

# Web Security for Developers

Web Application Developers



# Who am I?

I am Thejesh GN





- Currently Technical Architect at Peppo
- Previously NPTEL/IITM, Infosys etc

On a daily basis on I architect, design, develop web applications and services.

Why?

# Intro

English • | [Epaper](#) | [GadgetsNow](#)

SIGN IN    

THE TIMES OF INDIA  
GADGETS NEWS





[Tech](#) [Gadgets News](#) [Tech News](#) [Gadgets](#) [Reviews](#) [Top Gadgets](#) [Slideshows](#) [Videos](#) [How to](#) [Featured](#)


NEWS / TECH / [GROCERY APP BIGBASKET HACKED, DATA OF 2 CRORE USERS LEAKED; WHAT YOU SHOULD DO TO STAY SAFE](#)

TOP SEARCHES: [Flipkart App Quiz](#) [Amazon App Quiz](#) [Vivo V20 Pro Launch Date](#) [Xiaomi Black Friday Sale](#) [Xbox App](#) [Vivo Y1s Launched](#) [Bla](#)

## Grocery app BigBasket hacked, data of 2 crore users leaked; What you should do to stay safe

Debashis Sarkar | TIMESOFINDIA.COM | Updated: Nov 9, 2020, 20:29 IST


   



NEW DELHI: Popular grocery app BigBasket has been hacked. Personal data of over 2 crore users is sold on the dark web for over \$40,000 which translates to around Rs 30 lakh. As per a report by Cyble, a firm that tracks data breaches, its research team was able to find Big Basket database for sale on the dark web.

"The leak contains a database portion; with the table name 'member\_member'. The size of the SQL file is ~ 15 GB, containing close to 20 Million user data. More specifically, this includes full names, email IDs, password hashes (potentially hashed OTPs), pin, contact numbers (mobile + phone), full addresses, date of birth, location, and IP addresses of login among many others," claims the company.

Cyble informed the management team of BigBasket about the leak and later BigBasket confirmed the breach. In a statement to news agency *PTI*, the company said, "A few days ago, we learnt about a potential data breach at Bigbasket and are evaluating the extent of the breach and authenticity of the claim in consultation with



#MASKINDIA


### THE CORONA LETTER

Covid-19 daily briefing


SUBSCRIBE

### TOI STORIES


SEE ALL >




Boeing's 737 Max saga wasn't just about faulty software



Why rising prices are pinching all of India hard



Would you like to buy 1,000 people for \$1,000?



How apps, AI could fight world's deadliest killer

# Why?

BENCHMARKS CLOSED

Sensex 44,749.72 ↓ -20.02

NSE LOSER-LARGE CAP

Avenue Super... 2,289.20 ↓ -83.85

FEATURED FUNDS

Axis Long Term Equity DL... 14.27% [INVEST NOW](#)

BY RETURN

MARKET WATCH ▼

THE ECONOMIC TIMES

Rise

Subscribe | Sign In

English Edition • | E-Paper

Home

ETPrime

Markets

News

Industry

RISE

Politics

Wealth

MF

Tech

Jobs

Opinion

NRI

Panache

ET NOW

More ▼

Q

ET Rise Top MSMEs

SME

Policy

Trade

Entrepreneurship

Money

IT

Legal

GST

Biz Listings

Marketing

HR

▼

Business News

RISE

IT

Security

Zomato hacked: Security breach results in 17 million user data stolen

## Zomato hacked: Security breach results in 17 million user data stolen

By Anu Thomas, ET Online • Last Updated: May 19, 2017, 10:18 AM IST



### Synopsis

Zomato attributed the breach to human error, where an employee's development account got compromised and hackers got to lay their hands on the data.



According to Hackeread.com, a user by the name of "nclay" claimed to have hacked Zomato and was willing to sell data pertaining to 17 million registered users on a popular Dark Web marketplace.

**Zomato** has suffered a security breach with over 17 million user records stolen from the food-tech company's database. The stolen information has email addresses and hashed passwords of customers.

According to **Hackeread.com**, a user by the name of "**nclay**" claimed to have hacked Zomato and was willing to sell data pertaining to 17 million registered

users on a popular **Dark Web** marketplace.

This included emails and password hashes of registered Zomato users with the price set for the whole package at \$1,001.43 (BTC 0.5587) - BTC here stands for Bitcoins. Hackeread adds the vendor also published data and evidence to prove it was genuine.

Feedback

# Why

Millions of Indians are going online for one reason or the other. It's our responsibility as web developers to make it safe for them.

Think about next billion internet users .....

# Field is vast

The field of websecurity is vast. Everyday there are new things to learn and do. Here I give you pointers to start with or to kick start your thinking process.

So

Where do we start?



# Design

It needs to start form the design process.

- What data you will collect?
- Is it really required?
- How do we minimize the data collection?
- How do we keep it safe?
- How do we make interaction safe?

# 12 Factor Development

Process is equally important. Sticking to standards makes it easy to manage the web project, in general keeps it secure and maintainable.

<https://12factor.net/>

I. Codebase - One codebase tracked in revision control, many deploys

II. Dependencies - Explicitly declare and isolate dependencies

III. Config - Store config in the environment

IV. Backing services - Treat backing services as attached resources

V. Build, release, run - Strictly separate build and run stages

# 12 Factor Development

VI. Processes - Execute the app as one or more stateless processes

VII. Port binding - Export services via port binding

VIII. Concurrency - Scale out via the process model

IX. Disposability - Maximize robustness with fast startup and graceful shutdown

X. Dev/prod parity - Keep development, staging, and production as similar as possible

XI. Logs - Treat logs as event streams

XII. Admin processes - Run admin/management tasks as one-off processes

# Think about security

What's the biggest pitfalls that can be avoided?

- Learn from previous mistakes
- Learn from standards

What should I know as I am just starting?

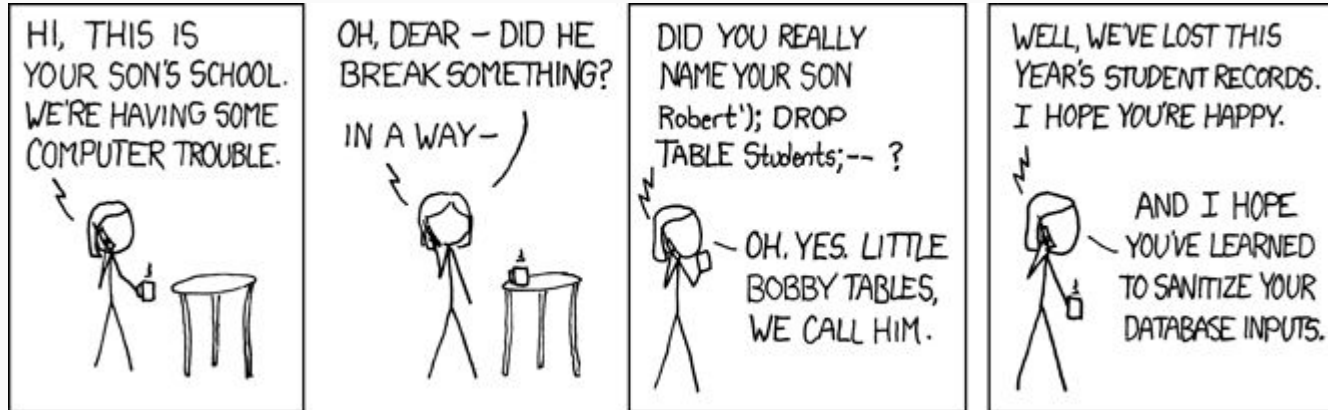
# OWSAP Top Ten

Globally recognized by developers as the first step towards more secure coding.

<https://owasp.org/www-project-top-ten/>

- We can go one by one.
- We will understand what they mean
- See how do we go about avoiding making mistakes

# How can this happen?



# OWSAP Top Ten

**Injection** - Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- Don't use the user submitted form attributes directly
- Use parameterized queries
- Use Object Relational Mapping (ORM)

# Guess?

- 123456
- 123456789
- picture1
- password
- 12345678

- 111111
- 123123
- 12345
- 1234567890
- senha



# OWSAP Top Ten

**Broken Authentication** - Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

- No default passwords
- Use two factor auth
- Suggest users to use strong password
- Suggest users to change password when it gets leaked , using services like <https://haveibeenpwned.com/>
- Hash passwords
- Use TLS (https)

Home

Latest

Trending

My Reads

HTLS 2020

Long Reads

Plain Facts

Primer

Coronavirus Vaccine Tracker

Market Dashboard

Pivot Or Perish

Money With Monika, Season 3

Mint Money Conversation

Home > Money > Personal Finance > How to avoid being a victim of SIM swap fraud



SIM swap fraud is increasing in India too (Photo: iStock)

## How to avoid being a victim of SIM swap fraud

4 min read · Updated: 23 Sep 2019, 02:56 PM IST

Bindisha Sarang

- Being vigilant about the information you reveal to others is the most important thing you can do to ensure fraudsters don't steal your personal data
- Always use genuine softwares on your smartphone and never tamper with its security settings



Earlier this month, Twitter co-founder and chief executive officer [Jack Dorsey](#) was in the news for becoming a victim of a SIM swap fraud. In this type of fraud, the original SIM is cloned, and the duplicate is misused to get access to the victim's mobile phone and, thereby, to the victim's online bank account from where funds are transferred to the fraudster's account. For Dorsey, the issue was resolved without any financial damage, but when ordinary investors become the victims of such a fraud, the damage may be difficult to control and it may

# OWSAP Top Ten

**Sensitive Data Exposure.** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

- Classify data
- Apply different ACL
- Don't store it if it's not required. Like credit card, birth date etc
- Encrypt all sensitive data at rest
- Hash passwords
- Use TLS (https)

**XML External Entities (XXE).** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

- Use less complex data formats such as JSON

BENCHMARKS CLOSED Nifty 12,968.95 ↓ 18.05 NSE GANER LARGE CAP ICL 496.40 ↑ 48.25  
FEATURED FUNDS Axis Focused 25 Direct PL ↑ 16.21 % INVEST NOW 5Y RETURN MARKET WATCH ▼

THE ECONOMIC TIMES | tech  
English Edition | E-Paper

Subscribe | Sign In

Home ETPrime Markets News Industry RISE Politics Wealth MF Tech Jobs Opinion NRI Panache ET NOW More Q

ITES Tech & Internet Funding Startups Tech Bytes The Catalysts Tech and Gadgets

Business News > Tech > Internet > German firm finds one million files of Indian patients leaked

## German firm finds one million files of Indian patients leaked

By Anandi Chandrashekar, ET Bureau • Last Updated: Feb 04, 2020, 11:11 AM IST

SHARE FONT SIZE SAVE PRINT COMMENT

### Synopsis

ET has reviewed a screenshot containing a list of patient names (but blurred to protect privacy) and corresponding patient identification numbers, study descriptions and names of doctors who referred and reviewed the cases. These include ones from Breach Candy Hospital and Utkarsh Scans in Mumbai.

Agencies



The servers on which these records are stored have been left vulnerable, Greenbone said.

Feedback

**Broken Access Control.** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

- ACL
- Time limited access even for real users
- Avoid world access to any kind of files
- Rate limit



Business For Home

Products Solutions Why Trend Micro Research Support Partners Company

Alerts Download Buy Region Log In Contact Us

Security News > Virtualization & Cloud > Misconfigured AWS S3 Bucket Leaks 36,000 Inmate Records

# Misconfigured AWS S3 Bucket Leaks 36,000 Inmate Records

February 12, 2020



An unsecured and unencrypted Amazon Simple Storage Service (S3) bucket was found leaking 36,077 records belonging to inmates of correctional facilities in several U.S. states. The leak, which was discovered by **vpnMentor**, exposed personally identifiable information (PII), prescription records, and details of the inmate's daily activities. The leaky repository belongs to **JailCore**, a cloud-based application utilized in correctional facility management.



The researchers first discovered the leak through a web mapping project, where they scanned ports to identified vulnerable systems. The findings were then reported to JailCore, and the bucket was closed some days after.

[Related: [Unsecured AWS S3 Bucket Found Leaking Data of Over 30K Cannabis Dispensary Customers](#)]

## The exposed data

The exposed data included the inmates' PII, such as their full names, date of birth, booking number, mugshot, and cell location. The researchers noted that some of the information were already publicly accessible even before the leak.

## Related Posts

- Online Dating Websites Lure Japanese Customers to Scams
- Data of U.K. Train Commuters
- Leak from Misconfigured AWS Cloud Storage
- Unsecured AWS S3 Bucket Found
- Leaking Data of Over 30K Cannabis Dispensary Customers
- Unsecure Paggers in Vancouver
- Expose Sensitive Patient Data: What This Means for Enterprises
- Recognizing Enterprise Mission-Critical Assets

## Recent Posts

- Securing IoT Apps
- Navigating Gray Clouds: The Importance of Visibility in Cloud Security
- Exploiting AI: How Cybercriminals

**Security Misconfiguration.** Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

- Hardening
- Don't use if not required
- Automated testing of the configuration





Hussain Adnan (hussain\_0x3c)

3165

Reputation

-

Rank

3.82

Signal

80th

Percentile

18.47

Impact

89th

Percentile

36

#191810

## Reflected XSS in lert.uber.com

Share:


State: ● Resolved (Closed)

Disclosed

December 20, 2016 4:16am +0530

Reported To: [Uber](#)

Reported at: December 17, 2016 3:43am +0530

CVE ID

Weakness: Cross-site Scripting (XSS) - Reflected

Bounty: \$3,000

Severity: Medium (4 - 6.9)

Participants



Visibility: Disclosed (Limited)

Collapse

## SUMMARY BY UBER



Due to a lack of input validation from the search field on `lert.uber.com`, it was possible to obtain a Reflected XSS from the URL path, e.g. `https://lert.uber.com/s/search/All/Home?>PAYLOAD`.

Thanks, @hussain\_0x3c

## TIMELINE


hussain\_0x3c submitted a report to [Uber](#).

Dec 17th (4 years ago)


jmline-uber changed the status to ● Triaged.

Dec 17th (4 years ago)



hussain\_0x3c posted a comment.

Dec 17th (4 years ago)


fletcher closed the report and changed the status to ● Resolved.

Dec 17th (4 years ago)



hussain\_0x3c posted a comment.

Dec 17th (4 years ago)



hussain\_0x3c posted a comment.

Dec 17th (4 years ago)



Uber rewarded hussain\_0x3c with a \$3,000 bounty.

Dec 20th (4 years ago)

**Cross-Site Scripting XSS.** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

- Use standard frameworks which by default handles XSS, like RoR, Django etc
- Keep the frameworks updated

**Insecure Deserialization.** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

- Don't accept serialized objects as much as possible
- Accept only signed objects
- Details in a Cookie



Abhay Rana aka Nemo

## Aadhaar Vulnerability Public Disclosure



15 Sep 2018

### The Vulnerability

The UIDAI Resident Portal (with read access to entire Aadhaar Demographic data) is running a vulnerable version of LifeRay software. It is running LifeRay 6.1, which was declared End-of-Life in February 2016.

This release includes multiple known vulnerabilities, including:

1. A XSS issue, for which a PoC can be found at [resident.uidai.gov.in](https://resident.uidai.gov.in) (Picture Credits: [@sanitarypanels](#))
2. Multiple RCEs: See [issue-62](#) for eg.

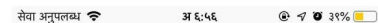
In fact the release is so old it does not even appear on the "Known Vulnerabilities" page on the LifeRay website; you have to go look at their [Archived Vulnerabilities](#).

### The PoC

You can find a simple Proof of Concept for the XSS issue at [resident.uidai.gov.in](https://resident.uidai.gov.in).

The `cdn_host` parameter injects javascript from `$CDN_HOST/Resident-theme/js/custom.js`, in this case `https://scan.bb8.fun/Resident-theme/js/custom.js` which hosts a small snippet to overwrite the HTML of the page.

It shows up like:



### **Using Components with Known Vulnerabilities.**

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.


[CVE](#) is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.


[NVD](#) - The NVD is the U.S. government repository of standards based vulnerability management data.

**Insufficient Logging & Monitoring.** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

- Someone should see the the logs
- Automated analysis and alerts
- Store the old logs for sufficient amount of time
- Don't log sensitive data

# Tools

 **TOOLS**

[Home](#) [Tools Listing](#) [Metapackages](#) 

## Kali Linux Tools Listing

Information Gathering	Vulnerability Analysis	Wireless Attacks	Web Applications
<ul style="list-style-type: none"><li>• <a href="#">ace-voip</a></li><li>• <a href="#">Amap</a></li><li>• <a href="#">APT2</a></li><li>• <a href="#">arp-scan</a></li><li>• <a href="#">Automater</a></li><li>• <a href="#">bing-ip2hosts</a></li><li>• <a href="#">braa</a></li><li>• <a href="#">CaseFile</a></li><li>• <a href="#">CDPSnarf</a></li><li>• <a href="#">cisco-torch</a></li><li>• <a href="#">copy-router-config</a></li><li>• <a href="#">DMitry</a></li><li>• <a href="#">dnmap</a></li><li>• <a href="#">dnsenum</a></li><li>• <a href="#">dnsmap</a></li><li>• <a href="#">DNSRecon</a></li><li>• <a href="#">dnstracer</a></li><li>• <a href="#">dnswalk</a></li><li>• <a href="#">DotDotPwn</a></li><li>• <a href="#">enum4linux</a></li><li>• <a href="#">enum4linux</a></li><li>• <a href="#">EyeWitness</a></li><li>• <a href="#">Faraday</a></li><li>• <a href="#">Fierce</a></li></ul>	<ul style="list-style-type: none"><li>• <a href="#">BBQSQL</a></li><li>• <a href="#">BED</a></li><li>• <a href="#">cisco-auditing-tool</a></li><li>• <a href="#">cisco-global-exploiter</a></li><li>• <a href="#">cisco-ocs</a></li><li>• <a href="#">cisco-torch</a></li><li>• <a href="#">copy-router-config</a></li><li>• <a href="#">Doona</a></li><li>• <a href="#">DotDotPwn</a></li><li>• <a href="#">HexorBase</a></li><li>• <a href="#">jQuery Injection</a></li><li>• <a href="#">Lynis</a></li><li>• <a href="#">Nmap</a></li><li>• <a href="#">ohrwurm</a></li><li>• <a href="#">openvas</a></li><li>• <a href="#">Oscanner</a></li><li>• <a href="#">Powerfuzzer</a></li><li>• <a href="#">sfuzz</a></li><li>• <a href="#">SidGuesser</a></li><li>• <a href="#">SIPArmyKnife</a></li><li>• <a href="#">sqlmap</a></li><li>• <a href="#">sqlninja</a></li><li>• <a href="#">sqlsus</a></li><li>• <a href="#">THC-IPV6</a></li></ul>	<ul style="list-style-type: none"><li>• <a href="#">Airbase-ng</a></li><li>• <a href="#">Aircrack-ng</a></li><li>• <a href="#">Aircap-ng and Airdedaoak-ng</a></li><li>• <a href="#">Aircap-ng</a></li><li>• <a href="#">Aircrack-ng</a></li><li>• <a href="#">Airmo-ng</a></li><li>• <a href="#">Airodump-ng</a></li><li>• <a href="#">airodump-ng-oui-update</a></li><li>• <a href="#">Airoh-ng</a></li><li>• <a href="#">Airserv-ng</a></li><li>• <a href="#">Airtun-ng</a></li><li>• <a href="#">Asleap</a></li><li>• <a href="#">Besside-ng</a></li><li>• <a href="#">Bluelog</a></li><li>• <a href="#">BlueMaho</a></li><li>• <a href="#">Bluepot</a></li><li>• <a href="#">BlueRanger</a></li><li>• <a href="#">Bluesnarfer</a></li><li>• <a href="#">Bully</a></li><li>• <a href="#">c0wPAtty</a></li><li>• <a href="#">crackmap</a></li><li>• <a href="#">eapmd5pass</a></li><li>• <a href="#">Easyside-ng</a></li><li>• <a href="#">Fern Wifi Cracker</a></li></ul>	<ul style="list-style-type: none"><li>• <a href="#">apache-users</a></li><li>• <a href="#">Arachni</a></li><li>• <a href="#">BBQSQL</a></li><li>• <a href="#">BlindElephant</a></li><li>• <a href="#">Burp Suite</a></li><li>• <a href="#">CurlCap</a></li><li>• <a href="#">DAVTest</a></li><li>• <a href="#">deblaze</a></li><li>• <a href="#">DIRB</a></li><li>• <a href="#">DirBuster</a></li><li>• <a href="#">fimap</a></li><li>• <a href="#">FunkLoad</a></li><li>• <a href="#">Gobuster</a></li><li>• <a href="#">Grabber</a></li><li>• <a href="#">HURL</a></li><li>• <a href="#">jboss-autopwn</a></li><li>• <a href="#">joorscan</a></li><li>• <a href="#">jQuery Injection</a></li><li>• <a href="#">Maltigo Teeth</a></li><li>• <a href="#">Nikto</a></li><li>• <a href="#">PadBuster</a></li><li>• <a href="#">Paros</a></li><li>• <a href="#">Parsero</a></li><li>• <a href="#">plecost</a></li></ul>

List of good

Tools at

[Kali Linux](#)

# Information

- Open Web Application Security Project,  
<https://owasp.org>
- Kali Linux and Tools -  
<https://tools.kali.org/tools-listing>
- India CERT  
<https://www.cert-in.org.in/>
- Have I been Pwned  
<https://haveibeenpwned.com/>
- Common Vulnerabilities and Exposures  
<https://cve.mitre.org/>
- Bleeping Computer  
<https://www.bleepingcomputer.com/news/security/>
- Krebs's on Security  
<https://krebsonsecurity.com/about/>
- Schneier on Security  
<https://www.schneier.com/blog/about/>
- HackerOne  
<https://www.hackerone.com/>



# Thanks!

Thejesh GN

<https://thejeshgn.com>

i@thejeshgn.com

## Thejesh GN

A container for all my views with excerpts from technology, travel, films, books, kannada, friends and other interests. I am Thejesh GN, friends call me Thej.

THEJESH GN > ABOUT

### ABOUT

Thejesh GN (ತೇಜೇಶ್ ಜಿ.ಎನ್) "Thej" is an independent technologist, developer, hacker, maker, traveller, blogger and an open data/internet enthusiast from Bangalore, India. He is the co-founder and chairman of DataMeet trust. [DataMeet](#) is the biggest community of data science and open data enthusiasts in India. They organise community meetups around the country and runs unconferences called Open Data Camps (ODC). His belief in open data and open research lead him to [open up his genome data\(DNA\)](#) in 2013.

He loves hacking open source software, researching and developing products, [speaking](#) at events and hosting workshops. His passion for using technology for social change won him the Infosys Community Empathy Fellowship in 2010. In 2018, he was awarded the IBM Champion title.

His core skills are research and development of new ideas, building proof of concepts, technical architecture, design and development.

Easiest way to reach him is by emailing [ i @ [thejeshgn dot com](mailto:i@thejeshgn.com)] or [use this form](#).

You can subscribe to his personal blog by RSS: [All posts](#) or just the [technology](#) posts.

He lives with [fictionhead](#) and [Max](#).

