

Web browsers and iPhone hacked at contest

March 26 2010, by Lin Edwards



(PhysOrg.com) -- Hackers had a field day on the first day of the Pwn2Own contest, successfully attacking Safari, iPhone, Internet Explorer, and Firefox. The Pwn2Own contest is an annual event that encourages security specialists to win hardware by successfully attacking it. Hackers register the attack has run by having the exploit code read a particular file on the system. Winners receive cash prizes as well as the hardware.

This year's winner, security analyst Charlie Miller, was awarded \$10,000 and a MacBook for hacking into Apple's [Safari browser](#) running on [Snow Leopard](#) on a MacBook Pro to which he had no physical access. Miller also successfully attacked Safari in the 2008 and 2009, and now works as principal security analyst with Independent Security Evaluators. While he gave no details, Miller said the attack was triggered by the

target computer visiting a specifically designed malicious website. The exploit, written in only a week, was reliable, and the user had no idea the computer was being attacked.

The \$15,000 second prize winners were Ralf Philipp Weinmann from the University of Luxembourg and Vincenzo Iozzo of Zynamics, who successfully attacked the [iPhone](#). This exploit also featured a website with [malicious code](#) that enabled the hackers to lift the SMS database from the phone in around 20 seconds. They were even able to read text messages that had been deleted and upload them to their own server. They could also have exfiltrated the email database, phone list, photographs, and music files. Weinmann said they took two weeks to find the vulnerability and write the exploit, and while the attack crashed the browser, he said with a little more work they could have avoided that.

Other successful hackers at the event attacked [Internet Explorer 8](#) and Firefox 3.6.2, both running on 64-bit Windows 7. The attack on IE 8 by Peter Vreugdenhil, a security researcher from the Netherlands, bypassed both ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention), which are both designed to stop attacks on the browser. The exploit won him \$10,000. The Firefox hack, by Nils (no surname given), chief researcher with MWR InfoSecurity in the UK, also won \$10,000 for an attack that bypassed ASLR and DEP. The attack allowed him to run the Windows calculator, but he said he could have started any process. In both exploits the browsers visited malicious websites.

Pwn2Own is sponsored by Tipping Point's Zero Day Initiative, which gives vendors details of the attacks to allow them to patch the vulnerabilities. Pwn2Own is run as part of the CanSecWest [security](#) show in Vancouver, Canada.

© 2010 PhysOrg.com

Citation: Web browsers and iPhone hacked at contest (2010, March 26) retrieved 10 April 2024 from <https://phys.org/news/2010-03-web-browsers-iphone-hacked-contest.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.