Web application security
Executive brief

Rational. software

Managing a growing threat: an executive's guide to Web application security.

Danny Allan, strategic research analyst,
IBM Software Group

Contents

Introduction

More and more companies are relying on Web-based applications to provide online services to their employees, to support e-commerce sales and to leverage portals, discussion boards and blogs that help staff better communicate with customers, partners and suppliers. However, as the number and complexity of Web applications have grown, so have the associated security risks. With increasing frequency, incidents of Web application breaches resulting in data theft are popping up as front-page news. And such attacks now have more serious consequences than ever before. Customers are demanding corporate accountability, and regulations such as California Senate Bill 1386 require full disclosure when there is a breach of security connected with sensitive or personal information.

Further, over the past five years, two key trends have emerged in the security world:

1. Hackers are no longer attacking for pride and ego, but for profit and property.
2. Software is now the most common target of exploitation—specifically, Web applications.

As a result, companies can no longer afford to ignore Web application security. This paper discusses the security challenges created by Web applications and suggests some steps you can take to address them.

Responding to evolving security needs

In the past, companies have relied on perimeter defenses to keep their networks and data secure. Unfortunately, network firewalls and network vulnerability scanners can't defend against application-level attacks. By design, Web applications allow unknown users to interact with your data and systems. This interaction passes through network defense mechanisms such as firewalls and intrusion detection systems, leaving your business vulnerable to malicious attacks.

Web applications have increasingly become high-value targets for hackers. Since so many Web sites contain vulnerabilities, hackers can leverage a relatively simple exploit to gain access to a wealth of sensitive information, such as credit card data, social security numbers and health records. Therefore, it's more important than ever to examine your Web application security, assess your vulnerability and take action to protect your business.

Table 1 lists just a few of the potential threats to Web applications, the effect they could have on your business, and the average percentage of Web sites that are vulnerable to this type of attack.

Threat	Gives attackers the ability to …	Average percentage of vulnerable Web applications
Cross-site scripting	… impersonate a trusted user to gain access to your sensitive business data	80%
Structured query language (SQL) injection	… access all the data in your database, resulting in a complete data compromise	62%
Parameter tampering	… navigate your database and retrieve or modify its contents	60%
Cookie poisoning	… steal one or more of your customers' identities	37%

Table 1

Emerging regulations and requirements

As the number of Web application security breaches has increased, regulatory and industry requirements have become more stringent. New standards, such as the Payment Card Industry (PCI) Data Security Standards*—a protocol that includes requirements for security management, policies, procedures, network architecture, software design and other protective measures—now include directives for establishing and maintaining Web application security. Such measures dictate that companies protect all Web-facing applications against attacks by either engaging an application security organization to review all custom application code for vulnerabilities or installing an application-layer firewall in front of all Web-facing applications.

Establishing proper security practices in your company

To combat the growing threat of Web application breaches, it's important to address three key areas of your business: your people, your processes and your technology.

Your people

It is imperative that the people developing and deploying your Web applications—whether they are staff members or external contractors—understand the fundamentals of secure design principles and security threats. In the past, security was viewed as an IT problem, not a development problem. But now, security experts have realized that security starts at the code level. Therefore, it's important to provide your developers with the training they need to stay on top of changing security threats and learn about existing and emerging methods for mitigating them.

Your processes

As almost anyone who's ever developed software can tell you, it's both easier and significantly cheaper to get it right the first time. That's why integrating Web application security testing into the software development lifecycle from the very start is essential for establishing good risk management. And while it's important to have a dedicated and knowledgeable security assessment team perform a final review, it's equally important to integrate security into the early stages of application development to focus on security issues as they appear. By approaching the issues proactively, you can save time and reduce

your development costs. It's also important to document and evaluate the results of these initiatives. Metrics to examine can include key components such as threats, vulnerabilities, remediation tasks and criticality. Documenting these measurements can help you establish baselines and further aid your security efforts over time. Without such an evaluation, it's impossible to determine whether adequate protection has been implemented to mitigate your potential security risks.

Your technology

There are a number of ways to implement proper security protocols in your Web-based applications. Although effective, manual penetration testing alone can be time consuming, labor intensive and costly. Supplementing manual testing procedures with an automated Web application security tool can help you gain a consistent, reliable and scalable analysis of your Web application security vulnerabilities—even across large, diverse IT environments. And such tools can help drive down testing costs by automating many manual tasks. Further, today's scanning tools are very sophisticated, capable of providing complete coverage of the latest application technologies including Web 2.0, which can greatly extend your manual testing capabilities.

Delivering the software and services you need to secure your Web applications

IBM is a marketplace leader in Web application vulnerability assessment software. Providing a range of security software products, IBM offers individual tools for dedicated security auditors as well as comprehensive enterprise platforms for large auditing organizations.

In addition, IBM can provide executive, management and developer reporting that is specifically designed for the role of each individual. While your security auditor may be interested in security issues for an entire line of business, your chief compliance officer may require reports on the specific compliance issues he or she is responsible for. The IBM enterprise platform also contains critical features such as issue management, role-based access, customization and powerful integration application programming interfaces (APIs).

IBM can also help train your people through detailed advisories and fix recommendations tailored for your unique business needs. Through its client services branch, IBM provides both security and product training classes that are specifically targeted to your industry.

Conclusion

As incidents of Web application breach continue to increase, so too does the threat to your business. If you rely on Web applications to support any part of your business, it's time to take control of your application security. IBM can help you examine your existing security practices and make recommendations that can help you protect your enterprise from the devastating consequences of a security breach.

For more information

To learn more about IBM Web application security solutions, contact your IBM representative or IBM Business Partner, or visit:

ibm.com/software/rational/offerings/testing/webapplicationsecurity

To download a free evaluation copy of the IBM Rational® AppScan® Web security application, visit:

www.watchfire.com/securearea/appscan.aspx

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

Produced in the United States of America
12-07

* Payment Card Industry (PCI) Data Security Standard, Version 1.1, September, 2006. https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

RAE14000-USEN-00