

## ▼ **Armorize Technologies Releases CodeSecure™ 3.0**

**Santa Clara, January 07, 2009**

### **Web Based Appliance Provides Multi-Language Source Code Analysis and Verification**

Armorize Technologies, a leading provider of web application security solutions, has released Version 3.0 of CodeSecure™. This appliance-based solution provides Static Source Code Analysis and Verification for major web application languages through a single browser interface.

Deployed throughout development, CodeSecure™ identifies source code that leaves web applications vulnerable to attacks such as Cross Site Scripting (XSS) and SQL Injection. This proactive approach to security facilitates remediation when it is most cost-effective, and represents a risk-free alternative to the common build-first secure-later paradigm.

Building on previous releases, CodeSecure™ 3.0 now offers the following features:

- Unified web-based platform for analyzing ASP.NET, Java/J2EE, PHP and Classic ASP source code independent of build environment or IDE.
- Interactive reporting identifying vulnerable entry points, code functions handling tainted input, and the resulting exploit(s).
- Active Directory integration for ease of user/group management and project access control.
- Integration with SmartWAF™ Web Application Firewall (WAF) for immediate mitigation of code level vulnerabilities.

### **Proactive Security Solution Addresses Explosive Growth in Web Application Attacks**

Armorize CodeSecure™ offers a web-based, automated static source code analysis and verification platform for web application source code. This low-overhead solution provides a repeatable and efficient means of identifying and removing vulnerabilities during development. This results in web applications resistant to exploits that target flawed code seeking to compromise both the application itself and the end-user computers browsing to it.

Detecting vulnerabilities as the code is developed and offering guidance on remediation, CodeSecure™ ensures security flaws are identified, understood and remedied by the developers with minimal cost and impact on project progress.

### **Compiler-independent Source Code Analysis Improves Speed, Accuracy and Overhead**

CodeSecure™ is a stand-alone appliance. It does not require any integration with the build-environment or IDE but instead utilizes its own onboard parsers for ASP.NET, Java/J2EE, PHP and Classic ASP code analysis. The only requirement is to identify the location of the source code.

Through automated source code scans, CodeSecure™ forms an overall picture of the web application behavior, tracing data flow and calculating all possible outcomes of tainted input propagation through the application.

CodeSecure™ is highly accurate in identifying vulnerabilities such as Cross Site Scripting (XSS) attacks and SQL Injection that leave web applications, corporate resources and client data open to compromise.

## ▼ Armorize Technologies Releases CodeSecure™ 3.0

### **Prioritized Reports and Guidance Facilitate Efficient Remediation**

Customizable reports are accessed through the interactive web interface or can be distributed automatically in HTML, PDF or XML format. They provide a detailed trace of tainted data flow through the application identifying all code functions that the data crosses between the attack entry-point and the resulting exploit.

In addition to ranking vulnerabilities based on the overall risk they bring to the application, CodeSecure™ provides guidance and vulnerability-specific secure-coding samples to facilitate remediation. This ensures that developers and security personnel can prioritize remediation while focusing efforts at the code level.

### **Active Directory Integration Eases CodeSecure™ User Management**

Developers, managers and security personnel authenticate to CodeSecure™ based on their Active Directory Credentials. This streamlined authentication model greatly reduces account management overhead as users retain a single set of credentials.

### **Integration with SmartWAF™ Ensures Immediate Remediation**

Armorize has integrated CodeSecure™ with the SmartWAF™ Web Application Firewall (WAF) to ensure that Armorize customers can enjoy immediate “hot fix” protection while vulnerable code is rewritten.

Importing the CodeSecure™ findings, SmartWAF™ dynamically reconfigures its policies to specifically protect existing applications against exploits targeting vulnerabilities identified in the Source Code Analysis process.

### **CodeSecure™ Key Differentiators**

**Unified web-based appliance:** - Through a single web interface, CodeSecure™ offers a centralized source code analysis platform for developers, managers and security personnel supporting scanning of multiple projects across multiple platforms and programming languages (ASP.NET, Java/J2EE, PHP, Classic ASP). It is highly accurate in identifying vulnerabilities such as Cross Site Scripting (XSS) and SQL Injection.

**Ease of Deployment and Scalability:** - As a self-contained appliance accessed by web browser, CodeSecure™ features extremely fast deployment schedules with minimal software management overhead.

**Complete Automation:** - CodeSecure™ supports complete automation of policy assignment, source code retrieval, scan scheduling and report distribution ensuring prompt reaction and remediation.

**Accuracy:** - Onboard compilers and parsers allow true behavior modeling and analysis that pinpoints the specific vulnerable code statements with near-zero false positives and negatives.

**Complete Reporting:** - Reports trace all vulnerabilities from the application entry point to exploit, highlighting all functions that the data crosses. Detailed remediation guidance offers secure coding samples and prioritizes vulnerabilities based on the risk they bring to the application.

## ▼ Armorize Technologies Releases CodeSecure™ 3.0

**Active Directory Integration:** - Integration with LDAP directory services reduces the load associated with account creation and password management.

**WAF Integration:** - By Integrating with SmartWAF™, CodeSecure™ ensures that existing applications with vulnerable code can be protected while the root vulnerabilities are addressed.

### **About Armorize**

Armorize Technologies is a leading provider of web application security solutions. From static source code analysis with CodeSecure™, to real-time web application protection with SmartWAF™ and malware injection monitoring and detection with HackAlert™, the Armorize award-winning solution suite provides security at key points in the web application lifecycle.

With deep roots in academia, the Armorize team won two consecutive awards at the prestigious 2003 and 2004 International World Wide Web Conferences. Subsequent recognition for innovative technology and business practices since founding include winning the Red Herring Asia 100 award and being invited to present at the Dow Jones Venture Wire Technology Showcase 2008.

With its headquarters in Santa Clara, CA, and its R&D center in the Nan Kang Software Park in Taipei, Taiwan, Armorize has a global customer base with clients from among finance, telecom, government and technology sector leaders.

For more information, visit <http://www.armorize.com>

Armorize Technologies Inc.

Phone: +1-408-216-7893 ext 401

Email: [pr@armorize.com](mailto:pr@armorize.com) [sales@armorize.com](mailto:sales@armorize.com)

Armorize Technologies, Inc. 2009.