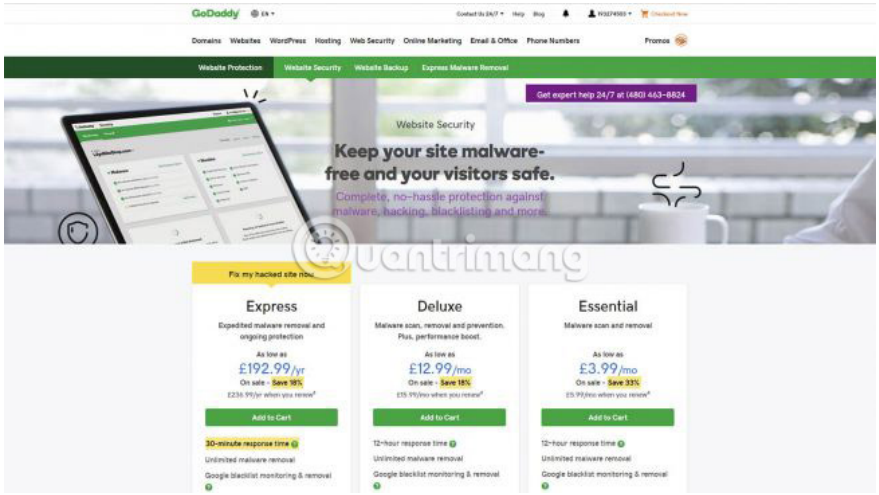
1. **Distributed Denial of Service (DDoS)** - Many remote computers, often infected with Trojans, operate on sites that continually send requests and servers that cannot handle the number of requests.
2. **Malware infection** - Somehow, files containing malicious code are placed on the website with the intention of uploading it to anyone who visits.
3. **SQL injection** - The malicious code is inserted into the form or input, then executed on the server by SQL Database. This code may allow access to customer data or open the device for external access.
4. **Brute force** - A vulnerability in the operating system that allows repeat attacks, resulting in a reset, opening the port for the next attack. With the complexity of modern operating systems, new vulnerabilities are found quite often.
5. **Cross-site scripting** - This hack method redirects the browser to another website or replaces the content on the hacked website without the visitor's knowledge.
6. **Zero** day attacks - These are new and difficult to block attacks, using obscure weaknesses. The time period between when the vulnerability was discovered and when it was fixed was very important, and could temporarily disable some server features until a fix was released.

Weakness in design

Although many websites work with the following features, they are also the source of many security issues:

1. **Forms** - Anything that handles input on the server is a potential 'vulnerability' to malicious code and can be exploited to extract user data.
2. **Forums** - Placing scripts and redirecting users to malware distribution sites are just a few potential problems in user-created forums.
3. **Log in to a social network** - Using a Facebook or Google account to log in to a website is quick and easy, but it can also be a reason that these accounts are hacked.
4. **E-commerce** - Criminals smell the money and hackers will spend more effort to hack an e-commerce website.
5. **Uncontrolled content** - If you get news and articles from other websites, your site depends on their security measures, regardless of what they are.

Obviously, removing all these functions from a website will make it unattractive to visitors. It is necessary to decide what preparation factors to use and how to mitigate the relevant security issues.



Have appropriate protection

There is no way to ensure that your site is never hacked. Finally, you can try to hack your own website and make sure it can be quickly recovered after every problem.

The accuracy of the security efforts offered is something that all companies struggle with, but for online sales sites, 100% of the personal and financial details of the customers must be ensured. goods are secure.

Many companies and organizations have stolen all customer data, then this information is used to fake identity information, and leave extremely expensive consequences.

Any level of protection and supervision chosen should be consistent with the purpose. Finally, consider that there are better security measures with minimal costs.

Wish you find the right solution!

See more:

1. Don't ignore these 10 security tips when creating a new website
2. Enhance the effectiveness and security of Website with CloudFlare