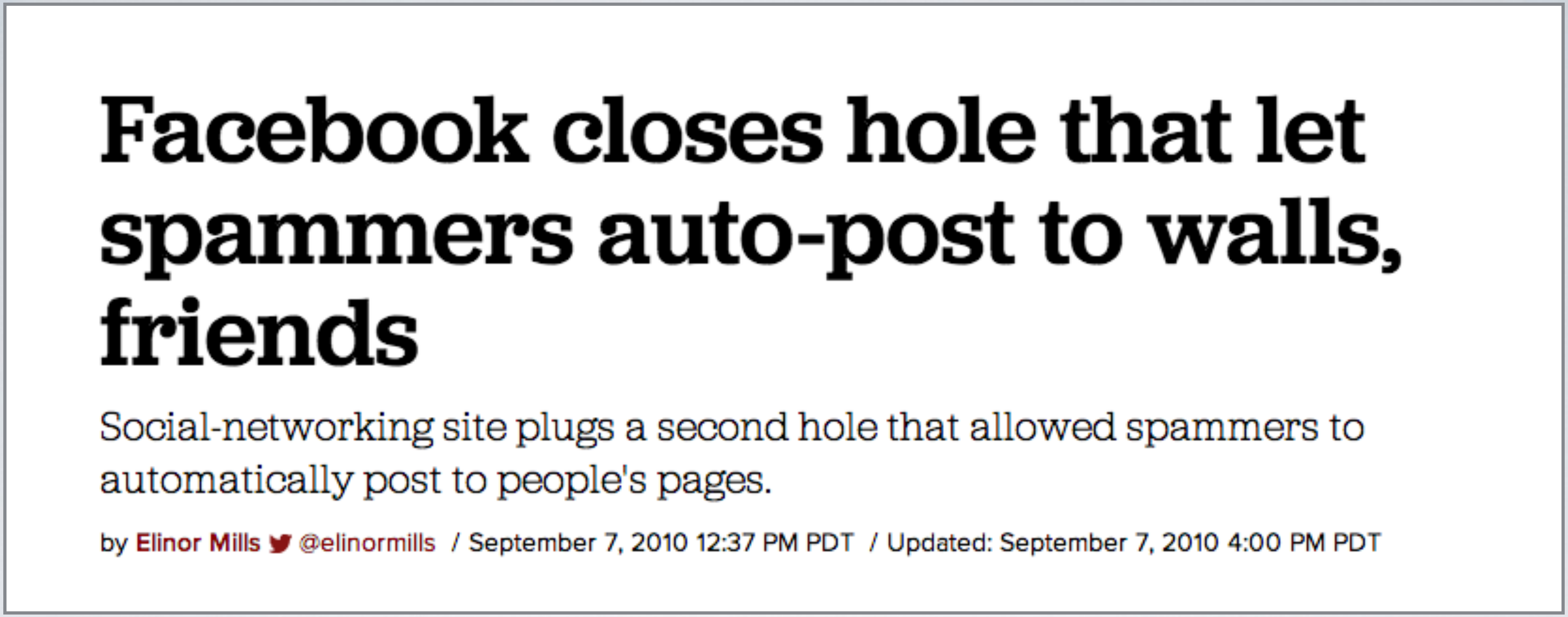
Web Security : The Big Picture

Thierry Sans

Securing the web architecture means securing ...

- The network
- The operating system
- The web server (*Apache* for instance)
- The administration server (*SSH* for instance)
- The database (*Oracle* for instance)
- The web application

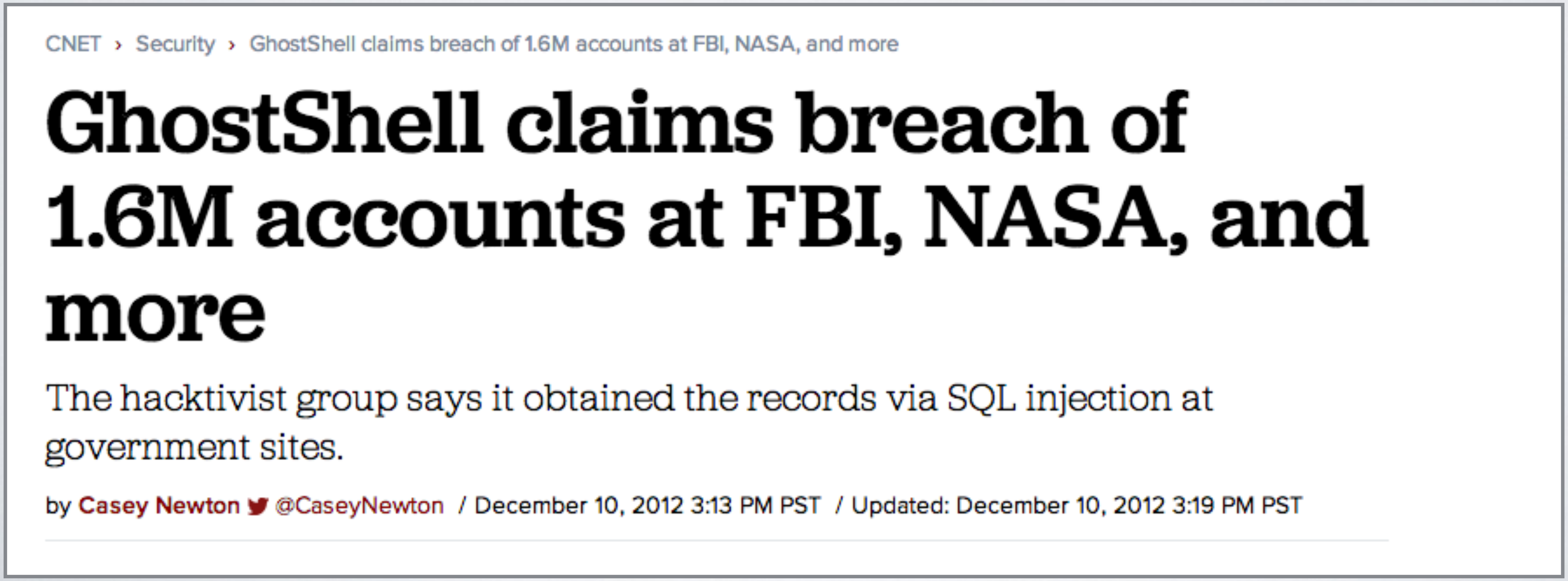
Our focus here!



Facebook closes hole that let spammers auto-post to walls, friends

Social-networking site plugs a second hole that allowed spammers to automatically post to people's pages.

by Elinor Mills @elinormills / September 7, 2010 12:37 PM PDT / Updated: September 7, 2010 4:00 PM PDT

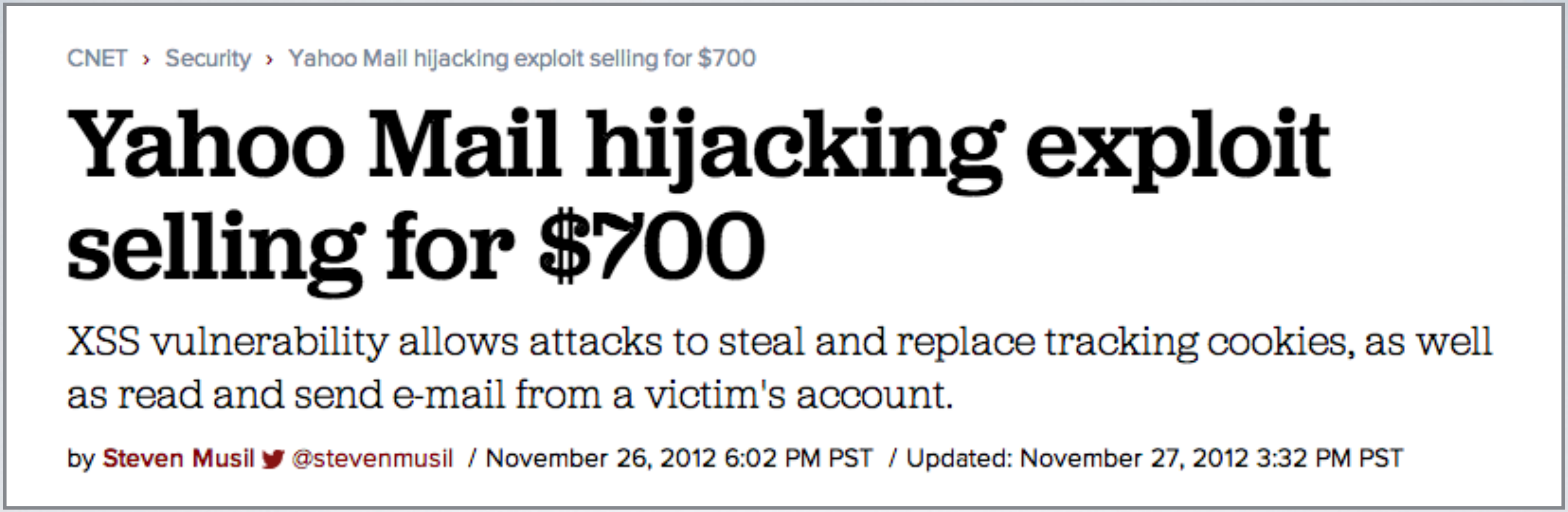


CNET › Security › GhostShell claims breach of 1.6M accounts at FBI, NASA, and more

GhostShell claims breach of 1.6M accounts at FBI, NASA, and more

The hacktivist group says it obtained the records via SQL injection at government sites.

by Casey Newton @CaseyNewton / December 10, 2012 3:13 PM PST / Updated: December 10, 2012 3:19 PM PST

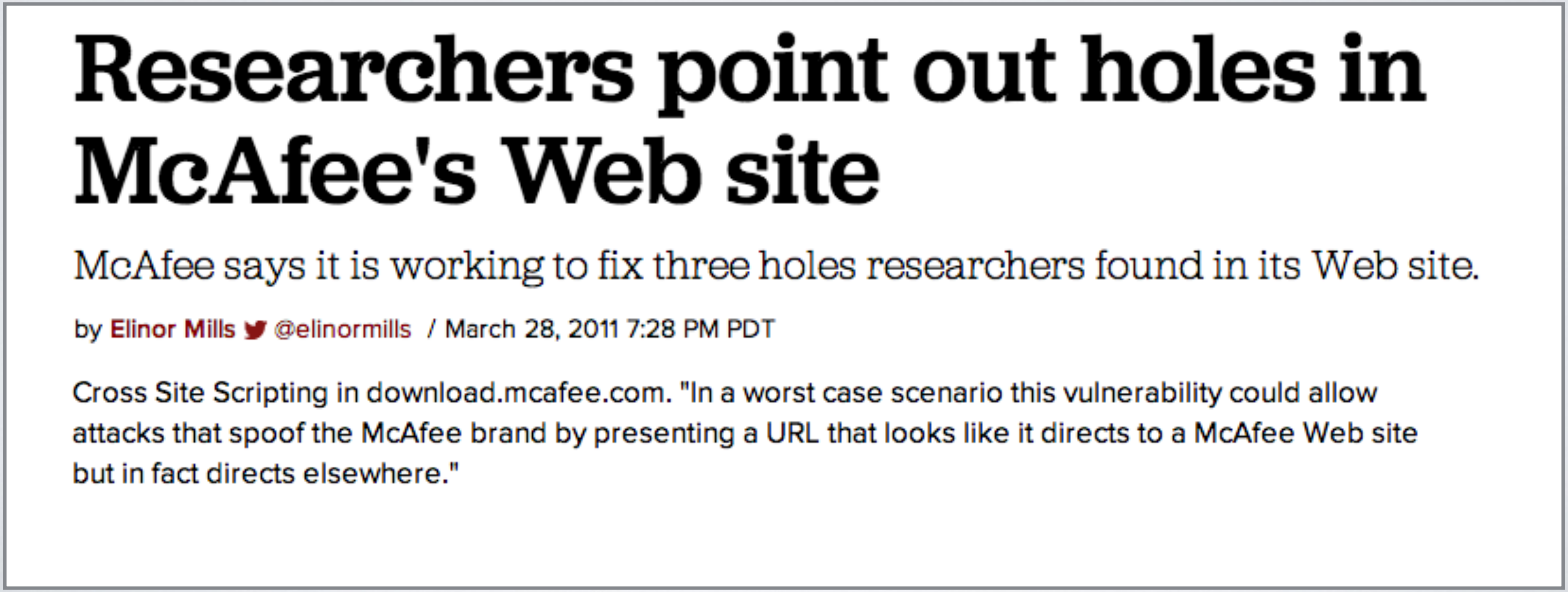


CNET › Security › Yahoo Mail hijacking exploit selling for $700

Yahoo Mail hijacking exploit selling for $700

XSS vulnerability allows attacks to steal and replace tracking cookies, as well as read and send e-mail from a victim's account.

by **Steven Musil** @stevenmusil / November 26, 2012 6:02 PM PST / Updated: November 27, 2012 3:32 PM PST

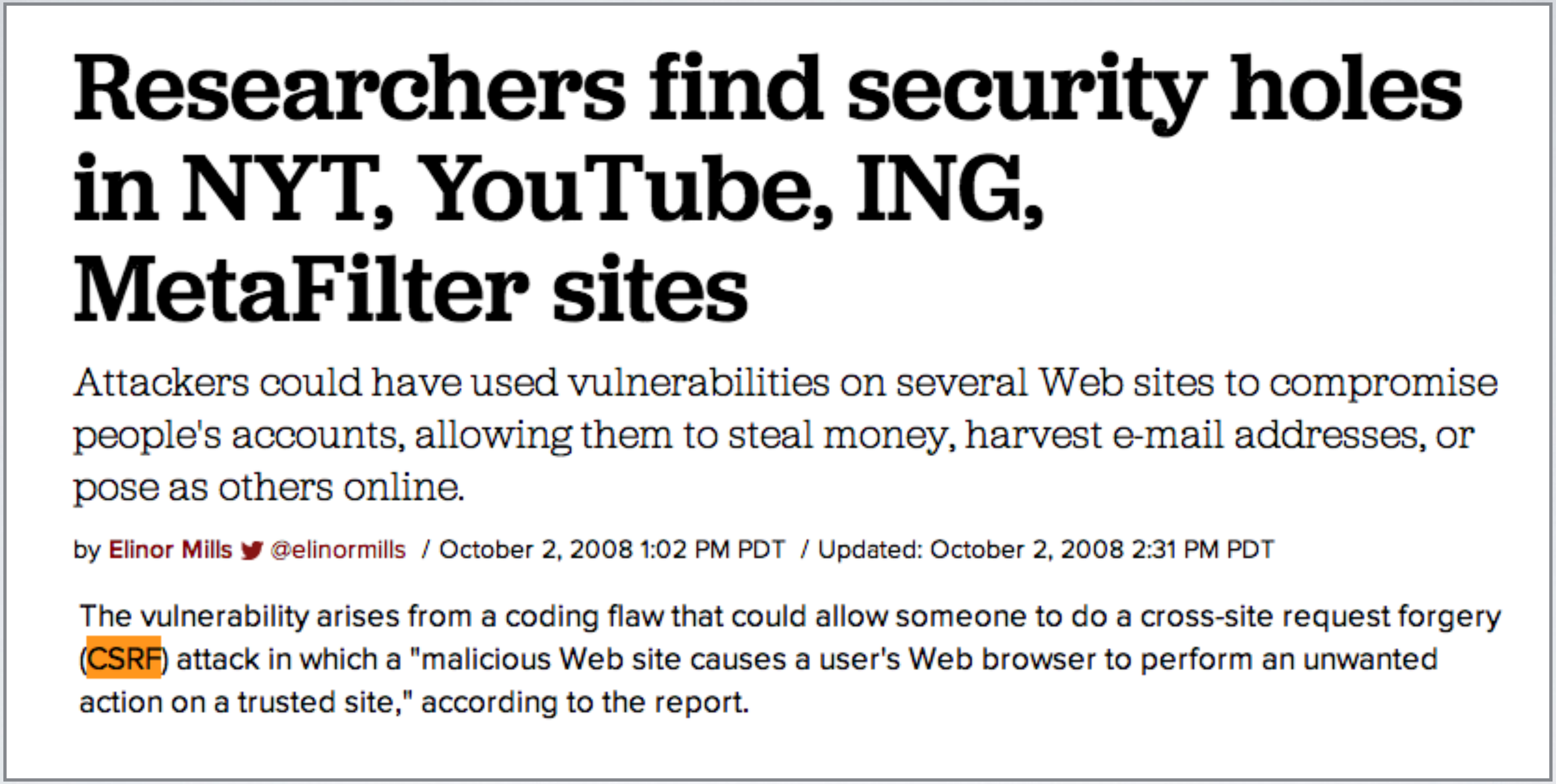


Researchers point out holes in McAfee's Web site

McAfee says it is working to fix three holes researchers found in its Web site.

by **Elinor Mills** @elinormills / March 28, 2011 7:28 PM PDT

Cross Site Scripting in download.mcafee.com. "In a worst case scenario this vulnerability could allow attacks that spoof the McAfee brand by presenting a URL that looks like it directs to a McAfee Web site but in fact directs elsewhere."

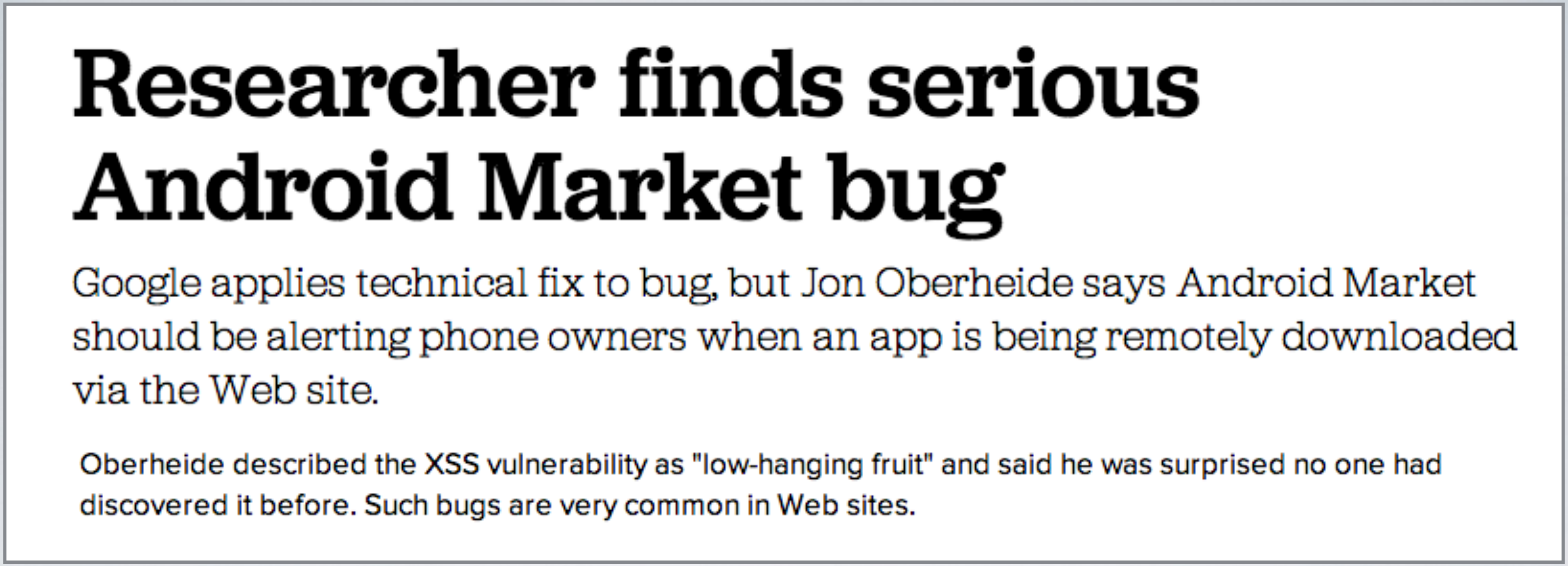


Researchers find security holes in NYT, YouTube, ING, MetaFilter sites

Attackers could have used vulnerabilities on several Web sites to compromise people's accounts, allowing them to steal money, harvest e-mail addresses, or pose as others online.

by Elinor Mills @elinormills / October 2, 2008 1:02 PM PDT / Updated: October 2, 2008 2:31 PM PDT

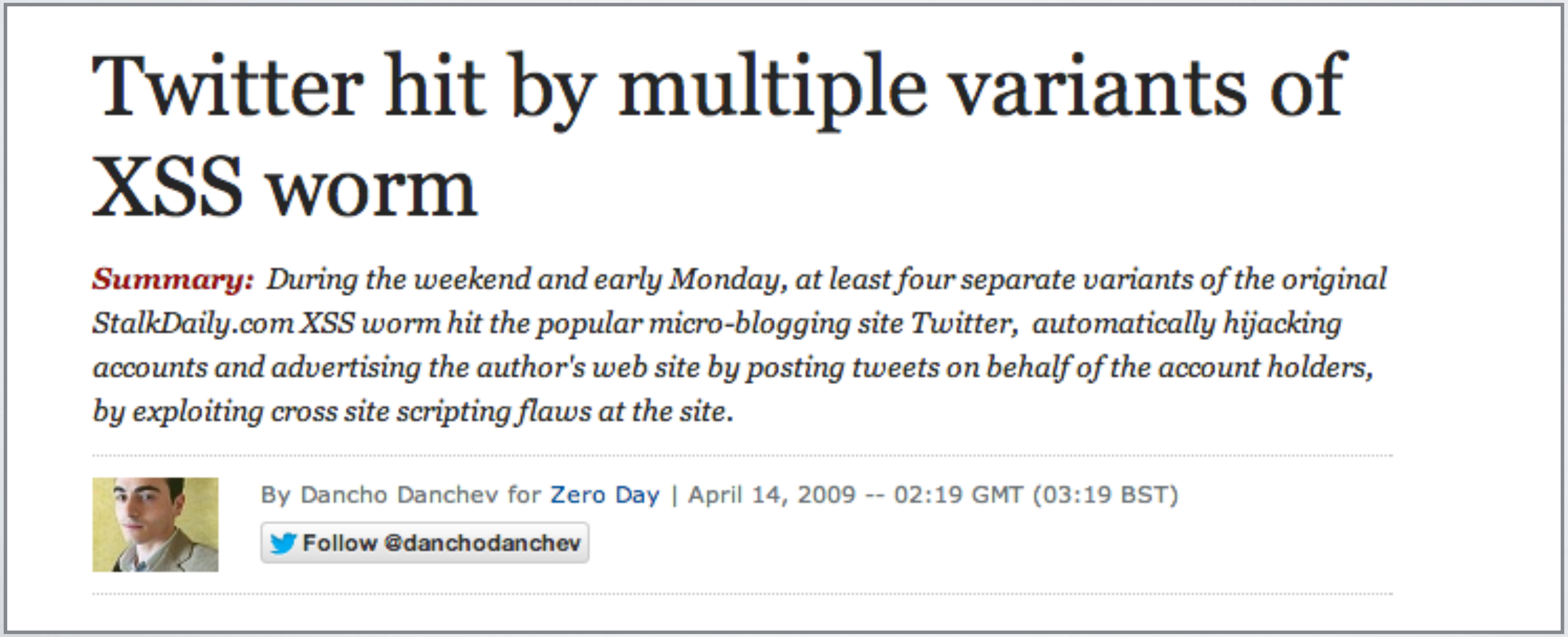
The vulnerability arises from a coding flaw that could allow someone to do a cross-site request forgery (CSRF) attack in which a "malicious Web site causes a user's Web browser to perform an unwanted action on a trusted site," according to the report.



Researcher finds serious Android Market bug

Google applies technical fix to bug, but Jon Oberheide says Android Market should be alerting phone owners when an app is being remotely downloaded via the Web site.

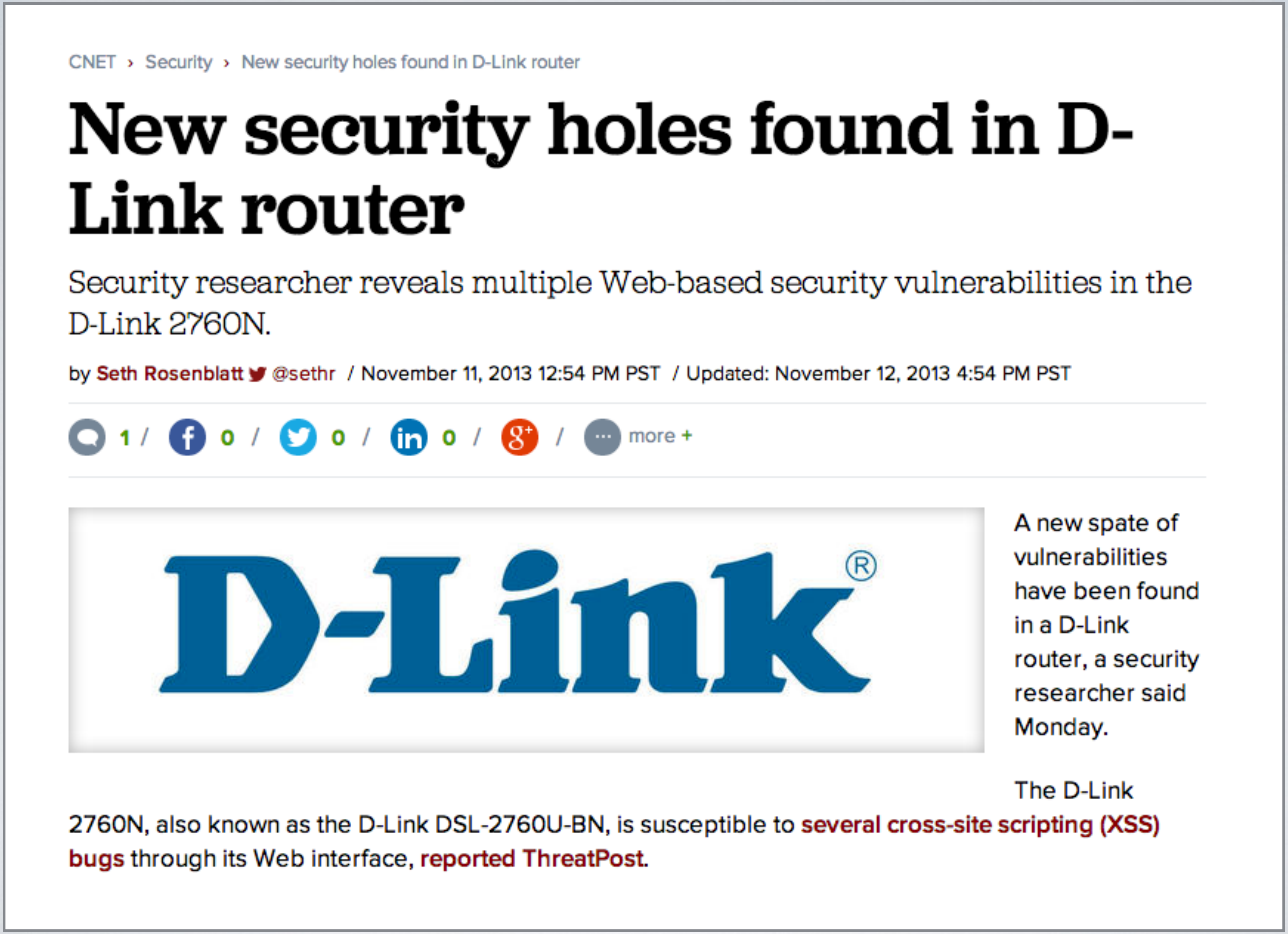
Oberheide described the XSS vulnerability as "low-hanging fruit" and said he was surprised no one had discovered it before. Such bugs are very common in Web sites.



Twitter hit by multiple variants of XSS worm

Summary: *During the weekend and early Monday, at least four separate variants of the original StalkDaily.com XSS worm hit the popular micro-blogging site Twitter, automatically hijacking accounts and advertising the author's web site by posting tweets on behalf of the account holders, by exploiting cross site scripting flaws at the site.*

By Dancho Danchev for Zero Day | April 14, 2009 -- 02:19 GMT (03:19 BST)



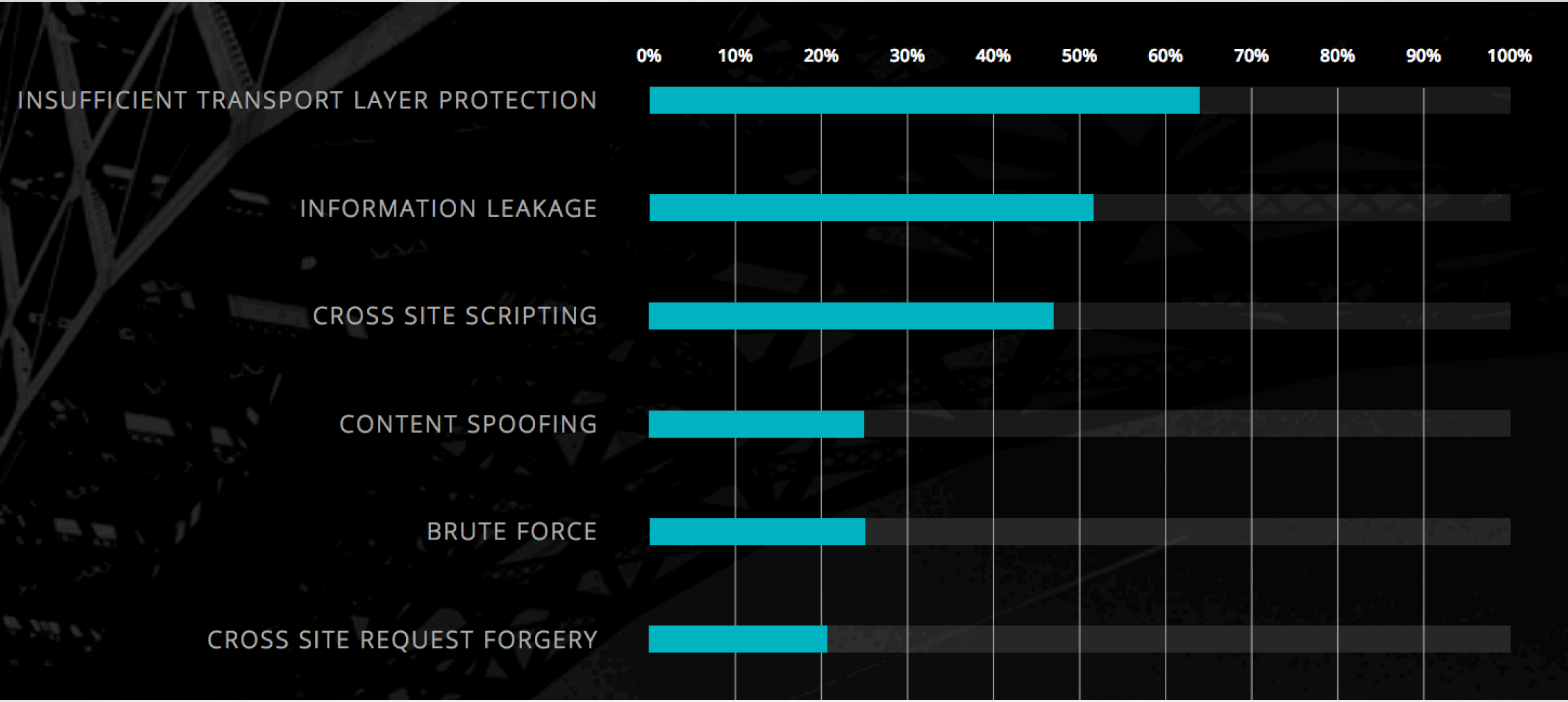
New security holes found in D-Link router

Security researcher reveals multiple Web-based security vulnerabilities in the D-Link 2760N.

by Seth Rosenblatt @sethr / November 11, 2013 12:54 PM PST / Updated: November 12, 2013 4:54 PM PST

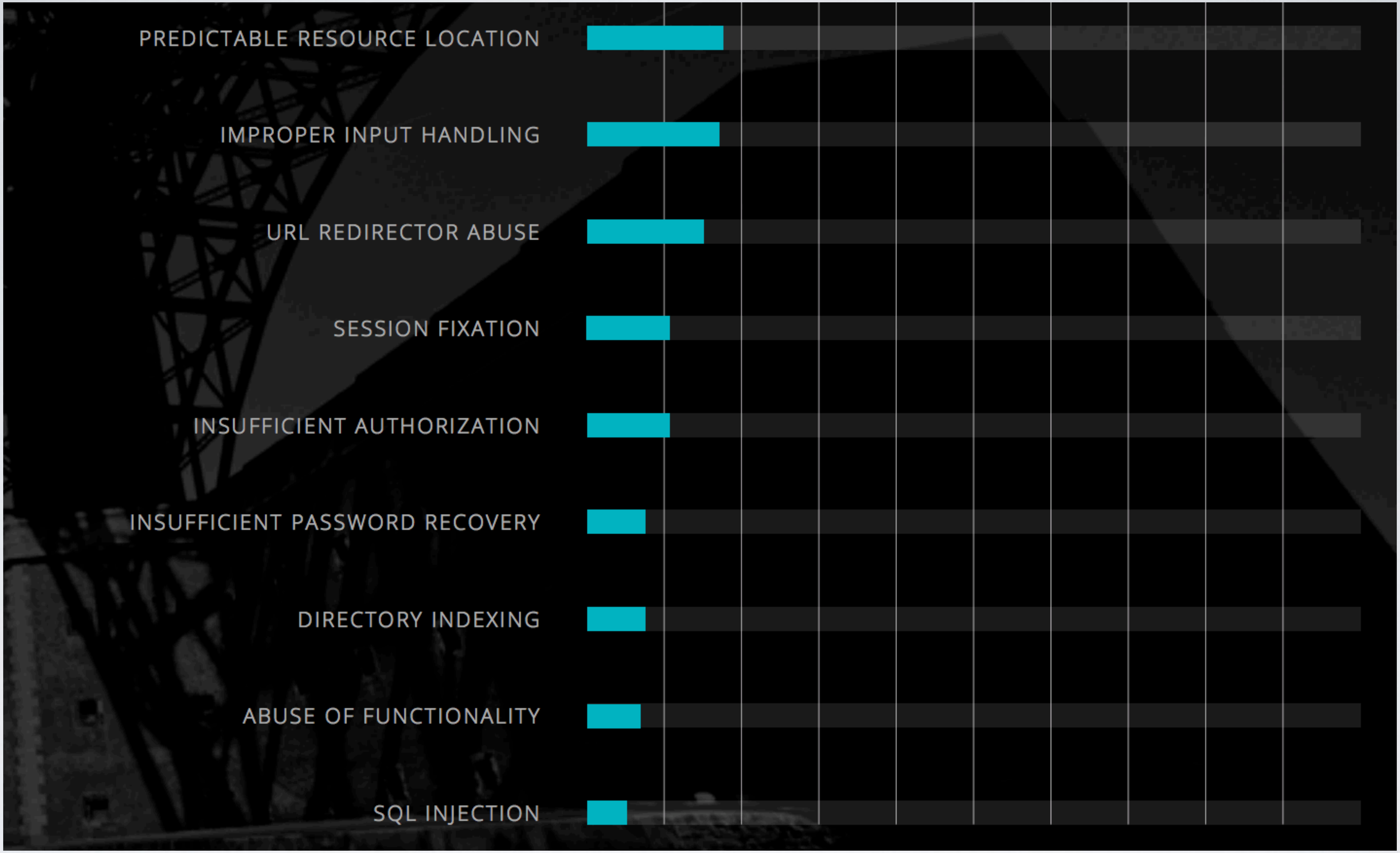
A new spate of vulnerabilities have been found in a D-Link router, a security researcher said Monday.

The D-Link 2760N, also known as the D-Link DSL-2760U-BN, is susceptible to several cross-site scripting (XSS) bugs through its Web interface, reported ThreatPost.



Vulnerability Likelihood

source *“WhiteHat Website Security Statistics report 2016”*
from *WhiteHat Security*



Vulnerability Likelihood

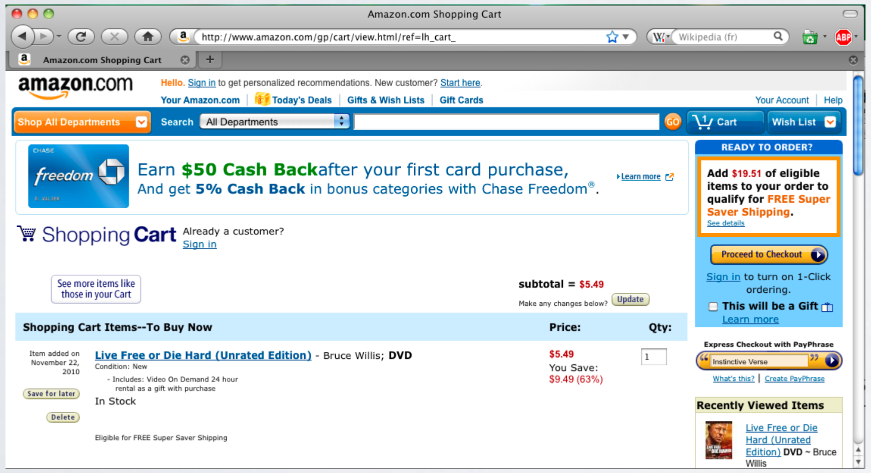
source *"WhiteHat Website Security Statistics report 2016"* from *WhiteHat Security*

Problem

You have **absolutely no control** on the client and the network

Client Side

Server Side



Hello. Sign in to get personalized recommendations. New customer? Start here.

Earn **$50 Cash Back**after your first card purchase, And get **5% Cash Back** in bonus categories with Chase Freedom®. Learn more

READY TO ORDER?

Add $19.51 of eligible items to your order to qualify for FREE Super Saver Shipping. See details

Sign in to turn on 1-Click ordering.

□ **This will be a Gift** Learn more

Express Checkout with PayPhrase

Shopping **Cart** Already a customer? Sign in

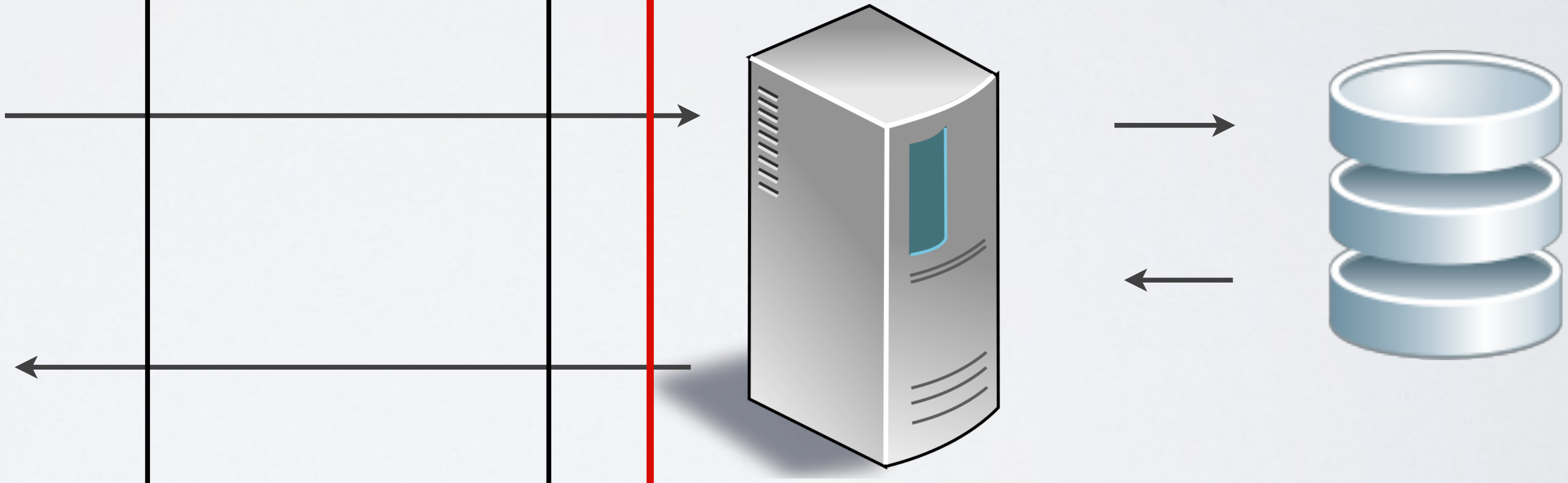
subtotal = $5.49

Make any changes below?

Shopping Cart Items--To Buy Now	**Price:**	**Qty:**
Item added on November 22, 2010 — Live Free or Die Hard (Unrated Edition) - Bruce Willis; **DVD** Condition: New - Includes: Video On Demand 24 hour rental as a gift with purchase In Stock Eligible for FREE Super Saver Shipping	$5.49 You Save: $9.49 (63%)	1

Recently Viewed Items

Live Free or Die Hard (Unrated Edition) **DVD** ~ Bruce Willis



Web Browser

Web Server

Database