

**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.**

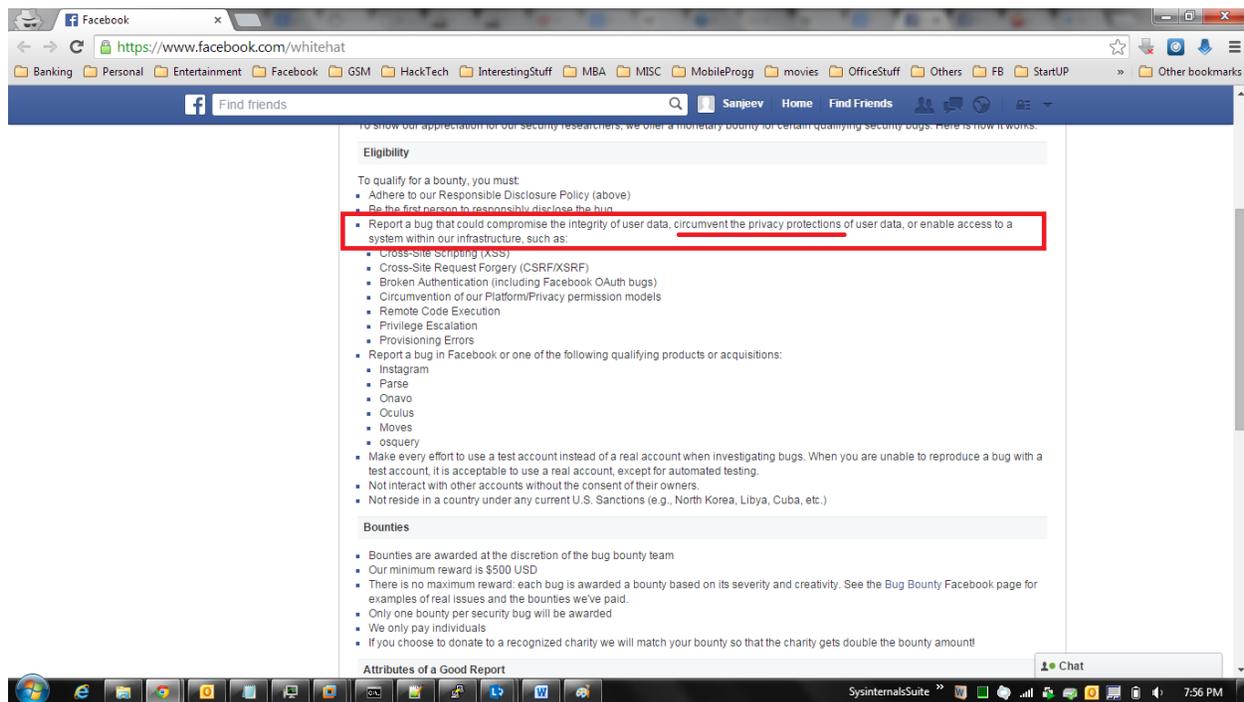
**Vulnerability Title:** Facebook Graph Search allows brute-forcing of phone numbers.

**Vulnerable Site:** [www.facebook.com](http://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 | 0999999798 Phone Num |

https://www.facebook.com

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

Sanjeev Home Find Friends

Sanjeev Sharma

Find all people named "919573522388"

919573522388 Search

Events Find Friends

FRIENDS

- Close Friends
- Acquaintances
- Family

APPS

- Games
- Photos
- Gifts
- Music
- Pokes
- Saved

PAGES

- Pages Feed
- Like Pages
- Create Page

INTERESTS

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

3:54 PM

Sanjeev Sharma | 09999999475 Phone Num |

https://www.facebook.com/sshuser0

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

Sanjeev Home Find Friends

Sanjeev Sharma

Update Info View Activity Log

Timeline About Friends Photos More

PEOPLE YOU MAY KNOW

See All

 Balaji Yadav Add Friend	 Divakar Kobhandan Add Friend	 Shanmuga Sheela Jayakumar Add Friend	 Syed Jabair Add Friend	 Venkata Subhash Murthyreddy Add Friend	 Dinesh Jaishwal Add Friend
---	--	--	--	--	--

ADD PROFILE INFO

Fill out your profile to help you connect with more friends.

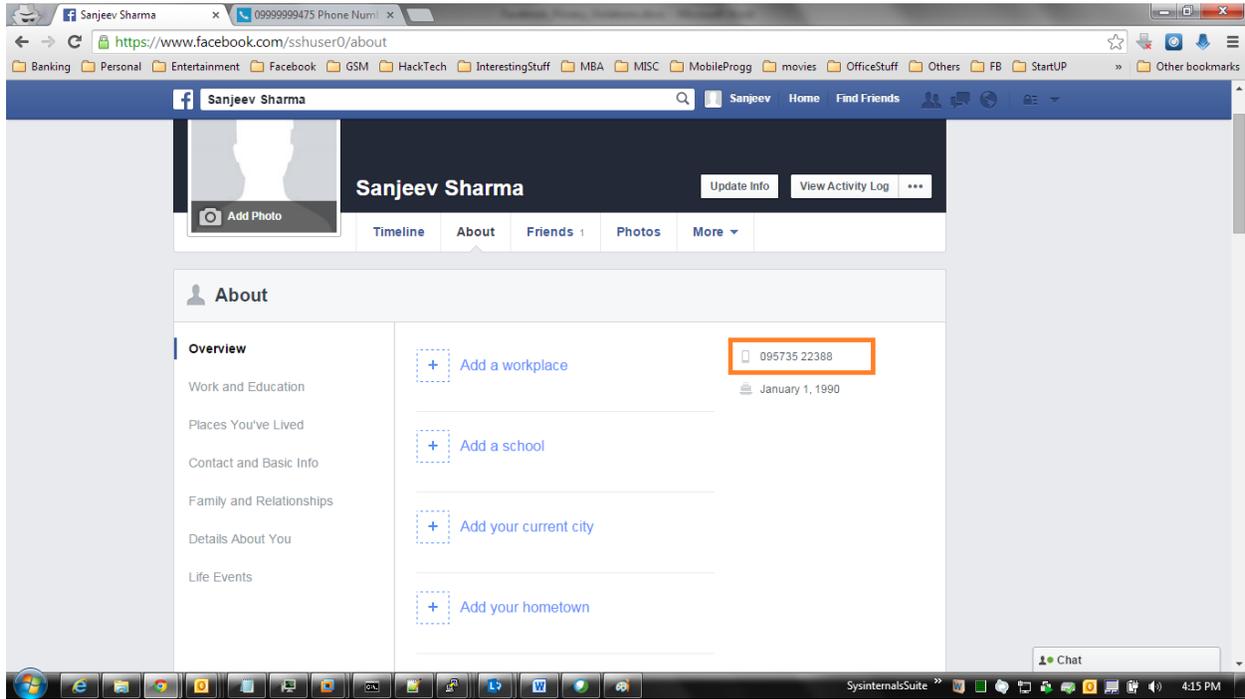
Status Photo / Video Life Event

What's on your mind?

Chat

4:13 PM

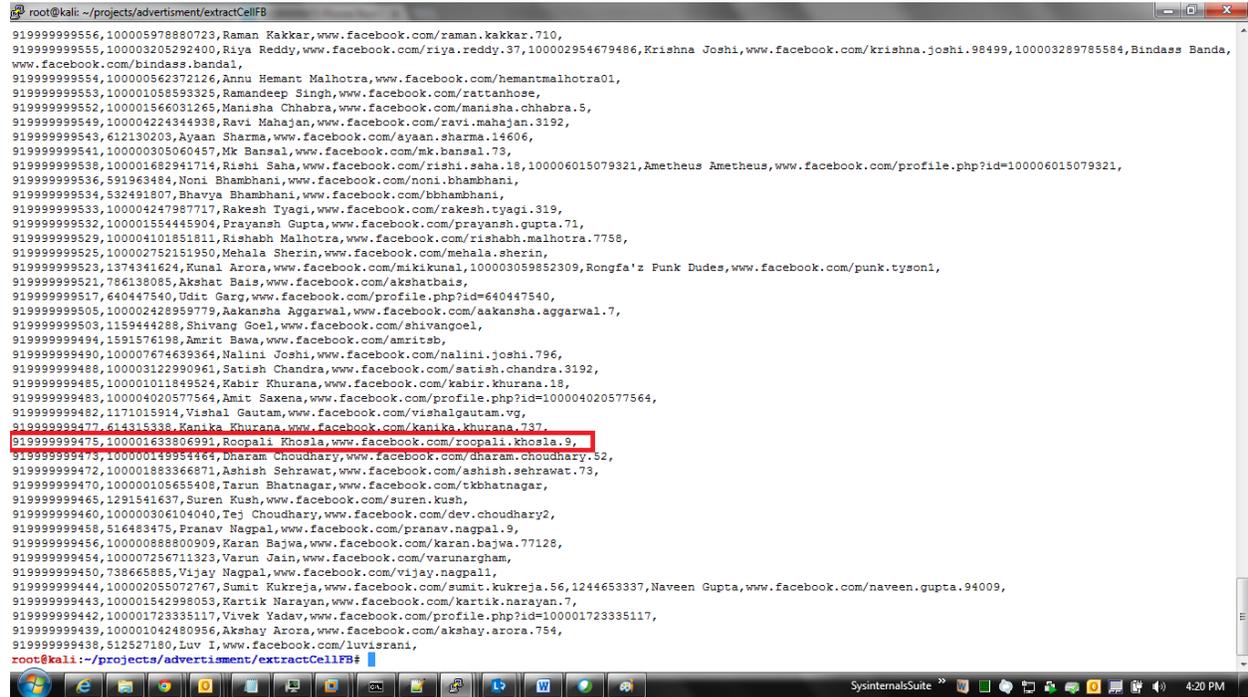
Upon seeing the "About" section for the specific user (in this case I am viewing the own fake id I created),



Now let's do it for some random number, say 91999999475 (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
91999999556,100005978880723,Raman Kakkar,www.facebook.com/raman.kakkar.710,
91999999555,100003205292400,Riya Reddy,www.facebook.com/riya.reddy.37,100002954679486,Krishna Joshi,www.facebook.com/krishna.joshi.98499,100003289785584,Bindass Banda,
www.facebook.com/bindass.banda,
91999999554,10000562372126,Annu Hemant Malhotra,www.facebook.com/hemantmalhotra01,
91999999553,100001058593325,Ramandeep Singh,www.facebook.com/rattanhose,
91999999552,100001566031265,Manisha Chhabra,www.facebook.com/manisha.chhabra.5,
91999999549,100004224344938,Ravi Mahajan,www.facebook.com/ravi.mahajan.3192,
91999999543,612130203,Ayaan Sharma,www.facebook.com/ayaan.sharma.14606,
91999999541,100000305060457,Mk Bansal,www.facebook.com/mk.bansal.73,
91999999538,100001682941714,Rishi Saha,www.facebook.com/rishi.saha.18,100006015079321,Ametheus Amethus,www.facebook.com/profile.php?id=100006015079321,
91999999536,591963484,Noni Bhamhani,www.facebook.com/noni.bhamhani,
91999999534,532491807,Bhavya Bhamhani,www.facebook.com/bhamhani,
91999999533,100004247987717,Rakesh Tyagi,www.facebook.com/rakesh.tyagi.319,
91999999532,100001554445904,Prayansh Gupta,www.facebook.com/prayansh.gupta.71,
91999999529,100004101851811,Rishabh Malhotra,www.facebook.com/rishabh.malhotra.7758,
91999999525,100002752151950,Mehala Sherin,www.facebook.com/mehala.sherin,
91999999523,1374341624,Kunal Arora,www.facebook.com/mkikunal,100003059852309,Rongfa'z Punk Dudes,www.facebook.com/punk.tyson1,
91999999521,786138085,Akshat Bais,www.facebook.com/akshatbais,
91999999517,640447540,Udit Garg,www.facebook.com/profile.php?id=640447540,
91999999505,100002428959779,Aakansha Aggarwal,www.facebook.com/aakansha.aggarwal.7,
91999999503,1159444288,Shivang Goel,www.facebook.com/shivangoel,
91999999494,1591576199,Amit Bawa,www.facebook.com/amitb,
91999999490,100007674639364,Nalini Joshi,www.facebook.com/nalini.joshi.796,
91999999488,100003122990961,Satish Chandra,www.facebook.com/satish.chandra.3192,
91999999485,100001011849524,Kabir Khurana,www.facebook.com/kabir.khurana.18,
91999999483,100004020577564,Amit Saxena,www.facebook.com/profile.php?id=100004020577564,
91999999482,1171015914,Vishal Gautam,www.facebook.com/vishalgautam.vg,
91999999477,614315338,Kanika Khurana,www.facebook.com/kanika.khurana.737,
91999999475,100001633806991,Roopali Khosla,www.facebook.com/roopali.khosla.9,
91999999473,100000149954464,Dharam Choudhary,www.facebook.com/dharam.choudhary.52,
91999999472,100001883366871,Ashish Sehrawat,www.facebook.com/ashish.sehrawat.73,
91999999470,100000105658408,Tarun Bhatnagar,www.facebook.com/tkhatnagar,
91999999465,1291541837,Suren Kush,www.facebook.com/suren.kush,
91999999460,100000306104040,Tej Choudhary,www.facebook.com/dev.choudhary2,
91999999458,516483475,Pranav Nagpal,www.facebook.com/pranav.nagpal.9,
91999999456,100000888800909,Karan Bajwa,www.facebook.com/karan.bajwa.77128,
91999999454,100007256711323,Varun Jain,www.facebook.com/varunargham,
91999999450,738665885,Vijay Nagpal,www.facebook.com/vijay.nagpal,
91999999444,100002055072767,Sumit Kukreja,www.facebook.com/sumit.kukreja.56,1244653337,Naveen Gupta,www.facebook.com/naveen.gupta.94009,
91999999443,100001542998053,Kartik Narayan,www.facebook.com/kartik.narayan.7,
91999999442,100001723335117,Vivek Yadav,www.facebook.com/profile.php?id=100001723335117,
91999999439,100001042480956,Akshay Arora,www.facebook.com/akshay.arora.754,
91999999438,512527180,Luv I,www.facebook.com/luvizrani,
root@kali:~/projects/advertisement/extractCellFB
```

Now let's check her profile out,

People named "roopali kh" x 0999999475 Phone Numi x

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

Banking Personal Entertainment Facebook GSM HackTech InterestingStuff MBA MISC MobileProg 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 X

SEE MORE FILTERS

Give Feedback

End of results

Chat

4:23 PM

People named "roopali kh" x Roopali Khosla x 0999999475 Phone Numi x

https://www.facebook.com/roopali.khosla.9?ref=br\_rs&fref=browse\_search

Banking Personal Entertainment Facebook GSM HackTech InterestingStuff MBA MISC MobileProg movies OfficeStuff Others FB StartUP Other bookmarks

Roopali Khosla



**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

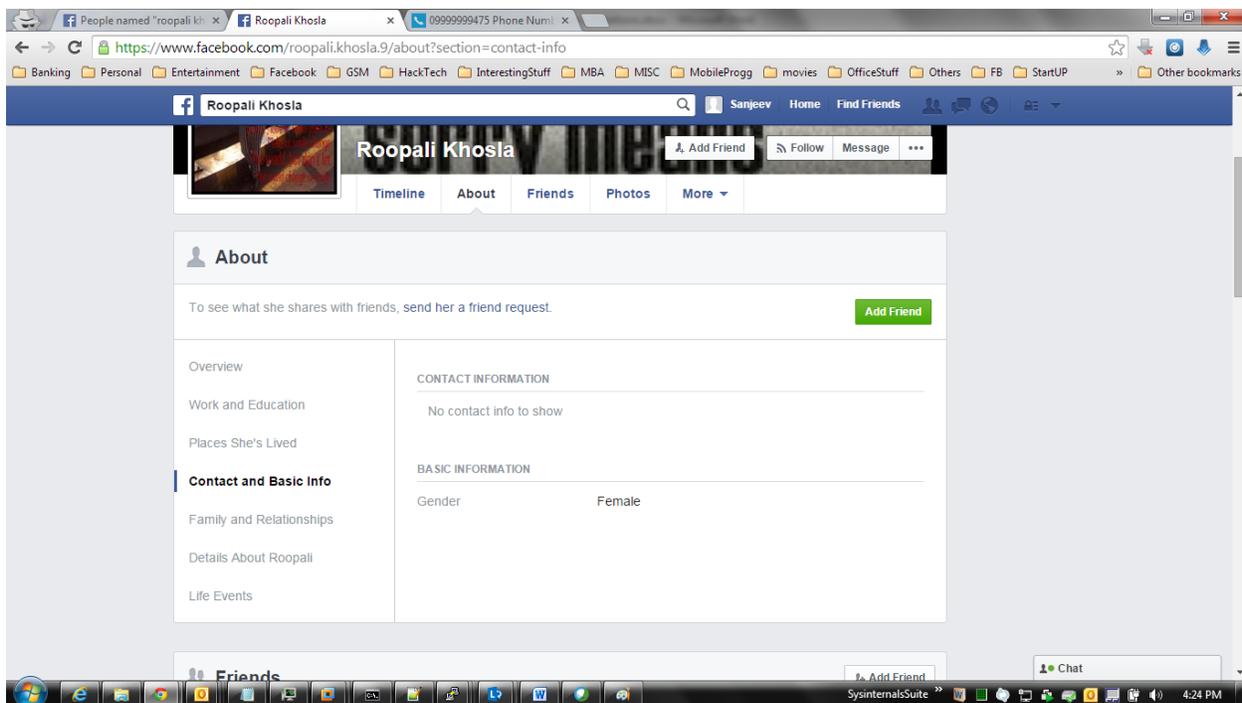
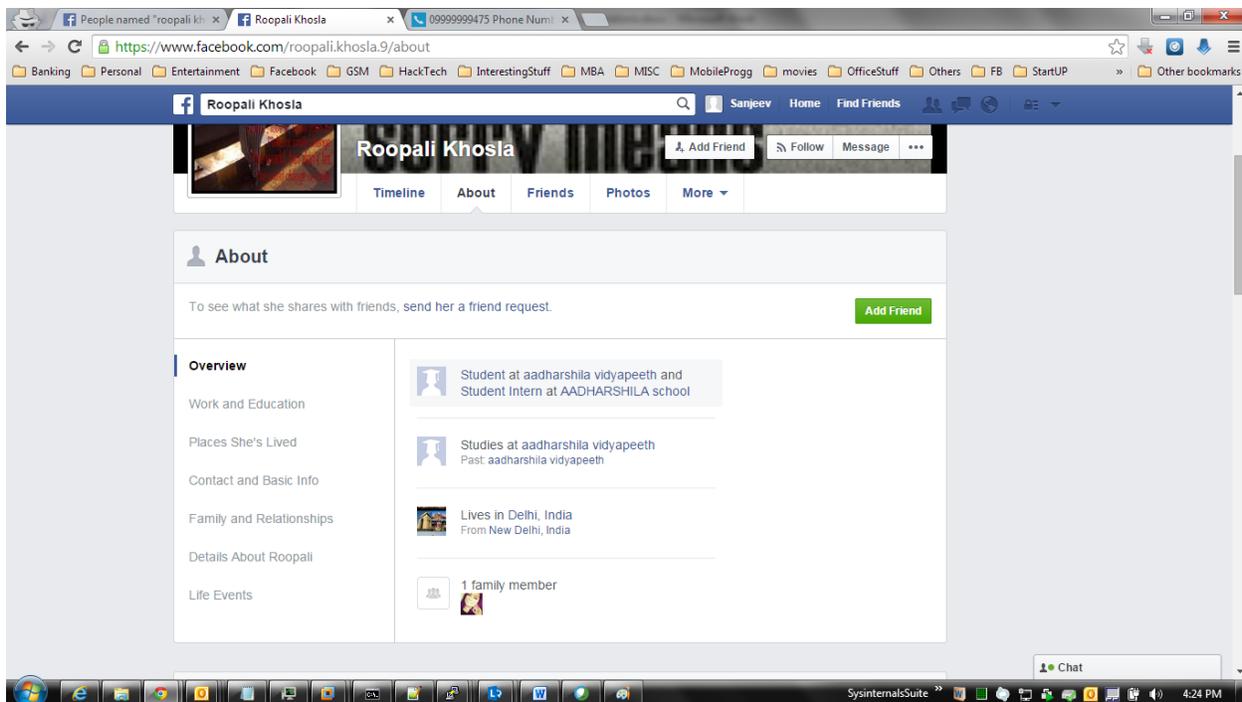
Student at aadharshila vidyapeeth and Student Intern at AADHARSHILA school

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



Chat

4:24 PM

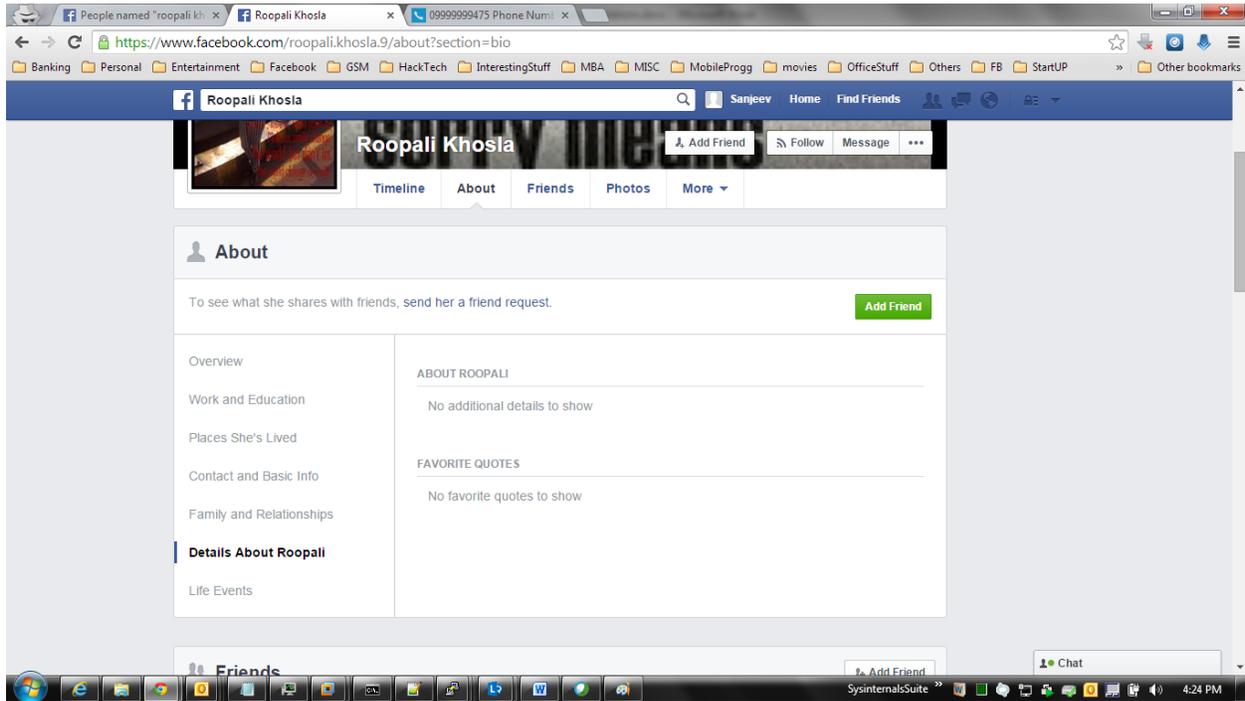


Nope, the phone number is not shown, i.e. Hidden or Private

**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.**

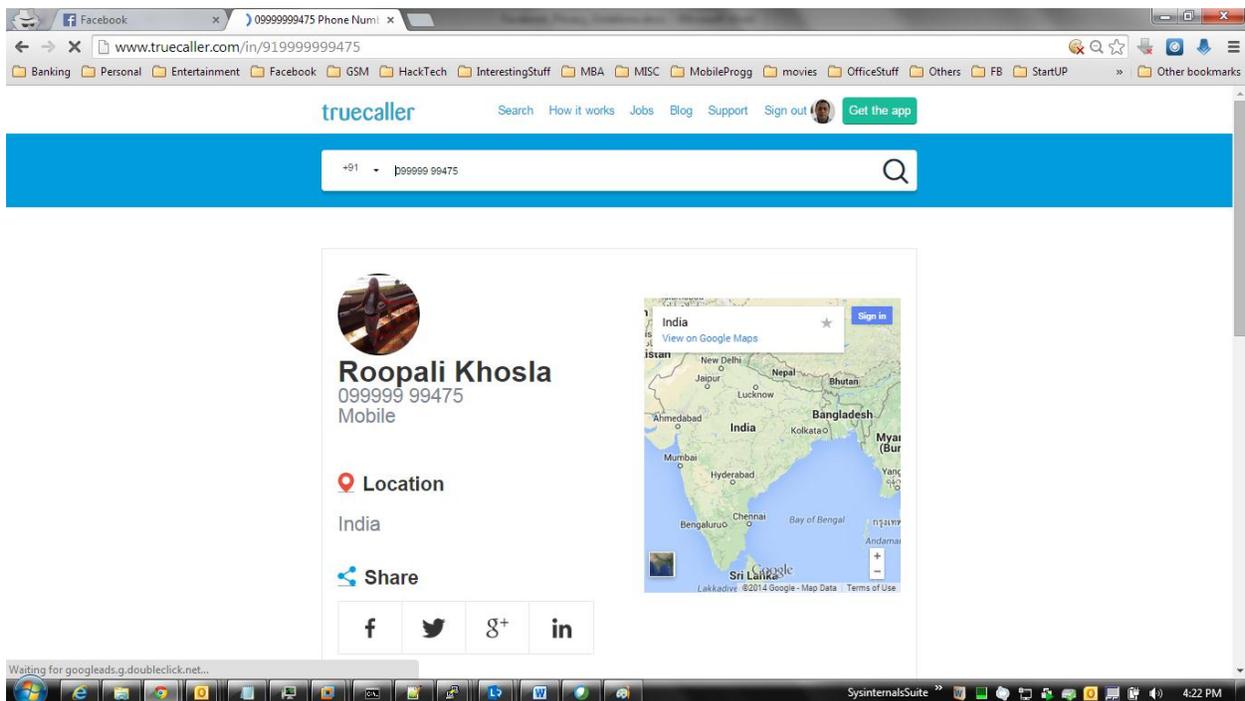
**This leakage of data is a breach of privacy**

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



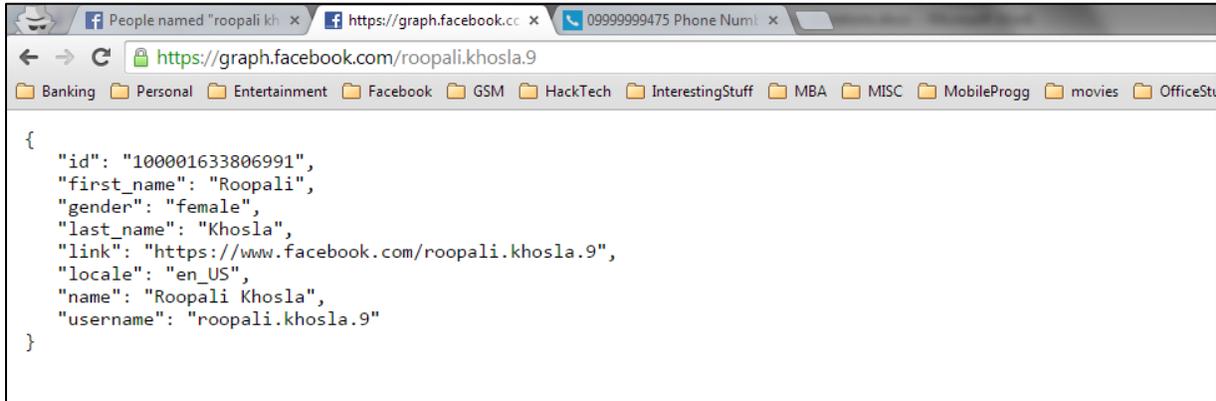
Nothing. Nowhere is the cell phone number “919999999475” listed on her profile.

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



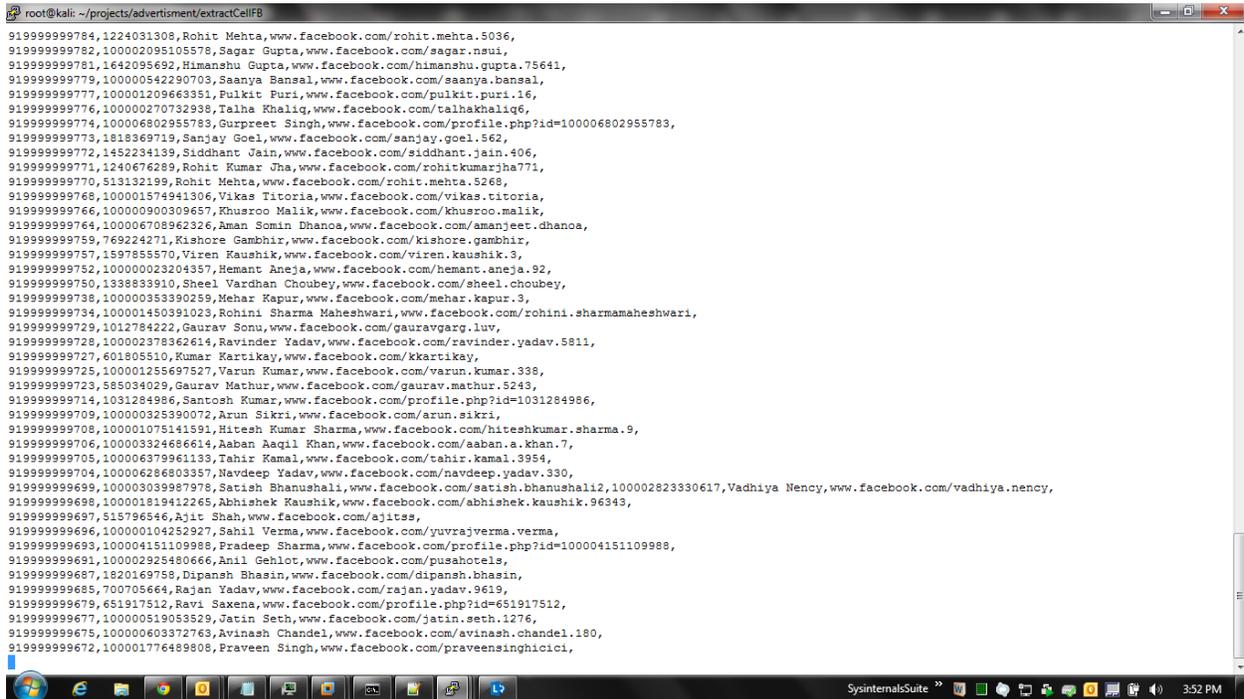
Bingo!

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
91999999784,1224031308,Rohit Mehta,www.facebook.com/rohit.mehta.5036,
91999999782,100002095105578,Sagar Gupta,www.facebook.com/sagar.nsui,
91999999781,1642095692,Himanshu Gupta,www.facebook.com/himanshu.gupta.75641,
91999999779,10000054290703,Saanya Bansal,www.facebook.com/saanya.bansal,
91999999777,100001209663351,Pulkit Puri,www.facebook.com/pulkit.puri.16,
91999999776,100000270732938,Talha Khaliq,www.facebook.com/talhakhaliq6,
91999999774,100006802955783,Gurpreet Singh,www.facebook.com/profile.php?id=100006802955783,
91999999773,1818369719,Sanjay Goel,www.facebook.com/sanjay.goel.562,
91999999772,1452234139,Siddhant Jain,www.facebook.com/siddhant.jain.406,
91999999771,1240676289,Rohit Kumar Jha,www.facebook.com/rohitkumarjha771,
91999999770,513132199,Rohit Mehta,www.facebook.com/rohit.mehta.5268,
91999999768,100001574941306,Vikas Titoria,www.facebook.com/vikas.titoria,
91999999766,100000900309657,Khusroo Malik,www.facebook.com/khusroo.malik,
91999999764,100006708962326,Aman Somin Dhanoo,www.facebook.com/amanjeet.dhanoo,
91999999759,769224271,Kishore Gambhir,www.facebook.com/kishore.gambhir,
91999999757,159785570,Viren Kaushik,www.facebook.com/viren.kaushik.3,
91999999752,100000023204357,Hemant Aneja,www.facebook.com/hemant.aneja.92,
91999999750,1338833910,Sheel Vardhan Choubey,www.facebook.com/sheel.choubey,
91999999738,100000353390259,Mehar Kapur,www.facebook.com/mehar.kapur.3,
91999999734,100001450391023,Rohini Sharma Maheshwari,www.facebook.com/rohini.sharmamaheshwari,
91999999729,1012784222,Gaurav Sonu,www.facebook.com/gauravqarg.luv,
91999999728,100002378362614,Ravinder Yadav,www.facebook.com/ravinder.yadav.5811,
91999999727,601805510,Kumar Kartikay,www.facebook.com/kkartikay,
91999999725,100001255697527,Varun Kumar,www.facebook.com/varun.kumar.338,
91999999723,585034029,Gaurav Mathur,www.facebook.com/gaurav.mathur.5243,
91999999714,1031284986,Santosh Kumar,www.facebook.com/profile.php?id=1031284986,
91999999709,100000325390072,Arun Sikri,www.facebook.com/arun.sikri,
91999999708,100001075141591,Hitesh Kumar Sharma,www.facebook.com/hiteshkumar.sharma.9,
91999999706,100003324686614,Aaban Aqil Khan,www.facebook.com/aaban.a.khan.7,
91999999705,100006379961133,Tahir Kamal,www.facebook.com/tahir.kamal.3954,
91999999704,100006286803357,Navdeep Yadav,www.facebook.com/navdeep.yadav.330,
91999999699,10000303987978,Satish Bhanushali,www.facebook.com/satish.bhanushali2,100002823330617,Vadhiya Nency,www.facebook.com/vadhiya.nency,
91999999698,100001819412265,Abhishek Kaushik,www.facebook.com/abhishek.kaushik.96343,
91999999697,515796546,Ajit Shah,www.facebook.com/ajitss,
91999999696,100000104252927,Sahil Verma,www.facebook.com/yuvrajverma.verma,
91999999693,100004151109988,Pradeep Sharma,www.facebook.com/profile.php?id=100004151109988,
91999999691,100002925480666,Anil Gehlot,www.facebook.com/pusahotels,
91999999687,1820169758,Dipansh Bhasin,www.facebook.com/dipansh.bhasin,
91999999685,700705664,Rajan Yadav,www.facebook.com/rajan.yadav.9619,
91999999679,651917512,Ravi Saxena,www.facebook.com/profile.php?id=651917512,
91999999677,10000519053529,Jatin Seth,www.facebook.com/jatin.seth.1276,
91999999675,10000603372763,Avinash Chandel,www.facebook.com/avinash.chandel.180,
91999999672,100001776489808,Praveen Singh,www.facebook.com/praveensinghicici,
```