

VERACODE

PRESS RELEASE

Highlights

VERAFIED is the industry's first standards-based mark of security quality for both internally developed and third-party software applications. By leveraging industry standards, Veracode provides a pragmatic and repeatable method for organizations developing or procuring software to measure, compare and reduce risks related to application security.

Veracode uses static binary analysis, dynamic analysis and/or manual penetration testing to identify security flaws in software applications. The basis for the VERAIFIED security mark is the Security Quality Score (SQS) which aggregates the severities of all security flaws found during the assessment and normalizes the results to a scale of 0 to 100. Applications found to have no "very high", "high" or "medium" severity vulnerabilities, nor any OWASP Top 10 or CWE/SANS Top 25 vulnerabilities that could be discovered using Veracode's automated analysis may earn the VERAIFIED mark. For applications of the highest criticality the VERAIFIED HIGH ASSURANCE marks for CWE/SANS 25 or for OWASP Top 10 indicate the software has been found to have no "very high", "high", or "medium" severity vulnerabilities, nor any CWE/SANS TOP 25 or OWASP TOP 10 vulnerabilities that could be discovered using Veracode's automated static binary analysis, automated dynamic web application analysis (if applicable) and additional manual application penetration testing to identify flaws in business logic and design.



Veracode announces VERAIFIED High Assurance Mark for Web Applications

New Mark Indicates Software Has Been Independently Assessed for OWASP Top 10 Vulnerabilities

Burlington, Mass. – August 10, 2010 – Veracode, Inc., the world's leader in cloud-based application risk management, today unveiled a new VERAIFIED™ mark of security quality that indicates an application has been independently assessed and found to have no "very high," "high" or "medium" severity vulnerabilities as defined by MITRE, nor any of the top 10 vulnerabilities as defined by the Open Web Application Security Project (OWASP Top 10). The independent high assurance assessment is performed with SecurityReview®, Veracode's patented cloud-based automated security verification service, and complemented by manual penetration testing by Veracode or its partners to identify flaws in business logic and design. Veracode inspects application code at the same level that it is attacked – the binaries.

According to the OWASP Foundation, "The OWASP Foundation is pleased to see Veracode using the OWASP Top 10 application security risks. Managing application security requires real visibility into exactly what has been verified and what has not. Veracode's transparency around its combination of manual and automated verification techniques stands in stark contrast to those product vendors that wrongly and dangerously assert complete automated coverage and compliance with the Top 10."

Software providers whose applications earn the VERAIFIED mark may display it as an indicator to customers that independent automated and manual testing did not detect the list of known, dangerous vulnerabilities and demonstrates the software is in successful compliance with the PCI Data Security Standard as well as other software assurance policies based on the OWASP Top 10. Additionally, the application may be identified with a VERAIFIED High Assurance mark in Veracode's VERAIFIED Software Directory. CIOs, CISOs and others who acquire software may also use the mark as a threshold for independently verified security quality delivered by commercial, outsourced or n source suppliers.

To earn the VERAIFIED High Assurance mark for the OWASP Top 10, software providers submit their final integrated application – binary or bytecode – to Veracode SecurityReview for assessment. The application is analyzed by Veracode's patented cloud-based automated security verification service and then subjected to additional manual penetration testing by Veracode or a security consultant in Veracode's growing partner ecosystem. Following the remediation of any vulnerabilities of severity medium or higher, as defined by FIRST's CVSS vulnerability scoring system, and any vulnerabilities identified in the OWASP Top 10, the application is then resubmitted to Veracode for complete security regression testing and verification. Given the ad hoc approach to security testing adopted by most organizations today, this

The OWASP Top 10

represents a broad consensus on the most critical web application security flaws. The errors on this list occur frequently in web applications, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

Although Veracode SecurityReview detects hundreds of software security flaws, we provide a razor focus on finding the problems that are "worth fixing". The OWASP Top 10 is a list of flaws so prevalent and severe that no web application should be delivered to customers without some evidence that the software does not contain these errors.



Veracode, Inc.
4 Van de Graaff Drive
Burlington, MA 01803

Tel +1.781.425.6040
Fax +1.781.425.6039

www.veracode.com

© 2010 Veracode, Inc.
All rights reserved.

SFS/ISR/2010

consistent and repeatable framework and process enables software suppliers to differentiate applications that are VERAFIED for OWASP Top 10 compliance and display the mark of independent verification.

"As web applications increasingly connect organizations to a network of their customers, partners and other stakeholders, malicious attacks have been on the rise and hackers have turned to web applications, which often represent a weak link in enterprise security," said Matt Moynahan, CEO of Veracode. "Displaying the VERAFIED mark for the OWASP Top 10 indicates an organization is serious about securing their applications deployed in SaaS, PaaS and other cloud-based environments, and should be recognized by potential customers and partners for their efforts in managing their application-related security risk."

To learn more about the OWASP Top 10, visit <http://www.owasp.org> or <http://tinyurl.com/Veracode-OWASP-Top-10>. OWASP does not endorse or recommend any company, product or service.

VERAFIED Security Mark for the OWASP Top 10

The table below identifies technical flaws found through automated analysis used to achieve the VERAFIED security mark and the additional coverage provided through manual penetration testing to detect business logic and design errors to achieve the VERAFIED HIGH ASSURANCE security mark for the 2010 OWASP Top 10.

Rank	OWASP Top 10 OWASP urges all companies to be aware of these concerns within their organization and start the process of ensuring that their web applications do not contain these flaws.	VERAFIED	VERAFIED HIGH ASSURANCE OWASP 10
A1	Injection	X	X
A2	Cross Site Scripting (XSS)	X	X
A3	Broken Authentication and Session Management	X	X
A4	Insecure Direct Object References		X
A5	Cross Site Request Forgery (CSRF)		X
A6	Security Misconfiguration	X	X
A7	Insecure Cryptographic Storage	X	X
A8	Failure to Restrict URL Access		X
A9	Insufficient Transport Layer Protection	X	X
A10	Unvalidated Redirects and Forwards	X	X

About Veracode

Veracode is the world's leader in cloud-based application risk management. With patented binary code analysis, dynamic Web assessments and developer e-learning, Veracode SecurityReview® is the most accurate and cost-effective way to independently verify application security in both internally developed applications and third-party software without requiring source code or expensive tools. Veracode provides the most simple, complete way to implement security best practices, reduce operational cost and comply with internal security policies or external standards such as OWASP Top 10, CWE/SANS Top 25 and PCI. Veracode works with global organizations across multiple vertical industries including Barclays PLC, California Public Employees' Retirement System (CalPERS), Computershare and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, follow on Twitter: @Veracode or read the ZeroDay Labs blog.

Copyright © 2010 Veracode, Inc. All Rights Reserved. All other brand names, product names, or trademarks belong to their respective holders.

Media Contact:

Liz Campbell
fama PR
phone: +1 617-758-4178
email: veracode@famapr.com