From Trust Mandate to Security Debacle

Executive Summary — IDRBT .bank.in Domain Registry Investigation

Srikanth L, CashlessConsumer — Fintech & DPI Research

June 2026

EXECUTIVE SUMMARY

The IDRBT Domain Registration Portal at registrar.idrbt.ac.in — the exclusive registry for `.bank.in` banking domains under RBI purview — exposed its REST API via 33+ endpoints without authentication or authorization. Any unauthenticated internet user could retrieve 5,576 user records with bcrypt password hashes, OTP hashes, and PII; 1,072 orphan accounts with global Super Admin privileges; internal system configuration; and DSC proxy session initiation endpoints. The vulnerability persisted for approximately 13 months (May 2025 to June 2026).

The vulnerability was reported to CERT-In on June 8, 2026 within 25 minutes of discovery. CERT-In confirmed on June 25, 2026 that IDRBT has fixed the immediate API exposure. This executive summary distils the full investigation's key findings.

Key Statistics:

- **5,576** unique users with exposed credentials
- **6,752** total bcrypt password hashes across endpoints
- **33+** unauthenticated API endpoints
- **1,497** registered `.bank.in` domains
- **90.6%** of domains (1,356) have no matching IFSC code or DICGC insurance record
- **80%** of cooperative banks have no DNSSEC
- **40%** have no DMARC email authentication

1. The Vulnerability: No Authentication on Any API Endpoint

The IDRBT portal exposes over 33 REST API endpoints that serve data without any server-side authentication check. The Angular frontend sends an `Authorization: Bearer <jwtToken>` header, but the backend never validates it — identical data is returned with or without the token. During static decompilation of the frontend JavaScript bundles, every endpoint path was extracted and verified via live HTTP GET requests with no credentials. The environment is labeled "UAT'' in the frontend configuration but is deployed on the production domain.

Key endpoints included: full user database export (`/api/dr/user/all`), deleted users (`/api/dr/user/deleted-users`), orphan users (`/api/dr/user/orphan-users`), invoice database (`/api/dr/invoice/getByOrgId/{orgId}`), internal system configuration (`/api/dr/static/getAll`), DNSSEC configuration (`/api/dr/dnssec/algorithmTypes`), and DSC proxy endpoints forwarding to eMudhra middleware at `localhost.emudhra.com:26769`. Spring Boot actuator endpoints were also exposed.

2. Phantom Registrations and Test/Production Overlap

Multiple test domains coexist with real bank registrations in the production database. VKTEST — a phantom organization registered under the email `jhgf@gmai.com` — was granted Super Admin privileges and registered real `.bank.in` domains including `nml.bank.in`, which received a live SSL certificate and appears in Certificate Transparency logs alongside SBI and HDFC. Other phantom entities (IKCONTESTBANK, IDTMAY) and gibberish test domains (`testtest23.bank.in`, `datatest98.bank.in`) were found in the production billing database alongside legitimate bank registrations.

3. Non-Bank Entities in the Banking Namespace

At least one housing finance company (KHUSH HOUSING FINANCE) registered a `.bank.in` domain and was granted Super Admin privileges — demonstrating that the registry cannot reliably distinguish between banks and non-banks.

4. No Mandatory Security Baseline

Unlike the global `.bank` TLD (managed by fTLD Registry Services), which mandates DNSSEC, DMARC `p=reject`, HSTS, CAA, EV/OV certificates, weekly compliance scanning, and bug bounty programs, India's `.bank.in` requires none of these. The comparison is categorical: on every measured security dimension, the global standard enforces mandatory controls while the Indian equivalent makes them optional or absent. The result is that `.bank.in` domains can be hosted on shared $5/month US servers with $0 Let's Encrypt DV certificates, no protection against email spoofing, and no cryptographic validation of DNS records.

5. Data Residency Violations

At least four cooperative banks host their `.bank.in` websites on foreign servers — including the United States, Singapore, and Lithuania — raising serious concerns about compliance with RBI data localization requirements. Customers using these `.bank.in` domains have no way of knowing their banking data may cross international borders.

6. No Public Tender for Portal Development

The portal was built by IKCON Technologies (Hyderabad) without any public tender, RFP, or contract award found across IDRBT's tenders page (90+ tenders spanning 2020–2027), MSTC eProcure, or GeM. At least 22 IKCON employee accounts exist in the system, including three with global Super Admin access (organisationId = 0). IDRBT's own 32-page IT Vendor Management handbook — published in 2015 to teach banks how to procure IT properly — was violated on multiple fronts: no open tender, no public notice, no vendor evaluation, no documented justification for single-source procurement.

7. No Public Consultation on `.bank.in` Design

RBI announced `.bank.in` in a bi-monthly monetary policy statement, not through a consultation paper or draft circular for public comment. Unlike the global `.bank` TLD — developed through years of multi-stakeholder consultation — India's banking namespace was designed and mandated in near-total opacity. IDRBT's own academic researchers have published peer-reviewed work on DNSSEC deployment and domain security that could have informed a secure-by-design registry, but none of this research appears to have influenced the implementation.

8. Impact Assessment

The exposure of 5,576 user records with bcrypt password hashes creates a credential compromise risk for employees across Indian banks, cooperative banks, and financial institutions. With recovered credentials, attackers could log in to the portal and manage domain registrations, DNS settings, and billing — enabling domain hijacking that could redirect banking traffic. The exact user list, mobile numbers, and organization context enable highly targeted spear-phishing against banking staff. The reputational damage to India's banking digital infrastructure is significant: the national domain registrar under RBI purview was the weakest link in the trust chain it was meant to enforce.

Responsible Disclosure Timeline:

- **June 8, 2026, 05:07 UTC** — Discovery of first unauthenticated endpoint during OSINT scan
- **June 8, 2026, 05:30 UTC** — Initial report filed with CERT-In
- **June 8, 2026, 07:30 UTC** — Extended findings filed (orphan users, phantom domains, DSC proxy)
- **June 25, 2026** — CERT-In confirms vulnerability fixed by IDRBT

Methodology: All findings were obtained using only passive, non-invasive reconnaissance — static decompilation of the Angular frontend from public JavaScript bundles, unauthenticated HTTP GET requests, Certificate Transparency log queries, standard DNS lookups, HTTP header inspection, and public geolocation APIs. No injection, no brute force, no exploit code, no password cracking, and no data exfiltration. Every finding can be independently reproduced with `curl` and `dig`.

Techniques explicitly NOT used: No port scanning, no network-level reconnaissance, no zero-day exploitation, no fuzzing, no phishing or social engineering, no MITM, no POST/PUT/DELETE requests, no data modification of any kind.

Recommendations: Force password reset for all 5,576 affected users; lock orphan Super Admin accounts; mandate DMARC `p=reject`, DNSSEC, HSTS, and EV/OV certificates for all `.bank.in` domains; enforce data residency requirements for cooperative banks; publish an open RFP for all future registry development; establish a vulnerability disclosure program and bug bounty; conduct weekly compliance scanning following the fTLD `.bank` model.

Full report: https://zo.pub/cashlessconsumer/idrbt-bankin-report/report.pdf \
Website: https://cashlessconsumer.zo.space/bankin-report \ **Open data & domain monitoring:** https://github.com/CCAgentOrg/bank-in-domains \ **Source code & scripts:** https://github.com/CCAgentOrg/idrbt-bankin-investigation

Report by Srikanth L, CashlessConsumer. June 2026.