YEHG is Proud to find and report this vulnerability because it has the Greatest Impact on Ning.com and its all social networks!

Ning.com Social Networks Captcha Protection Bypass Vulnerability

Discovered by: d0ubl3_h3lix
Date: April 2008
URL: All Ning sites (*.ning.com)
Vulnerability Type: **Weak Authentication**
Risk: **highest**
Threats: Spamming, Botnet/Worm Creation/Spreading/…etc

Note:

The vulnerability has been fixed since the same night I have reported. Nice response! I also reported Ning's output validation failure issue on user' profile page. Now the world knows that Myanmar/Burmese hackers exist on the planet.

Proof-Of-Vulnerability:

Small Spamming attacks were performed to my 0wn group YGN Ethical Hackers at http://mmitpros.ning.com and http://sgmyanmar.ning.com. I created about 150 bot accounts. The bot accounts I created are extremely easy to remove with one statement of SQL query since it has the same kind of name patterns – The_Burmese_Hacker _. If only I created totally random patterns, it would suck administrators. ☺ I had to do this for the sake of getting Ning's attention to fix immediately. Developers never realize the danger of threats till we show them small prototype.

Worst-case Scenarios

Malicious smart black hats can create much more devastating attacks using this flaw such as:

- Creating innocently-looking accounts with Human Name dictionary – You will never know those are bots!

- Using those accounts spreading spam containing links pointing to malicious web sites
- Using those accounts who profiles are filled with malicious scripts which contains browser/plugin remote exploits that lead to compromise of entire workstation
- Abusing other users by posting malicious links/replying their threads with gibberish messages, which subsequently creates bombing “Reply Message” notification mails to such users
- Flooding the database within a few minutes till allowable limits/quota; hence creating Denial-of-Service
- … much more

Lastly, no doubt, this flaw can stop the entire ning! At least to fix this issue, Ning has to stop its service for ……. minutes/hour to prevent further possible coming attacks. Don’t worry we’ll never report vulnerability info to Bugtraq which promotes script kiddies’ hunger for bulk attacking.

Additional Advisories

I took 5 days to test this vulnerability. On sixth day, I reported about it. Meantime, I found that Ning.com lacks web application or server level IDS/IPS that can detect anomalous behaviors. It seems that Ning.com failed to implement “Log – Alert – Monitor” secure practice. Ning.com sounds like a honey for black guys bee. This vulnerability has long been existed since Ning.com was born. Ning.com would never know their Captcha could be broken until it was hit by attacks like my worst-case scenarios.