The Five Myths of Web Application Security

Jeremiah Grossman, CTO and Co-founder
WhiteHat Security, Inc.
May 2005

Introduction

Web application security is a critical component of an organization's overall security posture because web applications are a gateway into backend databases that hold critical corporate information and assets. More companies than ever are doing business on the web, yet only a relatively small percentage of websites are regularly and professionally tested for vulnerabilities. As organizations tighten up the network perimeter, hackers are focusing attention toward weaker targets, the web applications. Increasing the challenge, most e-commerce websites are constantly changing, to update product information and business functionality. These trends drastically increase the likelihood of website vulnerabilities and eventually lead to compromise.

A website's custom application code is a dangerous point of insecurity for an organization conducting business online. Through web application vulnerabilities, attackers can gain access to customers' credit card data and other personal information, enabling fraud and identity theft. When a security issue is identified within a website, it can be classified as one of two types, "Technical Vulnerability" or "Logical Vulnerability." It's important to understand that while a scanner may find technical vulnerabilities, a security expert must identify the logical flaws because they are contextual. Only a security expert can evaluate business logic. It's essential that your security program cover both types of vulnerabilities on a continuous basis for comprehensiveness and also a demonstration of corporate due diligence.

Demonstrating due diligence is a fundamental tenet for governmental regulatory compliance. During the past three years, many regulations added serious penalties for failure to address information security risks. Sarbanes-Oxley, HIPAA, GLBA, and California Senate Bill 1386 all have provisions that require the implementation of various security controls. Failure to demonstrate an effort to exercise fiduciary responsibility in protecting private data now carries severe penalties. Recently the Federal Trade Commission has focused on web application security issues. Many of the regulations address improper access to customer, employee or patient data, and web applications control that access when data is available on-line.

Several myths have propagated throughout the security industry that have left websites vulnerable. The time has come to debunk these myths and lead organizations to an effective web application security strategy.

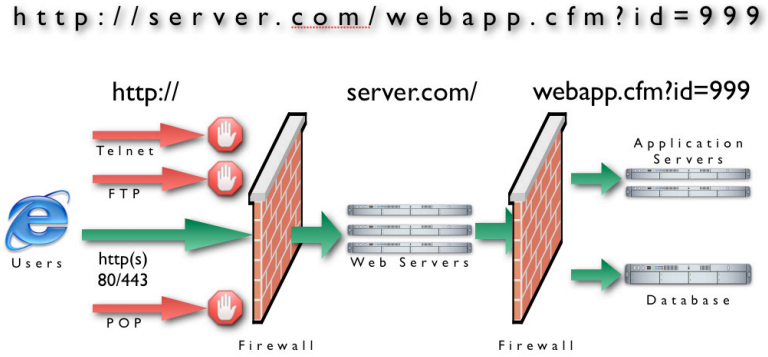

Figure 1: A typical corporate network map

The Five Myths of Web Application Security

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 web site 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 Web Application Attack
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 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 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 90's 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 site 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.

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 backend database and obtain customers' credit card numbers.

Myth #4
Web Application Vulnerabilities are the Developers' Fault
It's easy to blame developers for web application security failure, 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 Web Application Security Assessments are Enough
The high rate of change in normal web site 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 continuous website security is imperative--to catch these flaws as they occur.

WhiteHat Debunks the Myths: Real-World Solutions for Web Application Security

WhiteHat understands the challenges companies and security professionals face in creating a web application security strategy. Widespread belief in the five myths is leaving thousands of organizations vulnerable to attack. Only WhiteHat has developed a timely, practical solution to protect valuable data and ensure customer confidence.

WhiteHat Sentinel is the only continuous vulnerability assessment and management service for websites. WhiteHat Sentinel allows companies to identify, manage and remediate all web application vulnerabilities.

Continuous: To Ensure Maximum Coverage

WhiteHat knows that to be effective, website security must be continuous. In a dynamic environment, a single, exploited vulnerability can result in the loss of revenue or customer confidence. Protecting the company brand is a must. In addition, companies are subject to substantial fines for exposing customer information.

Prior to WhiteHat Sentinel, most companies were unable to obtain cost-effective, timely coverage. Now, one service provides up-to-date vulnerability assessment and management to give companies confidence in their web application security.

WhiteHat Sentinel is specifically designed to secure production websites with no impact on site performance. The service is fine-tuned for each website to maximize efficiency.

Comprehensive: To Cover All Types of Vulnerabilities

WhiteHat Sentinel is the most comprehensive service available, identifying and tracking both technical and logical vulnerabilities. Only the WhiteHat Sentinel service can detect flaws in the business logic that can create dangerous vulnerabilities. Scanning technology alone is unable to identify these contextual vulnerabilities.

The WhiteHat Sentinel scanning technology builds on a unique knowledgebase derived from WhiteHat's team of engineers who have assessed thousands of websites in numerous industries including financial services, e-commerce, healthcare, and manufacturing.

In addition, WhiteHat's team assesses each web application, as part of the WhiteHat Sentinel service, to identify logical vulnerabilities. Like technical vulnerabilities, they are reported to the customer via WhiteHat's web-based customer interface. The assessment process is repeated as often as necessary, but always when the business logic in the web application changes.

Verified: To Reduce False Positives

WhiteHat Sentinel saves customers time and money by verifying all vulnerabilities, nearly eliminating false positives. WhiteHat Sentinel also identifies the severity of each vulnerability, and highlights which vulnerabilities are most dangerous to the web application if exploited.

Customers are given comprehensive remediation steps to make resolving vulnerabilities easier and faster. This information is immediately available to customers via email alerts and the web-based management console.

Conclusion

Websites, by their nature, are continuously evolving and their source code frequently changing. They are designed to fuel business, which creates a constant pressure for additional code. New code means new risk of vulnerabilities. Any company transacting business on the Web needs to have a continuous, comprehensive web application security solution as part of an overall corporate security strategy. WhiteHat Sentinel provides a comprehensive and timely vulnerability assessment and management service to enable its customers to mitigate risk and protect corporate and customer data.

For more information, please contact WhiteHat Security:
Email: WH-Info@whitehatsec.com
Website: www.whitehatsec.com
Telephone: (408) 492-1817

About the Author

Jeremiah Grossman is the founder and Chief Technology Officer of WhiteHat Security, where he is responsible for web application security R&D and industry evangelism. As a seven-year industry veteran and well-known security expert, Mr. Grossman is a frequent conference speaker at the Black Hat 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, ZDNet, eWeek, BetaNews, and others. 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 founding 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 web application security services. WhiteHat develops comprehensive, easy-to-use, cost-effective solutions that enable companies to secure valuable customer data, meet federal compliance standards and maintain customer confidence. WhiteHat Sentinel, the company’s flagship service, provides continuous vulnerability assessment and management for web applications.

