FOR IMMEDIATE RELEASE

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

# Citigroup's Breach Was Easily Preventable
## *How webApp.secure would have protected personal data of 218,000 customers*

**Minneapolis, MN – June 21, 2011** – The recent Citigroup security breach that resulted in the theft of personal data from over 200,000 customers would have been prevented by webApp**.secure™** Professional Edition. Its unique protection capabilities would have blocked all attempts by the hackers to gain access to other accounts by altering URL query string parameter values.

At its core, webApp**.secure** PE was designed to track HTTP/HTML elements that are pushed out to the browser, ensuring they return unaltered. This includes not only URL query string parameter name/value pairs, but also cookies, hidden fields, option lists, checkboxes, radio buttons, and input field lengths. Even the most vulnerable Web applications containing common programming errors like the Citigroup site cannot be exploited when protected by webApp**.secure**.

It is important to note that Web application firewalls (WAF) operating in transparent or in-line mode are not capable of preventing this type of attack. Without the ability to modify the HTTP stream sent to the browser, it would be impossible to recognize the URI that should have been "/app/myaccount.jsp?acct=12345" had been changed to "/app/myaccount.jsp?acct=22345" in the browser address bar. While both are valid from an overall system perspective, each should only be used by their respective authorized users. Some mechanism is needed to identify a URI valid in one context is not valid in another.

The Citigroup breach shattered three widely-held myths:

1. Programmers don't make these kinds of obvious errors
2. Any WAF can mitigate URL Query String Parameter Tampering attacks
3. Authenticated users are not hackers

To find out if webApp**.secure** PE is right for you, or if you simply want to gain detailed insight into the kind of traffic aimed at your website, please take a few minutes to download webApp**.secure** LiveCD, a self-contained ISO image that can be booted as a physical or virtual machine. This provides a no-cost, low-risk opportunity to experience how easy it can be to protect your Web assets. The 6MB ISO image can be downloaded at http://www.webscurity.com/livecd.htm.

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.

### ###