Are You Scrubbing the Twitter Stream on Your Web Site?

Lori MacVittie, 2010-25-03

Never **never** *trust content from a user, even if that user is another application.*

Web 2.0 is as much about integration as it is interactivity. Thus it's no surprise that an increasing number of organizations are including a feed of their recent Twitter activity on their site. But like any user generated content, and it is user generated after all, there's a potential risk to the organization and its visitors from integrating such content without validation.

A recent political effort in the UK included launching a web site that integrated a live Twitter stream based on a particular hashtag. That's a fairly common practice, nothing to get excited about. What happened, however, is something we ***should*** get excited about and pay close attention to because as Twitter streams continue to flow into more and more web sites it is likely to happen again.

Essentially the Twitter stream was corrupted. Folks figured out that if they tweeted JavaScript instead of plain old messages that the web site would interpret the script as legitimate and execute the code. You can imagine where *that* led – Rickrolling and redirecting visitors to political opponents sites were the least obnoxious of the results.

> It **[a web site]** was also set up to collect Twitter messages that contained the hashtag #cashgordon and republish it in a live stream on the home page. However a configuration error was discovered as any messages containing the #cashgordon hashtag were being published, as well as whatever else they contained.

> Trend Micro senior security advisor Rik Ferguson commented that **if users tweeted JavaScript instead of standard messages, this JavaScript would be interpreted as a legitimate part of the Cash Gordon site by the visitor's browser.** This would redirect the user to any site of their choosing, and this saw the site abused to the point of being taken offline.
>
> The abuse was noted and led to Twitter users sending users to various sites, including pornography sites, the Labour Party website and a video of 1980s pop star Rick Astley.
>
> – Conservative effort at social media experiment leaves open source Cash Gordon site directing to adult and Labour Party websites, SC Magazine UK

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com