

The Top Five Myths of Website Security

February 2007

Jeremiah Grossman

Founder and CTO, WhiteHat Security

A large, light blue, stylized graphic that resembles a wide-brimmed hat or a protective shield, positioned in the lower half of the page.

A WhiteHat Security Whitepaper

Introduction

Hackers behave like water, taking the path of least resistance. Today this path leads over SSL, and past the firewall, where nothing exists between them, the website, and the information it holds. This is how a Web hacker views the world. Using a browser and a few simple tricks, hackers can penetrate a website, access the credit card database, and make off with critical data, customer databases or even intranet information, unseen.

With network firewalls and patch management now standard practice, the network perimeter has become increasingly secure. Determined to stay a step ahead, hackers have moved up the software stack, focusing on the website itself. Gartner Group has stated that over 70% of cyber attacks occur at the application layer. Even more alarming, WhiteHat Security has found that 8 in 10 websites currently have serious vulnerabilities.

These website vulnerabilities may have familiar names like SQL Injection and Cross-Site Scripting, or less common monikers like Insufficient Authorization or Predictable Resource Location. When securing our networks, we are conditioned to immediately think of firewalls, SSL, Intrusion Detection, and Anti-Virus as components of a complete solution. While they improve certain aspects of security, their impact on protecting the website is marginal. New vulnerabilities require new solutions. Contrary to popular belief, deploying a network firewall will not prevent a hacker from penetrating a gaping hole in your website. To improve the security of the Web, we must dispel this and other widely held misconceptions including:

"A website that uses SSL is secure."

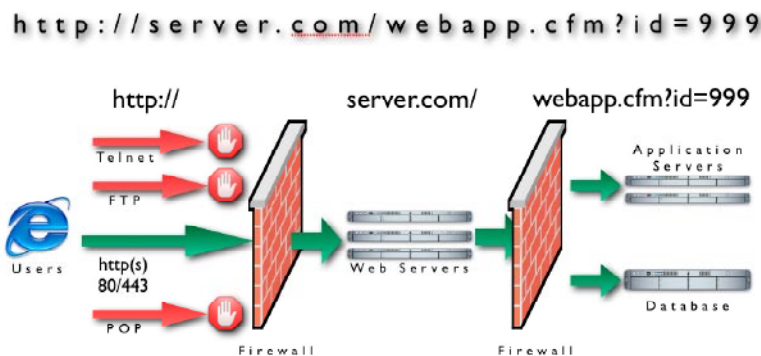
"A firewall protects the website, so it's safe from hackers."

"The vulnerability scanner did not report any website security issues, so it's secure."

"Website security is a developer problem."

"We conduct annual security assessments on our website, so it's secure."

Let's examine these myths and find the truth behind them.



Myth #1: Secure Socket Layer (SSL) Will Secure My Website

SSL does NOT make a website secure. The tiny SSL lock symbol located at the bottom of a Web browser indicates that the information sent to and from a website is encrypted. Nothing more. SSL has no ability to protect the information stored on the website once it arrives.

Websites using strong 128-bit SSL have been hacked with the same frequency as those that do not. WhiteHat has found that the use of SSL has virtually no impact on the difficulty of breaking into a website and pillaging its confidential information.

It's important to understand what the lock symbol represents in the security landscape. Secure Socket Layer (SSL) is an encryption protocol that enables a website to prove to a user that it is what it claims to be, and not an imposter eavesdropping on the conversation. SSL also ensures that if someone intercepts the conversation between the user and the website, the exchange cannot be read. SSL has absolutely no impact on website security or the manner in which a user's private information is safeguarded. When private data is stored on the website, the risk is at the server level, not in the connection.

“Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench.”

– Gene Spafford Ph.D.

Professor of Computer Sciences, Purdue University

Myth #2: Firewalls Protect Against Website Attacks

Firewalls allow Web traffic to pass through to a website, but lack the ability to protect the site itself from malicious activity. Web applications are software that turns a website into an e-commerce bank, store, auction, credit union, message board, etc. These Web applications remain vulnerable to attack regardless of whether a firewall is in place.

In the traditional network security mindset, the idea has been to “Let the good guys in and keep the bad guys out.” This is done through the use of firewall ACLs (“Access Control Lists”). Securely configured ACLs will deny traffic entering a network except for a permitted set of activities, such as Web traffic and email. A port scan of most websites will reveal port 80 open (for http traffic) and often port 443 (for SSL traffic). Generally speaking, all other traffic is blocked by the firewall. No one from the Internet really needs to share your printer do they?

After an ACL has allowed a visitor beyond the firewall and through to the website, all security protections provided become meaningless. The firewall has protected the printer, escorted email to where it belongs, and let the whole world into the website. The firewall's job is done. There is a new security problem – the website. How do you let the whole world in and make sure they play nice?

Myth #3: Network Vulnerability Scanners Protect My Website

Beginning in the early '90s with SATAN, system administrators and security professionals have utilized vulnerability scanners to point out “well-known” network security flaws. After resolving all the reported security issues, the website should be secure enough to be placed on the Internet. However, vulnerability scanners neglect the security of the custom Web applications running on the Web server, which usually remain full of holes.

Vulnerability scanners operate by transmitting specially crafted network traffic to target servers and collecting responses. The responses are analyzed and compared to thousands of “well-known” security vulnerability signatures (also known as: “checks”). When a match is made between a check and a response, a security issue is reported. Up-to-date vulnerability scanners now achieve over 90% vulnerability coverage on the average network, but sparsely target the Web application layer.

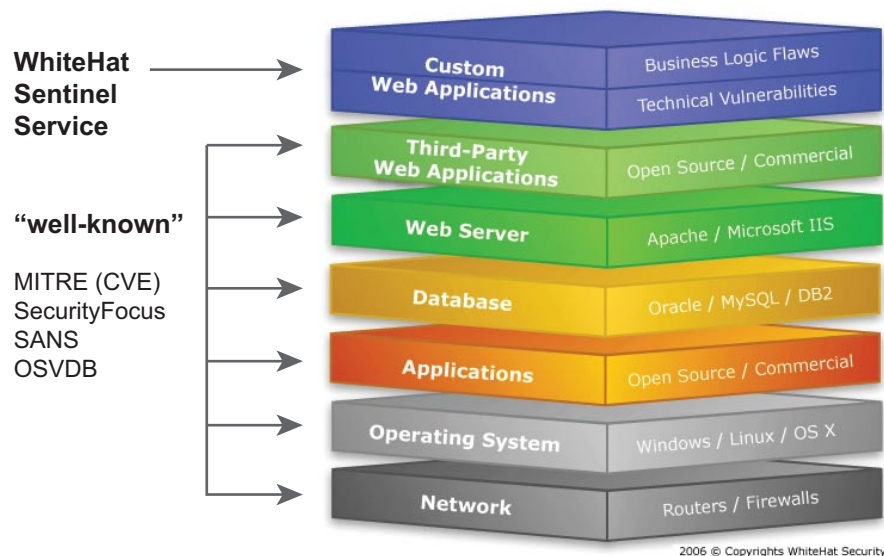


Figure 2.

Vulnerability scanners miss the Web application layer because there are no “well-known” security issues present in custom written Web code. Statistically speaking, there are issues within just about every website, but they remain unidentified until someone looks for them. A small percentage of organizations use the same off-the-shelf software to run their websites. Most opt for custom code. Therefore, no existing weaknesses can be preprogrammed into the vulnerability scanner. It is important to understand that while the average Web application in use today is woefully insecure, a network vulnerability security scanner is incapable of identifying flaws other than those within its signature database. An off-the-shelf vulnerability scanner would likely give your website a “thumbs-up.” Five minutes later, a WhiteHat Security expert would find a way to directly query the back-end database and obtain customers’ credit card numbers.

Myth #4: Website Vulnerabilities Are the Developers’ Fault

It’s easy to blame developers for Website security failures, but that’s not fair. Many factors beyond their control contribute to software insecurity. For example, source code can originate from a variety of locations in addition to the in-house development team. A company might have code developed by an offshore firm to intermingle with existing code. A patch from a commercial vendor may be applied to dependent system libraries. Developers may even use example or

open source code from the Web. It's never clear that the entire code base for a software project is unique, or that the combined interaction is safe and secure. Additionally, as the rush to meet deadlines intensifies, developers are often forced to take shortcuts.

Given these facts, let's say two developers at a company independently create two completely secure software modules. They are secure in and of themselves, but their combined interaction with each other may not be. Now, multiply this interactivity by tens of thousands, hundreds of thousands, or even millions of lines of code all intermingling. The possibility of a security loophole in business logic becomes likely.

Realistically, software has bugs. In computing, we witness this fact everyday. Security vulnerabilities are nothing more than a type of bug. Training staff to develop secure code makes a marked improvement in code quality. But remember, training developers to write secure code does not mean the code they write will be secure. There is no way to prove software is secure and bug free. Everyone makes mistakes that are sometimes buried, undiscovered for years.

What security professionals must remember is that business logic review is a key component of any Web application security strategy.

Myth #5: Annual Website Vulnerabilities Assessments Are Enough

The high rate of change in normal website code rapidly decays the accuracy (and thus, the value) of last week's security report; and, last year's is useless. While it is responsible, and often required, to have yearly security assessments performed on a website, the common Web application life cycle requires more frequent security review. As each new revision of a Web application is developed and pushed, the potential for new security issues increases.

In WhiteHat's experience with e-commerce websites, holidays are a particularly significant time for website updates. For example, Valentine's or Christmas specials are backed with new Web code for various promotions. New features are hurriedly implemented before and after the deadline hits, regardless of any security issues left outstanding. If the business does not publish functioning code, there is a financial loss – so getting the code up and running always takes precedence. This is why ongoing website security is imperative – to catch these flaws as they occur.

Conclusion

Whether a website is in the process of being developed or currently serving customers, there are many security considerations that must be evaluated. Here are some recommendations to help improve website security:

Business Managers: We recommend Website security reviews be performed as often as websites are updated. Every new line of code is potentially a new security issue.

Security Professionals: Use Website vulnerability scanners in combination with a manual testing process. The pairing ensures completeness throughout a large site and allows the operator to focus their attention on finding the logical issues where they are most effective.

Software Developers: Never trust client-side input. This is the #1 cause of security vulnerabilities. Hundreds of millions of visitors you don't know have access to your software. Don't use what you don't expect to receive.

Resources:

Web Application Security Consortium (WASC): A source of up-to-date web application security information: <http://www.webappsec.org/>

The Center for Internet Security: A best practices resource for platform security guidelines and utilities.

The WhiteHat Sentinel Service – Complete Website Vulnerability Management

Find Everything, Protect Everything – The WhiteHat Sentinel Service is a unique combination of expert analysis and proprietary automated scanning technology that delivers the most comprehensive website vulnerability coverage available. Worried about the OWASP Top Ten vulnerabilities or the WASC Threat Classification? Scanners alone cannot identify all the vulnerabilities defined by these standards. WhiteHat Sentinel can. Many of the most dangerous vulnerabilities reside in the business logic of an application and are only uncovered through expert human analysis.

Continuous Improvement and Refinement – WhiteHat Sentinel stays one step ahead of the latest website attack vectors with persistent updates and refinements to its service. Updates are continuous – as often as one day to several weeks, versus up to six months or longer for traditional software tools. And, Sentinel uses its unique “Inspector” technology to apply identified vulnerabilities across every website it evaluates. Ultimately, each site benefits from the protection of others.”

No False Alarms – No busy security team has time to deal with false positives. That’s why the WhiteHat Sentinel Security Operations Team verifies the results of all scans. Customers see only real, actionable vulnerabilities, saving time and money.

Total Control – WhiteHat Sentinel runs on the customer’s schedule, not ours. Scans can be manually or automatically scheduled to run daily, weekly, and as often as websites change. Whenever required, WhiteHat Sentinel provides a comprehensive assessment, plus custom prioritization recommendations based on threat and severity levels, to better arm security professionals with the knowledge needed to secure them.

Unlimited Assessments, Anytime Websites Change – With WhiteHat Sentinel, customers pay a single annual fee, with unlimited assessments per year. And, the more applications under management with WhiteHat Sentinel, the lower the annual cost per application. High volume e-commerce sites may have weekly code changes, while others change monthly. WhiteHat Sentinel offers the flexibility to assess sites as frequent as necessary.

Simplified Management – There is no cumbersome software installation and configuration. Initial vulnerability assessments can often be up-and-running in a matter of hours. With WhiteHat Sentinel’s Web interface, vulnerability data can be easily accessed, scans or print reports can be scheduled at any time from any location. No outlays for software, hardware or an engineer to run the scanner and interpret results. With the WhiteHat Sentinel Service, website vulnerability management is simplified and under control.

About the Author

Jeremiah Grossman is the Founder and Chief Technology Officer of WhiteHat Security (www.whitehatsec.com), where he is responsible for web application security R&D and industry evangelism. As an industry veteran and well-known security expert, Mr. Grossman is a frequent international conference speaker at the BlackHat Briefings, ISSA, ISACA, NASA, and many other industry events. Mr. Grossman’s research, writings, and discoveries have been featured in USA Today, VAR Business, NBC, ABC News (AU), ZDNet, eWeek, BetaNews, etc. Mr. Grossman is also a founder of the Web Application Security Consortium (WASC), as well as a contributing member of the Center for Internet Security Apache Benchmark Group. Prior to WhiteHat, Mr. Grossman was an information security officer at Yahoo!, responsible for performing security reviews on the company’s hundreds of websites.

About WhiteHat Security, Inc.

Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of website vulnerability management services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company’s flagship service, is the only solution that incorporates expert analysis and industry-leading technology to provide unparalleled coverage to protect critical data from attacks. For more information about WhiteHat Security, please visit www.whitehatsec.com.



WhiteHat Security, Inc. | 3003 Bunker Hill Lane, Suite 220 | Santa Clara, CA 95054-1144 | www.whitehatsec.com

Copyright © 2007 WhiteHat Security, Inc. | Product names or brands used in this publication are for identification purposes only and may be trademarks or brands of their respective companies.

05.02.07