Mar 15, 2011, 12:09pm EDT

Researchers Say Hijackable Bug Infects 30% Of Websites

Andy Greenberg Former Staff
Security
Covering the worlds of data security, privacy and hacker culture.

This article is more than 10 years old.

Italian researcher Marco Balduzzi

The security world has long seen the Web as a buggy, infected tangle of sites vulnerable to hacks like cross-site scripting and SQL injection. Now a group of researchers has dug into a Web security problem that's lesser-known and by some measures more dangerous, and they've found that it applies to as many as three in ten sites.

On Thursday, Italian researcher Marco Balduzzi plans to present a paper at the Black Hat security conference in Barcelona on the scourge of HTML Parameter Pollution, or HPP. For pages that are vulnerable to the trick, a malicious hacker can craft a link that replaces some variable in the page with anything that the hacker chooses. That link can be used to lure a user into doing something that he or she didn't intend--say, posting a spam link to his or her Facebook page or voting for the wrong choice in an online poll, Balduzzi says. Or it can be used to corrupt a site's functionality, changing the price of an online purchase, for instance.

"You can override existing values coded in the application and cause it to do something different from one it was supposed to do," says Balduzzi, a

researcher at France's Eurecom technology-focused institute. "If you control the parameters, you can do anything."

Though HTML Parameter Pollution was first revealed as a vulnerability two years ago, Balduzzi has created a tool that combs the Web for the bug with a scanner he calls Parameter Pollution Analysis System, or PAPAS. By automating that tool and running it across 5,000 of traffic-counter Alexa's most popular sites, Balduzzi and two colleagues from universities in Madrid and Boston have showed that 30% were vulnerable to the HPP hack. Those vulnerable sites included domains owned by Google, Facebook, Microsoft, and Symantec, all of which the researchers contacted to alert the companies to the new Web bug.

The Web security world has long been aware of similar attacks like cross-site scripting, which can be used to steal the cookies from a user's browser and gain access to his or her accounts, and SQL injection, which allows a hacker to enter values into a site's SQL database. Balduzzi says HPP may be similarly serious, but hasn't received nearly as much attention. "No known exploits of this have been found, but it’s just a matter of time," he says. "Web developers need to become aware of this and code their sites safely. Otherwise, sooner or later, someone will take advantage of it."

You can read the researchers' full paper here.

Andy Greenberg

I'm a technology, privacy, and information security reporter and most recently the author of the book *This Machine Kills Secrets*, a chronicle of the history and future... **Read More**