

5 January 2009

By: Lucian Constantin, Web News Editor



Facebook password reset page open to phishing attacks Facebook (for the logo)

[New Critical XSS Flaw Plagues Facebook](#)

The password reset page is affected

A new cross-site scripting vulnerability affecting the Facebook social networking website has been disclosed on the XSSed project's [website](#). The flaw allows for injection of potentially malicious code.

The XSSed project tracks XSS vulnerabilities and its archive contains over 30,000 of documented such flaws affecting hundreds of highly popular websites. It is also a good source of information regarding the prevention and mitigation of cross-site scripting attacks. The XSSed report credits security researcher DaiMon with the discovery of this latest threat.

According to Alexa, Facebook currently has a global page rank of 5 and, as Dimitris Pagkalos, one of XSSed Project's co-founders, points out, this significantly increases the flaw's attack potential. "Malicious users can inject code to phish credentials and other sensitive personal information from millions of Facebook members," he explains.

This is not the first time that major XSS bugs are discovered in Facebook's pages. Less than a month ago, we [reported](#) four similar flaws affecting the Facebook developers, applications, user registration, and iPhone login pages. The XSS vulnerability on the apps.facebook.com page in particular was also discovered by DaiMon.

Analyzing DaiMon's [history](#) on the XSSed website suggests that he is also credited with the discovery of XSS flaws that affected many high profile pages belonging to Yahoo, ICANN, AVG, Symantec, Panda Security, Citibank, Unicef, UEFA, WorldBank, Harvard, Ericsson, Motorola, Siemens, Samsung, and Mozilla, just to name a few. An impressive number of governmental and military sites are also on his list of vulnerable pages.

At the time of publishing this article, this latest XSS vulnerability that affects Facebook's password reset page was not yet fixed. However, Dimitris Pagkalos' statement might be an indication that there is a good chance of Facebook acting promptly. "We hope that this serious flaw gets fixed quickly as is usually the case with security flaws in Facebook," he says.

According to MITRE's CVE vulnerability trends, cross-site scripting bugs are currently the most common and widely spread security threats, and literally thousands of new pages get exploited everyday in order to launch a wide variety of attacks. Such flaws are often combined with other types of vulnerabilities, in order to instrument more complex and harder to track schemes.