A Proactive Approach to Identifying and Reducing Web Application Security Vulnerabilities

By: Patrick Vandenberg, Security and Compliance Marketing Manager, IBM Rational

Few innovations have proven as flexible and valuable as Web applications. Although extremely innovative, they can be vulnerable to malicious attacks. As more business is conducted online, it creates new challenges for organizations to meet Web application security and compliance standards. As Web applications become increasingly more complex; so do the Web security vulnerabilities. According to the latest statistics from the IBM X-Force Trend & Risk Report [1], 37 percent of all issues reported were Web application related.

The Application Security Landscape

Web applications present a number of unique security challenges. The most apparent is exposure because Web applications reach millions of users; they also reach millions of potential hackers. Web applications stretch across multiple infrastructure tiers and incorporate many process layers, elements that expose them to a wide range of prospective attackers. Also, Web applications have become the attack surface of choice for hackers because they are designed to have access to back-end data and are often built with the intention of a one-off development effort. Though Web applications can be built by a dedicated in-house development team, they are also often outsourced. As Web applications get more complex, so do their vulnerabilities; as they become more useful and pervasive, they become higher value targets. And cybercriminals have taken note.

Recent research supports these observations. According to the IBM X-Force 2011 Report:

- An explosion of security breaches has opened 2011, and almost daily reports continue to mark this year as the “Year of the security breach.”
- SQL injection continues to be a favorite attack vector as demonstrated by

the numerous mass SQL injection attacks occurring over the past several years.
- Top high-volume signatures from IBM Managed Security Services (MSS) demonstrate that favorite attacker methods are SQL injection, and the brute forcing of passwords, databases, and Windows shares that continue to rank at the top of MSS sensor traffic. People are scanning the Internet for open services and attempting to break into them.

Vulnerabilities are real, and the business implications of exploits are well documented. The financial risk of security breaches is not going away anytime soon. If anything, it is only going to increase.

According to a recent Ponemon report, in 2010 the average cost per compromised record was $214. In addition, the Verizon 2010 Data Breach Investigations Report found that there were 143 million records compromised in 2009. When you put these figures together it results in an annual cost to corporations in the range of $30B. Not only are security issues cheaper to fix when you catch them early but public data breaches through web applications are frequent and can result in serious consequences, including lost revenue and business opportunities, revelation of highly confidential or damaging information, brand and reputation erosion, adverse media attention, unwanted scrutiny from consumer advocates, and growing costs to support litigation and compliance.

How Organizations Can Proactively Address Vulnerabilities

New methods for attacking Web applications are growing in volume and frequency. Security teams are under intense pressure and many cannot keep up with the volume of applications they need to test. Currently, teams are generally 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 patches is a constant battle against threats.

In the software development world, enterprise applications used to be in a class by themselves. They often ran on mainframes, were written in different languages, and were accessed by a privileged few. These applications often contained the most critical and valuable data that an organization owned.

As organizations move to open up their applications for self-service, they are typically putting a Web interface in front, with some associated business logic. As Web interfaces are the attack surface of choice for hackers, the enterprise applications are now subject to hacking and potential data breaches in ways that they never were before.

The typical – and prudent – initial reaction is to do a security review of Web applications before they go live. This can be effective, but it is an expensive way of being secure. A better approach is to proactively build in security from the beginning, making use of the existing development tools to communicate with the development team. This will help drive out security flaws early in the development cycle, when code is cheaper to fix. Then the security review becomes a verification step, ensuring that vulnerabilities are not present as development teams move

applications into production environments.

Application security is not an option. Once a development team accepts that premise, then the only question is how to reduce the cost of an application security program. For example, IBM has developed a set of solutions to enable automated security testing, and these solutions integrate into development environments to help reduce the cost of being secure.

The considerable benefits of deploying application security solutions include:

- Reducing the risk of outage, defacement or data theft associated with Web applications
- Improving the ability to meet various compliance requirements
- Protecting brand image and reputation
- The effective integration of business-critical applications
- Management of long-term security costs by focusing on building security into application development and delivery, instead of retrofitting it after the fact
- Better management of the business infrastructure overall

The most effective way to prevent, uncover and defeat attacks that exploit Web application vulnerabilities is to adopt a comprehensive approach to Web application security. The emphasis must be on the entire application life cycle, from development through deployment.

Links:
[1] http://www-935.ibm.com/services/us/iss/xforce/trendreports/