Managing business infrastructure
White paper

Staying a step ahead of the hackers: the importance of identifying critical Web application vulnerabilities.

September 2008

IBM Service Management
Visibility. Control. Automation.™

Contents

2 Overview
5 Understanding the most common Web vulnerabilities
6 Building security into your Web applications from day one
7 Taking advantage of industry-wide recommendations and best practices
8 Your first step: a proper assessment of your custom Web applications
9 Embedding application security from design to production with Rational AppScan
10 Summary
11 For more information
11 About IBM Service Management

Overview

Security managers may work for midsize or large organizations; they may operate from anywhere on the globe. But inevitably, they share a common goal: to better manage the risks associated with their business infrastructure. Increasingly, Web application security plays a significant role in achieving that goal.

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, e-mail and user satisfaction feedback.

Unfortunately, the increased use of Web applications makes them very attractive to hackers. As the number and complexity of Web applications grows, so do the number of vulnerabilities introduced into your Web environment. As Gartner points out, "Highly damaging attacks continue to focus on application vulnerabilities."[1] In fact, the number of vulnerabilities affecting Web applications is one of the fastest growing security problems.

Highlights

With the growing number of security attacks, failure to properly secure your Web applications can leave your organization open to costly breaches

With security attacks growing more ingenious and malicious by the day, failure to properly secure your Web applications can leave your organization open to costly breaches. Often highly public, these incidents can result in the theft of sensitive data, defacement of Web sites and the planting of malware (which involves the use of exploitable Web sites to launch attacks).

The specific risks of these types of attacks include:

- Lost revenue and business opportunities.
- Brand and reputation erosion.
- Adverse media attention.
- Unwanted scrutiny from consumer advocates.
- Litigation.

In addition, if your organization is legally bound – and most are – to protect the privacy and security of personally identifiable information and hackers gain access to this 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), Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley. The PCI DSS, for example, was designed to protect cardholder information by maintaining secure electronic commerce. Newer updates to the PCI standard include additional requirements for merchants to protect Web-facing applications against known attacks or face noncompliance.

Some organizations persist in the belief that network security measures (for example, firewalls and intrusion detection systems) are enough to make their applications secure. Many also believe that nonpublic-facing Web applications (those facilitating an organization's intranet) are immune to attacks. Neither

Highlights

is true. In fact, the published list of vulnerabilities from MITRE Corporation indicates that Web application issues (cross-site scripting and SQL injection) are the top two vulnerabilities. For that reason, security managers in forward-looking organizations are concentrating on identifying and resolving security vulnerabilities while Web applications are still in the design and development process. In this way, they can help protect the organization from threats that could compromise data and systems once these applications are deployed.

Many organizations have found that IBM Web application security solutions have helped them eliminate vulnerabilities and keep their Web applications secure

Only such a comprehensive approach to Web application security – in which security concerns play an important role in every stage of the application's life cycle – can keep an organization a step ahead of the hackers. Many organizations have found that IBM Web application security solutions have helped them eliminate vulnerabilities and keep their Web applications secure. IBM Web application security software solutions leverage knowledge gained from the IBM Rational® security team and the IBM X-Force® security team, two of the best-known commercial security research groups in the world, which continually research and evaluate vulnerabilities, security issues and emerging Internet threats. IBM capabilities are based on these objectives:

- To design and build security into applications from their inception, in order to help mitigate the risk of internal and external threats once applications are deployed.
- To test all applications before they go into production.
- To ensure built-in security defenses are effective before and after deployment.
- To protect vital customer data and information assets from external and internal threats.
- To build internal security awareness and provide secure coding training for developers.

Understanding the most common Web vulnerabilities

As Web applications become ever more commonplace – and more complex – so do the strategies that hackers use to compromise them. Recent vulnerabilities and attack methods demonstrate an alarming trend toward attacks with multifaceted damage and even antiforensics capabilities. This means while the hackers are causing significantly more damage, at the same time they are able to cover their tracks more easily.

According to the Open Web Application Security Project (OWASP), the "top ten" current and most serious Web application security vulnerabilities are:

Application threat	Business impact
Cross-site scripting	Impersonates legitimate users to control their accounts
Injection flaws	Allows hackers to access back-end databases for the purpose of theft or alteration
Malicious file execution	Modifies site so all interactions are transferred to hacker
Insecure direct object reference	Allows Web applications to return contents of sensitive file instead of harmless one
Cross-site request forgery	Creates blind requests to bank account to transfer funds to hacker
Information leakage and improper error handling	Facilitates malicious system reconnaissance that may assist in developing further attacks
Broken authentication and session management	Allows hacker to "force" session token on victim; session tokens can be stolen after logout
Insecure cryptographic storage	Allows confidential information to be decrypted by malicious users
Insecure communications	Allows hacker to locate unencrypted credentials and use them to impersonate user
Failure to restrict URL access	Allows hacker to forcefully browse and access a page past the login page

IBM X-Force Trend Statistics Report
The IBM X-Force security research team biannually releases statistical information regarding Internet security threats, including software vulnerabilities and public exploitation, Web-based threats and general cyber-criminal activity. Interestingly, the majority of disclosed vulnerabilities in the latest report are related to Web applications. As this year has shown with the rash of automated SQL injection attacks and compromises, Web-facing applications can be very vulnerable to attacks. The number of vulnerabilities affecting Web applications has grown at a staggering rate — from 2006 to the first half of 2008, vulnerabilities affecting Web server applications accounted for over half of all vulnerability disclosures.[2]

The way to fix the vulnerabilities that allow these attacks is to identify them in the application, then remediate it to eliminate the flaws. The window of exposure for these vulnerabilities can be quite significant – because they often go undetected until a breach has occurred.

Building security into your Web applications from day one

To beat the hackers, Web application security must be a key element in the application development process and integrated early on in the development life cycle.

Unfortunately, this does not occur as often as it should. Many software developers were never trained on security issues or mandated to adhere to security requirements. And security teams often find themselves unable to keep up with the volume of applications they need to test. Consequently, they are either catching issues late in the development cycle or not at all. The continuous cycle of developing, updating and auditing applications – combined with trying to keep up with the latest threats – represents an endless, challenging and resource-intensive campaign against the hackers.

The key to incorporating security into application development is a change of attitude and awareness among the development team: security flaws must be seen as just another kind of software defect. Throughout the application development life cycle – from secure coding, through testing during QA, to ongoing vulnerability testing and periodic security assessments – the impetus must be on addressing the ever-changing threat landscape, and the discovery of new vulnerabilities and exploitation techniques. In addition, allowances must be made for coding changes in the application once it is released and live – because new threats and vulnerabilities can be discovered at any time, and applications should be monitored and retested on an ongoing basis to detect new flaws and fix them.

Highlights

When it comes to application security, an even more difficult challenge is finding unknown vulnerabilities. For instance, the code your developers write may introduce vulnerabilities that you had never considered before. And often it's hard to be certain that the packaged or custom software applications you have purchased and deployed have been properly secured.

IBM Web application security software solutions, including IBM Rational AppScan®, provide software development and security teams with solutions to identify vulnerabilities as part of the development process. Through the ability to identify, validate and report on application security vulnerabilities, Rational AppScan not only finds problems, but also helps resolve them by generating intelligent fix recommendations, pinpointing the issues and helping users to remediate the vulnerabilities. Users can implement both automated and manual capabilities to explore applications and understand all their interfaces and inputs.

Rational AppScan can provide a proven Web application scanning and remediation process within the overall software development life cycle, helping customers deliver more secure and compliant applications

Complementary with IBM Rational application and development offerings, Rational AppScan can provide a proven Web application scanning and remediation process within the overall software development life cycle, thus helping customers deliver more secure and compliant applications to the market.

Taking advantage of industry-wide recommendations and best practices

In order to develop a Web application security strategy well-suited to your organization, it makes sense to study the recommendations and best practices that have proven effective in eliminating vulnerabilities. The following represents the guidelines followed by many forward-thinking organizations:

- Identify and mitigate or prevent security vulnerabilities while applications are still in the requirements, design and development process, to protect your organization from threats that could compromise data and systems after they are deployed.
- Improve overall security awareness and provide secure coding training for developers.
- Adhere to strict security testing standards from the development phase through the QA phase of the build cycle. This can be done through use of security scanning tools and penetration tests. And, as dynamic as Web applications are, it's important to continue periodic post-deployment security testing to monitor the live state of your Web site and its ever-evolving applications.
- Perform ongoing scanning and monitoring of your organization's threat exposure. Remember, threats change all the time.
- Provide users with role-based access to the resources they need and single sign-on capabilities to help optimize productivity — and minimize the administrative burden on IT staff.

Your first step: a proper assessment of your custom Web applications

An IBM Internet Security Systems (ISS) application security assessment is, in essence, a review of your custom Web applications to determine security weaknesses that can lead to compromise. Our security experts can thoroughly assess your most mission-critical applications, from both technical and non-technical perspectives, to uncover security weaknesses and demonstrate the consequences of an attacker taking advantage of those weaknesses. (For a more comprehensive assessment, you can supplement the hands-on IBM ISS application security assessment with automated scanning of additional applications.) The result is a detailed report of findings and specific recommendations for remediating any vulnerabilities found. The clear-cut benefits of an IBM ISS application security assessment often include:

- An increased awareness of the importance of best security practices.
- Outlined responsibilities to protect the confidentiality, integrity and availability of company assets and resources.
- A reduced risk of intentional or accidental information and IT assets misuse by your employees.
- Compliance with federal and state regulations that require security awareness training.
- A low-cost option for training all employees on your corporate security policies.
- Proactive analysis of existing security controls to uncover weaknesses and address them before they are uncovered by a malicious attacker.

Highlights

The broad portfolio of IBM security solutions can help you manage application security throughout the application's life cycle and can identify and quickly address vulnerabilities

Embedding application security from design to production with Rational AppScan

To help your organization adhere to Web application best practices, develop more secure applications and better manage your business infrastructure, IBM offers a broad portfolio of security solutions that can help you manage application security throughout the application's life cycle. These solutions can identify and quickly address vulnerabilities. Taking a preemptive approach to application security is just one of several entry points into IBM security solutions, which can assist you in establishing effective risk management strategies to manage and secure business information and technology assets, anticipating vulnerabilities and risks, and maintaining timely access to information.

Rational AppScan can help your organization embed application security testing from design to production. Prior to deployment, applications are tested for known and unknown vulnerabilities. Because this solution helps developers, security auditors and IT staff, it gives you the flexibility to address application security in the ways that make the most sense for your enterprise. And IBM Tivoli Access Manager can ensure that only authorized users have the appropriate access to Web applications.

IBM Proventia® Network Enterprise Scanner is designed to protect the network infrastructure that hosts these Web applications. It helps reduce network security risks by accurately identifying, prioritizing, tracking and reporting network vulnerabilities.

In addition, IBM Proventia Server Intrusion Prevention System (IPS) protects operating systems and applications from known and unknown threats with integrated firewall and vulnerability-centric intrusion prevention.

Summary

Hackers focus on an organization's Web applications – because that's where the vulnerabilities are. According to Gartner, "application security should become part of a formal software life cycle (SLC) process. It should be addressed at each phase of the SLC: application analysis, design, construction, testing and operations. Application security tools that automate security vulnerability detection should be used as early in the development process as possible."[3]

The most effective way to prevent – or uncover and defeat – attacks that exploit Web application vulnerabilities is to adopt a comprehensive approach to Web application security that covers the application's entire life cycle from development through deployment, and deals with both known and unknown attack types.

With Web application security tools such as IBM ISS application security assessment and Rational AppScan automated application security scanning, IBM can help your organization adopt just such a comprehensive approach to Web application security – and thus, stay a step ahead of the hackers. 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 various 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.
- Achieve the overriding goal of better managing your business infrastructure.

For more information

To learn more about deploying IBM Web application security solutions today, talk to an IBM representative or IBM Business Partner. They can help define the best solution and measure the business value of the software based on your individual environment. More information about IBM Web application security solutions is also available at **ibm.com**/software/tivoli/governance/security/appsec.html

About IBM Service Management

IBM Service Management solutions help organizations manage their business infrastructure and deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development, operations management and system administration, and draw on extensive customer experience, best practices and open standards–based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.

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

Produced in the United States of America
September 2008

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

[1] Gartner, "Protecting Customer Data and Meeting New PCI Web Application Security Requirements," John Pescatore, July 2008.

[2] IBM, "IBM Internet Security Systems X-Force 2008 Mid-Year Trend Statistics," July 2008. See http://www-935.ibm.com/services/us/iss/xforce/midyearreport/

[3] Gartner, "Gartner 2008 IT Security Threat Projection Timeline," August 2008.