WHITE PAPER:
REDUCING THE COST AND COMPLEXITY OF
WEB VULNERABILITY MANAGEMENT

Reducing the Cost and Complexity of Web Vulnerability Management

Who should read this paper

Business owners and IT managers who need a simpler way to detect critical Web vulnerabilities, prevent data security breaches, and protect their customers from identity theft.

Reducing the Cost and Complexity of Web Vulnerability Management

Content

The Need for Simplified Web Vulnerability Assessments

In June 2010, a group of hackers obtained the email addresses of more than 120,000 Apple iPad customers[1]—including top officials in government, finance, media, technology, and military[2]—by exploiting a security hole on an AT&T website. Unfortunately, events like this are all too common. The volume of Web-based attacks increased by 93 percent in 2010, exposing an average of 230,000 identities in each data security breach caused by hacking[3] throughout the year.

In a recent study[4] conducted by the Ponemon Institute, 90 percent of respondents indicated that they have had two or more breaches in the past 12 months, and nearly two-thirds responded that they have had multiple breaches during the same period of time. These breaches can be incredibly expensive. Studies show that the average cost per incident of a data breach in the United States is $7.2 million, with one of the largest breaches costing $35.3 million[5] to resolve. Security lapses involving personal information can also erode consumer trust; more than half of Internet users avoid buying online[6] because they're afraid that their financial information might be stolen. With stakes so high, organizations need to focus their security efforts to prevent these and other breaches.

Unpatched Vulnerabilities Compromise the Security of Your Website

There are countless methods that hackers and cybercriminals use to compromise the integrity, availability, and confidentiality of information or services. Many attacks rely on common flaws in computer software that create weaknesses in the overall security of the computer or network; others exploit vulnerabilities created by improper computer or security configurations. There are literally tens of thousands of known vulnerabilities, and Symantec recorded 6,253 new vulnerabilities in 2010[7]—more than any previous year on record.

Most of the time, software developers work quickly to fix vulnerabilities as they are discovered, releasing software updates and security patches. However, organizations don't always have the necessary resources or manpower to stay ahead of hackers who are always looking for the easiest way to infiltrate the largest number of websites in order to gather sensitive data or to implant malicious code.

The most dangerous attacks are those that can be automated, such as SQL injections, which hackers use to gain access to your database, and cross-site scripting which lets hackers add code to your website to execute tasks. These methods can give attackers control over the Web application and easy access to servers, databases, and other IT resources. Once the attackers have access to these resources, they can compromise customer credit card numbers and other private information.

6,253 New Vulnerabilities

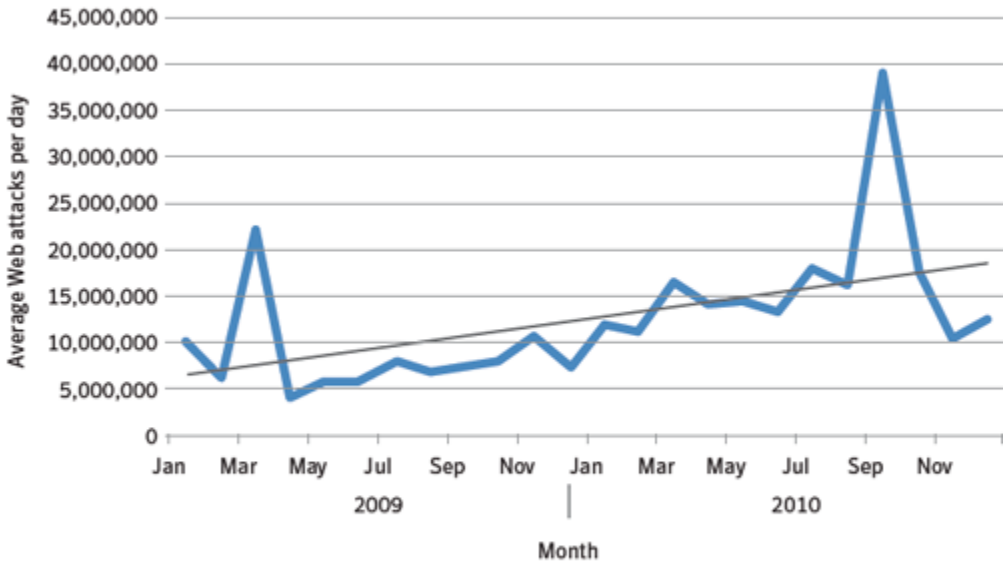
Symantec recorded more vulnerabilities in 2010 than in any previous year since starting this report. Furthermore, new vendors affected by a vulnerability rose to 1,914--a 161% increase over the prior year.

93% Increase in Web Attacks

A growing proliferation of Web attack toolkits drove a 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009. Shortened URLs appear to have also played a role. During a three-month observation period in 2010, 65% of malicious URLs observed on social networks were shortened URLs.

1-CNET News, "AT&T Hacker Indicted, Report Says" (July 7, 2011)
2-CNET News, "AT&T Web Site Exposes Data of 114,000 iPad Users" (June 10, 2010)
3-Symantec Internet Security Threat Report 2011
4-Ponemon Institute, "Perceptions About Network Security" (June 2011)
5-Ponemon Institute and Symantec, "2010 Annual Study: U.S. Cost of a Data Breach" (March 2011)
6-Javelin Strategy and Research (March 2009)
7-Symantec Internet Security Threat Report 2011

Symantec recorded over 3 billion malware attacks in 2010, and the volume of Web-based attacks increased by nearly 90 percent from 2009. Some of this increase can be attributed to the growth of automated scripts and Web attack "toolkits". These kits are usually composed of prewritten malicious code for exploiting vulnerabilities, and make it easy to launch widespread attacks for identity theft and other purposes.



Average Web-based attacks per day, by month, 2009–2010
Source: Symantec Corporation

Traditional Solutions Are Costly and Complex

As the risk of Web-based attacks and data breaches grow, managing vulnerabilities keeps getting harder. Many traditional solutions are designed for large enterprise organizations that must adhere to strict compliance requirements such as Payment Card Industry (PCI) Data Security Standard. These solutions are highly calibrated to detect a finite number of threats, and may generate volumes of unneeded data about low-priority vulnerabilities, which can obscure essential security measures that need to be taken immediately.

Not surprisingly, nearly half of organizations surveyed by the Ponemon Institute list complexity and limited access to IT resources as the biggest challenges to implementing network security solutions, and 76 percent favor streamlining or simplifying network security operations.

Simplifying Web Vulnerability Detection: A Managed Approach

To stay ahead of hackers, organizations need an agile solution that will help them quickly and easily identify the most critical vulnerabilities on their websites. VeriSign Authentication Services, now from Symantec, offers a simple, cloud-based vulnerability assessment that can help you quickly identify and take action against the most exploitable weaknesses on your website.

The VeriSign Vulnerability Assessment at a Glance

VeriSign vulnerability assessments by Symantec Trust Services help you quickly identify exploitable weaknesses on your website. Free with the purchase of VeriSign Premium, Pro and Extended Validation (EV) SSL Certificates, this assessment complements existing protection with:

- An automatic weekly scan for vulnerabilities on public-facing Web pages, Web-based applications, server software and network ports.
- An actionable report that identifies critical vulnerabilities that should be investigated immediately, and items that pose a lower risk.
- An option to rescan your website to help confirm that vulnerabilities have been fixed.

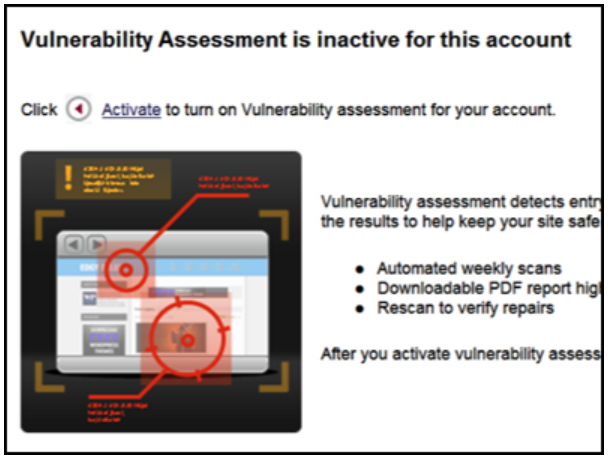
When used in combination with your VeriSign SSL Certificate and daily website malware scan, the vulnerability assessment helps you secure your website and protect your customers.

Vulnerability Assessments vs. Malware Scanning

Vulnerability assessment scans for and reports on entry points for security breaches. Malware scanning attempts to find harmful software already on your site and network. If you have malware on your site, this probably means that an entry point already has been breached. When you repair the vulnerabilities on your site, you help deter potential breaches, including malware.

Configuring Your Vulnerability Assessment Service

Whether you are a current, renewing, or new customer, you can enable the vulnerability assessment service as an option through your VeriSign Trust Center, VeriSign Trust Center Enterprise, or Managed PKI for SSL management console*. This service will start from the same Fully Qualified Domain Name (FQDN) that is used as the common name of the associated SSL Certificate. If you protect multiple domains with SSL Certificates, you can activate vulnerability assessments for each through your management console.



Configuration and alert options vary, depending on the management console you use.

Scanning for Vulnerabilities

The VeriSign vulnerability assessment examines the entry points most frequently used for common attacks. Once activated, the first vulnerability scan will start within 24 hours. After that, the vulnerability assessment scans your site automatically each week, and you can request a rescan whenever you want.

The VeriSign vulnerability assessment scans all commonly used network ports—more than 1,000 in total. The scan detects the most common types of vulnerabilities, including outdated or unpatched software, cross-site scripting (XSS), SQL injection, and "backdoors," and is updated frequently as new vulnerabilities are discovered.

Table 1. Details of vulnerability assessment scanning activities

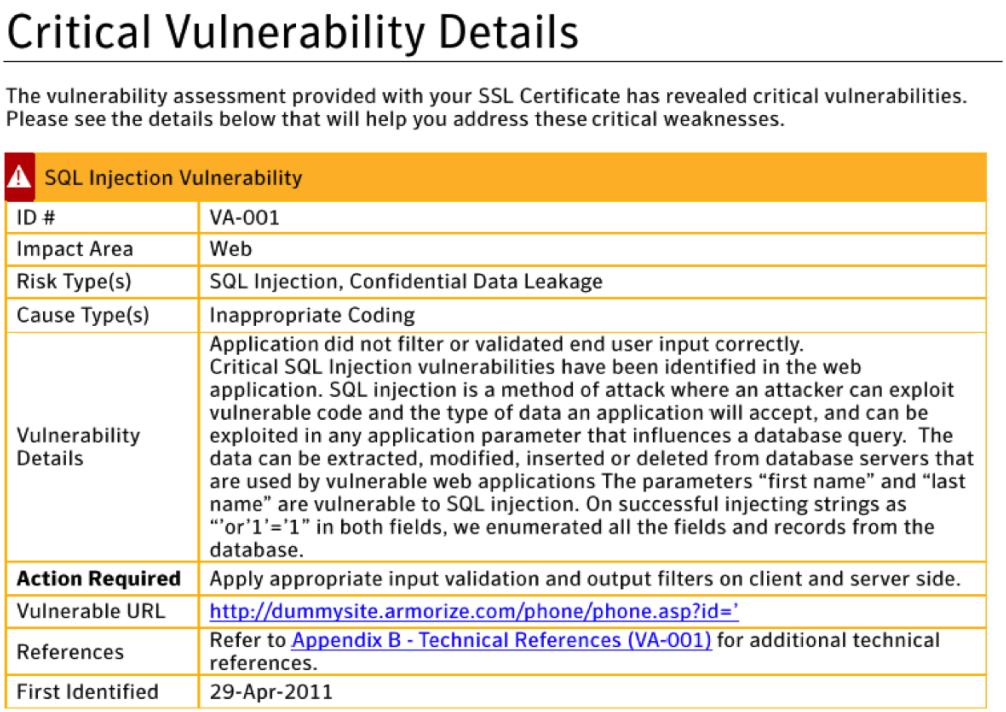
Area	Examples of Items Scanned
Network Level	• Basic port probing and data analysis to non-intrusively identify potential vulnerabilities.
Web Server Software	• Apache HTTP Server (and popular plugins) • Microsoft IIS • Tomcat • JBoss
SMTP Software	• Sendmail • Postfix • Microsoft Exchange Server
Telnet Services	• Unix systems
SSH Services	• OpenSSH • SSH.com software
FTP Services	• Popular FTP daemons
Web Frameworks	• Microsoft ASP .NET, Adobe JRun, Adobe ColdFusion, Perl, PHP, ColdFusion, ASP/ASP .NET, J2EE/JSP • Popular CMS systems (WordPress, Django, Joomla, Drupal, etc.) • E-commerce apps (CubeCart, ColdFusion Shopping Cart, KonaKart, etc.) • Web management software (phpMyAdmin) • Forum software • Ad/stat tracking apps
Web Application Vulnerabilities	• Reflective cross-site scripting vulnerability • Basic SQL injection vulnerability
Potential SSL Certificate Usage Issues	• Non-trusted SSL certificate (signed by unknown CA) • Self-signed certificate check • Certificate common name mismatch • Weak ciphers used • Expired or revoked certificates
Unencrypted Data Transmission	• Login pages with non-SSL target form submissions

If an assessment detects a vulnerability and you take action to remediate the problem you have the option to request a re-scan so that you can verify that the vulnerability has been patched.

Reviewing Vulnerability Assessment Reports

Once the vulnerability scan is complete, you can obtain a full report in PDF format from your VeriSign Trust Center, VeriSign Trust Center Enterprise, or Managed PKI for SSL management console. If the scan detects critical vulnerabilities, it will also trigger an alert in your console.

Each report contains actionable data for IT employees to investigate issues and to communicate them clearly with management. The report highlights critical vulnerabilities, with information about each risk, including severity, associated threat, and potential impact. The report also describes the corrective action(s) that you will need to take in order to remediate each problem.



Critical Vulnerability Details

The vulnerability assessment provided with your SSL Certificate has revealed critical vulnerabilities. Please see the details below that will help you address these critical weaknesses.

SQL Injection Vulnerability	
ID #	VA-001
Impact Area	Web
Risk Type(s)	SQL Injection, Confidential Data Leakage
Cause Type(s)	Inappropriate Coding
Vulnerability Details	Application did not filter or validated end user input correctly. Critical SQL Injection vulnerabilities have been identified in the web application. SQL injection is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept, and can be exploited in any application parameter that influences a database query. The data can be extracted, modified, inserted or deleted from database servers that are used by vulnerable web applications The parameters “first name” and “last name” are vulnerable to SQL injection. On successful injecting strings as “’or’1’=’1” in both fields, we enumerated all the fields and records from the database.
Action Required	Apply appropriate input validation and output filters on client and server side.
Vulnerable URL	http://dummysite.armorize.com/phone/phone.asp?id=’
References	Refer to Appendix B - Technical References (VA-001) for additional technical references.
First Identified	29-Apr-2011

Conclusion

Hackers and cybercriminals are constantly refining their attacks and targets; you need agile tools to stay ahead of them. By using automated vulnerability assessments to identify exploitable weaknesses and taking corrective action, you can reduce the risk of hackers finding your site and attacking it.

VeriSign vulnerability assessments help to reduce the cost and complexity of vulnerability management with automated scans, actionable reports, and a cloud-based architecture that requires no software installation or maintenance. This solution is a good starting point for organizations that want to quickly assess the extent of their website vulnerabilities. VeriSign vulnerability assessments are also ideal for organizations that already use a compliance vulnerability scanning solution such as those for PCI and need a complementary solution to cross-check the results of their scan for an added layer of security. When used in combination with your VeriSign SSL Certificate and daily website malware scan, vulnerability assessments help you to secure your website and protect your customers.

Learn More

VeriSign vulnerability assessments are included at no additional charge with your purchase of any VeriSign Premium, Pro and Extended Validation (EV) SSL Certificates. In addition, VeriSign has identified industry leaders who can work with you to eliminate your vulnerabilities and help keep your site and network running optimally. These referrals range from consultants to software vendors, all of whom specialize in vulnerability remediation.

Glossary

Crimeware	Crimeware is software that is used to commit a criminal act. Like cybercrime, crimeware covers a wide range of malicious or potentially malicious software.
Cross-site scripting (XSS)	Attacks that allow intruders to inject unauthorized scripts that can bypass browser security barriers.
Identity theft	Identity theft is the act of stealing and assuming another person's identity in order to commit fraud or other crimes.
SQL injection	Web-based attack that lets outsiders issue unauthorized SQL commands through unsecured code on a part of a site that's connected to the Internet. Through these unauthorized SQL commands, confidential information in a database could be accessed, as could the organization's host computers.
Vulnerability	A (universal) vulnerability is a state in a computing system (or set of systems) that allows an attacker to execute commands as another user, access data that is contrary to the specified access restrictions for that data, pose as another entity, or conduct a denial-of-service attack.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.