



Newsletters Subscriptions Forums Safari Store Career Media Kit About Us Contact Search Home

FOUR HUNDRED Stuff
Hardware, Software & Services

Volume 11, Number 6 -- February 15, 2011

App Security Vendor Addresses XSRF Attacks

Published: February 15, 2011

by **Alex Woodie**

A Web application security company called [Mykonos Software](#) claims to have found an automated way to stop cross-site request forgery (XSRF) attack in their tracks. The new XSRF-fighting technology is included in the latest release of the company's security appliance, which focuses on detecting attacks on Web applications and stopping them in real time.

XSRF is a Web application vulnerability that allows hackers to trick victims' Web browsers into unknowingly performing actions, such as logging onto a bank account or a initiating a trade in a brokerage account. The XSRF attacker takes advantage of the trust that a bank or brokerage website has for its users, and the fact that the victim's Web browser stores cookies that automate the log-in process.

The XSRF attack is initiated when a hacker gets a victim to unknowingly consume a malicious piece of code, often an HTML image file, or a segment of JavaScript, that's downloaded to the victim's Web browser from an Internet forum or other interactive website open to the public. This malicious code can be used to instruct the victim's Web browser to request an action against the website associated with a cookie. The XSRF is often called a "one-click" attack, and is often exploited alongside cross-site scripting (XSS) vulnerabilities.

The XSRF attack mechanism was first documented more than 20 years ago, but it can be difficult to detect, and leave users and their trusted websites wondering which party was the source of fraudulent transactions. While it's not particularly difficult to block, some high-profile e-commerce companies have nevertheless succumbed to XSRF attacks, including [Google](#), whose Gmail service was hacked in 2007 through the XSRF vulnerability, and [NetFlix](#), which was subjected to an XSRF attack that resulted in changes to users' movie rental queues.

Recently, XSRF has been climbing out of the shadow of the XSS vulnerability and developing a nasty reputation of its own. The [Open Web Application Security Project](#) listed XSRF as the number five threat to Web application security in [last year's top 10 list](#). And according to David Koretz, president and CEO of Mykonos, the Department of Homeland Security has rated XSRF as more severe threat than most buffer overflows, "because there is no limit to its potential impact."

One surefire way to secure against the XSRF vulnerability is to make sure that Web developers architect and build their applications correctly, with all the proper checks and balances. (Of course, this is the same piece of advice that developers are given to avoid every other Web security vulnerability in the known universe, and you can see how far that's gotten us?)

Instead of relying solely on solid development techniques from the outset, practitioners of good security practices increase their odds of surviving the Web's rough seas by installing secondary security check points. Whereas firewalls and intrusion-prevention systems (IPS) concentrate on network-level protocols, devices such as the Mykonos Security Appliance look at what's going on with the application layer, which is where the majority of hacking is occurring.

Last week, Mykonos announced that it has added new XSRF detection routines to its appliance. The Burlingame, California, company says its appliance automatically eliminates XSRF as an attack vendor for customers who use it. "This is another major milestone for Mykonos," Koretz says.

Mykonos claims its appliance is superior to other devices by the way it actively participates with Web activity, and how it analyzes hackers to determine their skill levels following the detection of an attack. The vendor says its software tracks hackers over time, and creates tailored defenses designed to thwart the hacker and his techniques.

THIS ISSUE SPONSORED BY:

Software Engineering of America
Help/Systems
ASNA
Linoma Software
Shield Advanced Solutions



Printer Friendly Version

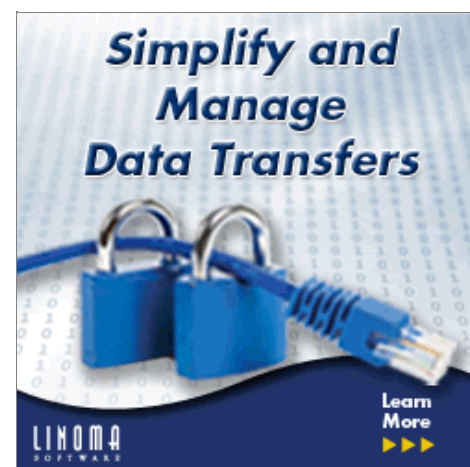


TABLE OF CONTENTS

TPS Delivers IBM i Version of MFT Solution

Hubspan Automates B2B from the Cloud

Linoma Adds Enterprise Features to MFT Offering

App Security Vendor Addresses XSRF Attacks

TrendMicro Claims Full Coverage of 64-Bit Domino with ScanMail

News Briefs and Product Shorts:

Vision Re-Brands HA Portfolio Under 'Availability' Moniker . . . Aldon Rolls Out Windows Version of Agile ALM Tool . . . Open Source COBOL-IT Tools to be Distributed by Speedware . . . Paessler Updates Network Monitor . . . FIS Sells Missouri Bank and Trust on IBM i Solution . . .

Four Hundred Stuff

RSS

There is still much to be desired when it comes to Web application security. According to a recent report from the [Ponemon Institute](#), the majority of organizations spend more time on coffee than securing Web applications.



[Post this story to del.icio.us](#)



[Post this story to Digg](#)



[Post this story to Slashdot](#)

Sponsored By
LINOMA SOFTWARE

Secure File Transfers and Encryption Solutions - GoAnywhere Suite

GoAnywhere Director is a [secure file transfer](#) solution with features to support the most demanding environments. GoAnywhere Director streamlines and secures the exchange of data with your customers, trading partners and servers. It allows your organization to consolidate all of its data transmission and processing needs under one solution with a single point of control and administration. With GoAnywhere Director, clients are saving significant time and money by eliminating the custom programming and manual steps traditionally required for moving data.

Key Benefits include:

- Simplifies and automates FTP processes
- Connects to secure FTP servers (SFTP and FTPS) for protected communication
- Encrypts and decrypts files using Open PGP encryption standard
- Compresses and decompresses files using ZIP, GZIP, and TAR standards
- Translates data to/from database tables, Excel, XML, Delimited text, and Fixed Width file formats
- Provides a comprehensive built-in scheduler
- Produces complete logging reports
- Includes integrated Key Management tools

GoAnywhere Director can be installed onto IBM System i, IBM System p (AIX), IBM System z (Mainframe), Windows, Linux, UNIX, HP-UX, Mac OS and Solaris platforms.

GoAnywhere Services is a [secure file server](#) that allows trading partners (both internal and external) to securely connect to your system and exchange files within a fully managed and audited solution. Popular file transfer and encryption standards are supported without the need for proprietary client software.

Key Benefits include:

- Installs onto most platforms including Windows, Linux, IBM i, AIX, UNIX and Solaris
- Provides an intuitive browser-based interface for remote administration and monitoring
- Includes trading partner account management with permission controls
- Supports standard transfer protocols of FTP, SFTP, FTPS, HTTP and HTTPS
- Secures transmissions with SSL/TLS or SSH encryption
- Automatically processes files based on user-defined trigger events
- Provides an optional web client for browser-based file transfers
- Generates detailed audit logs and alert messages
- When integrated with **GoAnywhere Gateway** ([Reverse Proxy Server](#) for the DMZ), no sensitive information (files, users, passwords, certificates, etc) is stored in the DMZ and no inbound ports need to be opened into the private (internal) network.

To download a free trial of the **GoAnywhere Suite** visit:
www.GoAnywhereMFT.com

Editor: Alex Woodie

Contributing Editors: Dan Burger, Timothy Prickett Morgan

Publisher and Advertising Director: Jenny Thomas

Advertising Sales Representative: Kim Reed

Contact the Editors: To contact anyone on the IT Jungle Team
Go to [our contacts page and send us a message](#).

Sponsored Links

Help/Systems: [Robot/SAVE, complete backup and recovery for the i. FREE Webinar. Feb. 17](#)

BACK ISSUES

Live Online Training for IBM i

Upcoming Classes

RPG IV Programming 5-Day Workshop
Control Language Programming 5-Day Workshop
System Operations 3-Day Workshop
Expanded System Operations 5-Day Workshop
System Administration 5-Day Workshop
COBOL Programming 5-Day Workshop
Security Management 4-Day Workshop

400school.com

[eEye Network Security](#)

Corp. Vulnerability & Compliance.
Free Demo & Trial. Download Now!
www.eEye.com/Network-Security

[Database Security Guide](#)

Practical Guide to Database Security & Compliance. Free Copy!
www.mcafee.com

[Ethical Hacking Training](#)

Learn how to find holes in your network before the bad guys do.
InfoSecInstitute.com

[FISMA Compliance Guide](#)

Agentless Scanning for FISMA and FDCC Policy Compliance.
www.ncircle.com/FISMACompliance

[Data Security](#)

New Technologies from Oracle. Learn More. Free Download.
www.quberasolutions.com

[Dns Cache Poisoning](#)