Whitepaper on

Vulnerable Facebook Applications

A Case Study.

Author : Abhinav Singh a.k.a DaRkLoRd

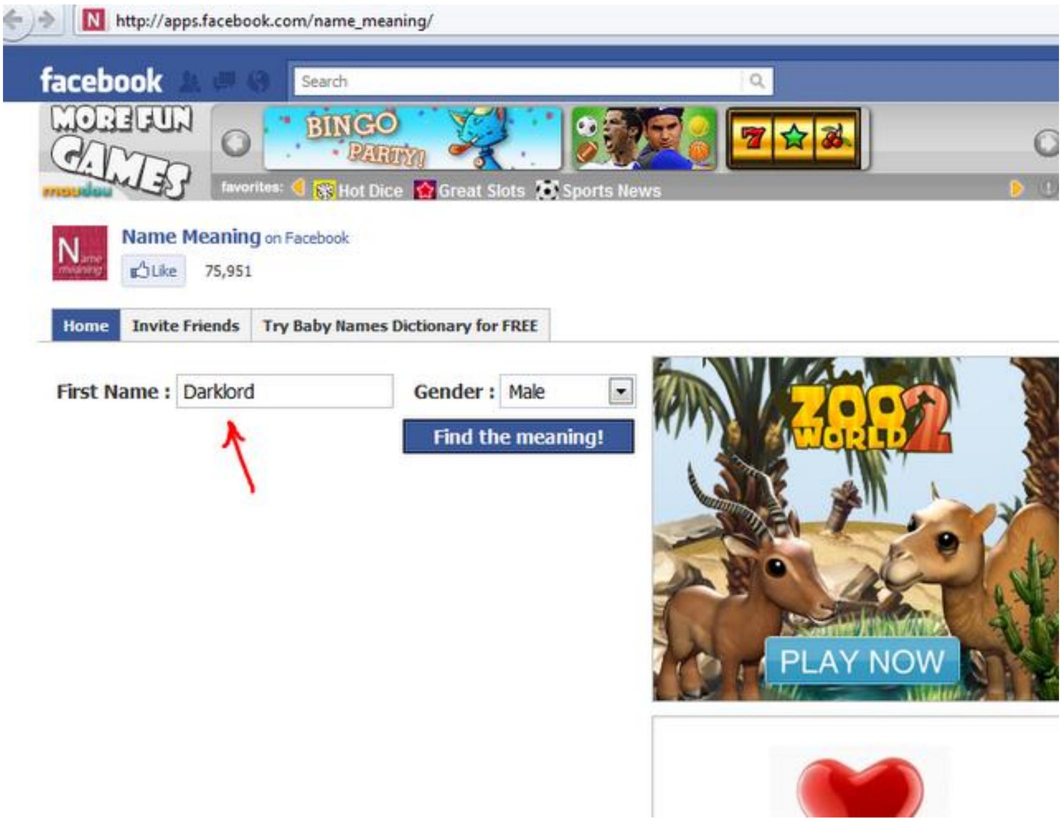
(Information Security Specialist)

http://hackingalert.blogspot.com

Facebook has always been under the scanner because of its privacy issues. Since its release in 2004, it has been target several times because of its security measures. Over the course of time Facebook did learn from its mistakes and improved its security measures of how people share information on the platform. But an area where they still don't have much control is the applications that are built using the platform. Here is a statement from Facebook's privacy policy about Third party applications - *we do not own or operate the applications or websites that use Facebook Platform. That means that when you use those applications and websites you are making your Facebook information available to someone other than Facebook.*

This is where the users should be careful. Applications running on Facebook cannot be trusted unless it belongs to a popular app builder. There are various such malicious and vulnerable Facebook applications running on the platform which can misuse the information that you share. Facebook has become the prime target of spammers and hackers because of its heavy popularity among people and because most of the users are unaware of such issues, they keep on clicking every application that comes in their notification. The main aim of this paper is to make users aware of the fact that every application on Facebook cannot be trusted.

While performing some tests on Facebook platform, I came across a vulnerable application that can be attacked using Cross site scripting. The application can be found at this link : http://apps.facebook.com/name_meaning/ . This application tells you the meaning of your name.



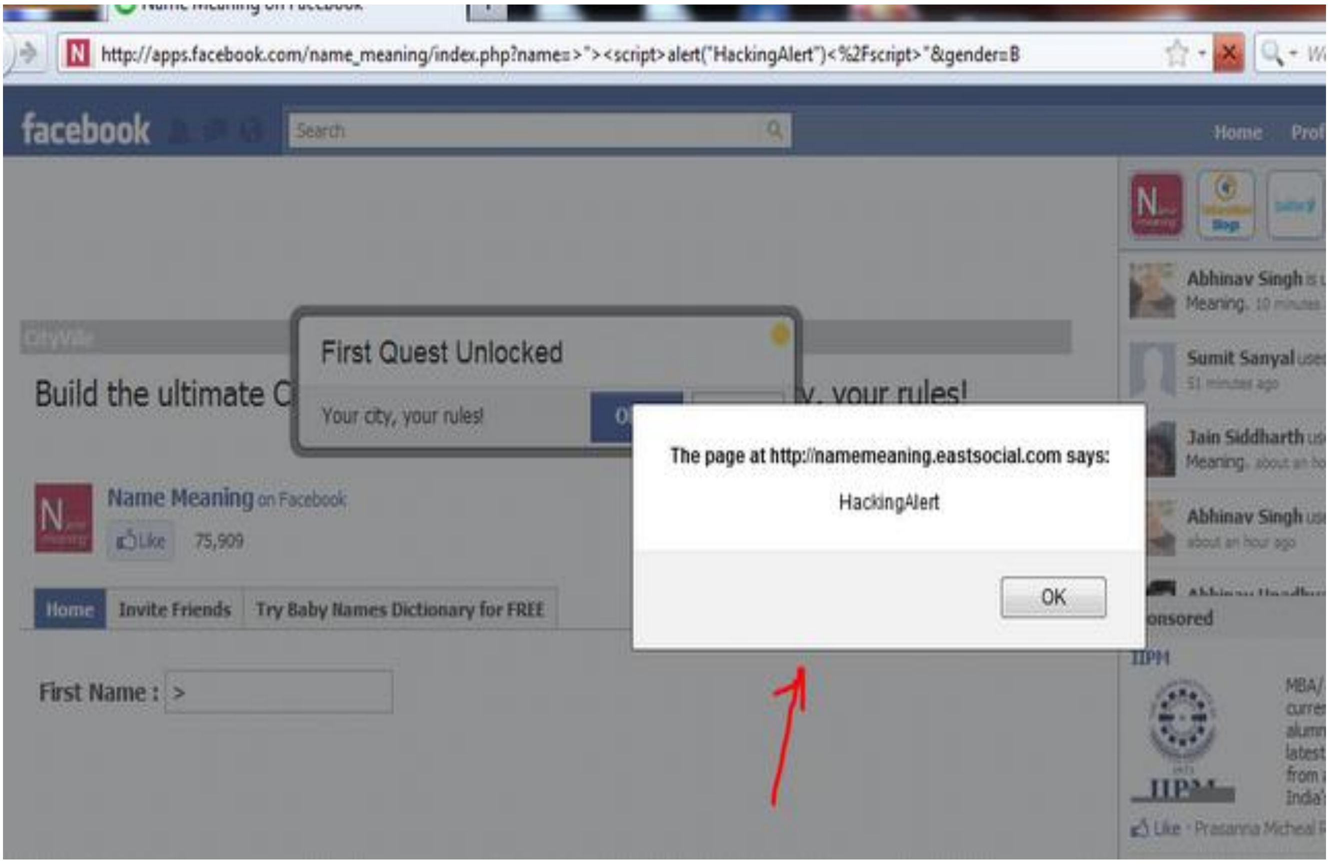
First Name : Darklord

Gender : Male

As you can see that the application has a text box where the user can enter his/her name to find out the meaning. I went on to check this application with a normal reflected XSS attack by entering a small javascript : ***<script>alert("HackingAlert")</script>***

This injection didn't work. So I went on to try my second dork with a bit of advanced script injection to bypass the filter mechanism. The next javascript that I tried was :
>"><script>alert("HackingAlert")</script>" .

This time the attack succeeded and an alert message was generated showing the successful execution of the script.



http://apps.facebook.com/name_meaning/index.php?name=>"><script>alert("HackingAlert")<%2Fscript>"&gender=B

The page at http://namemeaning.eastsocial.com says:

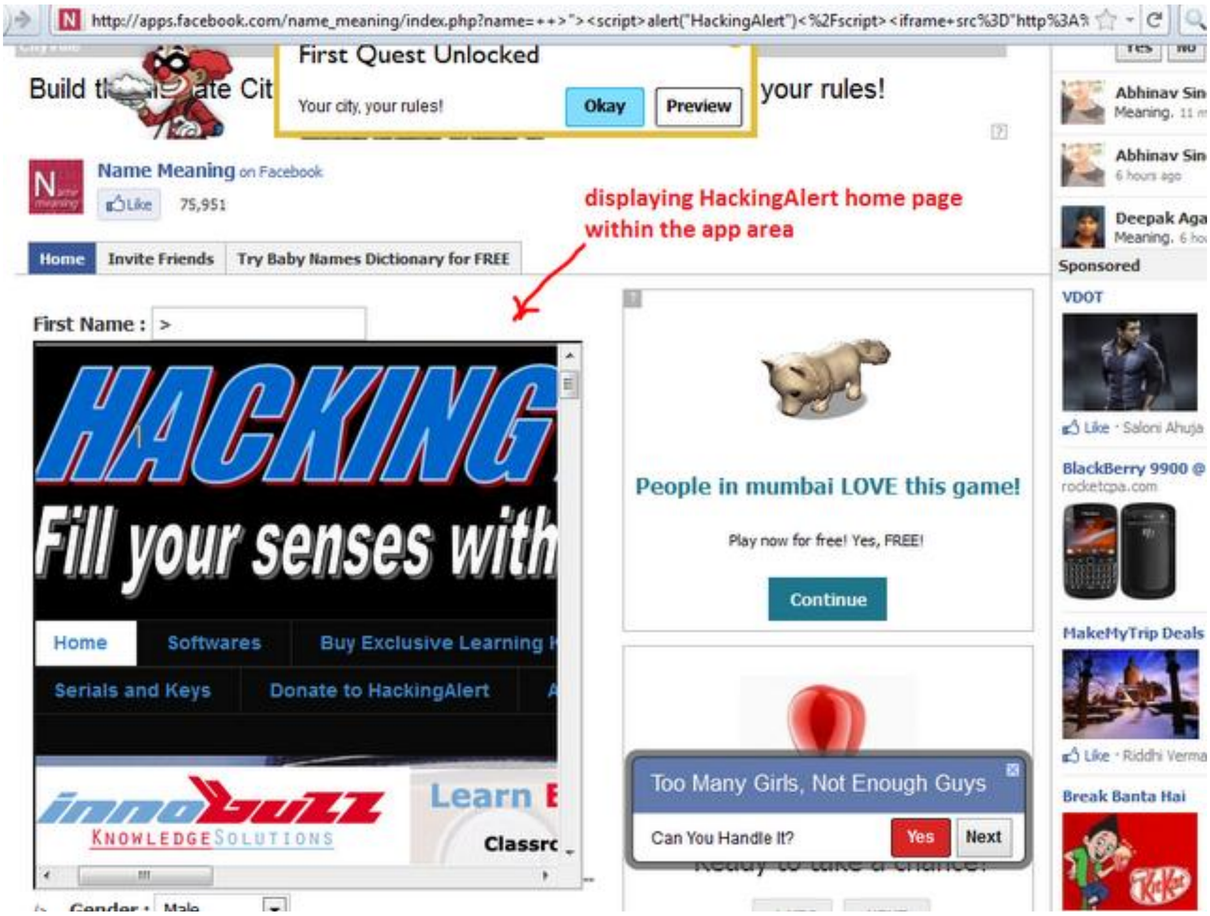
HackingAlert

I further went on to check if I can insert more dangerous tags or not. The next script that i crafted contained an <iframe> tag to check if my respective iframe gets displayed in place of the application or not. The attack succeeded again and instead of displaying the application in the iframe area, it displayed my blog url which I had inserted in my script.

Here is my crafted script :

>"><script>alert("HackingAlert")</script><iframe src="http://hackingalert.blogspot.com" width="400" height="400"></iframe>"

<u>NOTE</u> – You will have to shift to http version of Facebook instead of https in order to use any of its third party applications.



http://apps.facebook.com/name_meaning/index.php?name=++>"><script>alert("HackingAlert")<%2Fscript><iframe+src%3D"http%3A%

displaying HackingAlert home page within the app area

Now any attacker can display a malicious link in the iframe area and spread the url. The attacker can use this technique to steal cookies and perform session hijacking.

http://apps.facebook.com/name_meaning/index.php?name=++%3E%22%3E%3Cscript%3Ealert%28%22HackingAlert%22%29%3C%2Fscript%3E%3Ciframe+src%3D%22http%3A%2F%2Fhackingalert.blogspot.com%22+width%3D%22400%22+height%3D%22400%22%3E%3C%2Fiframe%3E%22&gender=B

Looking at this url, any normal user would believe that it belongs to the Facebook application. In-fact it does belong to it but it has been crafted to attack the user information. This vulnerability can easily be used to steal cookies of legitimate users and lead to their security breach.

Hence it is highly recommended that you should not trust any facebook application blindly. Recently lots of spam and such vulnerable apps have flooded the platform and Facebook will not take any responsibility for any information that you share with third party applications within the platform. So think before you CLICK!!