Disclaimer:

By reading this document, you agree to the following:

1. **This is just a vulnerability disclosure. I have not saved any information that I have shown in this disclosure.**
2. **The author is not responsible for what you do with this information detailed in this document/pdf.**
3. **I will not be responsible for anything you do with this information.**
4. **Make sure you perform this test using your own ID or test IDs that you have created. Any damages that are performed by you is your responsibility and the author is no way responsible.**
5. **This information is only intended for proof-of-concept / demonstration purpose and not for anything else.**

If you do not agree to the above mentioned clauses, please do not proceed ahead and close the document immediately.

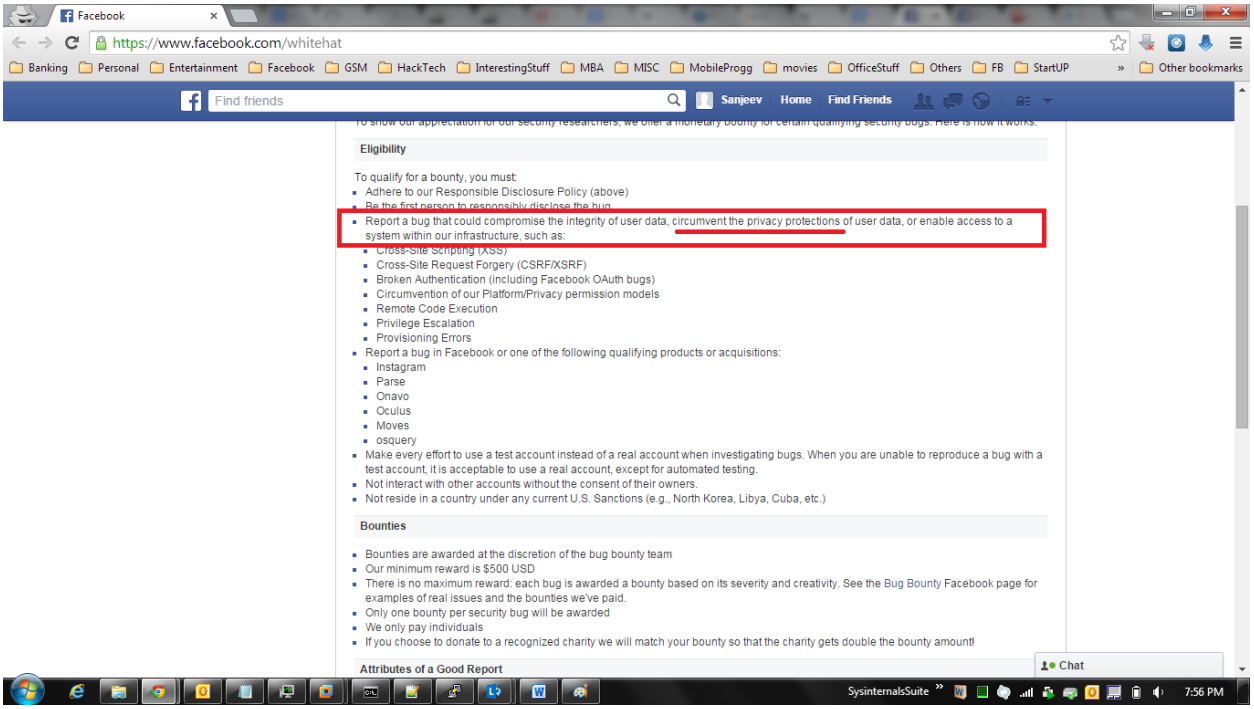
Vulnerability Title: Facebook Graph Search allows brute-forcing of phone numbers.

Vulnerable Site: www.facebook.com

Description: Facebook allows discovery of users via their listed phone number. However no control is present to restrict users from discovering users who have their phone number hidden or restrict to a certain set of people/ users.

Impact: An attacker with a fake account can perform a brute force attack on facebook to harvest users and other details mentioned in their profile and map it with the registered phone numbers.

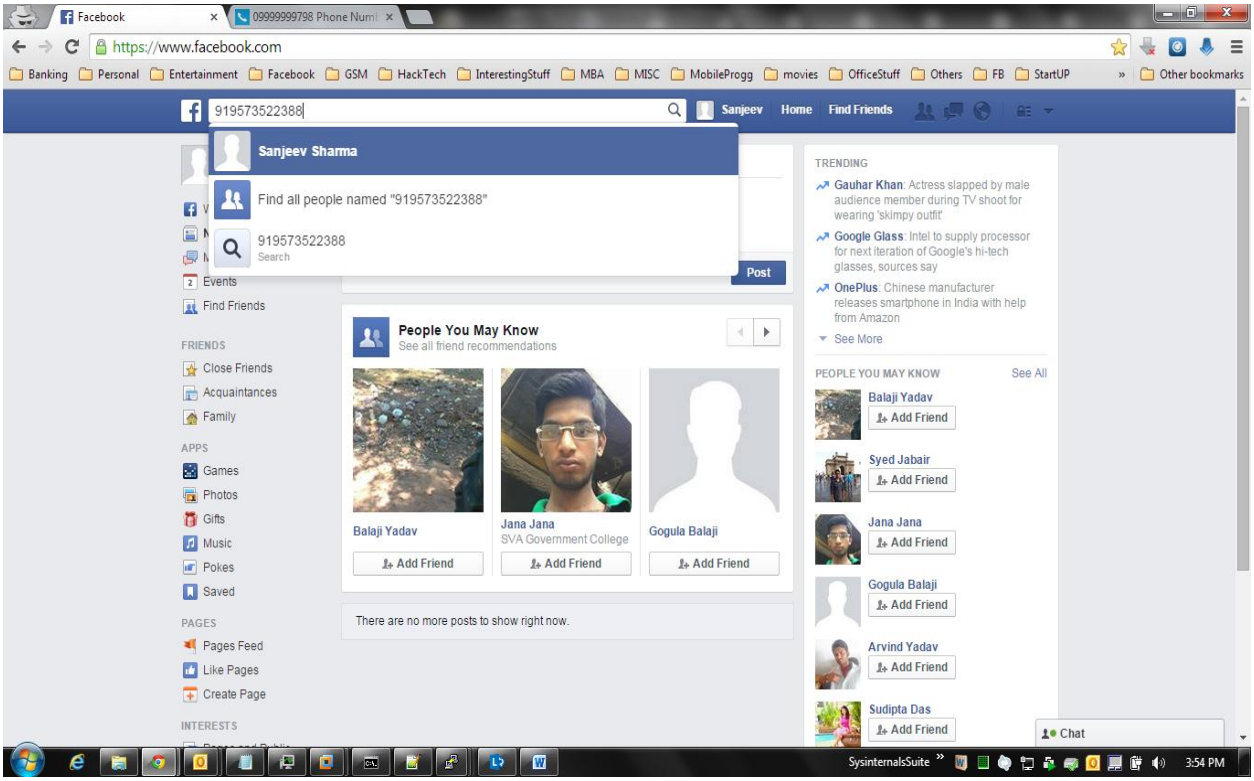
https://www.facebook.com/whitehat



Detailed Description

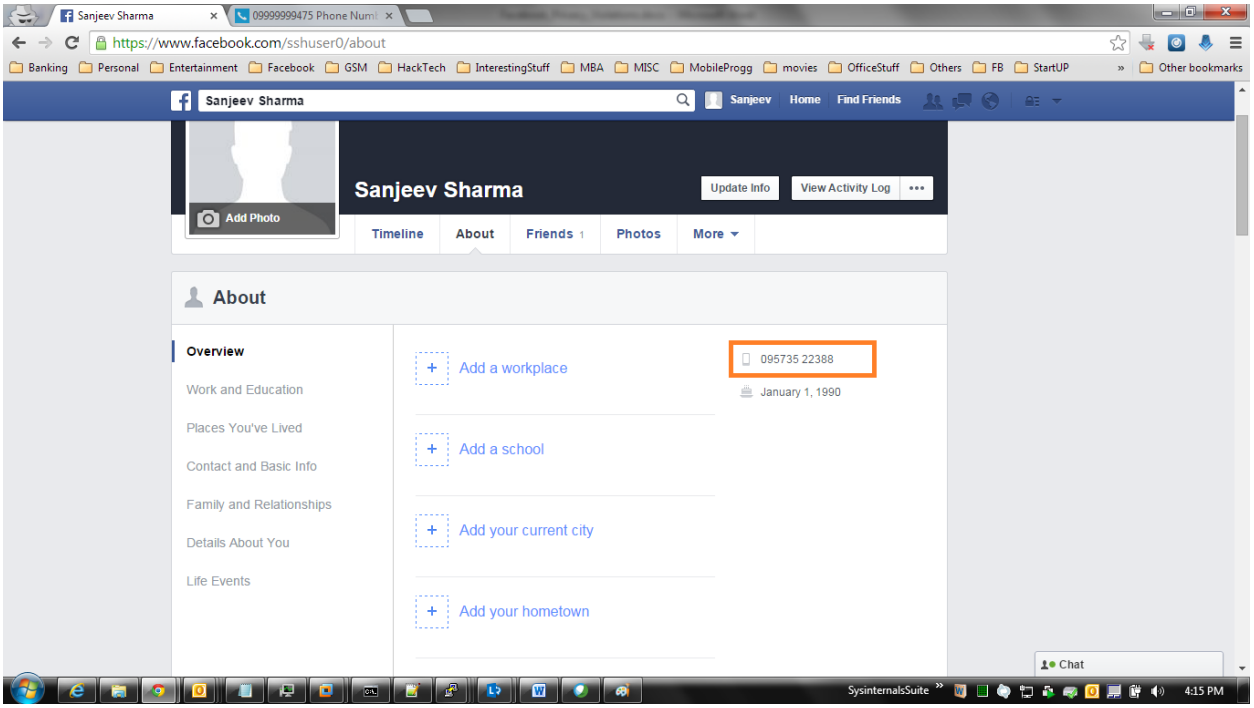
Example where a search of cell number “+91-9573522388” led to discovery of the profile.

Note: In this case, this profile is a fake profile belonging to “Sanjeev Sharma”.


Facebook
https://www.facebook.com
919573522388
Sanjeev Sharma
Find all people named "919573522388"
919573522388
Search
Sanjeev
Home
Find Friends
Post
People You May Know
See all friend recommendations
Balaji Yadav
Add Friend
Jana Jana
SVA Government College
Add Friend
Gogula Balaji
Add Friend
There are no more posts to show right now.
TRENDING
Gauhar Khan: Actress slapped by male audience member during TV shoot for wearing 'skimpy outfit'
Google Glass: Intel to supply processor for next iteration of Google's hi-tech glasses, sources say
OnePlus: Chinese manufacturer releases smartphone in India with help from Amazon
See More
PEOPLE YOU MAY KNOW
See All
Balaji Yadav
Add Friend
Syed Jabair
Add Friend
Jana Jana
Add Friend
Gogula Balaji
Add Friend
Arvind Yadav
Add Friend
Sudipta Das
Add Friend
Chat
FRIENDS
Close Friends
Acquaintances
Family
APPS
Games
Photos
Gifts
Music
Pokes
Saved
PAGES
Pages Feed
Like Pages
Create Page
INTERESTS
Events
Find Friends
SysinternalsSuite
3:54 PM


Sanjeev Sharma
https://www.facebook.com/sshuser0
Sanjeev Sharma
Sanjeev
Home
Find Friends
Add Photo
Update Info
View Activity Log
Timeline
About
Friends
Photos
More
Recent
2014
Born
PEOPLE YOU MAY KNOW
See All
Balaji Yadav
Divakar Kothandan
Shanmuga Sheela Jayakumar
Syed Jabair
Venkata Subhash Muthireddy
Dinesh Jaiswal
Add Friend
ADD PROFILE INFO
Fill out your profile to help you connect with more friends.
Status
Photo / Video
Life Event
What's on your mind?
Chat
SysinternalsSuite
4:13 PM

Upon seeing the “About” section for the specific user (in this case I am viewing the own fake id I created),

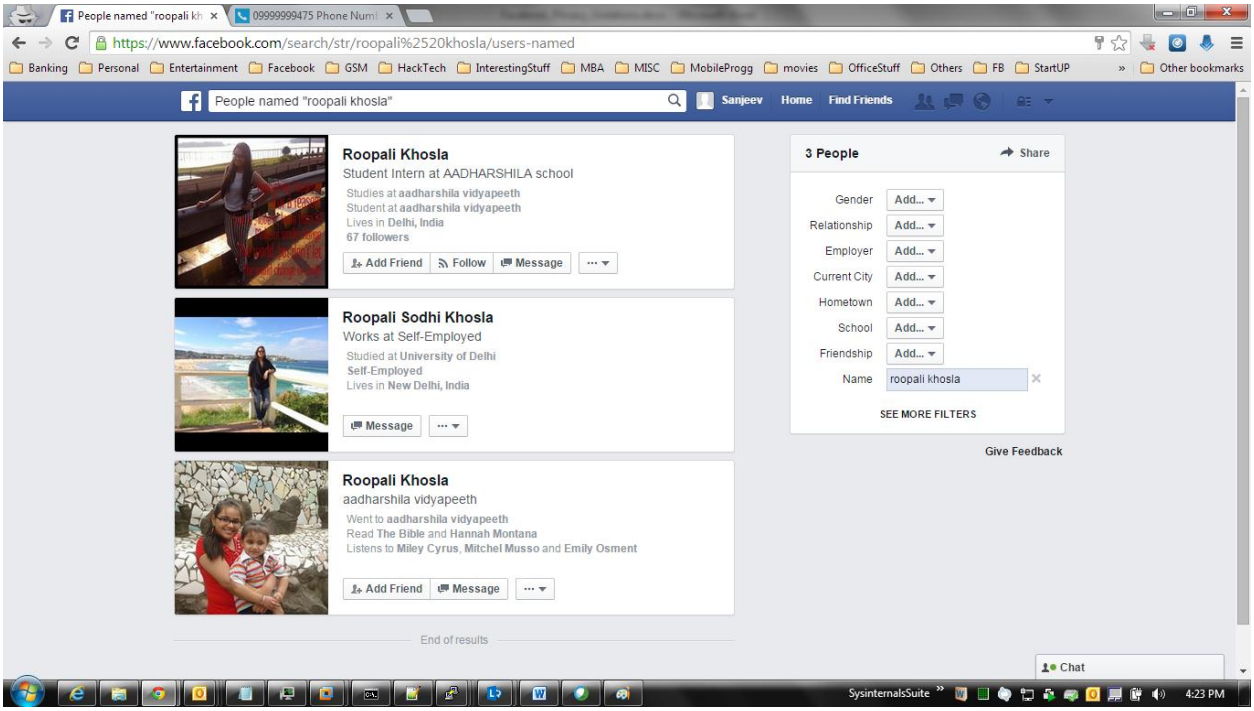


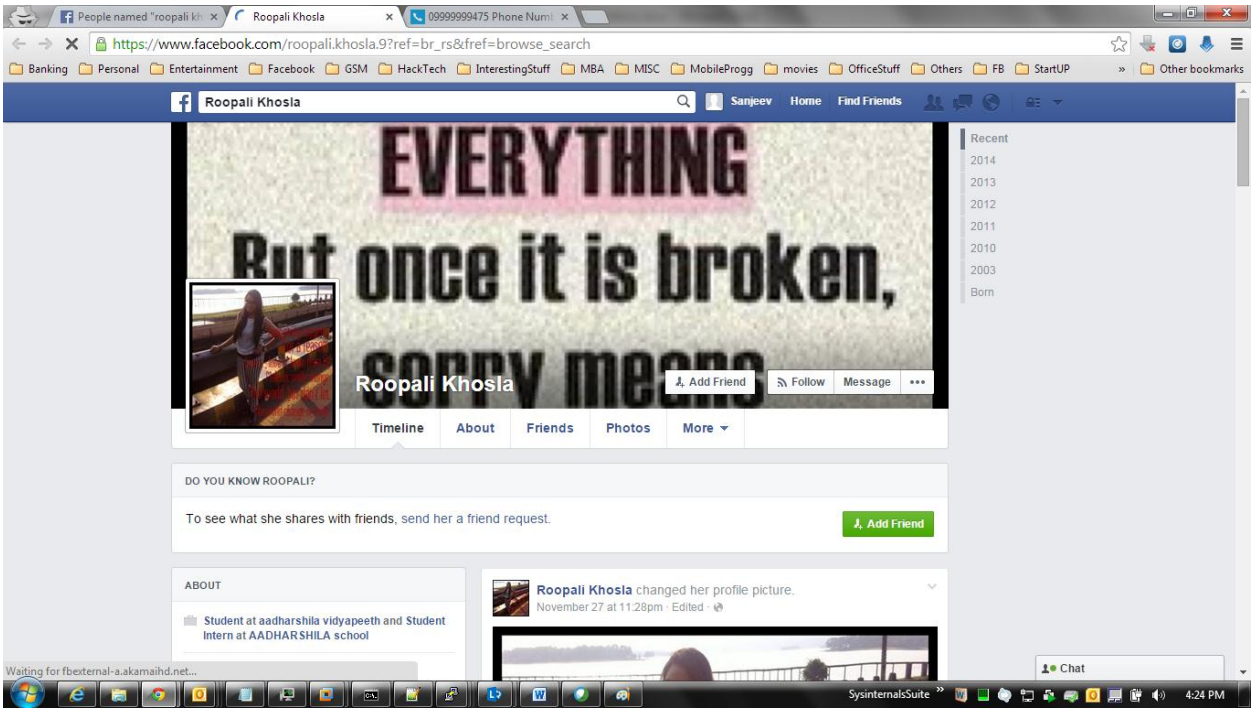
Now let's do it for some random number, say 919999999475 (for which I do not have any access and the number is hidden or private. We will check from the user's profile if the phone number is visible later.)

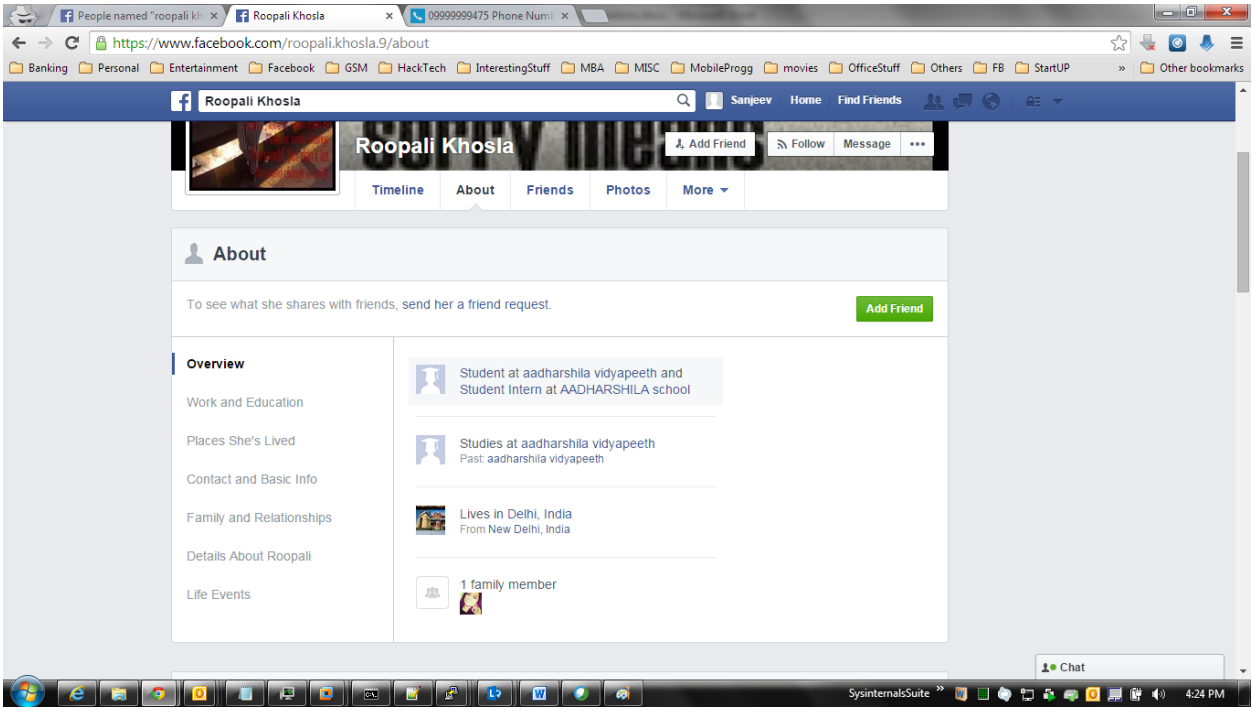
By the brute forcing tool, this phone number belongs to some Roopali Khosla with UID = 100001633806991

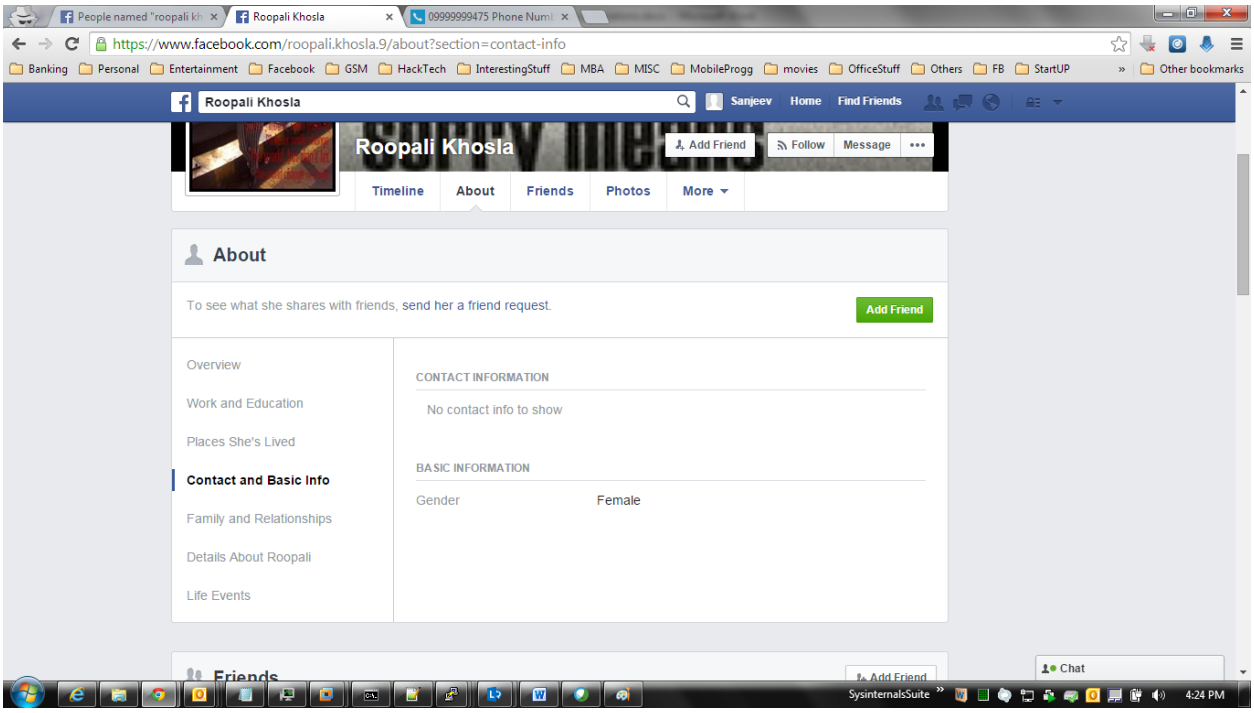
Note: The phone number has been selected randomly.

Now let's check her profile out,


People named "roopali kh
09999999475 Phone Numb
https://www.facebook.com/search/str/roopali%2520khosla/users-named
Banking Personal Entertainment Facebook GSM HackTech InteresingStuff MBA MISC MobileProgg movies OfficeStuff Others FB StartUP Other bookmarks
People named "roopali khosla"
Sanjeev Home Find Friends
Roopali Khosla
Student Intern at AADHARSHILA school
Studies at aadharshila vidyapeeth
Student at aadharshila vidyapeeth
Lives in Delhi, India
67 followers
Add Friend Follow Message
Roopali Sodhi Khosla
Works at Self-Employed
Studied at University of Delhi
Self-Employed
Lives in New Delhi, India
Message
Roopali Khosla
aadharshila vidyapeeth
Went to aadharshila vidyapeeth
Read The Bible and Hannah Montana
Listens to Miley Cyrus, Mitchel Musso and Emily Osment
Add Friend Message
End of results
3 People
Share
Gender Add...
Relationship Add...
Employer Add...
Current City Add...
Hometown Add...
School Add...
Friendship Add...
Name roopali khosla
SEE MORE FILTERS
Give Feedback
Chat
SysinternalsSuite
4:23 PM


People named "roopali kh
Roopali Khosla
09999999475 Phone Numb
https://www.facebook.com/roopali.khosla.9?ref=br_rs&fref=browse_search
Banking Personal Entertainment Facebook GSM HackTech InteresingStuff MBA MISC MobileProgg movies OfficeStuff Others FB StartUP Other bookmarks
Roopali Khosla
Sanjeev Home Find Friends
EVERYTHING
But once it is broken,
Roopali Khosla
Add Friend Follow Message
Timeline About Friends Photos More
Recent
2014
2013
2012
2011
2010
2003
Born
DO YOU KNOW ROOPALI?
To see what she shares with friends, send her a friend request.
Add Friend
ABOUT
Student at aadharshila vidyapeeth and Student Intern at AADHARSHILA school
Roopali Khosla changed her profile picture.
November 27 at 11:28pm · Edited ·
Waiting for fbexternal-a.akamaihd.net...
Chat
SysinternalsSuite
4:24 PM



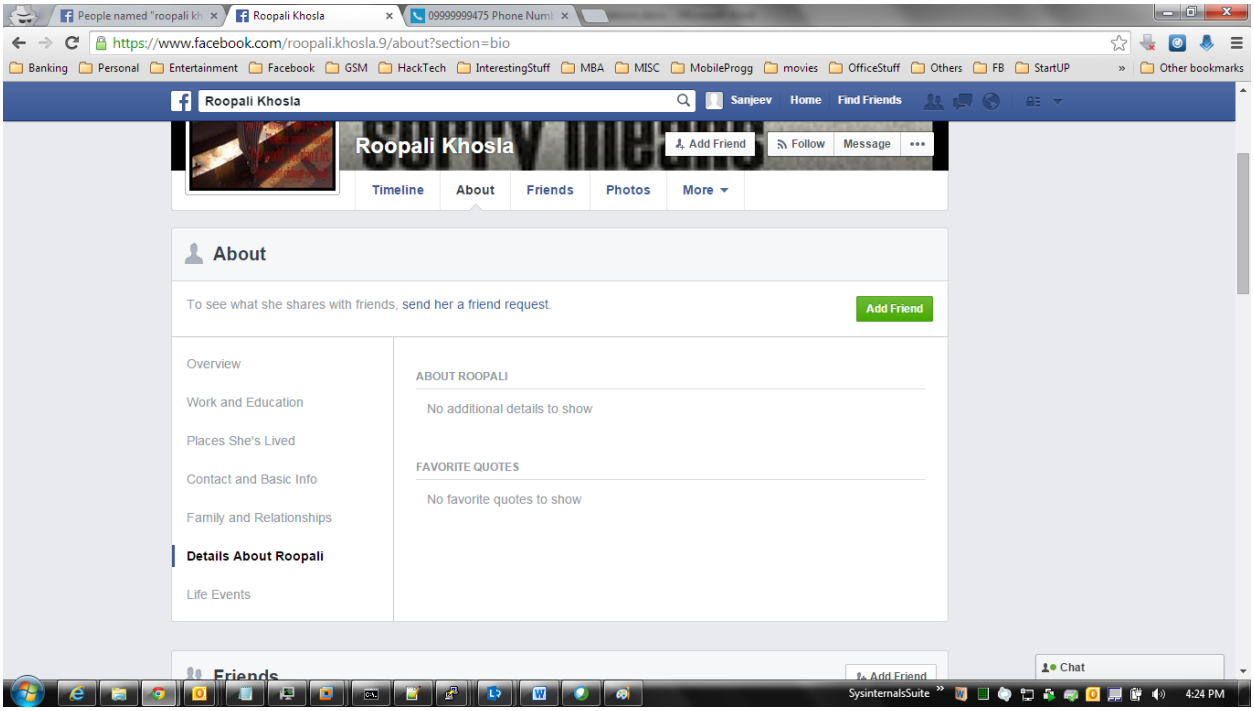


Nope, the phone number is not shown, i.e. Hidden or Private

NOW THIS IS THE ISSUE. Even if she has made her contact details private, it is possible to discover her phone number via Brute forcing.

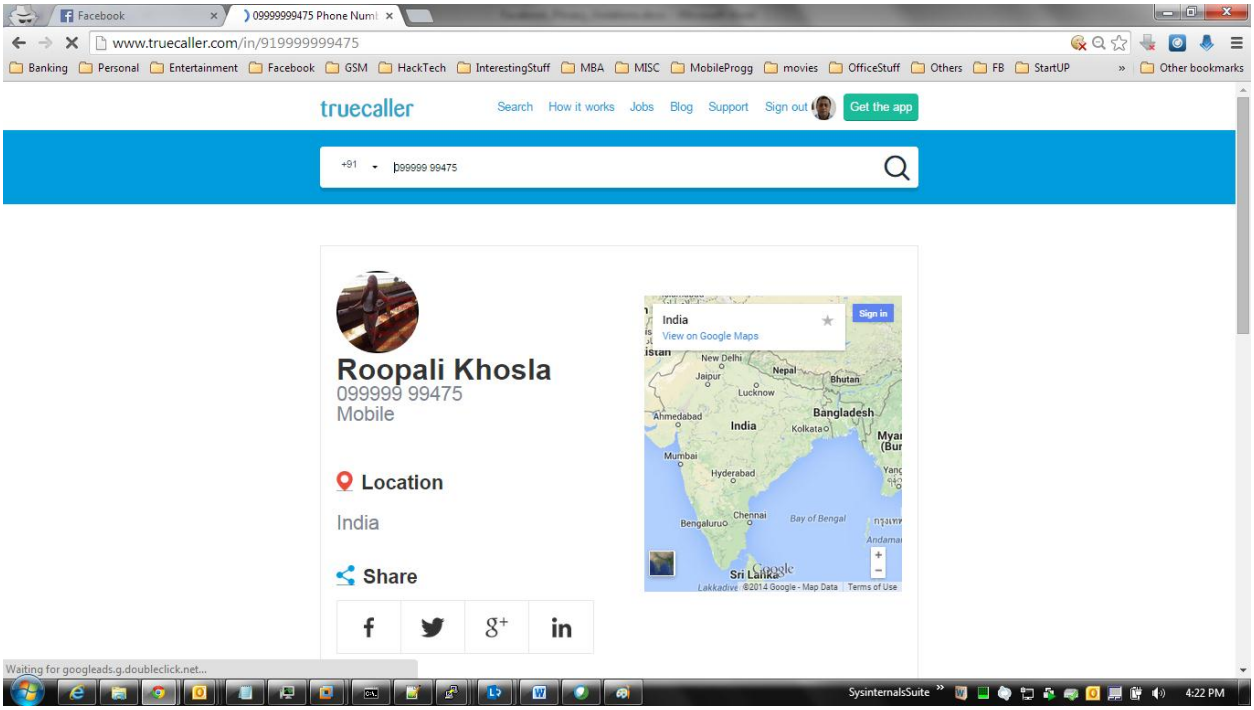
This leakage of data is a breach of privacy

P.S. This attack can aid several types of Social Engineering / Spear phishing attacks on the user.



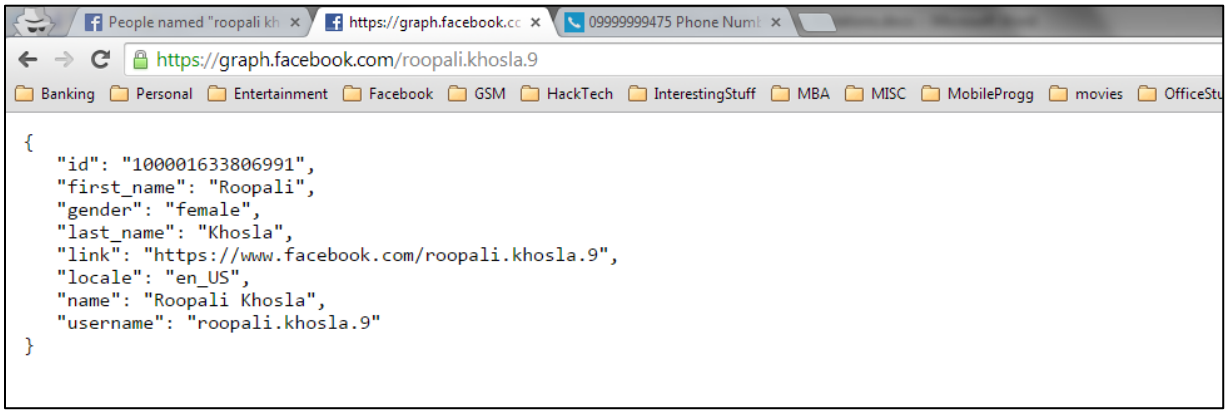
Nothing. Nowhere is the cell phone number “919999999475” listed on her profile.

Let’s see what TrueCaller has to say about this.



Bingo!

Upon getting her profile details from graph request the UID of 100001633806991 also matches.



Now running a script that starts from 919999999999 till 919000000000