Title	HTML parsing in Linkedin app V 6.1.2 - Sept 3, 2013
Author	Zouheir Abdallah, CISA
Date	September 5th, 2013
Contact details	Zouheir.abdallah@gmail.com zabdallah@ict.gov.qa
Disclaimer	This document is intended only as a demonstration for educational or testing purposes. It is not intended for any unauthorized or illicit purpose.

Description:

LinkedIn iOS app parses HTML in the messages, and this can be used to phish for credentials or be escalated into a full blown attack.

iFrames can also be created and manipulated.

Proof of Concept:

Send a message to a user with the following content

Hey,

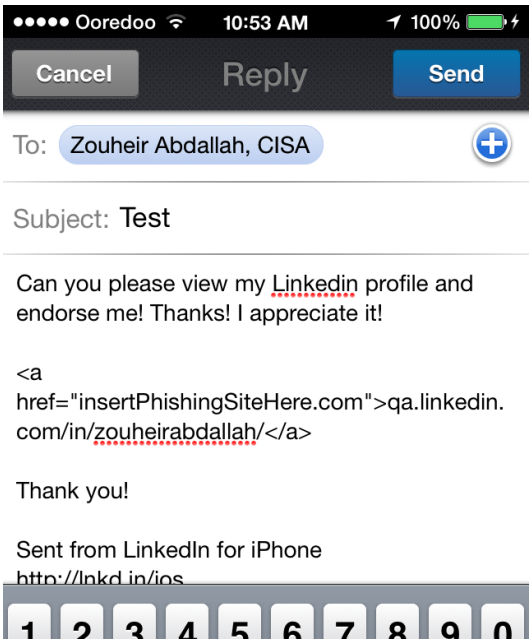
Can you please view my LinkedIn profile and endorse me! Thanks! I appreciate it!

 qa.linkedin.com/in/zouheirabdallah

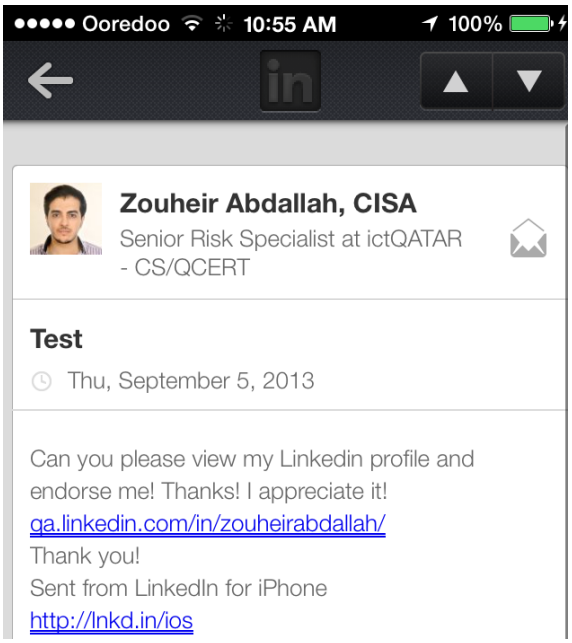
regards,
Zouheir

Screenshots:

Actual Message



Received Message



The phishing site can be a replica of LinkedIn and tricks the victim into giving out his username and password.

The iOS app will display the qa.linkedin.com/in/zouheirabdallah without the hyperlink embedded in the HTML a href , and the receiver will not even know that he is being redirected to a malicious site.

This attack can be used against LinkedIn too by claiming that LinkedIn requires re-authentication to view some article on LinkedIn.

This attack could also work on different devices such as Android and Blackberry, but I couldn't test as I don't have another handset at hand.

Regards,

Zouheir Abdallah