

# A Better Way to Evaluate Large Code Sets in Today's Fast-Paced Web Environment

## **SystemExperts Corporation**

*Brad C. Johnson*

---

### **Abstract**

Web applications are being deployed at incredibly fast rates. Unfortunately, exploiting vulnerabilities in these business transaction sites has become one of the highest security risks on the Internet today. Why is that? Simply, the need for rapid development and deployment of Web based business functionality has caused many organizations to put aside their time-tested application design and development methodologies used in pre-Internet environments. The result is a high percentage of business applications being deployed on the Internet before they have been scrutinized for security related issues. This affords hackers and other determined intruders ample opportunity to access or even compromise sensitive information.

Clearly, an efficient and effective security code review methodology is needed to compensate for the control deficiencies in today's typical Web application development process.

Since 1994, SystemExperts has helped companies to address some of the most publicized hacker attacks. Additionally, we have helped some of the leading companies in the world to proactively prepare their sites to resist intrusions. The content of this paper is distilled from the extensive experiences of the author and the SystemExperts team of consultants.

### **Inside**

- Why are most Web applications insecure?
- A novel approach for security code reviews.
- What do you look for?
- Understanding how to be efficient in an inefficient process.

## **SystemExperts Corporation**

**Boston   New York   Washington D.C   Tampa  
San Francisco   Los Angeles   Sacramento**

Toll free (USA only): +1 888 749 9800

From outside USA: +1 978 440 9388

[www.systemexperts.com](http://www.systemexperts.com)   <mailto:info@systemexperts.com>

## State of Affairs

The rapid deployment of business applications in general, and web-based applications in particular, comes at the price of using these applications before they are properly tested or secured. Most development organizations have their hands full just trying to perform function, unit, and feature testing. They are often frustrated because they don't have the time to put their applications through the rigors of an assessment focused on finding and resolving security related problems.

Security, thankfully, has become an important aspect of sound business practice and most organizations understand the need to proactively review their policies, procedures, and applications to help prevent security breaches. To really understand the overall security and business risk, one needs to consider several different aspects of the environment (e.g., networks, hosts, software infrastructure, and applications). There are a variety of techniques that are commonly used to assess these areas including conducting penetration analysis, hardening and scanning hosts and networks, running exploit tools, and performing 3<sup>rd</sup> party security assessments of applications.

For any Web based application, however, there is no substitute for a hands-on review of the actual source code. The problem lies in the fact that with object-oriented code, reusable modules, outsourced development, and with the time pressures of the marketplace, these often huge code-bases are deployed without a qualified review of the key features and functions that might be subverted by a hacker to gain direct access to data or systems.

Obviously, some type of code review process is needed. While a thorough line-by-line evaluation of every line of code would be helpful, it is usually an impractical option. Unfortunately, because most organizations can't afford (both time and money) a line by line code review, they perform no code review because they are unaware of viable alternative approaches.

### What is the Problem?

The typical business application is the result of a long and complex process: architecture, design, implementation, functional testing, quality assurance testing, production deployment, ongoing maintenance, and functional enhancement. During the last ten years, we have seen the need for security-oriented code reviews of business applications increase significantly. The main reason for this is simple. The time to market competitive pressure to introduce enhanced functionality in the fast paced Web world is compressing the development cycle. As a consequence, security issues are often unrecognized or ignored or are expected to be addressed at a later time, after the application has already gone into production.

This problem is compounded by a lack of security skills. Most business application developers are hired because of their skills in design, implementation, and testing of specific programming languages – and not on writing secure code. Therefore, many of these applications have a myriad of inherent security flaws that make them vulnerable when deployed in an intranet, extranet, or Internet environment. Significant benefit can be gained by identifying these problems before the applications are released into production.

## Another Approach

Recognizing this reality, SystemExperts has developed and refined an effective and practical alternative to the unaffordable line by line code review process. By combining interactive discussions (a "Workshop") and line-by-line review of a representative sample of "important" functions (a "Review"), one can quickly and cost effectively get to the heart of not only architectural and design issues and flaws but also specific coding problems. We call this the Code Workshop & Review Methodology.

The Code Workshop & Review is a well defined process that analyzes an application's functionality (or a selected portion) for security vulnerabilities. It consists of two distinct parts: an on-site interactive review of the application design and implementation and an off-site hands-on analysis of a selected portion of code. This process generates well grounded recommendations to make the networked based application more secure and less susceptible to attack.

## Code Workshop & Review

This Code Workshop & Review Methodology minimizes the burden it places on your budget and resources. For example, when done properly there is no need to prepare detailed documentation (something that is often missing for many business applications). Usually, prior to the on-site Code Workshop, all that is required is a brief conversation between the assessment team and key development personnel to discuss a handful of basic questions related to the code earmarked for analysis.

Proper staffing of the project will maximize efficiency and ensure success. Code Workshop & Reviews are most effective when staff that is familiar with your overall application architectures, design models, and development practices participate. Similarly, the review process is most efficient when programmers who are intimately familiar with the details of the specific project application participate as well. Broad participation in the Code Workshop is essential because creating effective and secure business applications is only secondarily about the technical details of coding in C(++), Java(script), XML, or whatever language is being used. It is primarily about ensuring that the key business objectives are implemented and supported by the entire application environment.

### A Better Way

The Code Workshop & Review Methodology takes place in two phases. The first phase is a day or two of highly interactive discussions between the code designers and developers and the development/security experts. The second phase is an off-site intensive independent review of a carefully selected subset of the application's code (this second phase requires virtually no participation from the original developers).

One of the primary objectives of the on-site Workshop phase is to identify the key security related modules and functions that will require the line by line analysis. Typically, it is not necessary to go over each and every line of the application to understand its security strengths and weaknesses. However, it is vital that the most sensitive security code be properly critiqued.

Just like every organization should use host, network, and exploit scanners to programmatically review its environment for unexpected problems, organizations should also use programmatic code analysis tools to look for common programming language specific problems. This Code Workshop & Review Methodology is intended to *complement* these automated tools.

Let's take a look at those two important phases.

## Workshop (Phase 1)

The first part of the Workshop is focused on understanding the driving business requirements and functional architecture of the application. This approach allows the team to put the code in proper business context. Generally, the Workshop discussions progress from high level (e.g., what the business is trying to accomplish with the application) to low level (e.g., how the code is actually constructed and how it works). It is not uncommon for the sessions to include an interactive walk-through of some of the code.

During the remainder of the Workshop, the team delves into the actual coding practices used to support the application and identifies the exact code to be analyzed during Phase 2, the Review phase.

One frequent unexpected benefit of the Code Workshop is that the highly interactive nature of the discussions provides a forum for the sponsor's staff to better understand the ideas behind their own design and how the application may be improved. It is surprising how often we've seen clients gain fresh insight into their environment just because they needed to explain something out loud to a team of independent experts!

## Review (Phase 2)

Once the Code Workshop phase is completed, the team spends an agreed upon amount of time off-site performing a manual inspection of the selected code. Depending upon the amount of code to be reviewed, this process typically takes 1-3 weeks. During that review the team looks for common security problems and issues such as unvalidated parameters, broken access control, broken account and session management, inappropriate state management, buffer overflows, error handling problems, and insecure use of cryptography. These types of issues are often the reason why Web based applications are subverted, providing access to back-end systems and data. These weaknesses also provide intruders opportunity to steal another person's identity (i.e., identify theft), a rightfully growing concern among corporations, public entities, and consumers alike.

## What Do You Look For?

It is impossible to articulate every type of problem that a code review might look for, but shown below are some general areas and specific issues that one would typically address.

- Functional hygiene
  - Unvalidated parameters
  - Unexpected parameter values (e.g., special, ".../", local files)
  - Improper handling of function return values
  - Buffer overflows
  - Error handling
- Base security handling
  - Access control (e.g., separate from authentication)
  - Account and session management (e.g., timeouts, segregation)
  - State management
  - Insecure use of cryptography
  - Cookie entropy
  - Information leakage
  - Username and password quality
- Intrusion handling
  - Unexpected parameter value logging
  - Unexpected function-call logging
  - General events and logging (e.g., escalation, timestamps)
- Exploit handling
  - Command injection
  - Improper/unauthenticated/unauthorized (SQL) calls

## The Last Word

While IT leaders and security experts alike agree that code reviews are necessary to ensure the security of critical applications, the cost (both time and money) has discouraged most organizations from performing them. Clearly there has to be a better solution than omitting critical reviews.

To address this need, SystemExperts has developed an innovative, lightweight code review methodology, the Code Workshop & Review. By combining an organization's key designers and developers with high level independent experts (in security, networks, and development), Code Workshop & Review is not only faster and less expensive than traditional code reviews, but its holistic approach frequently identifies architectural, design, and deployment problems that a standard Code Review would not discover.

Essential to a successful outcome for the project is participation of staff that genuinely understands the business drivers and the technology underlying the application. Finally, the Code Workshop & Review Methodology is a complement to an organization's own code analysis, quality assurance testing, and programmatic assessments, rather than a replacement.

## About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Networkworld-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

*Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.*

### Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

### Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker; it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

### Intrusion Detection and Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

### Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, UNIX, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

### Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

### Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

### VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1.888.749.9800

**Boston**   **Los Angeles**   **New York**   **San Francisco**   **Tampa**   **Washington DC**   **Sacramento**  
**www.SystemExperts.com**

**info@SystemExperts.com**