



INTERNET
SECURITY
SYSTEMS™

Web Application Protection

Using Existing Protection Solutions

July 2002

Introduction

The Internet has forever changed the way business gets done. Web-based applications are enabling interaction among customers, prospects, and partners. Unfortunately, many Web-based applications have inherent vulnerabilities and security-oriented design flaws. Internet-based attacks exploit these weaknesses to compromise sites and gain access to critical systems.

Security awareness for Web-based applications is, therefore, essential to an organization's overall security posture. The key to a successful program is an integrated, multilayer approach to vulnerability assessment (VA), intrusion detection (IDS), and event correlation.

This paper highlights emerging threats specific to Web application security and provides guidance on effective approaches to Web application protection. Web applications require a new approach to threat categories. Nevertheless, improved security relative to Web applications can be easily achieved through the effective leverage of existing software solutions.

A Growing Threat

As businesses open their networks to business partners, customers, and their mobile workforce, they are significantly increasing both the value and vulnerability of their online assets. Security incidents are costly, with organizations losing productivity as well as experiencing business interruption, legal exposure, and shareholder liability. Merger and acquisition due diligence and insurability concerns, as well as regulatory requirements, are generating even broader awareness that information protection is a critical need.

Most organizations already have some degree of online security infrastructure – firewalls, intrusion detection systems, operating system hardening procedures, etc. The problem is that they often overlook the need to secure and verify the integrity of internally-developed applications and coded pages against external attacks. In these circumstances, simple manipulation of client code or data, such as the price of goods in an online shopping basket application or sending corrupt and incorrect data to the server can lead to fraudulent transactions or theft of confidential information. An understanding of manipulation techniques combined with rigorous client-side security testing will lead to greater security.

Rigorous Client-Side Testing Is Required

Direct attacks against Web applications through manipulation of their inherent vulnerabilities have become commonplace due to the relative ease. Rigorous, client side security testing and an understanding of manipulation techniques is essential to identifying the potential failure points of Web applications.

The most prevalent methods of attack on applications include buffer overflow attacks, exploitation of application component privileges, and client-side manipulation. On top of the Web server's OS, several sub-categories of applications exist in which vulnerabilities may be exploited, including the following:

- **Database** – Database application vulnerabilities for Microsoft SQL Server, Oracle, Sybase and IBM DB2, including bugs, misconfigurations, and default/blank passwords.
- **Web and application server** – Includes vulnerabilities for CGI, Java, Xquery, default files, and other resources called by applications, as well as web servers (IIS, Apache) and development environments (ColdFusion, etc.)
- **Web site and application** – HTML and XML applications. Assessment functions include web crawling and step-through testing.

VA, the starting point for this process, is extremely important for both discovery and identifying vulnerabilities. This process allows an organization to turn off unused services, identify and patch vulnerable software, and make educated decisions about which elements of the overall infrastructure require the most extensive protection measures.

Information gained through VA helps set up significantly more effective IDS implementation and allows the IDS to feed attack and misuse information back into the VA process to ensure that successful penetrations cannot be repeated. This process takes place at the network, server, desktop, and application levels, and can additionally be used to validate that an intrusion protection system is in place and functional.

It can be extremely difficult for any automated audit and assessment application to know how custom applications will respond to cookie manipulation, form field manipulation, and other Web application threats without carrying out a complete, link-to-link, application-specific assessment. This is a time consuming, interactive analysis best performed by someone with both security and Web development knowledge – a rarely combined skill set. Organizations may need to dedicate additional staff to fully realize and take advantage of the results promised by such analysis, or to outsource the review to leverage the security and application programming expertise of an organization with the appropriate skills specialization.

Internet Security Systems Solutions

Internet Security Systems addresses Web application protection and security through our Assessment and Intrusion Protection solutions. Together, these products and services provide our customers with a wide variety of the most critical, Web-specific vulnerability checks.

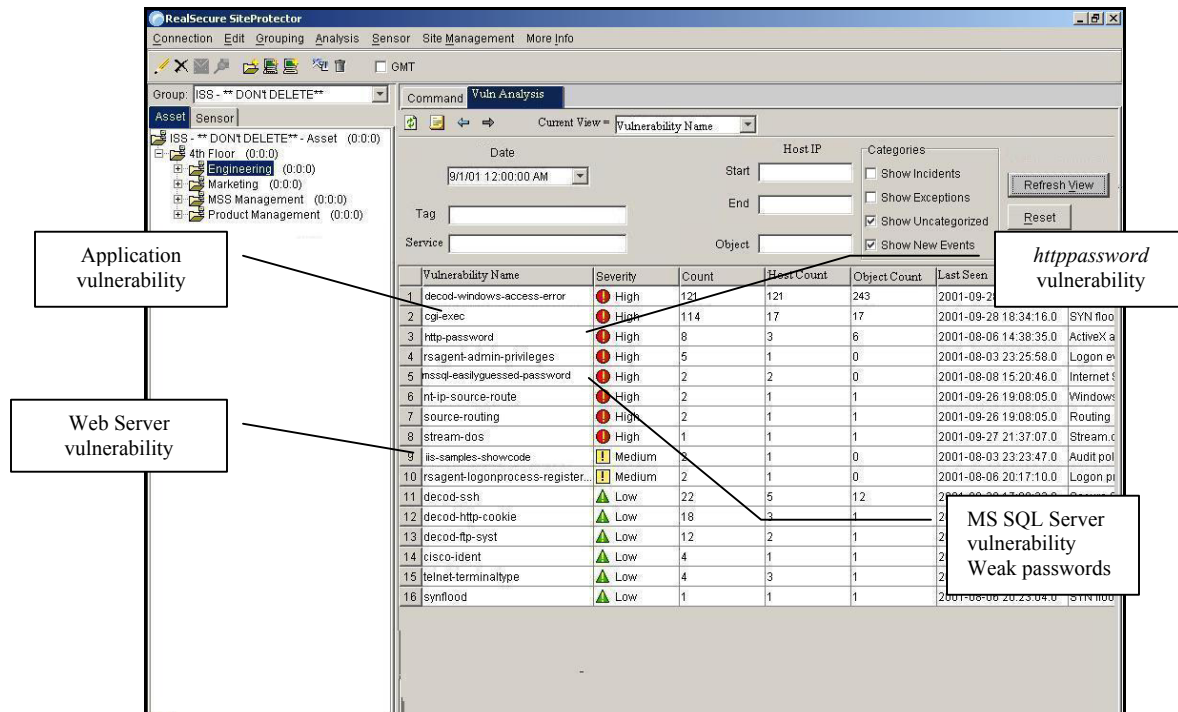
The following table shows how Internet Security Systems’ assessment products may be extended to help organizations improve their security posture with Web applications.

	<i>Internet Scanner</i>	<i>Database Scanner</i>	<i>Wireless Scanner</i>	<i>System Scanner</i>
Denial of Service	X			X
Application related – custom Web site (html, form validation, Web crawling)	X			X
Application related Web server (CGI, Java, etc.) and app server	X			X
Application related – database	X	X		X
OS-level – TCP/IP	X			X
Transport layer (vulnerabilities)	X		X	X
Discovery (detection, ident.)	X	X	X	X

Take Inventory

The *Internet Scanner*® application performs the widest variety of vulnerability detection, ranging from gathering information to finding vulnerabilities. Internet Scanner helps organizations take inventory of their servers – an important first step to assessing risk.

Internet Scanner has the ability to discover application-specific Web site structure by following normal links on sites, a feature known as Web crawling. In addition, Internet Scanner plays a key role in QA prior to deployment. Organizations often use Internet Scanner not only for traditional auditing and scanning over the network, but also for quality assurance purposes prior to system deployment. The following exhibit shows various vulnerabilities discovered by Internet Scanner and ranked in order of severity:



Examples of how Internet Scanner helps protect Web applications include:

- The **Web crawling** feature within Internet Scanner starts at the root of the Web site and follows .htm and .html links, accumulating a list of all the .htm, .html, .asp, and .cgi references that it encounters. A number of web-related checks analyze application-specific files and directories found on the site.
- The **cgexec** vulnerability is reported for CGI programs that can be made to execute “echo” commands inserted into form fields. Such programs lack proper validation of their inputs, and might allow attackers to insert commands that will be executed on the web server.
- The **httppassword** vulnerability is reported for pages protected by HTTP basic authentication that can be accessed by guessing the user name and password.
- The **noindex** vulnerability is reported for each directory whose contents can be listed due to the lack of an index.html file in the directory.
- The **aspdot** vulnerability is reported when it is possible to retrieve the source of an ASP script by appending a dot to the script’s URL.

These checks, among others, utilize the information discovered during the Web crawling phase of the scan in order to determine what vulnerabilities exist. All vulnerabilities flagged on the Web server are then recorded in the scan GUI and logs for output to several report formats. Both the online help and the reports provide comprehensive instructions for eliminating Web server’s security exposures.

Because applications depend on backend databases to perform critical tasks, no application is secure unless the underlying database is also secure. For example, this has been made all too apparent after the recent propagation of the Spida worm. In May 2002, Internet Security Systems’ X-Force™ learned of a worm spreading via Microsoft SQL servers. This worm attempts to locate and login to MS/SQL servers with the “sa” account and a blank password. Once a vulnerable

computer was found, the worm infected the target, send the system configuration and password information to an external host, and begin scanning for new targets. By actively scanning port 1433 for access into systems with blank system administrator accounts, Spida was responsible for large amounts of Internet traffic as well as millions of TCP/IP probes. According to the SANS Institute, a computer research organization, system administrators began noticing an upsurge in scans on port 1433, which is used by Microsoft's SQL servers, on Monday, May 20, 2002. Within the first 12 hours, the number of scanned and infected systems rose sharply to more than 1,600.

Internet Security Systems' **Database Scanner**® application has a check for a blank "sa" user password, which shows where vulnerabilities to Spida exist. This vulnerability check had been implemented into Database Scanner prior to the propagation of the Spida worm. Additionally, Internet Scanner scans for Spida-infected servers.

The **System Scanner**™ application is specifically designed to assess Web and other high-end servers via Web-related vulnerability and policy compliance checks. As such, System Scanner provides a powerful tool for security auditors and system administrators seeking to assess the security posture of **Web servers and overlaying applications on a continual basis**.

After a new Web server has been locked down and baselined by System Scanner, automated scans can be configured to detect deviations from the baseline such as a modified Web application, new user accounts, changed passwords and user groups, new services, modified registry entries, and literally anything on the Web server that differs from the baseline. Additionally, users can create custom checks for a wide range of activities such as monitoring/parsing Web server logs and web application logs.

IDS Completes the Integrated Solution

If the first step in protection for online resources is locating where information is stored, understanding the security measures in place that guard that information, and identifying vulnerabilities and suspect configurations that place information at risk, then intrusion detection is the next level. There are many types of attacks that are specific to Web servers and Web applications. As Internet Security Systems' network and host-based IDS solutions, RealSecure® Network Sensor and Server Sensor protect against these with sophisticated IDS technology that recognizes and responds to nearly every known and many unknown attacks.

Examples include IIS URL Decoding (used for the widespread Nimda worm attacks) and many other IIS attacks, DoS, and remote compromise vulnerabilities, PHP buffer overflow vulnerabilities, ColdFusion, FrontPage, and Netscape application vulnerabilities, and weaknesses found in many of today's shopping cart applications. Antivirus company Trend Micro's World Virus Tracking Center reported that 120,000 new infections were detected worldwide in a 24-hour period after Nimda first surfaced in 2001, bringing the total number of copies of the Nimda worm found by Trend Micro to 1.3 million. Although the full extent of damage caused by Nimda is still unknown, experts fear the attacks could prove to be more widespread than the Code Red infections of July and August 2001, which caused an estimated US\$2.6 billion in damage. RealSecure, Internet Scanner, and System Scanner were able to detect this vulnerability to prevent further damage for customers.

Unlike many other Web server protection products, RealSecure **monitors both inbound and outbound** network activity. This enables RealSecure to instantaneously investigate an event before taking action and to alter a response based on the analysis. Further, RealSecure Network Sensor and Server Sensor introduce sophisticated protocol analysis and pattern matching to interpret network activity. This functionality adds a whole new layer of protection as application protocols are examined for violations. Since RealSecure Network Sensor and Server Sensor automatically check for Web traffic on any port, not just defined ports (e.g., port 80), they detect incursions that other IDS products routinely miss.

RealSecure Server Sensor has Web-specific decodes and signatures, and also ships with default policies for Apache and IIS Web servers. Designed for today's heavily loaded servers, it monitors, detects, and prevents intrusions through packet interception and firecell blocking. It protects the Web server itself and its applications by monitoring kernel-level events, OS audit logs, and Web server network activity. Finally, RealSecure Server Sensor actively blocks attacks before they reach the OS or applications, and provides an SSL-encrypted application layer for intrusion monitoring, analysis, and response.

Users can also **create signatures** to detect and respond to custom Web application environments and/or specific Java patterns sent to a Web server, as well as access to user-specified URLs and files. RealSecure's protocol analysis capabilities protect the Web server and applications from attacks launched over the network. If a sensor is deployed in front of the Web server, malicious TCP-based traffic can be terminated.

Finally, the **RealSecure® SiteProtector™** management system offers a centralized, integrated administration and event monitoring for RealSecure sensors and Internet Scanner. With SiteProtector's security fusion module, RealSecure rapidly correlates security data from multiple sources to determine if an attempted attack was successful so that serious threats are immediately escalated. Administrators can then easily differentiate immediate threats from events requiring less urgent action.

Conclusion

Today more than ever, organizations are challenged with improving security without incurring a corresponding increase in cost or burden to their existing staff. By comparing the benefits that a new product to the total cost of that product, organizations will make better choices that ultimately lead to greater security. Leveraging existing products is quite often the quickest way to improving both security and the bottom line. In many cases, organization can address most of their Web application concerns or problems with the products they already own. Internet Security Systems' award-winning solutions easily adapt to Web application protection. These dynamic threat protection solutions go beyond basic access control to deliver multiple layers of defense that detect, prevent and respond to threats prior to damaging customers' business operations.

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 888-901-7477.

Copyright © 2002, Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, X-Force, System Scanner, X-Press Update SiteProtector and Wireless Scanner are trademarks, and RealSecure, Internet Scanner and Database Scanner registered trademarks, of Internet Security Systems, Inc. Other marks and trade names mentioned are marks and names of their owners as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.