

I D C V E N D O R S P O T L I G H T

Application Security: No Room for False Positives

Adapted from *Worldwide Security and Vulnerability Management Software 2005-2009 Forecast and Analysis: Taking Control of the Security Environment* by Charles J. Kolodgy and Rose Ryan, IDC #34604

Sponsored by Cenzip

The Internet continues to be an agent for business operation. More and more people and organizations are using the Internet for critical business transactions; however, this success becomes its own worst enemy. As the value of transactions occurring over the Internet increases, so too do security threats. Attackers have targeted communication protocols and operating systems as their avenues for exploitation. However, many of those avenues are protected with network defenses, so motivated attackers have turned their attention to Web-based business applications. These custom applications, which generally require customer interaction and which contain or access critical data, are now being attacked and exploited. Enterprises are responding to this new threat by hardening Web applications, and they are increasingly turning to Web application security assessment tools to improve the security of their applications. One of the key requirements for the security code review tools is high accuracy. This document examines why accuracy is critical to the effectiveness of the tools, and it discusses how Cenzip Hailstorm addresses this problem.

Introduction: How Secure Are We?

Fear of data exposure or loss from a successful Web site hack leads to sleepless nights. Many times, Web sites are put into production for business needs before they have been fully vetted. IT professionals face this decision all the time because information technology is an integral component of the business environment. A corporate Web site transforms the landscape in which businesses can provide wide-open, 24 x 7 admission to their business applications.

The nature of Web technology contributes to the fear security professionals experience. Today's Web sites are no longer static, informational electronic brochures; instead, they are multifeatured and dynamic showcases. Web applications have become ubiquitous and can generate dynamic Web pages based on input and databases. Most Web servers provide interfaces that are used to spawn and communicate with Web applications. Interface code, such as the common gateway interface (CGI), links an HTTP request (normally sent from a browser) with the executing application. It specifies which application should be invoked, the parameters/data passed to the application, and the mechanism used to provide the Web server with the dynamically generated page.

The expansion of user-enhanced Web sites has allowed the Internet to become an engine for improved business, but it's also the root of a security problem. Accepting input from users, which has created the dynamic Web, is fraught with danger. Because CGI allows for the execution of programs that process arbitrary data sent by a user, the danger exists that malicious commands will be directed through the CGI scripts. It is critical that only input in a format the application expects and can process be accepted.

Web Application Attack Mechanisms

Enterprises have spent billions of dollars to protect their information infrastructures. Confronted with steadily maturing network layer defenses, attackers are increasingly turning their attention to the application layer and the corresponding business applications that are running. The dynamic nature of Web applications offers users unique experiences, but the technology that makes a Web site so interesting also has a dark side. People with malicious intent can turn this same technology against the enterprise to cause considerable damage to a company's bottom line and reputation.

Nearly one in five businesses, both large and small, report that attackers have exploited flaws in Web applications. It's relatively easy, as many attacks are simple to launch. Anyone with a browser can unleash them. Other types of attacks require intimate knowledge of the host server and underlying applications. All are potentially damaging to an organization's Web presence. The following are some of the basic attack types employed against Web sites and Web applications:

- **Session management.** A session is hijacked for malicious purposes.
- **Authentication bypass.** A hacker can bypass authentication mechanisms and access Web applications illegally.
- **Cross-site scripting.** Malicious code is executed when a user clicks on the URL.
- **Application buffer overflow.** Very long requests exceed the allocated buffer size, which can allow hacker code to be executed.
- **Cookie poisoning.** Manipulating a session cookie's contents enables the attacker to obtain unauthorized information from the server.
- **Hidden field manipulation.** This attack involves changing the values of hidden fields, which are frequently used to provide status information to the server.
- **Stealth commanding.** Modifying Web-form input fields coerces the Web server into actions that it wouldn't ordinarily allow.
- **Forceful browsing.** Modifying a URL can bypass Web controls to break out of a server's root directory and access files on the rest of the file system.
- **Parameter tampering.** Submitting modified data to the Web server returns all member records in the database.
- **Third-party misconfiguration.** This attack involves exploiting an insecure server configuration.
- **Known vulnerabilities.** This attack involves exploiting known vulnerabilities or default settings that haven't been patched or changed.
- **Database sabotage.** This attack involves appending valid SQL commands to form fields.
- **Data encoding.** This strategy disguises attacks by using alternate encoding methods.

To be fully secure, enterprises need to be able to test the dynamic aspects of their Web sites to remove the vulnerabilities these attacks can exploit.

The Criticality of Web Application Vulnerability Assessment

IDC believes that network security tools, such as firewalls and intrusion detection systems (IDS), must be augmented by strong Web intrusion protection mechanisms. Enterprises, business units, and, importantly, Web developers are realizing that the weakest links in the security chain are Web servers, Web applications, and related back-end databases. As exploits associated with Web applications continue, IT professionals and management are coming to the conclusion that insecure coding is the root of many a breach – one might even say it's the source of security woes. The concepts of developing applications with security in mind and removing security defects from applications before they are released are gaining adherence.

Most people understand the need to perform functional testing to ensure that applications provide the services expected, but often overlooked is testing to ensure that applications do not include unintended operations, many of which become security vulnerabilities. Achieving application security requires the ability to search applications for issues that are unique and previously unknown. This is more critical in Web applications because of the way they receive and process unstructured user commands. The Web application has no control on user input, only on the output. A key to security testing of software is to uncover unexpected, unintended, undocumented, or unknown functionality. The best way to do this is to use Web application vulnerability assessment scanners, which are designed to deal with the specific needs associated with application and Web site security.

These tools usually utilize attack signatures or code, but the best of these scanners rely on the running of known techniques used to attack Web applications and servers. In other words, Web application vulnerability assessment scanners attempt to emulate the actions of experienced hackers. They avoid general vulnerability checks, such as port scans or patch checks, to concentrate on Web vulnerabilities that standard vulnerability assessment tools don't address.

Like other vulnerability assessment products, Web application scanners generate lists of discovered vulnerabilities, along with descriptions, impact statements, and recommended solutions. Typically, these tools are run as part of audits or other security assessments. However, IDC believes they should be utilized throughout the application development life cycle to check for vulnerabilities prior to fielding. Software is often full of bugs, and poorly written code creates vulnerabilities. Because many of the applications and all of the Web content is "homegrown," bugs are harder to find and fix because there's no vendor to issue a patch. Interestingly, organizations that use these tools realize that they not only inhibit malicious intrusions but also greatly enhance the reliability of software code being written in-house, which can limit the number of software bugs that lead to vulnerabilities but also reduce support costs.

Many tools are available in the market, but IDC believes that enterprises should look for Web application code testing products that have the following critical characteristics:

- **Low false positives.** It is critical that tools accurately call out vulnerabilities. Too many "ghosts" or false alarms greatly reduce the costs and time savings associated with the tools and may mean real vulnerabilities are overlooked.
- **Attack simulation.** Tools need to be able to duplicate how an attacker would attempt to penetrate the applications. This category also can be referred to as penetration testing, dynamic testing, and black-box testing.
- **Policy and regulatory checks.** Security isn't the only consideration; therefore, the products need to be able to check the application to see if it adheres to specific policies and regulatory requirements.

Reducing False Alarms Is a Value Multiplier

False alarms resulting in application vulnerability and penetration testing reduce the effectiveness of such tools. If the assessment tool produces a high number of alarms, many of which will be false positives, those items will need to be validated manually. Using tools that are more accurate allows for a scalable application testing process, reduces the number of people required on a job, and improves remediation. Specifically, such tools provide for a more efficient process. IDC believes the success of a black-box assessment should be measured by the thoroughness of the analysis and the accuracy of the results. To achieve accuracy, not in finding false positives but in discovering the most vulnerabilities possible, products incorporate fault injection and penetration testing, two attack simulation techniques.

Software fault injection is a dynamic approach to answer the question, "What if ...?" Fault injection has been used in hardware environments to test the robustness of the whole system. Software fault injection creates hypothesized errors by adding code to the code under analysis, changing the existing code, or deleting code from the code under analysis. The resulting behavior of the software is monitored. Software fault injection provides information about how the software is likely to behave under exceptional conditions – that is, how robust the software is. If this sounds familiar, it's because many of the attack methods mentioned earlier involve manipulating inputs or values. Software security assessment tools need to do the same.

Penetration testing is similar to fault injection, but it concentrates on scanning for vulnerabilities that have been found earlier from similar systems. It is heavily based on experience and on a database of known vulnerabilities. Strong software scanning tools will be able to combine the two. By understanding the types of vulnerabilities a hacker would use to penetrate a system, the Web application scanner, by using software fault injection, creates attack profiles on the fly that will uncover actual vulnerabilities within the Web application.

Through the use of advanced, hacker-like activities, successful Web application vulnerability assessment tools will be able to assess security vulnerabilities at very high speeds, resulting in high accuracy with extremely low false positives. It's important to be able to be flexible in the vulnerability assessment because Web environments are constantly changing and dynamic.

To be complete, Web application security tools should be able to use the attack simulation mechanisms to test for policy rules compliance in addition to vulnerabilities. The product should be able to tell users that their password policies or time-out policies are working correctly. This part is often overlooked, but in today's regulatory environment, IDC believes that policy compliance is a critical component.

To determine the ability of the Web application vulnerability assessment tools to reduce false positives and conduct attack simulation, companies should consider the following:

- **Robustness of advanced fault injection techniques.** Solutions should be able to inject thousands of vulnerability strings and monitor application responses.
- **Automated and comprehensive navigation.** Products need to automatically and thoroughly navigate through detailed and lengthy Web applications, including complex session management, Java script, and deep business logic. Many Web applications contain thousands of pages, and assessment tools must reach them all.
- **Customizable product.** Ideal tools should offer policies that allow organizations to modify security assessments or a precrafted attack objects library.
- **Alarm suppression mechanism.** Tools must be able to suppress previously verified false positives.

Cenzic Hailstorm is a strong example of a product that reduces false positives, uses advanced attack simulation technology, and includes policy checks. Cenzic has incorporated all three critical characteristics into its Stateful Assessment technology. Hailstorm is able to maintain the state of an application while testing, emulate a hacker, and assess security vulnerabilities at very high speeds while remaining highly accurate. The product has a flexible analysis engine that can be customized.

Cost of False Positives

False positives add considerable "hidden costs" to a Web application scanner. In some solutions, hundreds of false positives can be generated for each application. Even if it takes just half an hour to track down and adjudicate each false positive, actual costs add up quickly. For enterprises with many applications, the cost to analyze false positives is considerable. If an enterprise assumes that a standard scanning tool produces 500 false positives in an application, handled at an average of 30 minutes, it would take 250 man-hours to process all the false positives of that report. With an average fully loaded cost of \$100 per hour, that's \$25,000 for just one application. The worst outcome associated with a wildly inaccurate (both false positives and false negatives – that is, missing vulnerabilities) product is to discard Web application testing altogether. When that happens, the actual cost will be immeasurable when a breach occurs.

Considering Cenzic

Cenzic, headquartered in Santa Clara, California, provides automated application security assessment and compliance products and services to help enterprises secure commercial and custom Web applications. The company offers next-generation enterprise software as well as software as a service (SaaS) for automating application security assessment and compliance. These products and services allow Fortune 1000 corporations, midsize corporations, and government organizations to dramatically improve the security of their Web applications. Cenzic uses a nonsignature-based approach called Stateful Assessment, which emulates a hacker and looks for real-time responses at the browser level. This approach has helped Cenzic provide a very accurate solution with less than 1% false positives.

The company provides the following products and services:

- **Cenzic Hailstorm®** enables security experts, QA professionals, and developers to work together to assess, analyze, and remediate applications for security vulnerabilities. Hailstorm benefits include reduced security risk and liability, lower development and testing costs, and faster time to market. Leveraging its unique technology, Hailstorm provides coverage over a wide variety of attacks that go beyond standard attack methods. Hailstorm is well suited to perform application logic tests, session management attacks, and regulatory compliance tests for PCI, GLBA, HIPAA, SB 1386, AB 1950, and others. Hailstorm's Stateful Assessment approach is well suited to test both commercial and custom applications.
- **Cenzic ClickToSecure®** service is a SaaS offering that combines the functionality of an enterprise-class application security assessment product with the flexibility of a managed security service. Cenzic takes its managed service seriously and takes extra steps to ensure that customers feel comfortable in outsourcing their application security testing to Cenzic. Some of these special considerations include comprehensive employee background checks, secure infrastructure with full data protection, automated tests combined with analysis from security consultants, and free retest for fixed vulnerabilities.
- **Cenzic Assessment Methodology** completes the solution with a state-of-the-art business process consulting service to help customers improve their application security methodologies. Cenzic's current focus includes financial services, eretail, healthcare, high-tech, and government sectors.

Challenges and Opportunities

To be able to reach the market potential for Web application security scanning, vendors must overcome some hurdles. The primary hurdle is to get people to invest in this technology. The need for Web application security has been established, but the method to meet that need isn't fixed. IDC believes application scanning meets many of the requirements for security in this space, but the challenge to deployment is exacerbated by the perception that these tools generate too many false positives and false negatives.

As previously mentioned, when these tools first hit the market, they were fraught with problems. The technology has improved considerably over the past half decade, but the initial perception still exists; thus, organizations are less willing to look at improved technology and products. To overcome this sticking point, vendors must demonstrate effectiveness. Cenzic is demonstrating the effectiveness of its Stateful Assessment technology by challenging organizations to compare the Cenzic offering with others. Cenzic is offering a free ClickToSecure Web service scan of an application that was previously scanned using older technology in the hopes of demonstrating to customers the improved ability to find vulnerabilities that other scanners failed to find.

Conclusion

The use of Web technology to conduct business is becoming pervasive. The ever expanding use of the Internet for business operations has alerted the threat landscape. Attackers are now more professional; they are interested in profit, not notoriety. Strong network defenses have been deployed to fend off these attackers. Therefore, they have moved down the stack to the point that they are targeting the application layer, especially the Web application layer, because it is outward facing — and a breach in this layer will get attackers directly to the data they want. IDC believes that organizations must strengthen their Web applications at the application level. The applications must be designed to limit software flaws and vulnerabilities. To do that, IDC recommends that application security scanning be part of the software development life cycle.

There is considerable variety among the products on the market. To be successful in this space, these products need to be flexible, easy to use, well integrated into a software development life cycle, and, most importantly, accurate. Without accuracy, much of the value returned by using a Web application testing solution is negated. Accuracy in the field is measured by false positives and false negatives. IDC believes that the best way for these tools to remove the "false positives" is to employ automated penetration testing technology that can attack the Web site just as an attacker would. Cenzic Hailstorm does just that with its Stateful Assessment technology. Cenzic's process-oriented technology uses software fault injection to insert thousands of vulnerability streams into a Web application to correctly identify combinations of vulnerabilities that attackers can exploit.

Organizations presently using Web application scanners, as well as companies considering the technology, should investigate Cenzic Hailstorm and Cenzic ClickToSecure.

A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com