Leveraging Web Application Vulnerabilities for Reconnaissance and Intelligence Gathering

JSFoo 2019

$ whoami

- Researcher on technology and policy at the Centre for Internet and Society (karan@cis-india.org);
- Interested in exploring the various applications of OS/SIG/HUM-INT;

Primer

What is OSINT?

- Information which can be collected from *public* sources for use in intelligence contexts;
- Often used to aid investigative processes or journalistic endeavours;

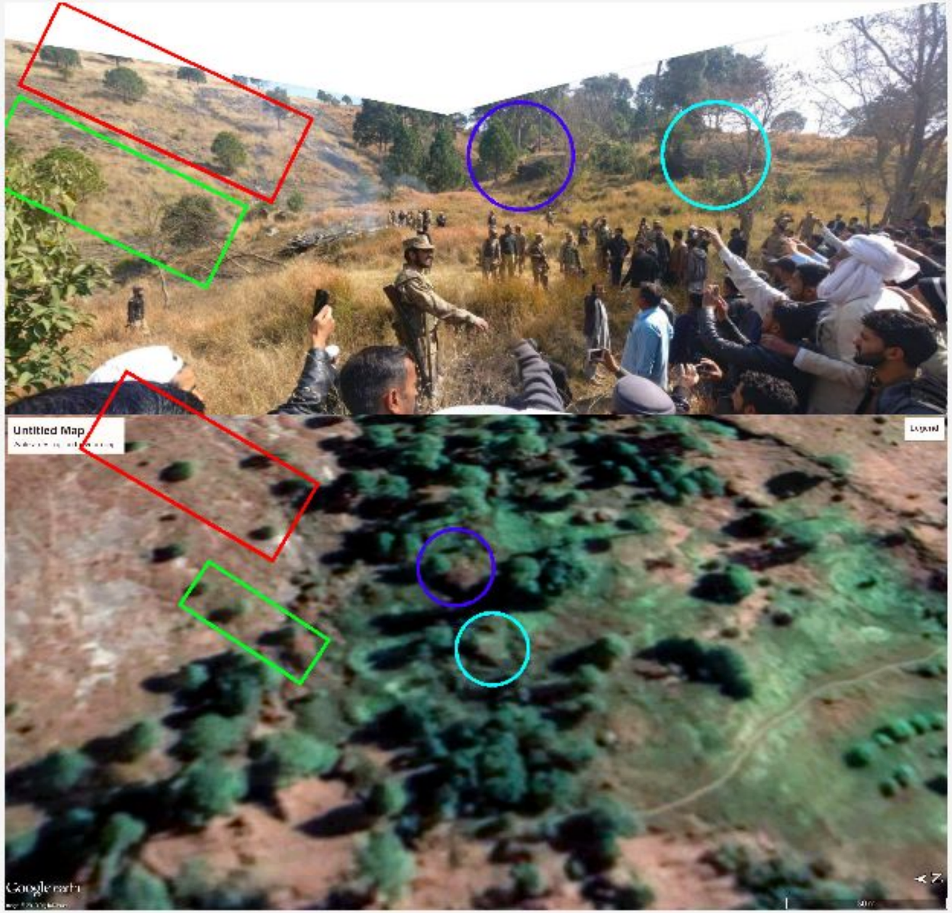
bellingcat

Case Studies Geolocation India Pakistan

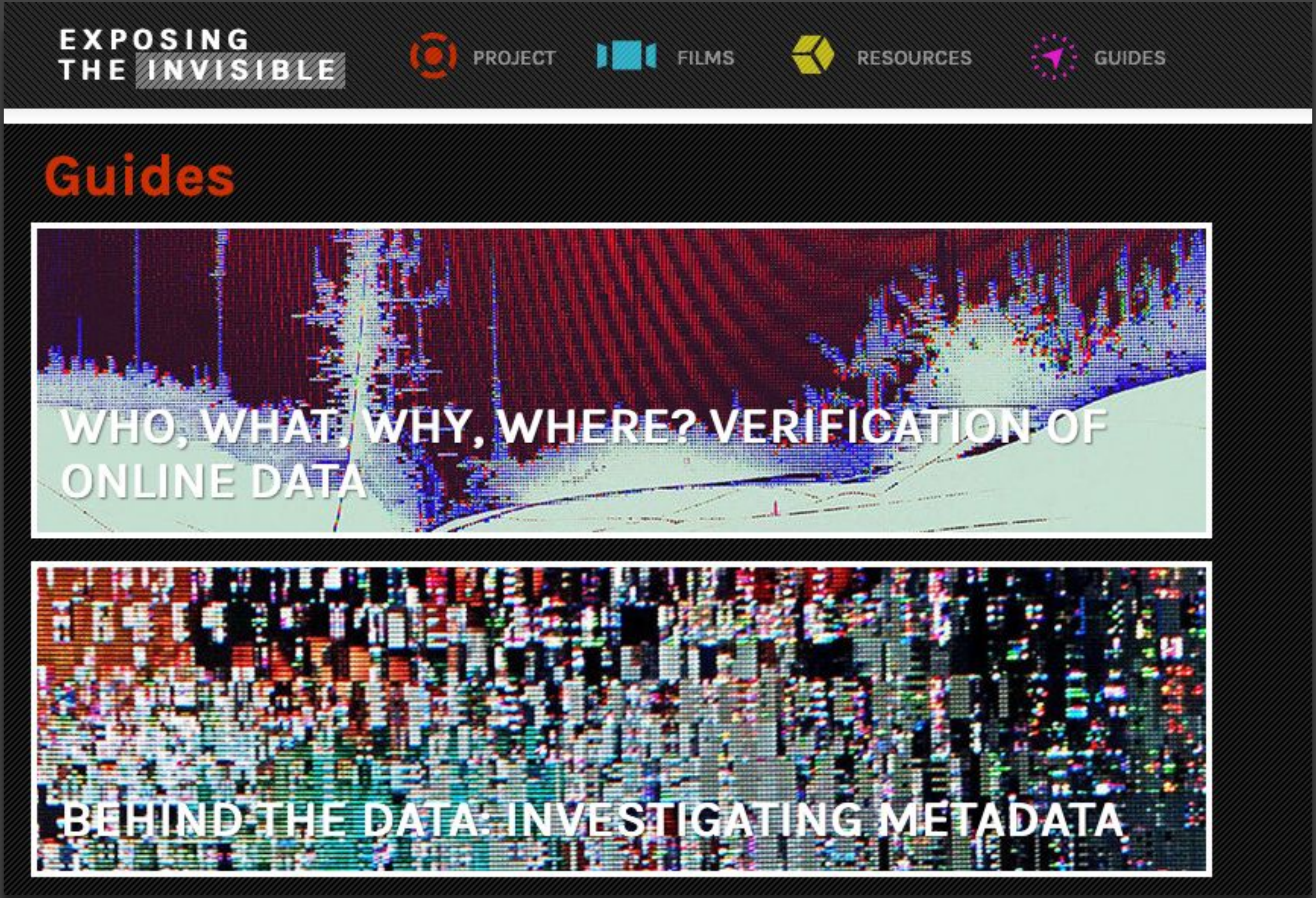
Geolocation and a Philosopher’s Stone in Kashmir

March 4, 2019 By Timmi Allen

Translations: Русский


Untitled Map
Legend
Google earth

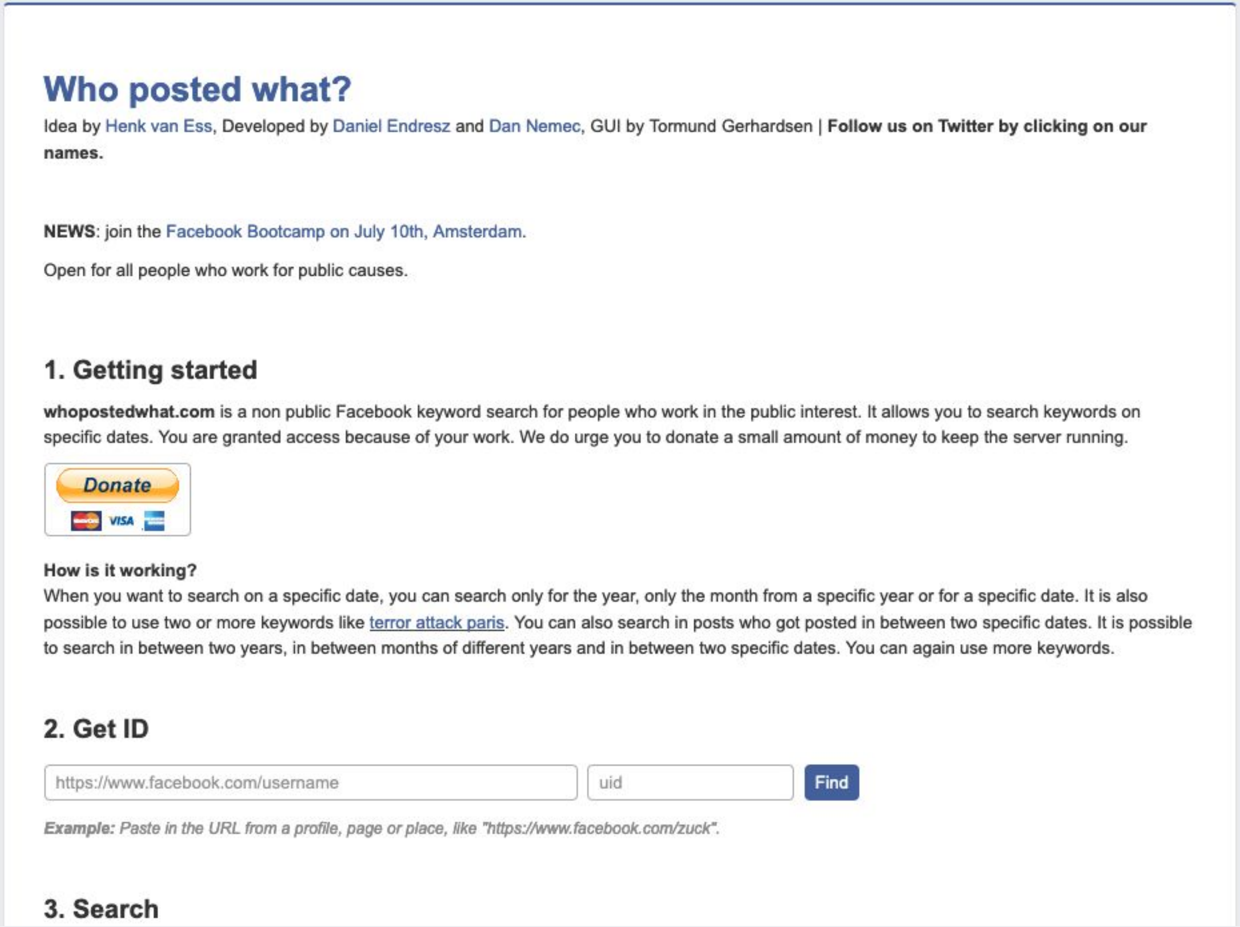
Intelligence and Investigations



Guides

WHO, WHAT, WHY, WHERE? VERIFICATION OF ONLINE DATA

BEHIND THE DATA: INVESTIGATING METADATA



Who posted what?

Idea by Henk van Ess, Developed by Daniel Endresz and Dan Nemec, GUI by Tormund Gerhardsen | **Follow us on Twitter by clicking on our names.**

NEWS: join the Facebook Bootcamp on July 10th, Amsterdam.

Open for all people who work for public causes.

1. Getting started

whopostedwhat.com is a non public Facebook keyword search for people who work in the public interest. It allows you to search keywords on specific dates. You are granted access because of your work. We do urge you to donate a small amount of money to keep the server running.

How is it working?
When you want to search on a specific date, you can search only for the year, only the month from a specific year or for a specific date. It is also possible to use two or more keywords like terror attack paris. You can also search in posts who got posted in between two specific dates. It is possible to search in between two years, in between months of different years and in between two specific dates. You can again use more keywords.

2. Get ID

***Example:** Paste in the URL from a profile, page or place, like "https://www.facebook.com/zuck".*

3. Search

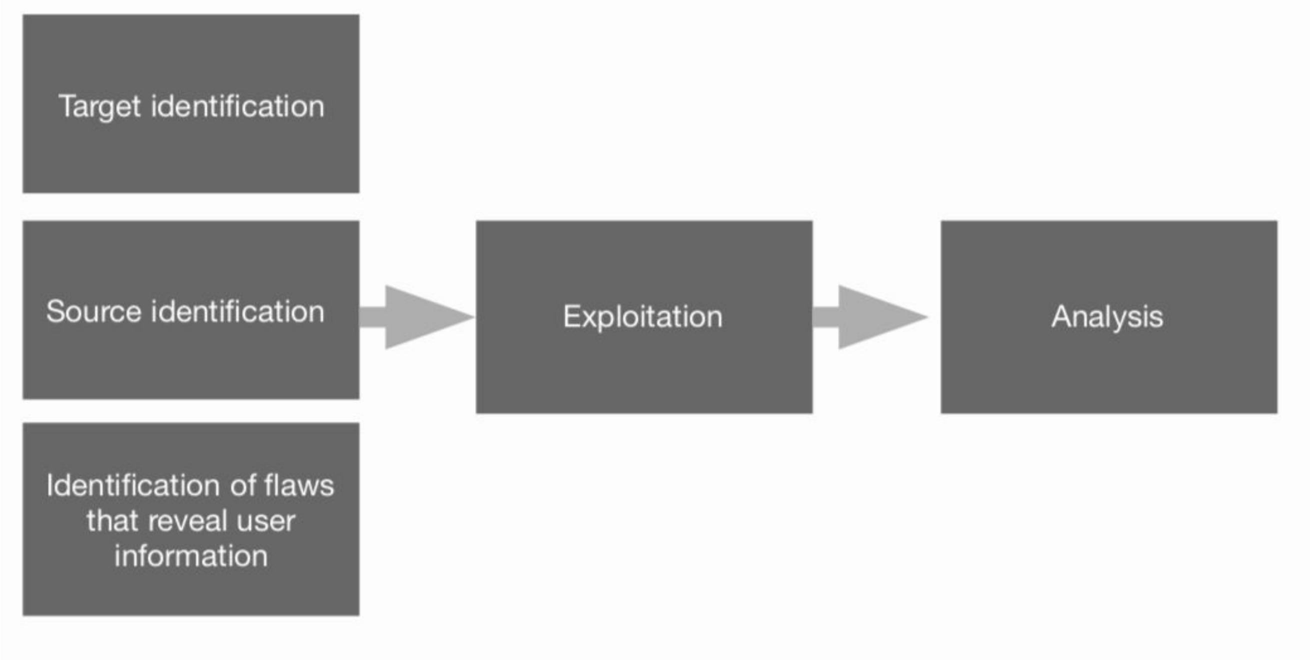
What will this talk cover?

- Active reconnaissance and intelligence gathering by discovering and exploiting flaws in web applications and services;

A case for living off the land

- A problem with publicly available intelligence resources is that access to data is usually restricted;
- Tools are often not flexible, i.e., can only operate within a defined set of parameters;
- Self-sufficiency is key!

Web Application Vulnerabilities and Intelligence Gathering



Target identification

Source identification

Identification of flaws that reveal user information

Exploitation

Analysis

Part I: Scoping

- In 2019, there are online services and platforms for just about everything;

What does this mean?

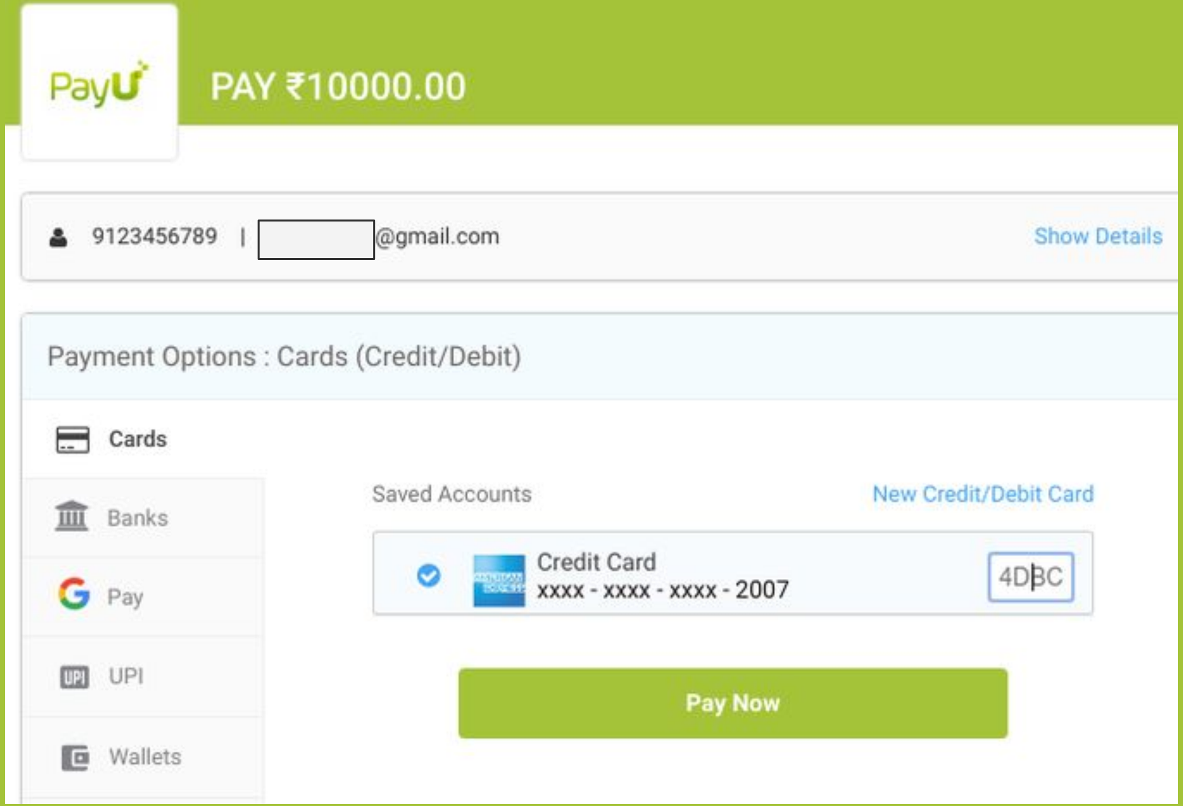
Information is available in abundance!

- Speculative targeting: The attacker has knowledge of the general demographic whose information they are looking to retrieve;
- Informed targeting: The attacker is targeting one particular individual and has knowledge of the services they use;

Part II: Common flaws

- Overly permissive application programming interfaces;
- Improper access controls and implicit user trust;
- Oversight in deprecating API functionalities;
- Use of insecure account or resource identifiers;

Examples



PAY ₹10000.00

9123456789 | @gmail.com

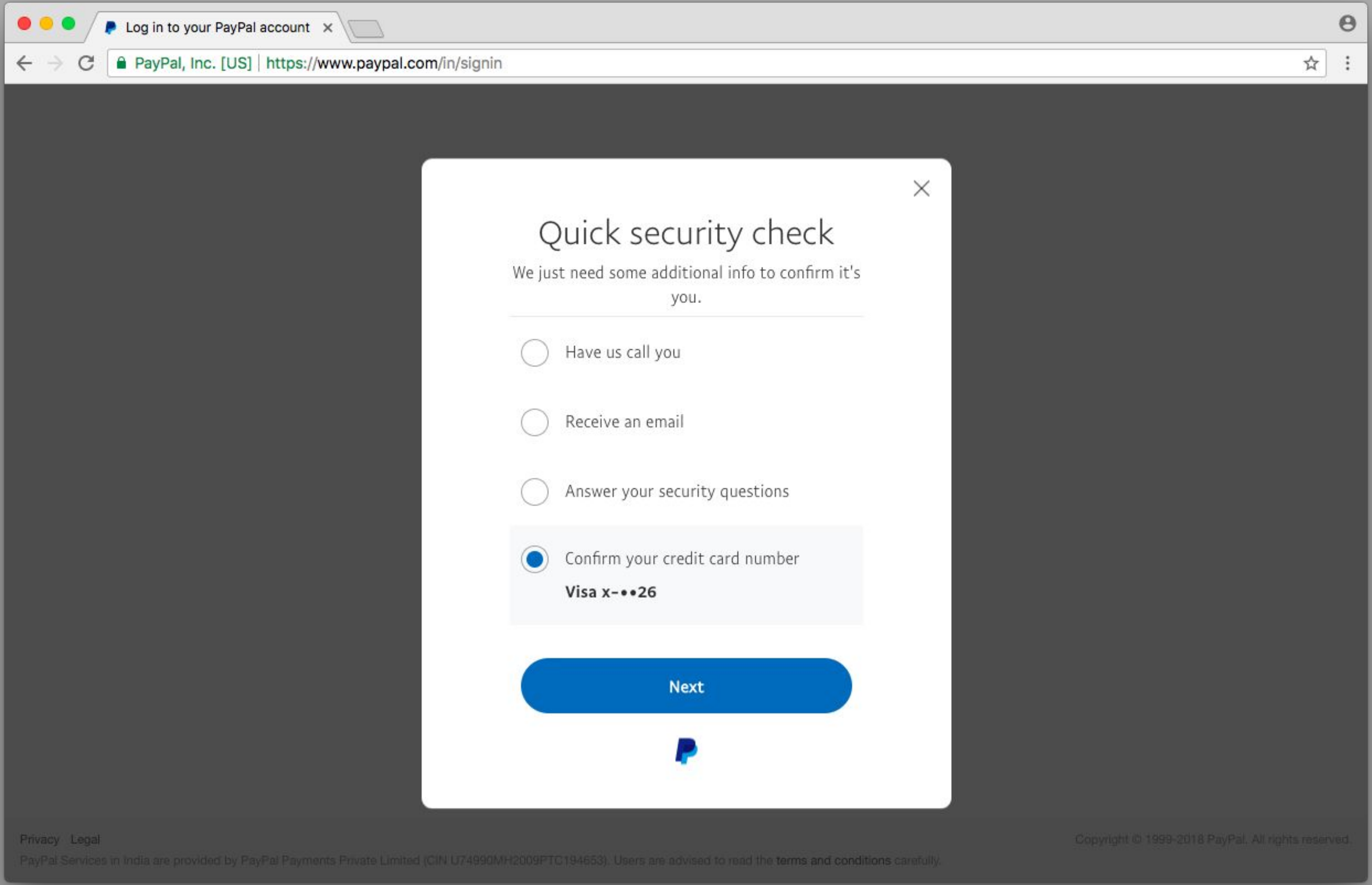
Payment Options : Cards (Credit/Debit)

Saved Accounts

Credit Card
xxxx - xxxx - xxxx - 2007

4DBC

Lessons


Log in to your PayPal account
PayPal, Inc. [US] https://www.paypal.com/in/signin

Quick security check

We just need some additional info to confirm it's you.

○ Have us call you

○ Receive an email

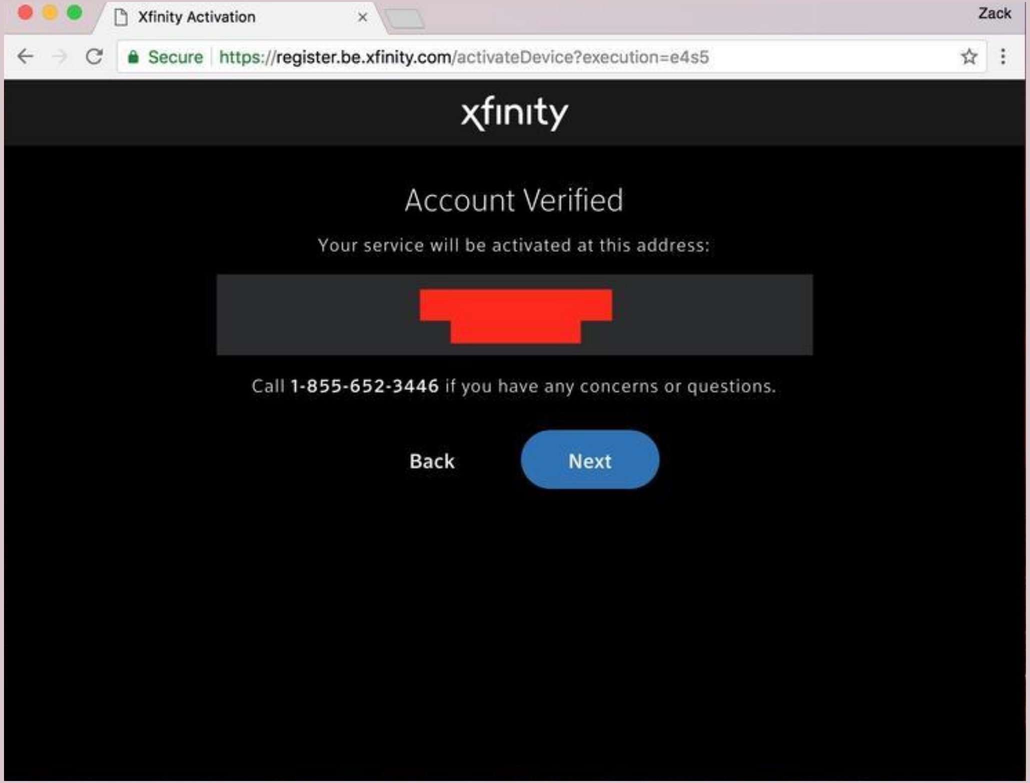
○ Answer your security questions

● Confirm your credit card number
Visa x-••26

Privacy Legal

Copyright © 1999-2018 PayPal. All rights reserved.

PayPal Services in India are provided by PayPal Payments Private Limited (CIN U74990MH2009PTC194653). Users are advised to read the terms and conditions carefully.

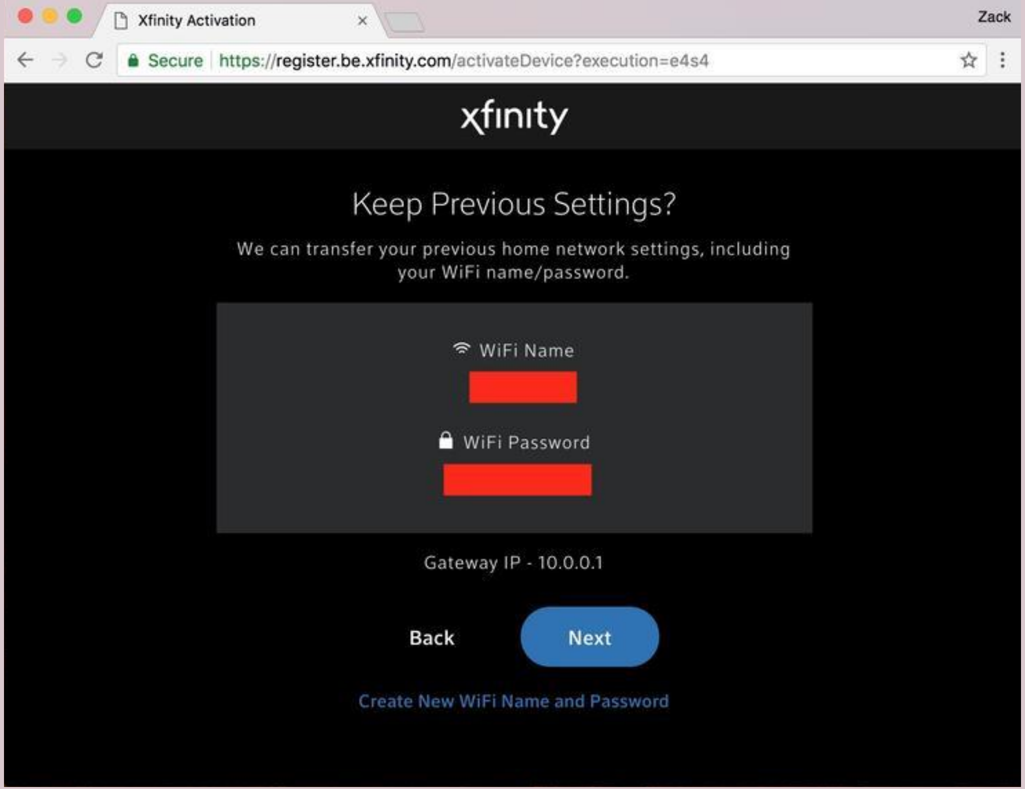

Xfinity Activation
Zack
Secure
https://register.be.xfinity.com/activateDevice?execution=e4s5
xfinity
Back
Next

Account Verified

Your service will be activated at this address:

[redacted]

Call **1-855-652-3446** if you have any concerns or questions.


Xfinity Activation
Zack
Secure https://register.be.xfinity.com/activateDevice?execution=e4s4
xfinity

Keep Previous Settings?

We can transfer your previous home network settings, including your WiFi name/password.

WiFi Name

[redacted]

WiFi Password

[redacted]

Gateway IP - 10.0.0.1

Back
Next
Create New WiFi Name and Password

Lessons:

- Don’t toss your bill in the trash, I guess;

Part III: Defense

Developers

- Where all can an attacker interact with and potentially acquire user data?

End-users

“Why would anyone want *my* data anyway?”

Good operational security goes a long way

In conclusion…

Questions?

Thank you for having me!

Karan Saini

twitter: @squeal

mail: karan [at] cis-india.org