IBM: Web application security for a smarter planet

The world is changing

More Instrumented

By 2010 there will be 1 billion transistors per human.[1]

More Interconnected

By 2011, 1/3 of the world's population (approx. 2 billion) will be on the Web.[2]

More Intelligent

15 petabytes of new information is generated every day, 8x more than the information in all U.S. libraries.[3]

More Dangerous Online

The number of malicious Web sites in the fourth quarter of 2008 surpassed the total number seen in all of 2007.[4]

[1,2,3.] Smart Objects: IBM Global Technology Outlook 2005

[4.] IBM Internet Security Systems X-Force® 2008 Trend and Risk Report

Every day, the world is becoming more instrumented, interconnected and intelligent. The Web and Web-enabled applications are driving these changes.

The Internet has moved well beyond static Web pages to power dynamic Web applications that enable business partners to work together in new ways, integrate business processes and handle payments more easily.

More and more, organizations rely on Web applications as a primary means of doing business. Applications may incorporate the use of forms to interact with personal information (such as credit card, bank account and medical history information), as well as classified/confidential organizational information. And as more sites adopt Web 2.0 technologies including Web Services, service oriented architecture (SOA) and AJAX to perform online transactions, one thing is certain—security risks will increase.

Powered by back-end databases, Web 2.0 and SOA for Web services, the dynamic nature of Web applications creates new challenges for security and compliance. The widespread growth of Web applications and the business value they deliver attracts hackers and cyber criminals to target Web-based applications to steal data, disrupt operations and infect clients.

As threats to Web applications continue to grow, IBM offers Web application security for a smarter planet—integrated, end-to-end security to build secure Web applications, run secure Web applications and protect SOA environments.

Notable Web Sites Successfully Attacked

MyBarackObama.com (2/2009, pointers to external malware)

Pennsylvania state government (1/2008, SQL injection)

Indian Embassy (1/2009, malicious injected iFrame attack)

Federal Travel Booking Site (2/2009, pointers to external malware)

Source: Web Hacking Incidents Database

In 2008, SQL injection replaced cross-site scripting as the predominant Web application vulnerability. In fact, the overall increase of 2008 Web application vulnerabilities can be attributed to a huge spike in SQL injection vulnerabilities, which was up a staggering 134 percent from 2007.

Source: IBM Internet Security Systems X-Force 2008 Trend & Risk Report

Web application security risks are multiplying

When applications are linked to the Web, their attack surface is greater. As they reach more users, they also reach more hackers. The number of vulnerabilities affecting Web applications is one of today's fastest-growing security problems. And as those applications become more complex, the security risks they pose also become more difficult to manage.

The response by hackers has been swift. It's profitable to target Web applications, and public data breaches are now frequent. Consequences include:

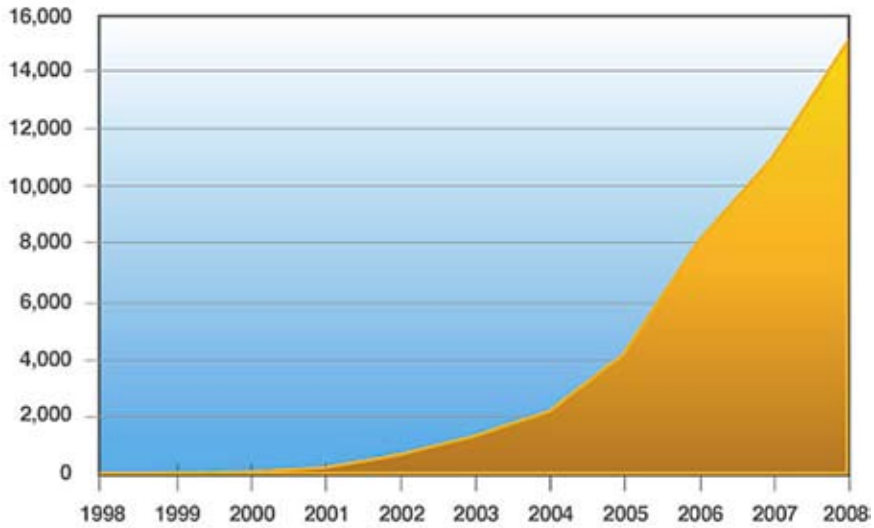
- *Lost revenue and business opportunities*
- *Brand and reputation erosion*
- *Adverse media attention*
- *Unwanted scrutiny from consumer advocates*
- *Growing litigation and compliance burdens*

Web-based applications are targeted gateways for stealing sensitive data, including credit card data and trusted data shared between business partners.

Some examples of common Web application attacks include:

- *Automated SQL injection attacks—SQL queries designed to steal sensitive information from databases—have increased in the last six months from a few thousand to a few hundred thousand a day.*
- *Cross-site scripting attacks allow code injection by malicious Web users into the Web pages viewed by other users. Vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits. End users can have their systems compromised and be exposed to financial loss.*
- *Cross-site request forgery (CSRF) is a type of malicious exploit of a Web site whereby unauthorized commands are transmitted from a user that the Web site trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser to create blind requests to a bank account (for example) to transfer funds to a hacker.*

Web Application Vulnerability Count 1998-2008



54.9% of all vulnerabilities are Web application vulnerabilities

Source: IBM Internet Security Systems X-Force 2008 Trend & Risk Report

It's critical to act

The average cost of a security breach is now $6.6 million.[5] Statistics reveal the likelihood that your Web applications are vulnerable.

- *75% of attacks are at the application layer*
- *67% of all Web applications are vulnerable*
- *42% of Web application attacks are focused on stealing sensitive information*
- *33% of consumers notified of a security breach will terminate their relationship with the business partner they perceive as responsible*[6]

In addition, if hackers gain access to sensitive information, you can run the risk of being noncompliant with a host of mandated legislation and requirements including the Payment Card Industry Data Security Standard (PCI DSS) which has specific application security requirements. Non-compliance can bring fines of up to hundreds of thousands of dollars a month.

[5] Ponemon Institute LLC, Fourth Annual US Cost of Data Breach Study, January, 2009. p. 4

[6] Ponemon Institute LLC 2007

Point solutions are ineffective

Web applications are the new attack vector for hackers to exploit. Just like other IT threats, the initial reaction to risk is to introduce a point solution for every threat. However, security professionals have grown weary of cobbling together security strategies that involve multiple point solutions—(each with its own management console and toll-free number for customer support.)

Today's security organization demands an integrated solution from a trusted vendor that provides a holistic and cost-effective approach to IT security. For complete Web security, enterprises demand end-to-end Web protection that fits within a framework of security governance, risk management and compliance.

IBM is uniquely positioned as the trusted security partner.

IBM is the only company that provides professional services, managed services and hardware and software solutions, that secure customers across the five domains as outlined in the COBIT security standards

End-to-end Web application security made easier by IBM

To simplify Web application security, IBM has integrated industry-leading solutions to provide end-to-end protection designed to reduce risk for Web-enabled applications, Web sites and Web traffic.

- **Discover application vulnerabilities—and how to fix them** using IBM Rational® AppScan®.
- **Help protect applications from potential attacks** using IBM Proventia® Web application security.
- **Protect XML and Web services traffic and SOA deployments** with the IBM WebSphere® DataPower® SOA Appliances.
- **Ensure that only authorized users have the appropriate access to Web applications** with IBM Tivoli® Access Manager.

Discover application vulnerabilities—and how to fix them using IBM Rational AppScan

To stay ahead of hackers, Web application security must be a key element in the application development process—as well ongoing vulnerability assessments.

Rational AppScan software scans and tests for a wide range of Web application vulnerabilities, including those identified by the Web Application Security Consortium (WASC) threat classification. IBM Rational AppScan also supports the latest Web 2.0 technologies; parsing and execution of JavaScript and Adobe® Flash applications; asynchronous JavaScript and XML (AJAX) and Adobe Flex-related protocols such as JavaScript Object Notation (JSON), Action Message Format (AMF) and Simple Object Access Protocol (SOAP); elaborate SOA environments; and custom configuration and reporting capabilities for mashup- and process-driven applications.

Rational AppScan automatically scans applications, identifies vulnerabilities and generates reports with intelligent fix recommendations. And it evolves along with today's threats with automatic updates from IBM so it continually tests for new exploits and vulnerabilities.

Rational AppScan software is used across an organization's software development lifecycle to increase visibility and control—helping to address the critical challenge of application security.

Help protect Web applications from potential attacks using IBM Proventia Web application security

Intrusion prevention just got smarter. IBM Proventia Web application security is now included in every Proventia IPS solution. The market-leading solutions designed to block attacks at the network perimeter and server now include the protection of a Web application firewall.

This proactive approach to Web application security is atypical of many Web protection solutions, which merely audit attacks and react to them. Proventia Web application security helps address the primary sources of attack for:

- *Web applications—helps block shell command injections, server-side include (SSI) injections, cross-site scripting (XSS) and directory traversal*
- *Databases—helps block SQL, Lightweight Directory Access Protocol (LDAP) and XML Path Language (XPath) injections*
- *Web 2.0—helps block Java™ Script Object Notation (JSON) hijacking, potential cross-site request forgery (CSRF) attacks and advanced cross-site scripting techniques*

Save time because Proventia Web application security is configured out of the box with X-Force® recommended policies, which are updated automatically. Use the wizard feature to quickly and easily build security policies to protect custom Web applications.

Enhance compliance because Proventia Web application security meets PCI compliance requirements for Web application protection.

Get the full protection of a Web application firewall when teaming IBM Proventia Network Intrusion Prevention System (IPS) with a Secure Sockets Layer (SSL) offloader.

Drive intelligent security with integration between AppScan and the Proventia IPS management console to:

- *Centrally manage vulnerabilities, IPS blocking/alerting policies and security events from a single dashboard*
- *Correlate reported vulnerabilities from AppScan with security events and attacks blocked by Proventia Web application security*
- *Consolidate reporting for compliance requirements and improved management*

Choose from several form factors to meet different requirements:

- *Proventia Network IPS—High bandwidth Web protection for large enterprises with Web server farms*
- *Proventia Multi-Function Security—All-in-one remote office / branch office protection with virtual private network (VPN) support*
- *Proventia Server IPS—Protect Web servers with host-based intrusion prevention*

Proventia Reviews

NSS Labs: NSS Gold Award

"Detection and blocking rates were impeccable, with 100% of all attacks being blocked under the most extreme conditions."

Forrester: If You Don't Have IPS, You Deserved to Be Hacked

Recognized as leader for "Performance and scalability to handle increased bandwidth and attack sophistication."

SC Magazine: Four out of Five Stars

"The high-end sports car of IPS appliances…built for speed…can handle almost any amount of traffic thrown its way."

IBM X-Force

The IBM X-Force research and development team is one of the best-known commercial security research groups in the world. This group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM ISS products and educates the public about emerging Internet threats. See samples of IBM X-Force research here.

Product of the Year for SOA Security

One judge's comments:
"These boxes work. In fact they work so well that people sometimes think they sound too good to be true. They aren't. Security doesn't have to be a problem, thanks in large part to gateway appliances."

Protect SOA deployments, and XML and Web services traffic with the IBM WebSphere DataPower SOA Appliances
WebSphere DataPower SOA Appliances are designed to be dropped into heterogeneous environments to begin immediately providing robust, open standards-based security enforcement points for SOA deployments, and XML and Web services transactions.

These appliances help provide comprehensive XML security and the wirespeed performance needed for today's distributed application architectures.

But DataPower appliances provide more than just an XML firewall. They're an XML proxy with carrier-grade features that can parse, filter, validate schema, decrypt, verify signatures, verify access control and transform, sign and encrypt XML message flows. They also offer robust service level management, policy enforcement and Web services management support, as well as detailed logging and auditing.

DataPower appliances also enable high-performance XML and Web services security. Because DataPower's policies are based on open standards, enterprises have fine-grained control of security without being locked into a proprietary framework. This inherent agility ensures that the DataPower appliances can easily adapt to changing standards, policies and partners for any number of applications.

Ensure that only authorized users have the appropriate access to Web applications with IBM Tivoli Access Manager
IBM Tivoli Access Manager for e-business software is a versatile solution for authentication and authorization problems. This access management software addresses the difficulty of executing security policies over a wide range of Web applications and other resources.

- *Defines and manages centralized authentication, access and audit policy with access management software geared toward a broad range of business initiatives*
- *Establishes new audit and reporting service with authentication software that collects audit data from multiple enforcement points, other platforms and security applications*
- *Reduces help-desk calls and other security problems associated with multiple passwords with flexible Single Sign-On (SSO) to Web-based applications that can span multiple sites or domains with a range of SSO options*
- *Provides a modular authorization architecture that separates security code from application code*
- *Manage and enforce fine-grained entitlement and data-level access control with Tivoli Security Policy Manager*

End-to-end Web security

Because your Web site and Web-enabled applications are increasingly vulnerable to potentially severe attacks, IBM has simplified and integrated solutions to maximize protection while minimizing security administration.

Only a comprehensive end-to-end approach to Web application security — in which security plays an important role in every stage of the application's life cycle — can keep an organization ahead of today's hackers.

By combining software and hardware solutions with professional and managed services, IBM can help your organization adopt just such a comprehensive approach to Web application security. The considerable benefits of IBM Web application security solutions include helping you:

- *Reduce the risk of outage, defacement or data theft associated with Web applications*
- *Improve your ability to meet compliance requirements*
- *Protect your brand and reputation*
- *Improve your ability to integrate business-critical applications*
- *Reduce long-term security costs by focusing on building security into application development and delivery, instead of retrofitting it after the fact*

An organization is only as secure as the applications that support it. Cost effectively securing and protecting the Web applications used to collect sensitive data from employees, customers and partners should be a priority for today's IT executive.

For more information on securing Web-based applications

Contact your IBM representative or visit:
ibm.com/security/application-process.html

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
July 2009

SES03007-USEN-00