WHITE PAPER

Assessing Application Vulnerabilities:

A 360 Degree Approach

Dr. Brian Chess
Founder and Chief Scientist
Fortify

WHITE PAPER

Assessing Application Vulnerabilities:
A 360 Degree Approach

Table of Contents

Abstract

Increasingly, the software applications that millions of people and businesses depend on every day are being exposed to escalating risks in the form of sophisticated attacks and other threats. This paper will explore how a 360 Degree approach, that employs the complimentary techniques of both static and dynamic analysis deployed at multiple points in the application lifecycle, enables organizations to more rapidly and effectively identify, prioritize and fix security vulnerabilities in software.

Introduction

In recent years, hackers, organized crime cartels and rogue governments have greatly increased the sophistication and frequency of their attacks on software applications — the operating systems and programs that millions of people use every day. The National Institute for Standards and Technology (NIST) reports that 92 percent of exploitable vulnerabilities are in software, while the research firm Gartner estimates that application vulnerabilities account for three out of every four security breaches.[1]

"The same Web 2.0 characteristics that enable creativity, productivity and collaboration also make the Web 2.0 ecosystem prone to successful attacks and theft."

Attackers take advantage of these security cracks to steal crucial data, such as identities, passwords and account information, and sabotage computer systems or influence processing or functionality for profit or nefarious intent. The consequences can be severe. The cost of recovering from even a single data breach now averages $6.3 million — up 31 percent since 2006 and nearly 90 percent since 2005.[2] Cunning attackers are also adept at quickly converting stolen information into cash by way of eBay-style black market Web sites that cater to cyber criminals.

Today, despite advances in firewalls, anti-virus systems and other perimeter protection solutions, attacks against applications continue to increase, affecting organizations across nearly every industry, including finance, healthcare, retail, telecommunication, education, ISVs and government agencies. Government regulations, such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA), mandate protections for certain industry sectors, while the Payment Card Industry (PCI) Data Security Standards require organizations that process credit card transactions to implement specific application security activities.

"The cost of recovering from even a single data breach now averages $6.3 million — up 31 percent since 2006 and nearly 90 percent since 2005."

Although security flaws in widely adopted operating systems grab all the headlines, much time and expense goes into finding these holes and providing solutions. The more serious danger lies in those applications that are not on everyone's radar — the thousands of customized applications and automation software that companies and their partners depend on to keep business running smoothly. To complicate matters, the type of software that is most susceptible to attack — applications that rely on Web 2.0, service-oriented architecture (SOA) and open-source development — represent the fastest growing application segment because of their low cost, flexibility, short development cycles and ease of use. On the plus side, these new technologies make more application functionality available to a far wider range of users. However, their wide adoption in often less-controlled circumstances also creates enormous opportunities for exploitation. Indeed, Gartner has concluded that "The same Web 2.0 characteristics that enable creativity, productivity and collaboration also make the Web 2.0 ecosystem prone to successful attacks and theft."[3]

Application Security Challenges

To find an effective approach to assure application security, companies must overcome numerous challenges. Foremost among these are: identifying as many potential vulnerabilities as feasible in a timely manner; prioritizing development efforts to determine which vulnerabilities pose the greatest risks; and fixing security flaws rapidly and cost-effectively with minimal impact on business productivity. What follows is a brief examination of the key issues within each of these challenges.

While spending on perimeter-only strategies continues to grow, reported breaches more than doubled in 2007.[4]

Detecting Vulnerabilities

Much time, effort and cost has gone into network "hardening" solutions designed to prevent attacks against applications. However, very little attention has been paid to actually hardening the applications these measures are designed to protect. Cyber criminals know this and are taking advantage. For example, while spending on perimeter-only strategies continues to grow, reported breaches more than doubled in 2007.[4] It's easy to understand why. To compromise a piece of software, an attacker merely needs to find a single route past network defenses — for example, by gaining access to a Web-based application through an open Web portal or by luring unsuspecting users through content spoofing. A far more effective approach to prevent attacks entails closing the security gaps that exist within the applications themselves. Once applications become impervious to attack, they cannot be compromised, even after a network breach.

In order to resolve security flaws in applications, organizations must be able to identify the broadest possible array of potentially exploitable vulnerabilities. There are two primary methods to accomplish this: static analysis and dynamic analysis.

- **Static analysis.** This is the most widely used technique for detecting vulnerabilities. It involves applying automated tools to analyze an application's source code. Automated static analyzers can locate more types of vulnerabilities than any other method. Indeed, the sheer number of vulnerabilities they identify can be difficult for IT staffs to handle effectively.
- **Dynamic analysis.** Some categories of vulnerabilities become manifest only while code is being executed, such as those involving an application's configuration and environment. Automated dynamic analysis tools are used to locate these vulnerabilities during runtime, for example, during testing. Indeed, dynamic analysis that can be applied in tandem with an organization's existing testing protocols is particularly effective. However, it is important to note that dynamic analysis can examine only those portions of code that are being executed; it cannot find vulnerabilities in areas of the system that are not running. As a consequence, the results from dynamic analysis reflect only the amount of code that has been covered. This carries important implications for testing.

Because most QA organizations are under constant pressure to meet release dates, they tend to concentrate only on the most important bits of application code — the "high traffic" areas, leaving less critical aspects to be dealt with after deployment. Knowing this, insidious attackers seek out remote areas of a system that are often not well used, because they have received less scrutiny during testing and therefore have a higher probability of containing vulnerabilities. To stay ahead of attackers, organizations should employ dynamic analysis, not only during testing, but also after deployment. Dynamic analysis applied to real-world deployments can ensure that potentially exploitable vulnerabilities in "low traffic" areas of code — the ripe targets for attack are identified and remediated before any damage can occur.

Prioritizing Remediation Efforts

Ensuring system security is critical for any enterprise, yet it cannot come at the expense of lost productivity and business delays. Most IT organizations are stretched to the limit handling the day-to-day tasks of keeping systems up and running. Development teams have other mission-critical priorities and typically can allocate just a certain amount of time to fix security issues. At the same time, the sheer numbers of vulnerabilities that static and dynamic analysis can uncover can be staggering. It's estimated that their density can range from hundreds to tens of thousands of vulnerabilities per million lines of code, depending on technology and programming practices. With such a daunting number of potential vulnerabilities and limited time and resources, prioritization becomes essential. Not all vulnerabilities are equal; some are extremely critical, others become more important in the presence of other security flaws, while still others present no exploitable threat at all. Determining which ones need to be addressed in what order can only be done effectively through prioritization, a key capability that many of today's automation tools lack.

Fixing Vulnerabilities

In its role, the security organization is responsible for understanding each application's risk profile, identifying real threats and assuring that exploitable vulnerabilities are repaired. However, developers are the ones tasked with actually fixing security issues — all the while balancing the ongoing demands to ensure system functionality, quality and availability for the business. The consequences of even a single serious vulnerability can be devastating. When it comes to closing security gaps in software, time is of the essence. To deal rapidly and effectively with evolving application security threats, security and development personnel must work together collaboratively and in close partnership. Automation is critical to maximizing the effectiveness of both parties and shortening response times required to remedy urgent vulnerabilities.

Fortify 360 Analysis — A New Approach for Detecting, Prioritizing and Remediating Application Vulnerabilities

Fortify 360 is a suite of integrated applications for identifying, prioritizing and fixing security vulnerabilities in software and managing the business of ensuring application security. By enabling enterprises to quickly identify and fix the security holes within their software applications, Fortify 360 dramatically reduces the risk of catastrophic attacks and helps ensure compliance with government and regulatory mandates.

> Fortify 360 detects more than 225 types of vulnerabilities — the most in the industry today.

Fortify 360 uses 360 Analysis for detecting vulnerabilities, giving enterprises the fastest, most comprehensive method for identifying threatening vulnerabilities in software. Using 360 Analysis, organizations can:

- Detect the broadest array of vulnerabilities by combining static and dynamic analysis. Fortify 360 detects more than 225 types of vulnerabilities — the most in the industry today.
- Choose from among multiple detection methods to select those that deliver the fastest results for their unique systems and environments.
- Ensure maximum code coverage with dynamic analysis by using their existing test suites to identify vulnerabilities and to monitor applications in production.
- Correlate and prioritize results from static and dynamic analysis deployed at multiple collection points. With a single integrated view of results from multiple detection methods and points, organizations can gain insight into priority-changing relationships between seemingly independent vulnerabilities.
- Fix vulnerabilities quickly and cost-effectively by easily sharing vulnerability insights among security and development teams and integrating them into existing tools and processes.

Detecting Vulnerabilities with Fortify 360

In contrast to other application security solutions, only Fortify 360 Analysis provides the most complete understanding of software from a security perspective. It is the first solution to integrate static and dynamic analysis. It incorporates a Static Code Analyzer (SCA) as well as two dynamic analysis tools: a test-phase-focused Program Trace Analyzer (PTA) and a production-phase-focused Real-Time Analyzer (RTA). Working in concert, each analyzer adds insight to the other, enabling organizations to find more vulnerabilities more efficiently than any one method used in isolation. In addition, Fortify provides ongoing threat intelligence in the form of periodic updates, which provide the underlying rules that fuel the analyzers and keep IT teams up to date on current hacking trends and vulnerabilities.

> Working in concert, each analyzer adds insight to the other, enabling organizations to find more vulnerabilities more efficiently than any one method used in isolation.

Fortify 360: Static Code Analyzer (SCA)

The Static Code Analyzer uses multiple algorithms and a knowledgebase of secure coding rules to analyze an application's source code for vulnerabilities that can be exploited once the application is deployed. This technique analyzes every feasible path that execution and data can follow to identify and help remediate more than 200 categories of vulnerabilities.

Key Benefits:

- Identifies vulnerabilities early in the software development life cycle, when they are least expensive to fix
- Educates developers about security while they work

Fortify 360: Program Trace Analyzer (PTA)

The Program Trace Analyzer identifies application vulnerabilities during runtime, while an application is being tested. With PTA, an enterprise can use existing test suites to find vulnerabilities. It reveals vulnerabilities that can be found or more easily identified only when an application is being executed, such as those that become apparent through unpredictable user behavior. With no customization required and zero security expertise needed, PTA enables QA and developers to cover a far wider range of code without changing their processes.

Key Benefits:

- Enables enterprises to repurpose test suites for detection of vulnerabilities
- Integrates seamlessly into existing QA testing processes
- Provides accurate results with the fewest false positives
- Operates from within an application, providing the best context to determine whether an issue is genuinely exploitable or simply benign
- Provides the exact code location for each vulnerability, enabling more rapid remediation

Fortify 360: Real-Time Analyzer (RTA)

The Real-Time Analyzer (RTA) component defends against evolving logicbased attacks, including fraud, hacking and data mining that can threaten applications once they've been deployed. Uniquely positioned inside an application, RTA provides a real-time view into how a deployed application is being attacked in the real world. At any point in time, IT personnel can see who is attacking (based on IP address and domain name), how the attack is being conducted, and what part of the application is being attacked, down to the exact line of code.

By correlating results from multiple analysis techniques, users can eliminate false positives, verify the exploitability of specific issues and prioritize the problems they find. This "360 degree view" brings greater understanding of how vulnerabilities interrelate to make triaging, auditing and remediation faster and easier.

Key Benefits:

- Provides true application-layer insight and can make use of application logic to make decisions
- Provides results in real time, including email alerts
- Accurately distinguishes between an actual attack and a legitimate request, improving the end-user experience while greatly boosting protection
- Can accommodate additional logic- and behavioral-based rules that address specific threats for individual Web applications

Prioritizing Efforts with Fortify 360

Fortify 360 integrates the results from the three analyzers into a central repository, providing IT organizations with a comprehensive view of the vulnerabilities. By correlating results from multiple analysis techniques, users can eliminate false positives, verify the exploitability of specific issues and prioritize the problems they find. This "360 degree view" brings greater understanding of how vulnerabilities interrelate to make triaging, auditing and remediation faster and easier.

An example illustrates how it works. A user runs SCA on the source code of an application and identifies a long list of vulnerabilities. While SCA prioritizes its findings, the list is still quite long. At the same time, the user runs a dynamic test using PTA. PTA produces a shorter list, but there is no guarantee that the tests exercised all of the code. Without Fortify 360, an organization would end up with two separate lists of vulnerabilities with no way to determine which issues were identified by both tools (duplicates), which were unique and that were related. Most importantly, an organization has no way to determine which issues pose the most serious risks and therefore should be addressed sooner. Fortify 360 combines the results from both tools and looks for patterns that indicate which issues need attention first. As a result, Fortify 360 provides organizations with an effective way to address their most important security issues rapidly and at less cost.

Remediating Vulnerabilities Collaboratively with Fortify 360

The rapid remediation of software vulnerabilities requires a great deal of teamwork and orchestration among key stakeholders, including security, QA and development organizations. With its centralized console, correlation and prioritization capabilities, Fortify 360 enables teams to collaborate more effectively to resolve security issues. For example, Fortify 360 integrates with the QA and development processes and tools that organizations use daily. It enables security auditors to submit issues to their company's bug-tracking system, upload issues to a developer's integrated developer environment (IDE), or send them to a central server where they can be managed and tracked. Fortify 360 enables security personnel to fix some issues themselves and provides plug-ins that allow developers to remedy vulnerabilities from within their IDEs. Additionally, Fortify 360 provides the industry's first collaborative auditing capability, which enables different teams to address multiple vulnerabilities on the same code base, concurrently. With Fortify 360, companies can work across organizational silos to fix security issues faster, while freeing up time and resources to meet ongoing business requirements.

Conclusion

Every indication is that hackers, organized crime and nations with malicious intent are greatly increasing their efforts to target thousands of applications around the globe. The potential cost in terms of lost revenue, customer trust and brand integrity of even one significant security breach can be devastating. Accordingly, company security policies and government mandates are placing growing pressure on IT organizations to bolster the security of the applications they create, procure, manage and deploy. With Fortify 360, IT organizations can detect, prioritize and resolve software vulnerabilities faster and with less effort, enabling them to address their most urgent security issues rapidly and at less cost. Moreover, Fortify 360 is the only application security solution that correlates results across detection techniques and integrates with existing security, QA and development processes and tools to enable organizations to collaborate more easily to protect applications from evolving threats.

Learn more. Discover what Fortify 360 can do for your application security at www.fortify.com.

References

1 Mark Curphey, *Software Security Testing: Let's Get Back to Basics*, October, 2004, SoftwareMAG.com; Theresa Lanowitz, *Now Is the Time for Security at the Application Level*, December 1, 2005, The Gartner Group.

2 Ponemon Institute Study, 2007.

3 John Pescatore, Joseph Feiman, *Security Features Should Be Built Into Web 2.0 Applications*, March 5, 2008, The Gartner Group.

4 Ponemon Institute Study, 2007.

FORTIFY®

FORTIFY SOFTWARE INC.

MORE INFORMATION IS AVAILABLE AT WWW.FORTIFY.COM

2215 BRIDGEPOINTE PKWY.
SUITE 400
SAN MATEO, CALIFORNIA 94404

TEL: (650) 358-5600
FAX: (650) 358-4600
EMAIL: CONTACT@FORTIFY.COM