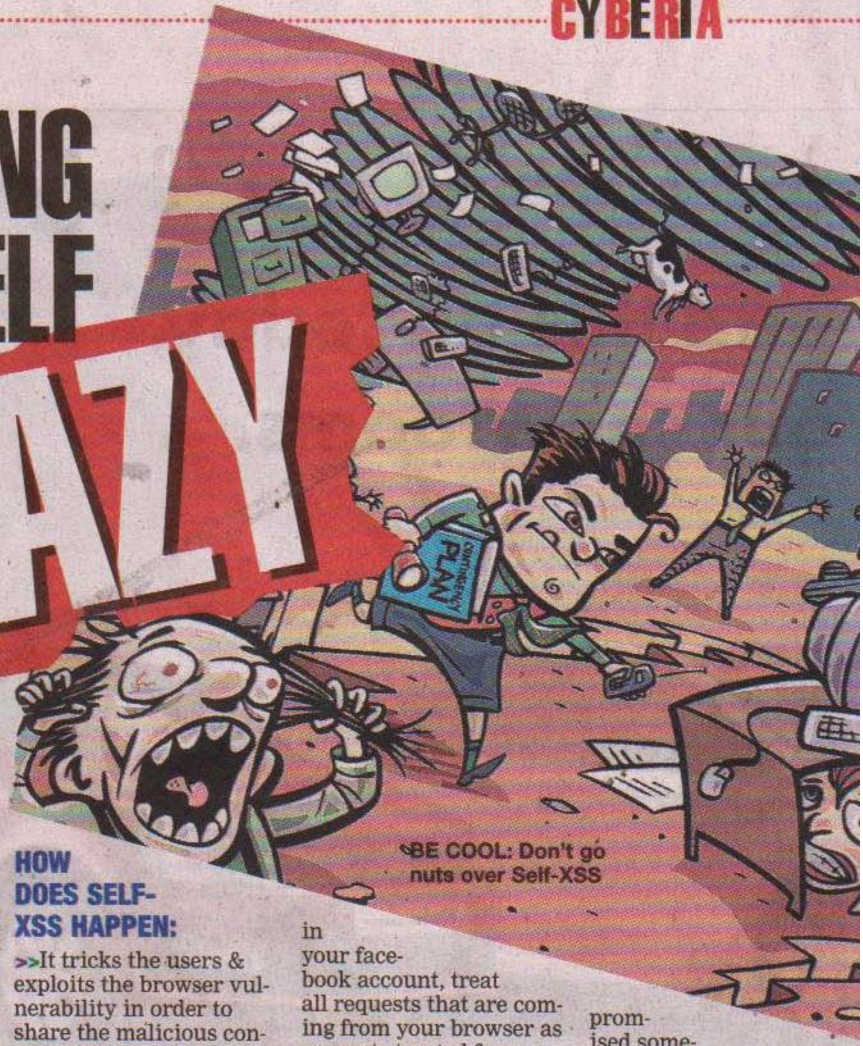
Bombay Times

10 December, 2011

STOP DRIVING YOURSELF CRAZY

Steer clear of self-XSS on social networking websites, which lead to spam attacks on your account



BE COOL: Don't go nuts over Self-XSS

Online vulnerabilities are becoming common with every passing day. The leading social networking website (you know the one... with 1000 million+ users) recently acknowledged the spam attack that began a couple of weeks ago. The site mentioned that users could see pornographic images and other "disturbing" photos on their friends' walls.

According to Govind Rammurthy, MD of a leading antivirus firm, whatever happened wasn't a hack attack and it was actually a Self-XSS (cross site scripting) attack as there were no viruses to blame, just that users were tricked into doing dangerous things.

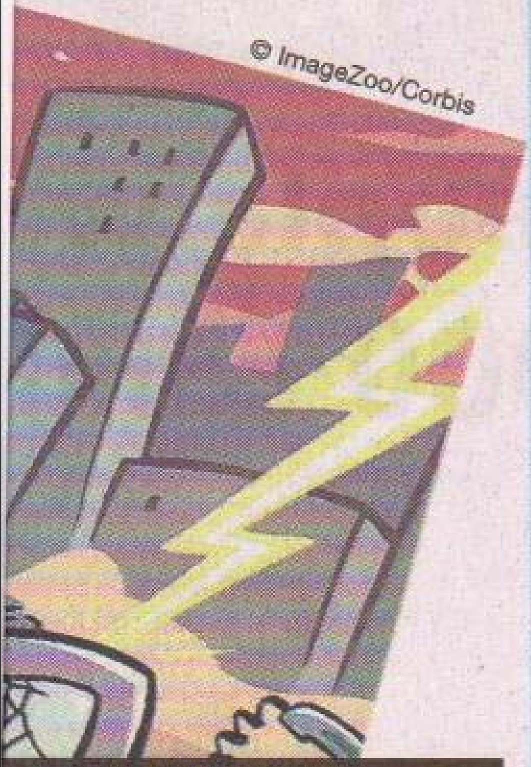
The browser vulnerability in this scenario is the result of having a feature intended for developers on by default for normal users. There are legitimate use cases for this feature, but they are only logical for a very small subset of users and when enabled for everyone. Self-XSS means that the malicious script was actually activated by a user and was not part of some hidden webpage code.

HOW DOES SELF-XSS HAPPEN:

>>It tricks the users & exploits the browser vulnerability in order to share the malicious content on facebook. Cross-site scripting essentially allows an attacker to execute JavaScript code in your browser that can access and control the website you are interacting with.

>> When you are logged in your facebook account, treat all requests that are coming from your browser as requests treated from you. Hence, in case of your browser being the reason to issue a request for a wall post without your knowledge, then Facebook would dutifully display the wall post.

>> In the recent facebook attacks, the users were promised something in exchange for pasting a line of text into their browser address bars. Though, this "something" was not clearly specified. The attack is said to be occurred using older versions or other browsers.



© ImageZoo/Corbis

THE LINKS USED FOR THIS SELF-XXS ATTACK WERE:

1 A link to a (rather gross) video that "95 per cent of people can't watch".

2 link to a free coffee voucher

3 A pornographic video

>> When a user pastes the text provided into their browser, they are effectively telling their browser to act on their behalf and do whatever the script says. In most of the cases, it will visit an external site (the cross-site of cross-site scripting) and then be asked to post a wall post or an event invite. This perpetuates the attack as friends see the posts and follow them.

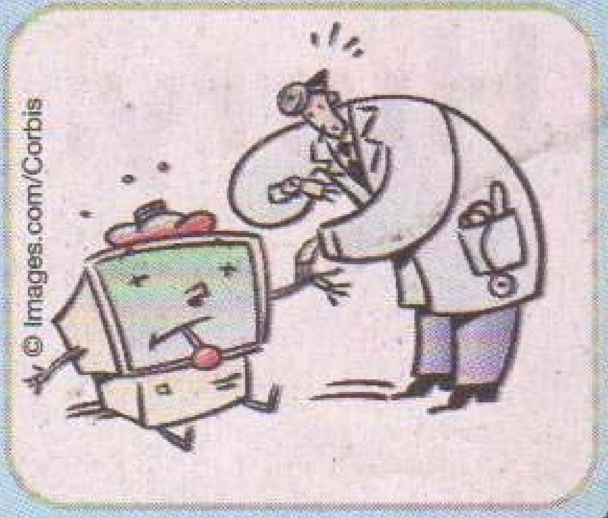
SAFETY MEASURES

>> Be smart and alert about what you click on.

>> Keep your security levels at high levels to protect your privacy and only share with those you wish.

>> Check your security settings.

>> The most important thing is to remember to check your data protection settings. You have to be very particular on which data will be seen by the people you accept as friends, wich data you want to be completely available for public and vice versa. Ensure that you fill out only necessary information that is required while you fill up a registration form on a social networking website.



© Images.com/Corbis

>> Be cautious of what you post on your wall. Before you type something and put it on display, be sure of the consequences. Careless chatter can be just as much of a problem as off-colour photos, binge-drinking videos, or memberships of dubious groups.

>> Be careful while choosing your 'friends' on social networking sites. Don't rush to accept 'friendship requests' just to balloon the 'friends' list. It's of utmost importance to protect your own identity on social sites or it may lead to identity theft in which criminals have created profiles for users and used them to blackmail their victims.

>> Ensure you keep yourself updated on malware attacks and keep yourself aware on preventing yourself from these attacks.

>> Pests like the Koobface worm use social networking sites such as Facebook and MySpace to distribute themselves. Users receive an invitation from a friend to view a photo album or to click on a link to watch a 'great video'. If you click, your PC becomes infected with malware. All infected computers are then incorporated into what's known as a botnet — a network of infected computers controlled by cybercriminals.