

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.

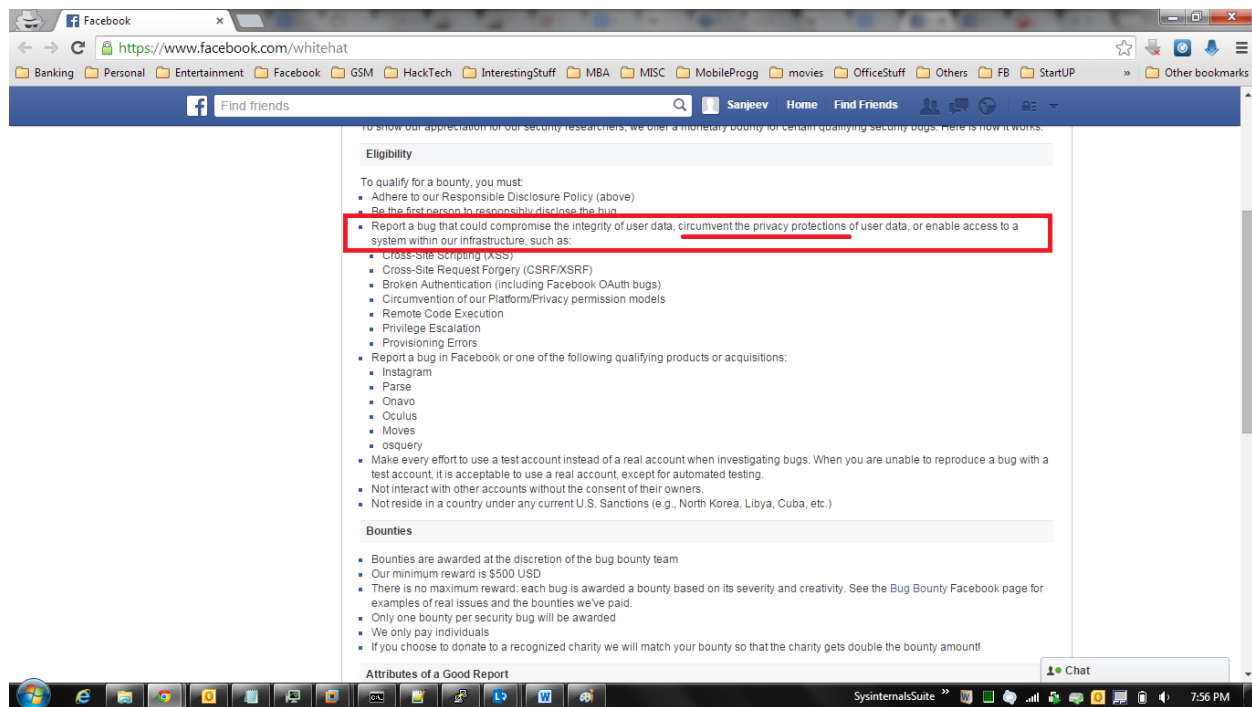
Vulnerability Title: Facebook Graph Search allows brute-forcing of phone numbers.

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.

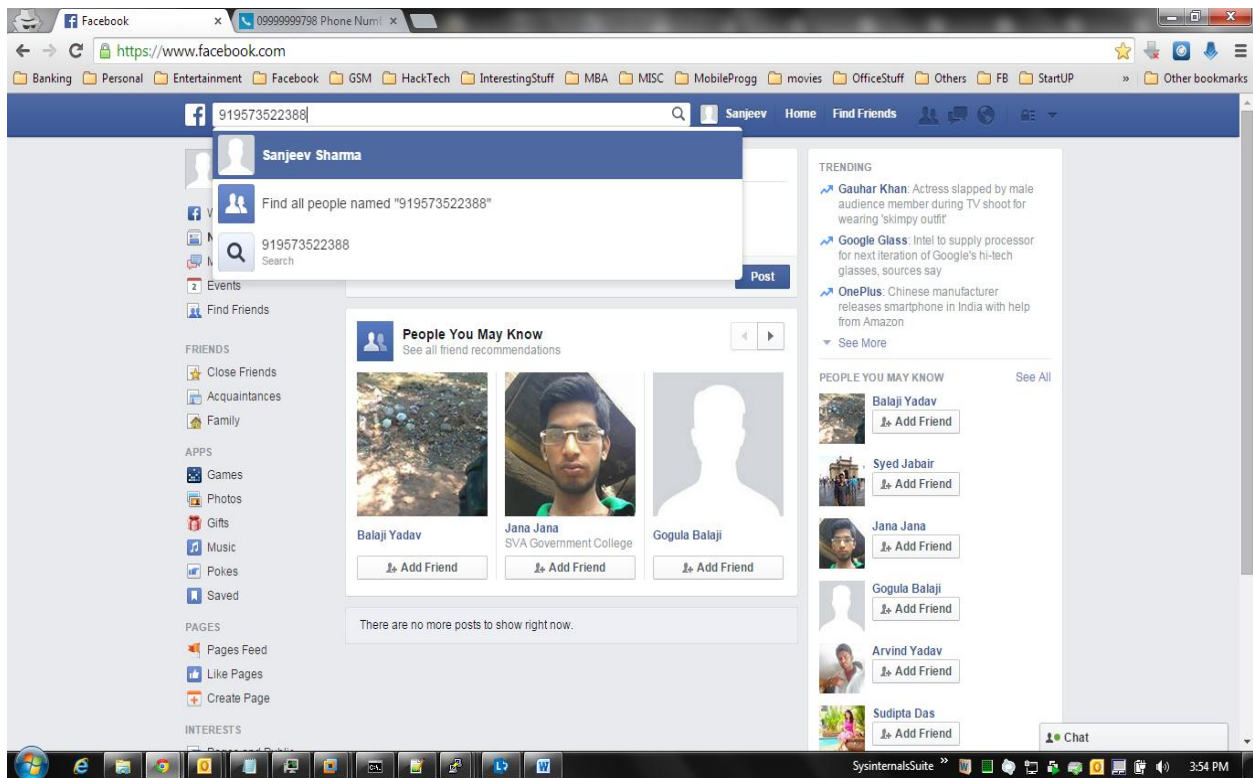
<https://www.facebook.com/whitehat>



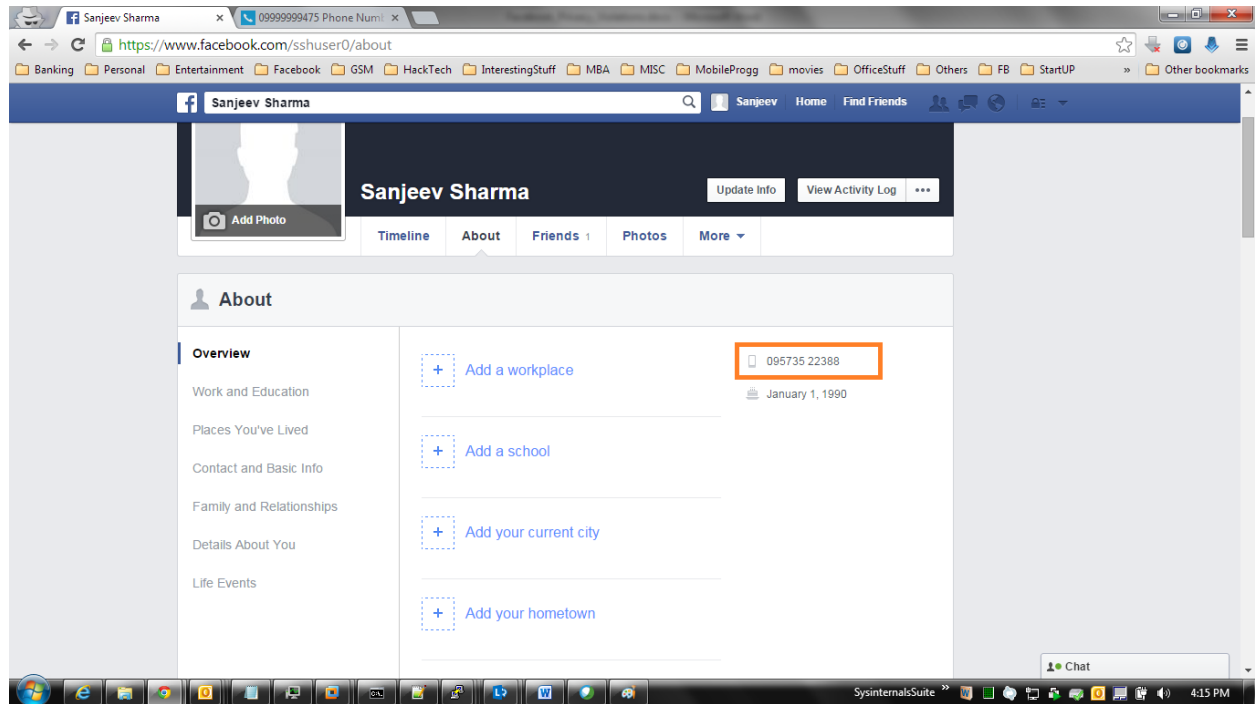
Detailed Description

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”.



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.



```
root@kali: ~/projects/advertisement/extractCellFB
919999999556,100005978880723,Raman Kakkar,www.facebook.com/raman.kakkar.710,
919999999555,100003205292400,Riya Reddy,www.facebook.com/riya.reddy.37,100002954679486,Krishna Joshi,www.facebook.com/krishna.joshi.98499,100003289785584,Bindass Banda,
www.facebook.com/bindass.banda1,
919999999554,10000562372126,Annu Hemant Malhotra,www.facebook.com/hemantmalhotra01,
919999999553,100001058593325,Ramandeep Singh,www.facebook.com/rattanhose,
919999999552,100001566031265,Manisha Chhabra,www.facebook.com/manisha.chhabra.5,
919999999549,100004224344938,Ravi Mahajan,www.facebook.com/ravi.mahajan.3192,
919999999543,612130203,Ayaan Sharma,www.facebook.com/ayaan.sharma.14606,
919999999541,100000305060457,Mk Bansal,www.facebook.com/mk.bansal.73,
919999999538,100001682941714,Rishi Saha,www.facebook.com/rishi.saha.18,100006015079321,Ametheus Ametheus,www.facebook.com/profile.php?id=100006015079321,
919999999536,591963484,Noni Bhamhani,www.facebook.com/noni.bhamhani,
919999999534,532491807,Bhavya Bhamhani,www.facebook.com/bhamhani,
919999999533,100004247987717,Rakesh Tyagi,www.facebook.com/rakesh.tyagi.319,
919999999532,100001554445904,Prayansh Gupta,www.facebook.com/prayansh.gupta.71,
919999999529,100004101851811,Rishabh Malhotra,www.facebook.com/rishabh.malhotra.7758,
919999999525,100002752151950,Mehala Sherin,www.facebook.com/mehala.sherin,
919999999523,1374341624,Kunal Arora,www.facebook.com/mikikunal,100003059852309,Rongfa'z Punk Dudes,www.facebook.com/punk.tyson1,
919999999521,786138085,Akshat Bais,www.facebook.com/akshatbais,
919999999517,640447540,Udit Garg,www.facebook.com/profile.php?id=640447540,
919999999505,100002428959779,Aakansha Aggarwal,www.facebook.com/aakansha.aggarwal.7,
919999999503,1159444288,Shivang Goel,www.facebook.com/shivangoel,
919999999494,1591576198,Amrit Bawa,www.facebook.com/amritb,
919999999490,100007674639364,Nalini Joshi,www.facebook.com/nalini.joshi.796,
919999999488,100003122990961,Satish Chandra,www.facebook.com/satish.chandra.3192,
919999999485,100001011849524,Kabir Khurana,www.facebook.com/kabir.khurana.18,
919999999483,100004020577564,Amit Saxena,www.facebook.com/profile.php?id=100004020577564,
919999999482,1171015914,Vishal Gautam,www.facebook.com/vishalgautam.vg,
919999999477,614315338,Kanika Khurana,www.facebook.com/kanika.khurana.737,
919999999475,100001633806991,Roopali Khosla,www.facebook.com/roopali.khosla.9,
919999999473,100000149954464,Dharam Choudhary,www.facebook.com/dharam.choudhary.52,
919999999472,100001883366871,Ashish Sehrawat,www.facebook.com/ashish.sehrawat.73,
919999999470,100000105655408,Tarun Bhatnagar,www.facebook.com/tkbhatnagar,
919999999465,1291541637,Suren Kush,www.facebook.com/suren.kush,
919999999460,100000306104040,Tej Choudhary,www.facebook.com/dev.choudhary2,
919999999458,516483475,Pranav Nagpal,www.facebook.com/pranav.nagpal.9,
919999999456,10000088880909,Karan Bajwa,www.facebook.com/karan.bajwa.77128,
919999999454,10000256711323,Varun Jain,www.facebook.com/varunargham,
919999999450,738665885,Vijay Nagpal,www.facebook.com/vijay.nagpal1,
919999999444,100002055072767,Sumit Kukreja,www.facebook.com/sumit.kukreja.56,1244653337,Naveen Gupta,www.facebook.com/naveen.gupta.94009,
919999999443,100001542998053,Kartik Narayan,www.facebook.com/kartik.narayan.7,
919999999442,100001723335117,Vivek Yadav,www.facebook.com/profile.php?id=100001723335117,
919999999439,100001042480956,Akshay Arora,www.facebook.com/akshay.arora.754,
919999999438,512527180,Luv I,www.facebook.com/luvirani,
root@kali:~/projects/advertisement/extractCellFB#
```

Now let's check her profile out,

People named "roopali kh" x 09999999475 Phone Numl x

https://www.facebook.com/search/str/roopali%2520khosla/users-named

Banking Personal Entertainment Facebook GSM HackTech InterestingStuff MBA MSC MobileProgg movies OfficeStuff Others FB StartUP Other bookmarks

People named "roopali khosla"

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

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

End of results

Chat

SysinternalsSuite 4:23 PM

People named "roopali kh" x Roopali Khosla x 09999999475 Phone Numl x

https://www.facebook.com/roopali.khosla.9?ref=br_rs&fref=browse_search

Banking Personal Entertainment Facebook GSM HackTech InterestingStuff MBA MSC MobileProgg movies OfficeStuff Others FB StartUP Other bookmarks

Roopali Khosla

Sanjeev Home Find Friends

EVERYTHING
But once it is broken,
sorry means

Roopali Khosla
Add Friend Follow Message

Timeline About Friends Photos More

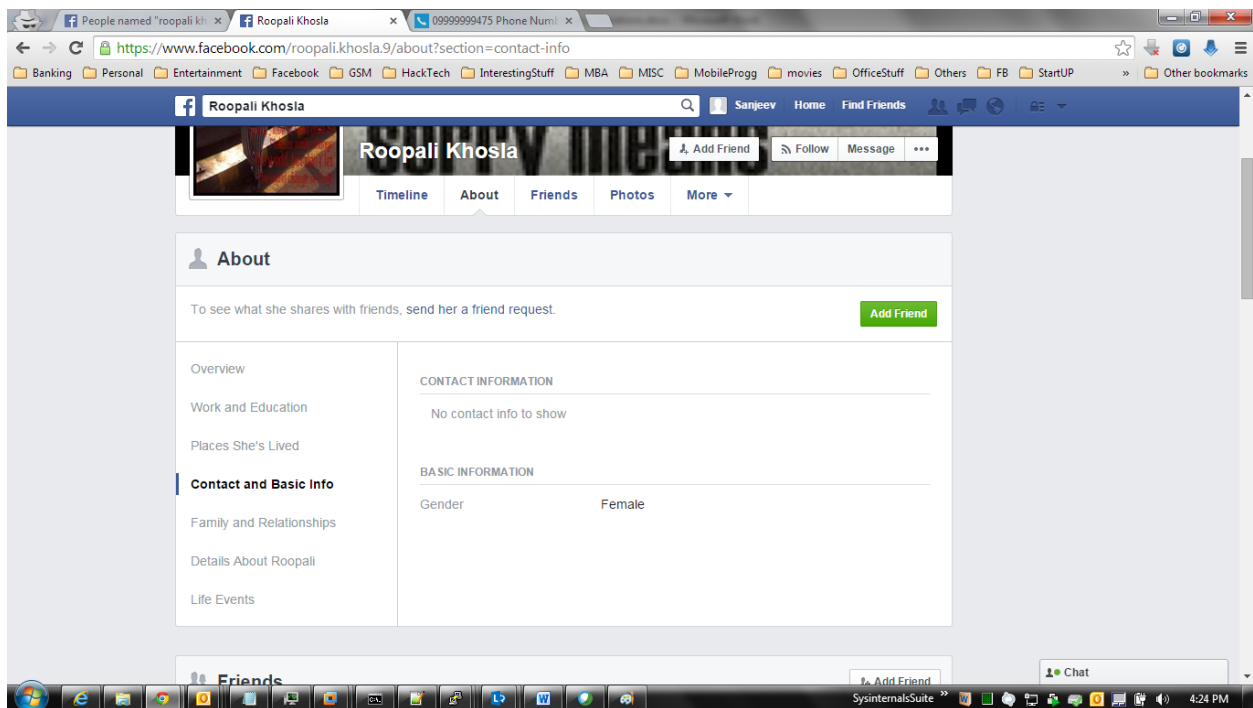
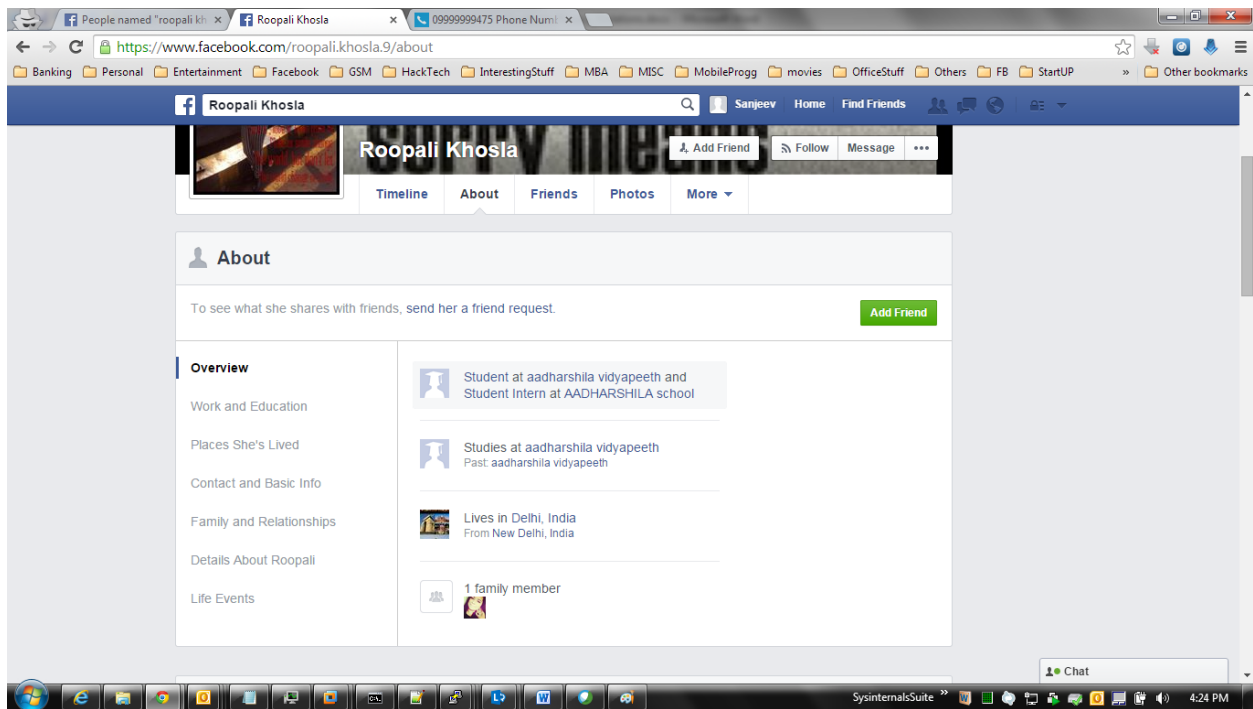
DO YOU KNOW ROOPALI?
To see what she shares with friends, send her a friend request.
Add Friend

ABOUT
Student at aadharshila vidyapeeth and Student Intern at AADHARSHILA school

Roopali Khosla changed her profile picture.
November 27 at 11:28pm · Edited ·

Chat

SysinternalsSuite 4:24 PM

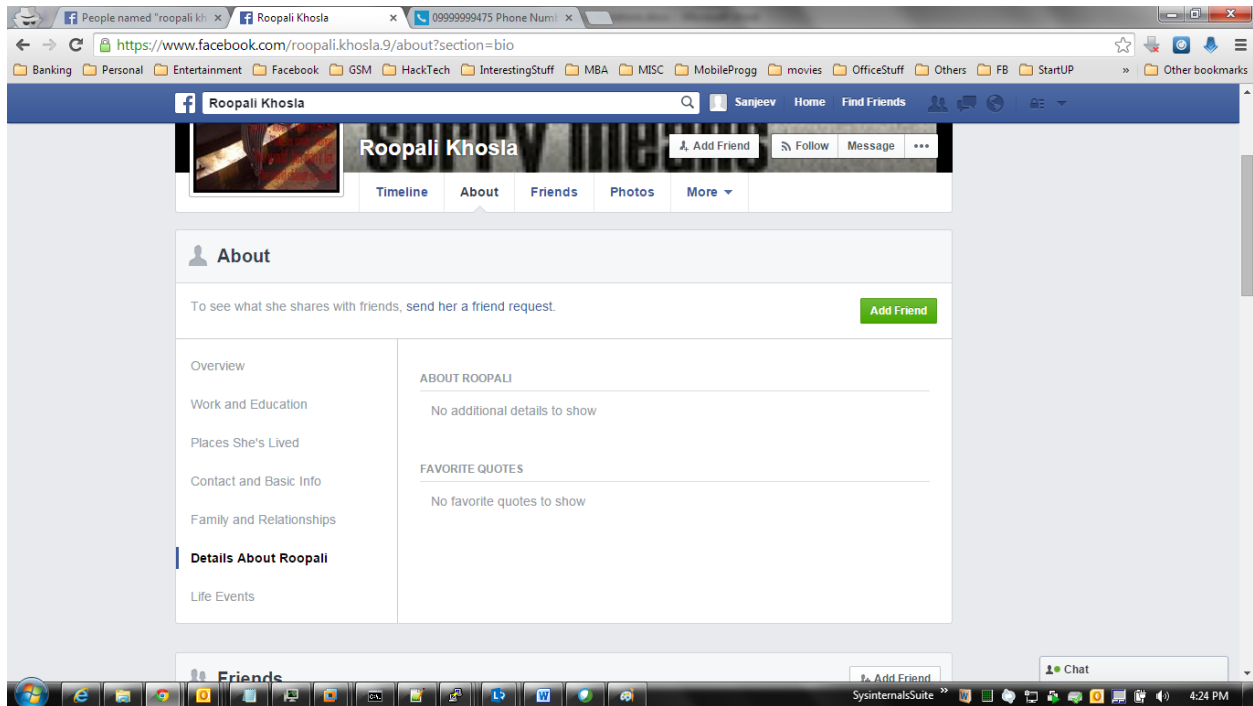


Nope, the phone number is not shown, i.e. Hidden or Private

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.

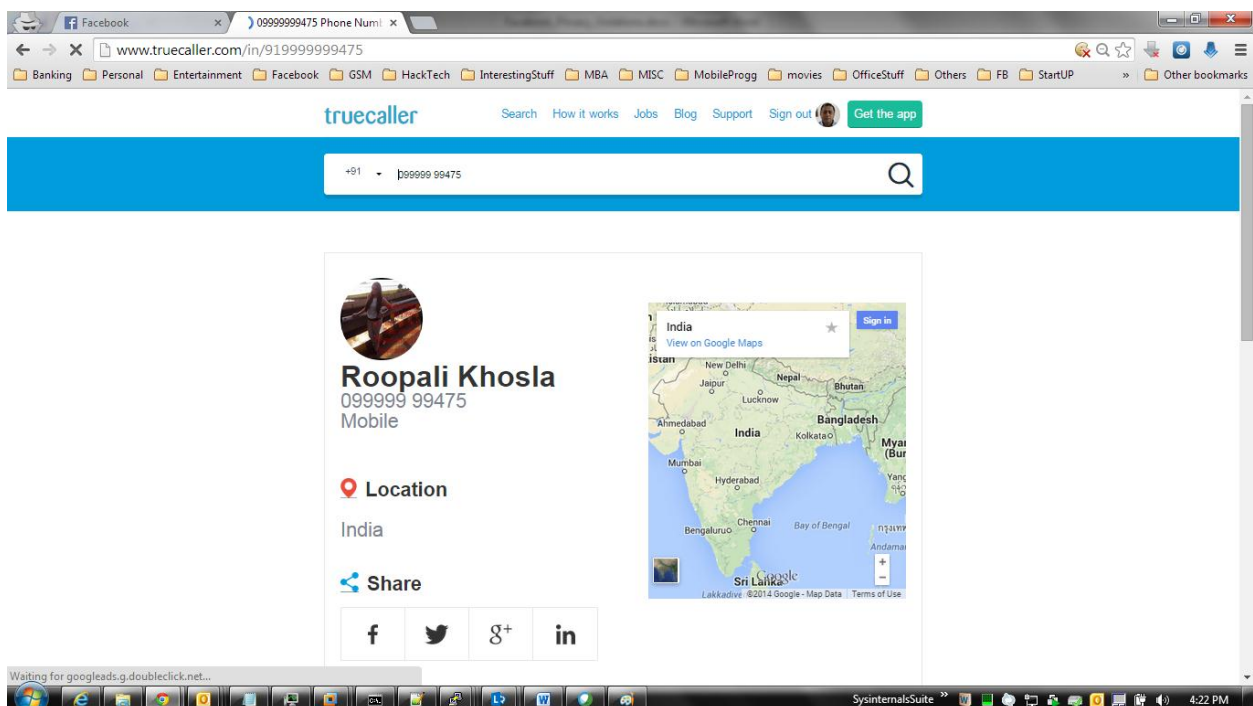
This leakage of data is a breach of privacy

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.



```
{
  "id": "100001633806991",
  "first_name": "Roopali",
  "gender": "female",
  "last_name": "Khosla",
  "link": "https://www.facebook.com/roopali.khosla.9",
  "locale": "en_US",
  "name": "Roopali Khosla",
  "username": "roopali.khosla.9"
}
```

Now running a script that starts from 919999999999 till 919000000000



```
root@kali: ~/projects/advertisement/extractCellFB
919999999784,1224031308,Rohit Mehta,www.facebook.com/rohit.mehta.5036,
919999999782,100002095105578,Sagar Gupta,www.facebook.com/sagar.nsui,
919999999781,1642098692,Himanshu Gupta,www.facebook.com/himanshu.gupta.75641,
919999999779,10000542290703,Saanya Bansal,www.facebook.com/saanya.bansal,
919999999777,100001209663351,Pulkit Puri,www.facebook.com/pulkit.puri.16,
919999999776,100002707322938,Talha Khaliq,www.facebook.com/talhakhaliq6,
919999999774,100006802955783,Gurpreet Singh,www.facebook.com/profile.php?id=100006802955783,
919999999773,1818369719,Sanjay Goel,www.facebook.com/sanjay.goel.562,
919999999772,1452234139,Siddhant Jain,www.facebook.com/siddhant.jain.406,
919999999771,1240676289,Rohit Kumar Jha,www.facebook.com/rohitkumarjha771,
919999999770,513132199,Rohit Mehta,www.facebook.com/rohit.mehta.5268,
919999999768,100001574941306,Vikas Titoria,www.facebook.com/vikas.titoria,
919999999766,100000900309657,Khusroo Malik,www.facebook.com/khusroo.malik,
919999999764,100006708962326,Aman Somin Dhanos,www.facebook.com/amanjeet.dhanos,
919999999759,769224271,Kishore Gambhir,www.facebook.com/kishore.gambhir,
919999999757,1597855570,Viren Kaushik,www.facebook.com/viren.kaushik.3,
919999999752,10000023204357,Hemant Aneja,www.facebook.com/hemant.aneja.92,
919999999750,1338833910,Sheel Vardhan Choubey,www.facebook.com/sheel.choubey,
919999999738,100000333390259,Mehar Kapur,www.facebook.com/mehar.kapur.3,
919999999734,100001450391023,Rohini Sharma Maheshwari,www.facebook.com/rohini.sharmamaheshwari,
919999999729,1012784222,Gaurav Sonu,www.facebook.com/gauravgarg.luv,
919999999728,100002378362614,Ravinder Yadav,www.facebook.com/ravinder.yadav.5811,
919999999727,601805510,Kumar Kartikay,www.facebook.com/kkartikay,
919999999725,100001255697527,Varun Kumar,www.facebook.com/varun.kumar.338,
919999999723,585034029,Gaurav Mathur,www.facebook.com/gaurav.mathur.5243,
919999999714,1031284986,Santosh Kumar,www.facebook.com/profile.php?id=1031284986,
919999999709,100000325390072,Arun Sikri,www.facebook.com/arun.sikri,
919999999708,100001075141591,Hitesh Kumar Sharma,www.facebook.com/hiteshkumar.sharma.9,
919999999706,100003324686614,Aaban Aqil Khan,www.facebook.com/aaban.a.khan.7,
919999999705,100006379961133,Tahir Kamal,www.facebook.com/tahir.kamal.3954,
919999999704,100006286803357,Navdeep Yadav,www.facebook.com/navdeep.yadav.330,
919999999699,100003039987978,Satish Bhanushali,www.facebook.com/satish.bhanushali2,100002823330617,Vadhiya Nency,www.facebook.com/vadhiya.nency,
919999999698,100001819412265,Abhishek Kaushik,www.facebook.com/abhishek.kaushik.96343,
919999999697,515796546,Ajit Shah,www.facebook.com/ajitss,
919999999696,100000104252927,Sahil Verma,www.facebook.com/yuvrajverma.verma,
919999999693,100004151109988,Pradeep Sharma,www.facebook.com/profile.php?id=100004151109988,
919999999691,100002923480666,Anil Gehlot,www.facebook.com/pusahotels,
919999999687,1820169758,Dipansh Bhasin,www.facebook.com/dipansh.bhasin,
919999999685,700705664,Rajan Yadav,www.facebook.com/rajan.yadav.9619,
919999999679,651917512,Ravi Saxena,www.facebook.com/profile.php?id=651917512,
919999999677,10000519053529,Jatin Seth,www.facebook.com/jatin.seth.1276,
919999999675,100000603372763,Avinash Chandel,www.facebook.com/avinash.chandel.180,
919999999672,100001776489808,Praveen Singh,www.facebook.com/praveensinghici,ci,
```