How much facebook is secure- Facebook MSG dropping

Akash Shukla
Corporate Trainer
(Virscent Technologies Pvt. Ltd.)
Certified Information Security Expert (CISE)

Web: www.hackersreloaded.com

Email: akash@hackersreloaded.com
akash@virscent.com
aks.zooming@gmail.com

SNL: https://facebook.com/hybridakash
https://twitter.com/akszooming

Biography of Author:

Akash Shukla is an IT Security researcher currently working with **Virscent Technologies Pvt. Ltd**. as a **corporate Trainer**. He is a **Certified Information Security Expert (CISE)**, **Member of Computer Society of India (CSI)**, **Founder and Admin of Hackersreloaded.com** as well as worked with **Kyrion Technologies Pvt. Ltd.** as a **Penetration Tester** for Two months. His expertise includes Research and Development in this domain, Computer and Network Security, exploit research, C, PHP, Perl, JAVA and website designing.

He has trained more than **1000+ students** and having more than 4 years' experience of IT Security field. He has conducted lots of workshops around the nation. He has also found some big security loopholes in high rank websites of cyber space like **Facebook, Orkut, Ebay, Paisalive**.

He has also made possible calling from OLD version of **Micromax modem MMX310G** whose process video got 1000's of hits on youtube. He has some videos on youtube because he strictly share only new hack stuffs ☺.

He has also helped in curing the vulnerability of **Gautam Budhh Technical University's** website which was earlier

hacked by him and reported to the Vice Chancellor as well, after which Vice Chancellor admired him for his sincere efforts in reporting the vulnerability, the news was also in Media. He has also worked on many projects in which **Snort-An Open Source Intrusion Detection System** was the project whose LOG problem on Windows 7 was resolved by him and successfully patched. Earlier he worked with various companies as a free-lancer.

Abstract:

As far as Facebook security is concern, they have one of the best security available. But our work is to find out the loopholes and loopholes can be anywhere. Basically Facebook provides you a facebook mail id when you register your facebook username viz. hybridakash@facebook.com. Now, here is the vulnerability where facebook provides you the flexibility that you can actually make comments and message using your Email ID by which you login into your account. Now, as we all know that Email Spoofing can be done in numerous ways. So we will use the PHP fake mail script for dropping Facebook MSG. This security loophole will not ask special skills to perform this hack, what it needs, your way of observation. Broadly speaking this is the Application of Email Spoofing. We can also perform Email Bombing on Facebook by using this hack.

Keywords: Facebook MSG Dropping, PHP, Email Spoofing, Email Bombing, Fakemail.

Introduction:

Facebook have the best security available on any social networking sites. That's why they believe in to keep on assessing their security time to time. Facebook provides a feature or can say flexibility to comment and make status using our own Email ID which we use to login into our facebook account when we register our facebook username viz. http://facebook.com/hybridakash .

Now, here we will do some manipulations, as we all know that Email can be spoofed using PHP or ASP script by uploading it on web servers or by implementing our own Email server. So there are certain requirements for dropping facebook MSG into any facebook account by the name of any person who will be on facebook.

Requirements:

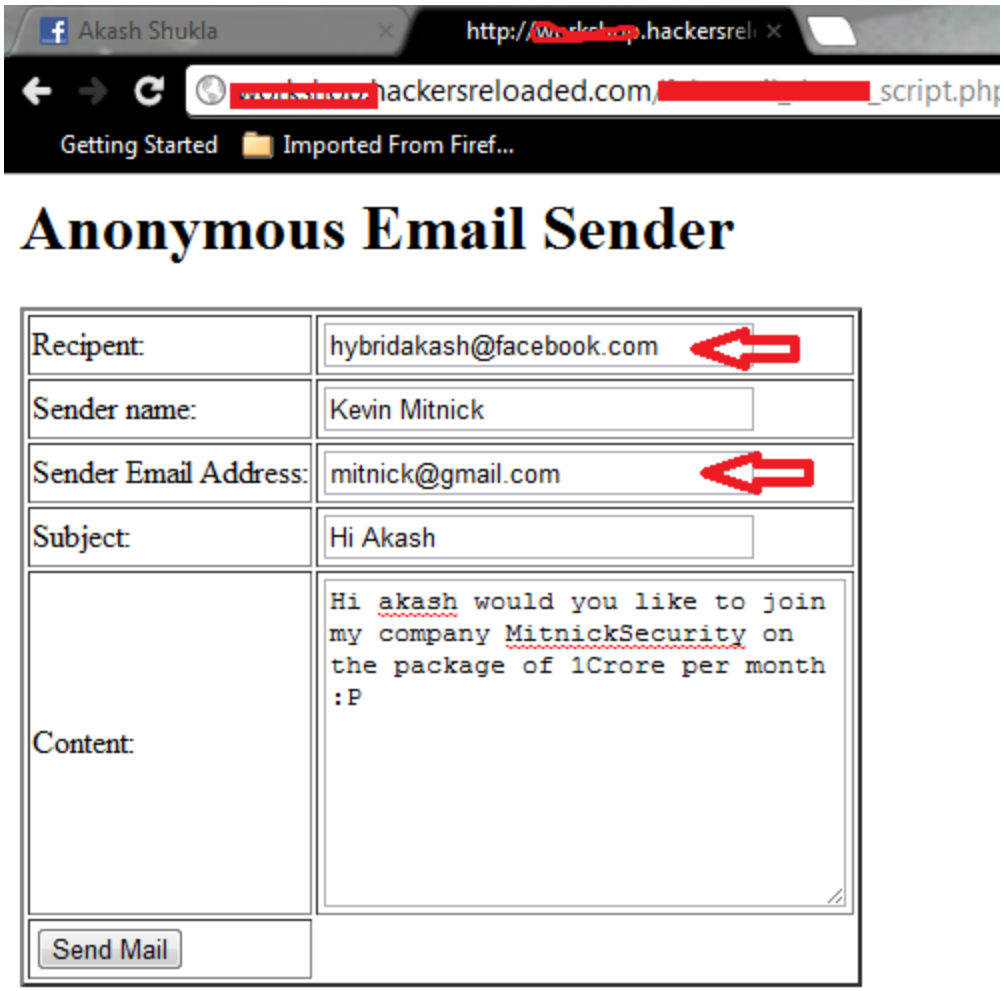
a) Select the target facebook account.
b) The target facebook account must have the facebook username viz. hybridakash@facebook.com .

c) Now, we need Email ID of any facebook account which he/she use to login into his/her account.
d) PHP/ASP fakemail script uploaded on web server or local server.

Facebook MSG Dropping:

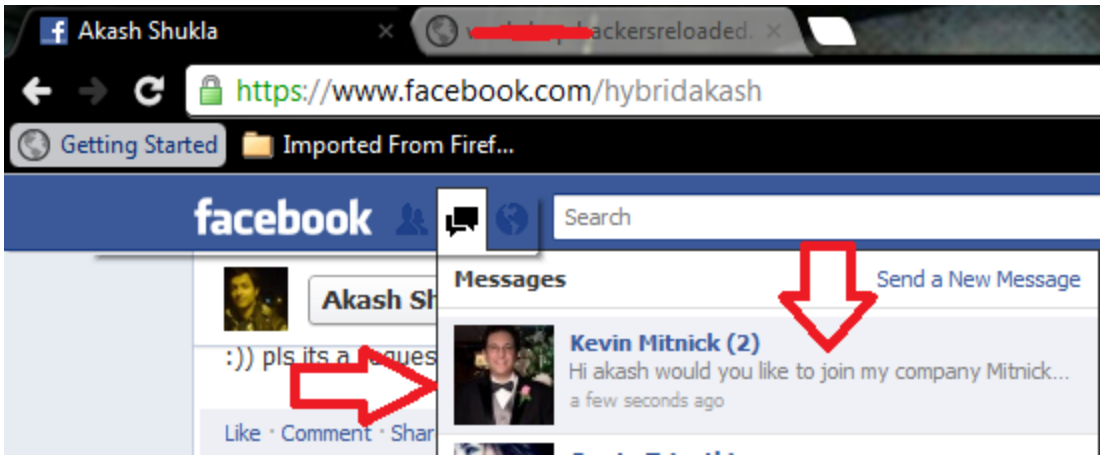
i) Target facebook account : http://facebook.com/hybridakash
ii) Email ID of other FB Account: mitnick@gmail.com (Sir Kevin Mitnick's Facebook Email id which he used to login into his facebook account ☺) http://facebook.com/mitnick007
iii) Now, we have almost done with Information gathering part of this hack. Now, I will use my uploaded Fake mail PHP script to drop the message into my facebook account which is http://facebook.com/hybridakash by the name of Sir Kevin Mitnick.

iv)



In the above snap we can see that I am using an uploaded fake mail PHP script for dropping MSG into the facebook account hybridakash@facebook.com by the name of Sir Kevin Mitnick using his Email ID mitnick@gmail.com without logging into his FB account.

v) Let's see whether the MSG arrived into my facebook account or not ☺.



Now, as we can see the message has been arrived into my facebook MSG inbox successfully which was never sent by Sir Kevin Mitnick to me originally ☺.

We can also perform Facebook MSG bombing by altering the same fake mail php script coding where we will run a loop like this one:

```
for ($i=1; $i <= 1000; $i++)
{
mail($to, $subject, $message, $headers );
}
```

Note: There should be no misconception that whether to make this hack possible both facebook account should be connected means be friends or vice-versa. This hack would work in both conditions but the condition is recipient must not disallowed the MSG from outside users.

Hack|Flex:

a) Sender Facebook account user will never come to know that the message was sent by his/her Facebook ID as there is no history of that Dropped MSG into his/her MSG.
b) Sender user can't prove that the message wasn't sent by his/her end because there is no header stuff like in Mail.

Counter Measure from user End:

a) Register for Facebook username but don't allow the Mail Option which you will get over-there when you will register for it.
b) Hide you Email ID section in about me section of Facebook to make cracker not to fetch your Email ID.
c) Changer your Primary Email ID by other Email ID which you don't use in your daily life. Make one for only Facebook.

Counter Measure from Facebook End:

a) Filter all the incoming messages by the IP or can disallow those messages which are not coming from the trusted server. viz. people often use gmail, yahoo, Hotmail for logging into their facebook account. So It would be very easy for Facebook to figure out which one is coming from the trusted server.

b) What if somebody using his/her own domain like akash@hackersreloaded.com to login into facebook account, in this regard Facebook can simply crawl the real IP of that domain and later on they can figure out whether the mail coming from hackersreloaded server or from other server.

Thanks ☺