Vulnerability in Facebook's OAuth allowed hacker full profile access

February 26 2013, by Bob Yirka

Credit: nirgoldshlager.com

(Phys.org)—Nir Goldshlager writer of a security blog, is reporting that he found a vulnerability in Facebook's OAuth that allowed him full access to an individual's profile information. Facebook confirmed the vulnerability and has subsequently fixed the problem, but questions still linger about how safe user data is from developers who possess expert knowledge of the social giant's inner workings.

As most Facebook users know, if they wish to add an app to Facebook, they must first click an "accept" button when presented with one from

the app asking for permission. It allows the app to access private profile information, which is necessary for the app to run. What Goldshlager found was a hole in this process—known as OAuth to developers—that allowed him to gain access to user information (in and outbox, ads pages, photo's etc.) without their permission.

The OAuth service is run by sending a URL—Goldshlager modified the URL in a way that allowed him to send a user to a page he had created himself where an access token would be stored, bypassing the instigation of the popup that would ask the user for access permission. Using this method, he was able to give himself permission to access a particular user's account profile information without the user being aware of what had occurred. There are two important things to note here: first, there is no evidence that any hackers knew of the vulnerability and used it to gain access to a user's information, and second, that the vulnerability works only on a single user account.

Because the vulnerability only works on one account at a time, it means a hacker would not have been able to use it to create a program to steal account information from groups of users—it would have had to have been a personal attack, i.e. a single hacker trying to crack a single account. For that reason, Goldshlager and Facebook are reasonably sure that no one ever took advantage of the vulnerability. Only those who develop applications might have ever stumbled across it, and had they, the monetary reward offered by Facebook via its White Hat program (which Goldshlager says he received for his efforts) would in most instances outweigh any other alternative actions they might be considering.

Goldshlager also reports that he's found other app authorization bugs with Facebook, though he didn't go into detail on them. But his findings have created an air of uneasiness surrounding the degree of access

developers gain with user accounts and what bugs might exist in the services they use that might allow a less honest hacker to gain personal data and use it for nefarious purposes.