FOR IMMEDIATE RELEASE

Media Contact: Ronald W. Holm
Phone: (651) 269-8863
holmr@webscurity.com

130 Million Reasons Why You Need a WAF

Are you one SQL injection attack away from becoming the next big headline?

Minneapolis, MN – August 25, 2009 – Last week's disclosure that an SQL injection attack led to the theft of 130,000,000 credit and debit card numbers from Heartland Payment Systems and other retailers provides stunning evidence of the need for improved Web application security measures. We would expect that these companies, like most institutions, believed (or were advised) their current perimeter firewalls, authentication, and encryption provided adequate protection and included protection for their Web applications.

If you have any doubts about your Web application security, you might do as hundreds of others have done in the last few months: take a few minutes to download webApp**.secure**™ LiveCD, a self-contained ISO image that can boot as a physical or virtual machine. When inserted between your current security solutions and your Web-enabled applications, it passively monitors all website traffic. All attempted breaches - including SQL Injection attacks - that pass through your existing defenses are reported. You will know when the attacks occurred, what type they were, and where they came from. The 6MB image is free, works in almost all environments, and requires little time to implement. To download, please visit http://www.webscurity.com/livecd.htm.

Although SQL injection attacks have been around for a decade, this latest example proves how difficult it is to reliably safeguard against them during the development process alone. Additional measures are required to ensure programming oversights, mistakes, and mishaps don't become vehicles for high-profile security breaches.

"Since 2001, we have been witness to countless applications written without security in mind," says Wayne Ziebarth, webScurity President and CTO. "Invariably, most are susceptible to SQL injection attacks, providing an opportunity for malicious users to bypass authentication, gain access to confidential information, elevate privileges, and generally manipulate the application into functioning in any number of ways that were not intended."

webScurity was founded in 2001 as a privately-held, Web application firewall publisher based in the Twin Cities. Its client list includes financial institutions, higher education, State of Minnesota, private and public sector organizations, hosting firms, Web developers and UTM manufacturers. webApp**.secure** has been protecting websites and applications since 2002.

###