

apply for your complimentary registration now



## Black Hat: JavaScript Flaws Ease Intranet Attacks

Security researchers at the Black Hat conference discussed the weaknesses in JavaScript that let an attacker take control of a user's browser.

By Larry Greenemeier, [InformationWeek](#)

Aug. 7, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=201300295>

Which of the following will protect your Web site from attack: network perimeter firewalls, encryption, antivirus, or multi-factor authentication?

None of the above, says one Web security researcher.

That leaves it up to Microsoft, Mozilla, and all of the foremost makers of Web browsers to protect cyber space from a litany of emerging Web-based attacks including [cross-site scripting](#), [cross-site request forgeries](#), and browser port scanning.

What's worse, poor Web site security can lead to browser infections, which can lead to malicious software installing itself on a user's computer and attacking corporate systems from the inside. "Intranet hacks are happening already," [Jeremiah Grossman](#), founder and chief technology officer of Web application security firm WhiteHat Security, told *InformationWeek*.

Grossman and Robert Hansen, CEO of security consulting firm SecTheory, described how it works during a presentation at last week's [Black Hat USA 2007 conference](#) in Las Vegas. It starts when a user visits any Web page -- a blog, social networking site, etc. -- that either has been designed to distribute malware or is a legitimate site infected with malware. Once that malware infects and takes control of the browser running on the user's PC, the browser can be instructed to hand over its [network address translation](#) ID, which is designed to keep internal network addresses hidden from the outside world. Once this is done, the attacker has been handed the information needed to peruse network addresses located inside the local network.

The problem isn't the result of security bugs or vulnerabilities. "You can patch all you want," Grossman said. "It's a design flaw in [JavaScript](#). Browser security is flawed in general."

At the 2006 Black Hat USA conference, [Grossman discussed the weaknesses in JavaScript](#) that let an attacker take control of a user's browser. Simply turning off JavaScript is not a great option, given that there's no Ajax -- and, consequently, no Web 2.0 -- without JavaScript.

New methods of attack have emerged in the year since Grossman first laid out the dangers of cross-site scripting, cross-site request forgeries, and JavaScript malware. One such attack is history stealing, whereby an attacker uses JavaScript running in a user's browser to reveal the sites the user has visited most frequently. Once the attacker knows the user's Web-surfing history, the attacker can create look-alike spoofed sites containing malware or infect the sites that the user visits.

In another type of attack, JavaScript can be used to do intranet port scans by forcing the browser to make certain types of requests to internal IP addresses. Even if a browser's JavaScript has been disabled for security purposes, Grossman said port scanning can be done [using HTML](#) as well.

One of the problems with securing Web sites is that the building and securing of Web sites is treated as two separate processes. "The security guys have no control over the Web site," Grossman said. "The developers do, and they don't work for

security."

While Microsoft and [Mozilla](#) have made strides in improving the security of Internet Explorer and Firefox, respectively, it's incumbent upon them to ensure that their browsers can fight off new threats.



Copyright © 2007 [CMP Media LLC](#)