



**FOR IMMEDIATE RELEASE**

**Contact:**

Dawn van Hoegaerden  
WhiteHat Security  
408-492-1817 ext.14  
dawn@whitehatsec.com

Rachel Miller  
SHIFT Communications  
617-681-1256  
rmiller@shiftcomm.com

**WhiteHat Security Releases Web Application Security Risk Report  
Identifying the Top Vulnerabilities**

*First-of-its-Kind List Provides Enterprises with Actionable Information to Raise  
Awareness of Web Application Threats*

**SANTA CLARA, CA.—November 15, 2006**—WhiteHat Security, Inc., a leading provider of Web application security services, today announced the availability of its inaugural Web Application Security Risk Report. The report, which offers a high-level view of vulnerabilities affecting enterprise Websites, focuses primarily on e-commerce, financial services, healthcare and high-tech sites and explains the percentage likelihood of vulnerability classes existing within these sites. This first-of-its-kind report will be published quarterly beginning in January 2007.

kdemella 11/15/06 8:59 AM  
Formatted: Font:Bold

Web applications have quickly become the top target for malicious attacks. WhiteHat research reveals that eight out of ten Websites have serious flaws, including Cross-Site Scripting and SQL Injection, making them susceptible to criminals looking to cash in on cyber crime. Common business logic flaws, such as insufficient authorization, that are often undetected but can lead to customer account compromise, top the list as well.

As Web application vulnerabilities are among the fastest growing and most serious threats, enterprises turn to WhiteHat Security's Sentinel service for continuous and comprehensive Web application assessments. It is the assessment of hundreds of real-world Websites each month that affords WhiteHat a unique and current perspective into custom Web applications and vulnerability trends. As the only company with access to timely, cumulative Web application security data, sharing its findings will enable enterprises to gain a clearer picture of the security issues affecting their Websites today. This data will also help companies realize the possible business impact of these attacks and how to prevent them from occurring.

WhiteHat Security uses the Web Application Security Consortium (WASC) threat Classification of 24 Web application vulnerability classes as a baseline for classifying vulnerabilities. This standard ensures comprehensive coverage of the known types of Web application vulnerabilities. Unlike other methods of common vulnerability assessments in commercial and open source software, the WhiteHat data is compiled and aggregated into a database of previously unknown vulnerabilities in custom Web applications, keeping WhiteHat on the forefront of the latest vulnerability trends.

“We are excited to be able to offer this insight into the growing issue of Web application security,” said Jeremiah Grossman, Founder and Chief Technology Officer of WhiteHat Security. “We expect these quarterly reports to shed light on prevalent vulnerabilities and help enterprises combat them efficiently. Through this type of industry awareness we expect to see a decrease in the number and severity of vulnerabilities across the board, especially among businesses which take a proactive approach to protecting their Websites.”

**About WhiteHat Security, Inc.**

Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of web application security services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company’s flagship service, provides continuous vulnerability assessment and management for web applications. For more information about WhiteHat Security, please visit our website, [www.whitehatsec.com](http://www.whitehatsec.com).

###