From Trust Mandate to Security Debacle

A Security Investigation of the IDRBT .bank.in Domain Registry Portal

Srikanth L, CashlessConsumer

June 2026

Contents

Contact: cashlessconsumerin@gmail.com

EXECUTIVE SUMMARY

The IDRBT Domain Registration Portal at registrar.idrbt.ac.in — the exclusive registry for `.bank.in` banking domains — exposed its entire REST API via 33+ unauthenticated endpoints. For over a year, anyone on the internet could retrieve bcrypt password hashes, mobile numbers, email addresses, login IPs, and device fingerprints for **5,576 bank employees** — the people entrusted with managing India's banking domains. The trust anchor meant to protect citizens was itself wide open.

Governance failures: The portal was built by IKCON Technologies without any public tender, RFP, or competitive process — in direct violation of IDRBT's own published procurement handbook (2015). IKCON held 22 employee accounts, including 3 with global Super Admin access. The `.bank.in` namespace itself was mandated without public consultation, impact assessment, or a published security baseline, and IDRBT's own academic research on domain security was ignored in its implementation.

Systemic gaps: Of 1,497 registered domains, only **6.9%** match across RBI IFSC and DICGC insurance records — the rest include phantom test domains, gibberish registrations, and non-bank entities, several with live SSL certificates. Unlike the global `.bank` TLD (which mandates DNSSEC, DMARC `p=reject`, HSTS, and EV/OV certificates), `.bank.in` enforces none of these: 80% of cooperative banks lack DNSSEC, 40% have no DMARC, and multiple banks host customer-facing sites on foreign servers in violation of RBI data localization rules.

Disclosure: The vulnerability was reported to CERT-In on June 8, 2026. CERT-In confirmed on June 25, 2026 that IDRBT has fixed the issue. This report documents the full investigation, findings, and systemic gaps in India's banking domain security framework.

Key Statistics:

- **5,576** unique users with exposed credentials (**6,752** bcrypt hashes)
- **1,072** orphan Super Admin accounts unassociated with any organization
- **33+** unauthenticated API endpoints
- **1,497** registered `.bank.in` domains; only **6.9%** verifiable against IFSC/DICGC
- **80%** of cooperative banks have no DNSSEC; **40%** have no DMARC
- **Zero** public tender for the registry's development

1 Introduction

1.1 What is `.bank.in`?

On February 7, 2025, the Reserve Bank of India announced the creation of `.bank.in` — a dedicated Internet domain namespace for Indian banks, managed by the Institute for Development and Research in Banking Technology (IDRBT). The intent was straightforward: create a "trusted zone'' where citizens could verify they were visiting a legitimate bank website.

A `.bank.in` domain is supposed to be the digital equivalent of a bank's physical branch — you see the name on the door, you know it's real. The RBI circular (RBI/2025-26/28, April 22, 2025) mandated that all scheduled commercial banks, cooperative banks, and regional rural banks migrate to `.bank.in` domains.

1.2 Why Domain Trust Matters

When a citizen types `sbi.bank.in` into their browser, the `.bank.in` suffix serves as a trust anchor. It answers one question: "Is this website genuinely operated by the entity it claims to be?''

This trust anchor is critical because:

1. **Phishing defense:** Scammers can register `sbi-secure-login.com` easily, but they should not be able to register `sbi.bank.in`. The `.bank.in` namespace is exclusive to verified banks.
2. **Consumer confidence:** The RBI stamp of approval on the domain gives citizens confidence that they are on a legitimate banking platform.
3. **Regulatory oversight:** A managed namespace enables RBI to enforce security standards across all banking domains.

However, domain trust is only as strong as the controls at the registry. If the registry itself has weak authentication, unpatched vulnerabilities, and no enforcement of baseline security, the trust anchor is compromised.

2 Domain Trust: `.bank` (Global) vs `.bank.in` (India)

2.1 Background

The global `.bank` Top-Level Domain is managed by fTLD Registry Services, a consortium founded by the American Bankers Association. It enforces the strongest security requirements of any TLD, including mandatory DNSSEC, DMARC `p=reject`, HSTS, and certificate authority authorization.

India's `.bank.in` was created as a sub-domain under the existing `.in` ccTLD (managed by NIXI). This architectural choice gives IDRBT far less control over security policy compared to a full TLD registry, but the security gaps found go well beyond what is explainable by this distinction.

2.2 Side-by-Side Comparison

Security Requirement	`.bank` (Global)	`.bank.in` (India)
DNSSEC	Mandatory	Optional — 80% not deployed
DMARC	Mandatory p=reject	Optional — 40% no DMARC
HSTS	Mandatory	Optional — 47% not deployed
CAA	Mandatory	Not checked — 0% deployed
TLS Version	TLS 1.2+ mandatory	Not enforced
Certificate Type	EV/OV minimum	DV (Let's Encrypt) accepted
Compliance Scanning	Weekly, 18+ ports	Not conducted
Bug Bounty / VDP	Active program	None — no security.txt
Phishing Takedown	24/7 monitoring	Not present
Data Residency	Jurisdiction-dependent	Not enforced
Registrar Auth	Mandatory MFA	33+ unauthenticated endpoints

2.3 What the Comparison Reveals

The gap between `.bank` and `.bank.in` is not incremental — it is categorical. On every measurable security dimension, the global standard imposes mandatory, enforceable requirements while the Indian equivalent makes them optional or ignores them entirely.

This is particularly concerning because:

1. **Cooperative banks are the most vulnerable:** 1,433 Urban Cooperative Banks and 352 District Central Cooperative Banks hold deposits of millions of ordinary

citizens. These banks typically lack the security teams and budgets of large commercial banks. The `.bank.in` namespace was supposed to provide a safety net for these institutions. Instead, our investigation found cooperative banks with:

- Hosting on shared servers in the United States, Singapore, and Lithuania
- No DNSSEC (80%+)
- No DMARC (40%+)
- Free Let's Encrypt DV certificates (no identity verification beyond domain control)

2. **The trust anchor is illusory:** A citizen visiting `sirsadccb.bank.in` sees the `.bank.in` suffix and reasonably assumes RBI-level security. In reality, the website may be hosted on a shared $5/month US server, have a 0$ certificate, no protection against email spoofing, and no cryptographic validation of its DNS records.
3. **The registry was the weakest link:** The portal that issues these "trusted" domains was leaking every employee's bcrypt password hash to anyone with `curl`. The trust anchor itself was untrustworthy.

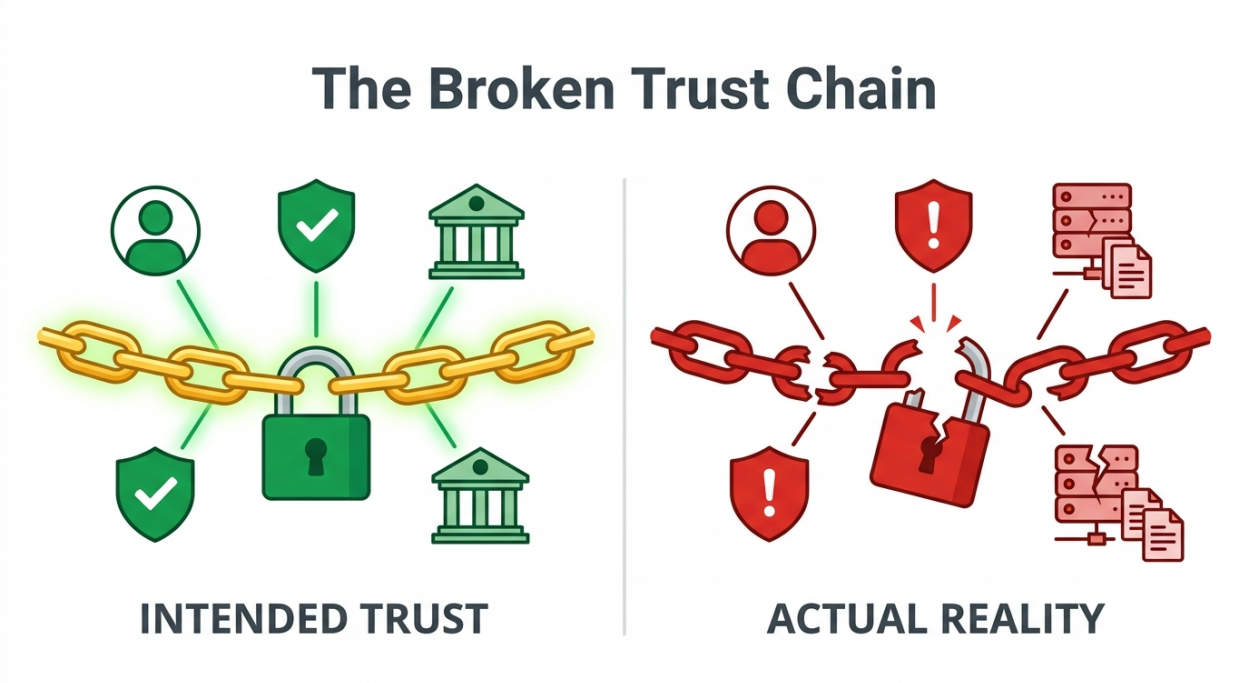

Figure 1: The Broken Trust Chain — how an open registry undermined the trust anchor meant to protect citizens.

3 Disclosure Timeline

Date	Event
Apr 8, 2026	IDRBT publishes Limited RFP for VAPT of its IT infrastructure (limited tender, not open).
Feb 7, 2025	RBI announces `.bank.in` namespace in bi-monthly monetary policy statement.
Apr 22, 2025	RBI circular RBI/2025-26/28 — formal mandate for `.bank.in` adoption by all scheduled commercial banks, cooperative banks, and RRBs.
May 2025	IDRBT Domain Registration Portal (registrar.idrbt.ac.in) launched. Portal developed by IKCON Technologies without visible public tender process.
Jun 8, 2026 05:07 UTC	CashlessConsumer discovers first unauthenticated user database endpoint during routine OSINT scan of `.bank.in` infrastructure.
Jun 8, 2026 05:30 UTC	Initial responsible disclosure report filed with CERT-In (`incident@cert-in.org.in`).
Jun 8, 2026 06:30 UTC	Discovery of unauthenticated invoice and billing endpoints (1,535 records).
Jun 8, 2026 07:30 UTC	Updated report filed with CERT-In documenting orphan users (1,072), phantom domains, DSC proxy exposure, and extended endpoint enumeration.
Jun 9, 2026	CERT-In assigns acknowledgement reference `CERTIn-62780526` and confirms receipt of disclosure.
Jun 25, 2026	CERT-In confirms vulnerability has been fixed by IDRBT (reference: `CERTIn-62780526`).

4 Impact Assessment

4.1 1. Credential Compromise [CRITICAL]

5,576 unique users have bcrypt password hashes exposed across multiple unauthenticated endpoints. Weak passwords (common for inter-bank portals) can be cracked offline. Affects employees of Indian banks, cooperative banks, and financial institutions.

4.2 2. Account Takeover Risk [HIGH]

With recovered credentials, attackers can log in to the portal and manage domain registrations for .IN banking domains, DNS settings, and billing. Domain hijacking could redirect banking traffic.

4.3 3. Phishing at Scale [HIGH]

Exact user list, mobile numbers, email addresses, organization names, and invoice context enable highly targeted spear-phishing against banking staff.

4.4 4. Domain Hijacking Risk [HIGH]

With portal access, an attacker could transfer domain registrations, change DNS records to redirect banking traffic, or modify billing information.

4.5 5. Reputational Damage [MEDIUM]

The national banking domain registrar under RBI purview leaking user data and financial records undermines trust in India's banking digital infrastructure.

4.6 6. Systemic Weakness [MEDIUM]

No mandatory DMARC, DNSSEC, HSTS, or CAA enforcement. The global `.bank` TLD requires all of these. India's `.bank.in` requires none.

5 Attack Scenarios: What If a Bad Actor Had Found This First?

The vulnerability documented in this report was discovered and responsibly disclosed within 25 minutes. But the portal had been live for over 13 months. Below are realistic attack chains a malicious actor could have executed — each one using only the data already accessible through the unauthenticated endpoints.

5.1 Scenario 1: Phishing at Scale

Time required: Under an hour.

An attacker downloads the full user database (5,461 records) containing names, email addresses, mobile numbers, and organization names. Each record identifies exactly which bank employee manages which bank's domain registration. The attacker crafts personalised spear-phishing emails:

- "Dear [Name], your bank's .bank.in domain registration is expiring. Click here to renew." — sent to the exact person responsible.
- "Dear [Name], IDRBT requires re-verification of your DSC. Use this link." — sent with the recipient's correct bank name, designation, and phone number.

These emails would appear legitimate because they contain correct internal details only the real IDRBT portal should know. A single compromised credential would give the attacker authenticated access to the portal.

5.2 Scenario 2: Domain Hijacking via Credential Theft

Time required: A few days to weeks, depending on password strength.

The exposed bcrypt hashes include those of 1,072 orphan Super Admin accounts — accounts with no organisation association, meaning they can access any bank's domain settings. Even bcrypt can be cracked for weak passwords. A bank employee whose password is something like `password123` or `bank@2025` would have their hash cracked in hours.

With Super Admin access, an attacker can:

- Transfer any `.bank.in` domain to a different registrar
- Change DNS records to point the bank's domain to a phishing server
- Modify the bank's contact email and billing information
- Lock legitimate bank administrators out of their own domain

5.3 Scenario 3: The Invisible Redirect

Time required: Minutes with portal access.

An attacker with portal credentials changes the A record for `sirsadccb.bank.in` (a real cooperative bank) from the legitimate server IP to a phishing site hosted on a

cheap overseas server. The SSL certificate on the phishing site is obtained via Let's Encrypt — free, automated, and requiring no identity verification. Since `.bank.in` does not mandate EV/OV certificates or Certificate Authority Authorization, the browser shows a green padlock next to the fake site.

A customer checking their balance sees a page that looks identical to their bank's website. They enter their username, password, and OTP. The attacker now has everything needed to drain their account. The customer has no way to know — every visible signal (the `.bank.in` domain, the padlock icon, the familiar layout) tells them this is legitimate.

5.4 Scenario 4: Insider Threat Amplification

Time required: Instant.

The exposed data includes device fingerprints and login IP addresses of every registered user. An attacker can map which employees have Super Admin access versus regular user access, which organisations have the weakest security postures (cooperative banks with minimal IT staff), and which employees have not logged in recently (orphaned or stale accounts ripe for takeover).

This intelligence would allow a nation-state actor or organised cybercrime group to target the weakest link in the trust chain with surgical precision.

5.5 Key Takeaway

None of these scenarios required exploiting a zero-day, bypassing a firewall, or writing a single line of exploit code. The attacker only needed `curl`. The data was already public. The only reason these scenarios did not materialise is that CashlessConsumer found the vulnerability first and reported it responsibly — before any malicious actor did.

6 Domain Triangulation

6.1 Methodology

IDRBT's database of registered `.bank.in` domains was cross-referenced against two authoritative datasets:

1. **RBI IFSC database** — 1,510 bank codes for scheduled commercial banks, cooperative banks, and RRBs
2. **DICGC insured banks list** — 1,933 banks covered by deposit insurance

6.2 Results

Category	Count	Percentage
Matched: Domain + IFSC + DICGC	104	6.9%
Matched: Domain + IFSC only	5	0.3%

Matched: Domain + DICGC only	27	1.8%
Unmatched: Domain only	1,356	90.6%
Total	**1,497**	

A caveat on name matching. Cross-referencing these three datasets is harder than it looks. Banks use varying legal names across registries (e.g. `State Bank of India'' vs`SBI’’, cooperative banks with regional names in multiple scripts), the IDRBT domain list does not carry a canonical organisation identifier, and IFSC/DICGC records key off different naming conventions. A domain that fails to match is not necessarily fake or invalid — it may simply use a name the fuzzy-matching did not catch. The figures below should therefore be read as indicative findings rather than a precise count of illegitimate domains.

The cross-reference surfaced the following categories:

- Cooperative banks registered in the IDRBT system but not in the IFSC database
- Test/phantom entities (VKTEST, IKCONTESTBANK, IDTMAY)
- Non-bank entities (housing finance companies, fintechs)
- Domains with no live DNS configuration (95 domains without NS records)
- UAT/test domains with active SSL certificates in CT logs

7 Systemic Issues

7.1 Test/Production Overlap

Multiple test domains were found alongside real banks in the production database:

- `vktest.bank.in` — Phantom org with live NS records
- `ikcontest-aug12.bank.in` — IKCON test domain
- `testtest23.bank.in`, `datatest98.bank.in` — Gibberish test domains
- `rbi.bank.in` — Registered but not pointing to RBI's actual website
- `jhgf@gmai.com`, `kjhghj@mgai.com` — Gibberish email registrations

These phantom domains are not just administrative noise — several have active SSL certificates in Certificate Transparency logs, confirming they went through the full domain validation pipeline.

7.2 No Public Tender

No public tender, RFP, or contract award for the development of the Domain Registration Portal was found across:

- IDRBT's tenders page (90+ tenders spanning 2020-2027)
- MSTC eProcure portal
- GeM (Government e-Marketplace)
- General web search

This gap becomes even more striking given that a separate Limited Request for Proposal for VAPT (Vulnerability Assessment and Penetration Testing) of IDRBT's IT infrastructure was published on April 8, 2026 at https://www.idrbt.ac.in/wp-content/uploads/2026/04/Limited-RFP-for-VAPT-of-IDRBT-IT-Infra-Apr-2026-V2.pdf — a limited, non-open tender just two months before the `.bank.in` portal vulnerabilities were discovered. The VAPT RFP itself was a limited tender, contradicting IDRBT's own procurement norms that mandate open tenders for security-critical work.

The portal footer states "Developed \& Maintained by IDRBT'' but technical evidence shows development by \textbf{IKCON Technologies} (Hyderabad), with 22 employee accounts in the system including 3 with global Super Admin access. IKCON's own public website lists the `.bank.in` registrar as a marquee client engagement and claims to have advised over 380 cooperative banks on domain migration https://www.ikcontech.com/our-story, while its core offerings (Unified Meeting Suite, ResolveGen ticketing system) are unrelated to banking domain security.

IDRBT's Own Security Claims Contradicted

The IDRBT Domain Registration Portal's Privacy Policy and Terms of Use, published on the same registrar portal, make explicit security representations that are directly contradicted by this investigation's findings:

- The Privacy Policy claims the portal "has been placed in protected zones along with firewall and IPS protection" — yet 33+ API endpoints were accessible without any authentication.
- It states the portal has been "audited for known application-level vulnerabilities before launch" — yet the unauthenticated user database endpoint was present from day one of the portal (May 2025).
- It asserts that "all known vulnerability was addressed before launching the web application" — yet bcrypt password hashes for 5,576 users were exposed for over 13 months.
- The Terms of Use state that "IDRBT shall endeavor to ensure that the website is available and secure at all times" — a commitment demonstrably broken.

These documents remain live on the portal at the time of this report's publication https://registrar.idrbt.ac.in.

7.3 Data Residency Violations

Multiple cooperative banks were found hosting their `.bank.in` websites on foreign servers:

- **United States:** Sri Satya Sai DCCB, multiple cooperative banks on shared US hosting
- **Lithuania:** `sps.bank.in` — bank email server in Amsterdam
- **Singapore:** Routing via CDN edge nodes outside India

This raises serious concerns about compliance with RBI data localization requirements and exposes cooperative bank customers to foreign jurisdiction risks.

7.4 Procurement & Governance

Beyond the technical vulnerabilities, an equally troubling picture emerges from how the `.bank.in` registry was procured, designed, and governed.

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

RBI announced `.bank.in` in its bi-monthly monetary policy statement on February 7, 2025 — not through a consultation paper, draft circular for public comment, or any stakeholder engagement process. The formal circular (RBI/2025-26/28, April 22, 2025) was issued with immediate effect, giving banks barely six months to migrate. Unlike the global `.bank` TLD — which was developed over years through multi-stakeholder consultation involving the ABA, fTLD Registry, financial institutions, and security researchers — India's `.bank.in` was designed and mandated in near-total opacity. No green paper, white paper, or impact assessment was published.

7.4.2 IDRBT's Own Procurement Handbook — Violated for `.bank.in`

IDRBT literally wrote the book on public procurement. In 2015, it published **ÏT Vendor Management: Principles & Practiceš** — a comprehensive 32-page handbook authored by Dr. G.R. Gangadharan (Assistant Professor, IDRBT) with a foreword by then-Director Dr. A.S. Ramasastri. It was meant to teach banks how to procure IT properly.

IDRBT then violated multiple principles from its own handbook for the `.bank.in` portal:

- The handbook mandates open/global tender for purchases above a cut-off amount — no tender of any kind was found
- It requires notice in at least one national daily and the bank's website — zero public notice was issued
- It mandates financial and technical evaluation of vendors — IKCON had no prior banking application projects
- Deviations from procedure must be documented with logical reasons — no documentation of procurement decision exists
- Single tender only in exceptional cases with recorded justification — single-source award to IKCON with no justification

The handbook itself warns: *Ïf the buyer knows neither his/her requirements nor about vendors' capabilities or products, then the IT project is certain to faïl.*

7.4.3 Academic Security Research — Published but Ignored

IDRBT is primarily a research and training institute. Its academic staff have published multiple papers on domain security, DNSSEC deployment, and cybersecurity benchmarks for the banking sector. Yet none of this research appears to have informed the `.bank.in` implementation. The registry mandates none of the security controls that IDRBT's own researchers have argued for in peer-reviewed literature — no DNSSEC requirement, no DMARC enforcement, no EV/OV certificate mandate, no data residency verification. Research that could have shaped a secure-by-design registry was published, filed, and apparently ignored by the same institution.

7.4.4 Unnecessary Exposure of Internal Systems

The `.bank.in` migration created a structural side effect that was entirely preventable: banks migrated far more than their public-facing websites. Certificate Transparency logs and the domain registration database reveal HRMS portals, payroll dashboards, employee self-service platforms, UAT instances, and staging environments all registered under `.bank.in` — each one publicly resolvable and carrying an SSL certificate that confirms domain validation.

This is harmful in two ways. First, every such registration leaks metadata about a bank's internal technology stack: hosting providers, server software, certificate issuers, and subdomain naming conventions that reveal network topology. An attacker

can enumerate HRMS platforms (typically running older, less frequently patched software), identify UAT instances (which may run unpatched code), and map the attack surface of a bank without sending a single packet past its production firewall.

Second, the `.bank.in` suffix itself lends credibility to these systems. A bank employee receiving an email linking to `hrms.sirsadccb.bank.in` is far more likely to enter credentials than one linking to `hrms.sirsadccb.com`. The trust marker intended for citizens has become an attack vector against employees.

A proper design review — the kind an open RFP or public consultation would have produced — would have anticipated this. The global `.bank` TLD explicitly limits registration to customer-facing banking services with strict subdomain controls. India's `.bank.in` has no such restrictions, and the oversight directly expands the attack surface of the banking sector.

7.4.5 What Should Have Happened

A proper process would have included:

1. A public consultation paper on `.bank.in` design inviting feedback from banks, security researchers, and the public
2. An open tender for the domain registration portal with published evaluation criteria
3. A published security baseline drawing on IDRBT's own academic research and global benchmarks like fTLD
4. Regular independent security audits
5. A vulnerability disclosure program

None of these happened. India's banking namespace — meant to be a trust anchor — was built without the trust-building processes that public infrastructure deserves.

8 Methodology

All findings in this report were obtained using only passive and non-invasive techniques. No exploit was written, no payload was delivered, and no authentication was bypassed through active means.

Techniques used:

- **Static decompilation:** The Angular frontend JavaScript bundles were downloaded from the public URL and decompiled to reveal API endpoint paths, request/response schemas, and authentication logic. This is equivalent to a user viewing a website's source code.
- **Unauthenticated GET requests:** Each discovered endpoint was accessed via HTTP GET with no authentication headers, tokens, or session cookies. No POST, PUT, DELETE, or PATCH requests were made. No data was modified or submitted.
- **Certificate Transparency log analysis:** Public CT logs (crt.sh) were queried for all known `.bank.in` subdomains. This is a public, rate-limited API that requires no authentication.
- **DNS resolution checks:** Standard `dig` and `nslookup` queries were used to verify domain delegation, name server configuration, DNSSEC status, and DMARC/SPF records.
- **HTTP header inspection:** Live `.bank.in` domains were probed with standard HTTP HEAD/GET requests to check security header deployment (HSTS, CSP, X-Frame-Options). No content was downloaded beyond headers.
- **Geolocation via public APIs:** Server IP addresses were checked against public geolocation databases (ip-api.com) to identify hosting jurisdictions.
- **Public source code analysis:** The portal's frontend code was examined for hardcoded configuration, test credentials, and API path structures — all visible to any browser that loads the page.

Reproducible Verification

All findings can be independently verified using the following techniques:

8.0.1 Unauthenticated API Access

```
# Returns full user database --- no token required
curl -s 'https://registrar.idrbt.ac.in/api/dr/user/all'
```

8.0.2 Phantom Domain Detection

```
# Check if registered domain has active DNS
dig +short datatest98.bank.in A @8.8.8.8
```

```
# Empty = registered but not published to NIXI
```

8.0.3 Data Residency Check

```
domain="sirsadccb.bank.in"
ip=$(dig +short $domain A @8.8.8.8 | head -1)
curl -s "http://ip-api.com/json/$ip" | jq '.country, .city'
```

Ethical Boundaries

Data used: Public APIs, CT logs, DNS, client-side source code. \ **Data NOT used:** No password cracking, no stolen tokens, no injection, no brute force.

What was NOT done:

- No brute force, injection, or privilege escalation
- No password cracking (bcrypt hashes were never extracted or processed offline)
- No phishing, social engineering, or MITM
- No port scanning or network-level reconnaissance
- No zero-day exploitation or fuzzing
- No data exfiltration — extracted data was never downloaded to persistent storage

Every finding in this report can be independently reproduced by any researcher with `curl` and `dig`. No specialized tools, authenticated access, or exploit code is required. This is not a testament to sophisticated research — it is evidence of how fundamentally broken the access controls were.

9 Recommendations

9.1 Immediate (Confirmed Fixed by CERT-In)

1. Block ALL unauthenticated GET endpoints behind server-side authentication
2. Implement server-side JWT validation on all API endpoints

9.2 Short-term

1. Force password reset for all 5,576 affected users
2. Purge soft-deleted user records containing PII
3. Lock orphan Super Admin accounts
4. Audit nginx access logs for potential data exfiltration
5. Implement rate limiting and IP allowlisting at API gateway
6. Disable Spring Boot Actuator on production

9.3 Long-term (Governance)

1. DMARC `p=reject` enforcement for all `.bank.in` domains
2. DNSSEC mandatory for all domain delegations
3. HSTS preload submission for `.bank.in` TLD
4. Mandatory EV/OV certificates for banking domains (minimum)
5. Open security.txt, bug bounty, and vulnerability disclosure program
6. Public RFP for all future registry development
7. Weekly compliance scanning, annual security audit
8. Data residency enforcement for cooperative banks
9. Automated compliance scanning (following fTLD `.bank` model)

10 Open Data

All non-sensitive datasets from this investigation are published for independent verification and further research. No PII, bcrypt hashes, or sensitive data is included in published datasets.

Dataset	Records	Published?
Domains (`domains.txt`)	1,497	Yes
Domains with NS (`domains-with-ns.txt`)	1,402	Yes
Domains without NS (`domains-without-ns.txt`)	95	Yes
Billing records (anonymized)	1,535	Yes
Certificate transparency log	3,797	Yes
User records (original leak)	5,461	**No — contains PII/hashes**
Orphan user records	1,072	**No — contains PII/hashes**

The domain list from this investigation feeds into the **bank-in-domains** project at https://github.com/CCAgentOrg/bank-in-domains — a daily automated audit of `*.bank.in` and parallel Indian financial TLDs. Every day at 02:30 UTC, it discovers new subdomains from Certificate Transparency logs, Wayback Machine, urlscan.io, and HackerTarget, then probes each one for DNS resolution, HTTPS reachability, HTTP status codes, and page titles. Results are published as CSV, JSONL, Parquet, and SQLite.

This data enables the broader public to build their own monitoring tools — including uptime monitors like https://uptime.cashlessconsumer.in which tracks the live status of Indian banking and financial domains in near real-time. Any researcher, journalist, or concerned citizen can use the open data to independently verify which bank websites are operational and which have security gaps.

Source code and scripts for all analysis: https://github.com/CCAgentOrg/idrbt-bankin-investigation

11 Conclusion

The `.bank.in` namespace is a well-intentioned initiative to create a trusted zone for Indian banking. However, the investigation reveals fundamental gaps at every level of the trust chain:

1. **The registry** (IDRBT) had critical vulnerabilities in its domain registration portal, exposing the credentials and data of every bank employee registered in the system.
2. **The registrar** (IKCON Technologies) was appointed without public tender and had un-deprovisioned Super Admin access.
3. **The security baseline** is voluntary — unlike the global `.bank` TLD, India's `.bank.in` does not mandate DNSSEC, DMARC, HSTS, or CA Authorization.
4. **Enforcement is absent** — cooperative banks host customer-facing websites on foreign servers, use basic DV certificates, and have no email authentication.
5. **Testing and production are not separated** — phantom test domains, gibberish accounts, and UAT configurations coexist with real bank registrations.

The good news: CERT-In confirmed the vulnerability is fixed. The exposed endpoints are no longer accessible.

The concerning reality: The fix addresses the immediate API exposure but does not address the systemic issues documented in this report — the lack of mandatory security baselines, the absence of public procurement, the data residency gaps, or the phantom domain problem.

This report is published as a responsible disclosure. No exploit code or active attack paths are included. All data was obtained from publicly accessible APIs with no authentication bypass — no brute force, no injection, no privilege escalation was used.

Full evidence archive: https://zo.pub/cashlessconsumer/idrbt-bankin-security \
Source code & scripts: https://github.com/CCAgentOrg/idrbt-bankin-investigation \
Proof-of-concept video: https://zo.pub/cashlessconsumer/idrbt-poc-video

12 Responsible Disclosure

This investigation was conducted under standard responsible disclosure principles.

Initial notification: June 8, 2026, 05:30 UTC — filed with CERT-In (`incident@cert-in.org.in`) within 25 minutes of discovery.

Subsequent filings: June 8, 2026, 07:30 UTC — extended findings including orphan users, phantom domains, and DSC proxy exposure.

Remediation confirmed: June 25, 2026 — CERT-In confirmed IDRBT has fixed the vulnerability.

Principles followed:

- Full discovery timeline disclosed to CERT-In before publication
- No exploit code published
- No active customer data published (all PII redacted in any public datasets)
- All evidence shared privately with CERT-In for verification
- Publication delayed until remediation was confirmed
- No data exfiltration — extracted data was never downloaded to persistent storage

The vulnerability was present for approximately 13 months (May 2025 – June 2026). CERT-In's confirmation of the fix means the exposed endpoints are no longer accessible. However, we cannot confirm how long the exposure existed before discovery, or whether any malicious actor accessed the data during that period.

13 References

Primary Sources & Official Documents

- Reserve Bank of India, *Statement on Developmental and Regulatory Policies*, February 7, 2025. Announces creation of `.bank.in` domain.
  https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=59693
- Reserve Bank of India, *Migration to `.bank.in` domain*, Circular RBI/2025-26/28, CO.DIT.DCD.No.S81/01-71-110/2025-26, April 22, 2025.
  https://rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=12837
- IDRBT Domain Registration Portal (`.bank.in` exclusive registrar). Opened May 2025.
  https://registrar.idrbt.ac.in
- Indian Computer Emergency Response Team (CERT-In). Vulnerability disclosure and remediation coordination.
  https://www.cert-in.org.in
- DICGC — Deposit Insurance and Credit Guarantee Corporation (insured banks list).
  https://www.dicgc.org.in

Security Standards & Technical References

- fTLD Registry Services, *Security Requirements for .BANK* — mandatory DNSSEC, DMARC `p=reject`, HSTS, EV/OV certificates.
  https://ftld.com/security
- fTLD Registry Services homepage.
  https://ftld.com
- Spamhaus, *Can you .bank on this registry for security?* — comparative analysis of `.bank` vs other TLD-level security.
  https://www.spamhaus.org/resource-hub/service-providers/can-you-bank-on-this-registry-for-security
- IDRBT, *IT Vendor Management: Principles & Practices* (2015). Authored by Dr. G.R. Gangadharan, foreword by Dr. A.S. Ramasastri. IDRBT's own procurement handbook.

Tools & Data Sources

- crt.sh — Certificate Transparency log search.
  https://crt.sh
- NIXI — National Internet Exchange of India (`.in` ccTLD registry).
  https://registry.in

- ip-api.com — Public IP geolocation API used for data residency checks. http://ip-api.com/json/
- Cloudflare Learning Center — Background on DNSSEC, DMARC, HSTS, and TLS. https://www.cloudflare.com/learning/

IDRBT Published Documents

- IDRBT, *Limited RFP for Conducting VAPT of IDRBT IT Infrastructure*, Tender No. IDRBT/SYS/ES/10/2025-2026, April 8, 2026. A limited (non-open) tender issued just two months before the vulnerability was discovered. The VAPT did not detect the unauthenticated API exposure. (https://www.idrbt.ac.in/wp-content/uploads/2026/04/Limited-RFP-for-VAPT-of-IDRBT-IT-Infra-Apr-2026-V2.pdf)
- IDRBT, *Domain Registration Portal — Terms and Conditions* (undated, portal launched May 2025). The governing terms for `.bank.in` domain registration. (https://registrar.idrbt.ac.in)
- IDRBT, *Privacy Policy* (domain registration portal). Contains security representations including "protected zones with firewalls and IPS", "audited for known application-level vulnerabilities before launch", and "all known vulnerability was addressed." Our investigation contradicts these claims. (https://registrar.idrbt.ac.in)
- IDRBT, *DRO Training Programme on Domain Registrar Operations* (August 12, 2025). Online training for bank officers on using the `.bank.in` registration portal.
- IDRBT, *Domain Registration Guidelines* — Registrant Registration Flow, Registration Terms, and governing policies.
- IKCON Technologies, *Official Website* — Banking Support service line. IKCON claims "380+ banks migrated" with the `.bank.in` portal as a marquee project. (https://ikcontech.com)
- Times of India, *Most banks shifted to 'bank.in' domain: IDRBT to RBI guv*, December 19, 2025. Reports 889 domains registered by 747 unique banks. (https://timesofindia.indiatimes.com/city/hyderabad/most-banks-shifted-to-bank-in-domain-idrbt-to-rbi-guv/articleshow/126064153.cms)
- EasyDMARC, *fTLD Registry Partners with EasyDMARC to Enforce Email Security for .BANK Domains*. Demonstrates the global standard's enforcement approach vs India's voluntary model. (https://easydmarc.com/blog/ftld-registry-partners-with-easydmarc-to-enforce-email-security-for-bank-domains)
- fTLD Registry Services, *Implementation Guide for .BANK Registrants*. Detailed security baseline requirements for the global TLD. (https://register.bank/implementation-guide)
- Hacker News, *RBI announces .bank.in domain for Indian banks*, February 2025. News coverage at launch. (https://news.ycombinator.com)

14 Appendix A: Explain It Like I'm Five (ELI5)

What happened?

India's central bank (RBI) created a special internet address ending in `.bank.in` so that people could tell real bank websites apart from fake ones. The idea was good: if a website ends in `.bank.in`, you should be able to trust it's a genuine bank — like seeing a government stamp on a document.

The company in charge of handing out these special addresses (IDRBT) built a website to manage them. But that website was left wide open. Anyone in the world — with no password, no login, nothing — could look up the private details of thousands of bank employees: their email addresses, phone numbers, and scrambled versions of their passwords. For over a year.

Why should I care?

- **Your money could be at risk.** If a bad actor had used this leak to take over a bank's website, they could have shown you a fake login page that looked 100% real — and stolen your username, password, and OTP. This is how people lose their life savings to phishing.
- **The "trust stamp" was broken.** The whole point of `.bank.in` was that seeing it means "this is safe." But the office issuing the stamps was itself unlocked. So the guarantee you were told to rely on wasn't actually reliable.
- **Small banks are the weakest.** Many cooperative banks (where ordinary people, farmers, and small businesses keep their money) run their websites on cheap foreign servers with almost no security. They're easy targets.
- **It was fixed, but the system wasn't.** The open door is now closed. But the deeper problems — no rules forcing banks to use basic security, no proper checks, no transparency in how this was built — are still there.

The short version

Someone left the keys to India's banking ''trusted zone'' under the doormat for over a year. A researcher found it, reported it quietly, and it's now locked. But the house itself still needs better locks, alarm systems, and rules about who gets to build the next one.

15 Appendix B: Glossary

`.bank.in` A special internet domain ending reserved for Indian banks, managed by IDRBT under RBI's direction. Meant to signal "this is a genuine bank website."

API (Application Programming Interface) A way for computer programs to talk to each other. Here, the registry's API was supposed to be private but was left public — like a bank vault with the door open.

Bcrypt hash A scrambled, one-way version of a password. Strong passwords are hard to unscramble; weak ones (like `password123`) can be cracked in seconds.

CAA (Certification Authority Authorization) A DNS record that says which companies are allowed to issue SSL certificates for a domain. Stops outsiders from getting fake certificates for your bank.

CERT-In India's official cybersecurity emergency response team. The place you report security holes to.

DICGC Deposit Insurance and Credit Guarantee Corporation. Insures your bank deposit up to **Rs. 5 lakh** if a bank fails.

DMARC A rule that tells email providers what to do if an email claims to be from a bank but isn't really. With `p=reject`, fake emails are blocked outright. 40% of `.bank.in` banks don't have this.

DNS The internet's phone book — turns names like `sbi.bank.in` into computer addresses.

DNSSEC A cryptographic signature for DNS records, proving the phone book entry hasn't been tampered with. 80% of cooperative banks lack it.

DSC (Digital Signature Certificate) A government-issued digital ID used to sign documents legally. The registry had endpoints to start DSC sessions — another sensitive function left exposed.

fTLD Registry The organization that runs the global `.bank` domain, which enforces the strongest bank-security rules in the world. The benchmark `.bank.in` falls short of.

HSTS Forces browsers to always use a secure (HTTPS) connection. Stops attackers from downgrading you to an insecure one. 47% of `.bank.in` sites lack it.

IDRBT Institute for Development and Research in Banking Technology. An RBI-owned body that runs the `.bank.in` registry.

IFSC Indian Financial System Code. An 11-character code that identifies a bank branch (used for transfers like NEFT/RTGS). A way to check a bank is real.

OSINT Open-Source Intelligence. Gathering information from publicly available sources — no hacking required.

Orphan account A user account with Super Admin powers but not attached to any real organization. 1,072 of these were found, all with top-level access.

Phishing Tricking someone into entering their password or OTP on a fake website that looks real. The main threat this leak would have enabled.

Public tender / RFP An open, competitive process for hiring a vendor. IDRBT skipped this entirely when building the registry portal.

Super Admin The highest level of access in the portal — can do anything, including changing any bank's domain settings. Left exposed for IKCON staff.

TLS / SSL certificate The padlock in your browser's address bar. Proves a website is encrypted and (with EV/OV types) verified. Many `.bank.in` sites use the free, identity-free kind.

16 Appendix C: About the Author

CashlessConsumer

CashlessConsumer is a consumer collective that tracks the digital payments industry in India, producing awareness resources, technical analysis, open data, and policy inputs toward a fair cashless society [1]. It is not a legal entity and collects no personal data or analytics [2]. Srikanth L, a contributor to the collective, authored this report.

Prior investigations and published work:

- **KillerLoanApps** (2020–2024) — Analysis of predatory digital lending apps operating across India, tracking how unregulated platforms harvested user data, evaded Play Store oversight, and operated through shell company networks [3][4][5]. Presented at Hasgeek [6]. Engaged with Ministry of Home Affairs' @CyberDost initiative on combating the issue.
- **BFIL Consent Scam / Citizens' Report** (2021–2022) — Investigated Bharat Financial Inclusion Limited's (IndusInd Bank subsidiary) disbursal of 84,000 loans without customer consent, attributed to a 'technical glitch' [7]. The report was cited by Internet Freedom Foundation [8] and led to the **DigitalLending WatchTower** initiative tracking the digital lending space from a consumer protection perspective [9].
- **IDRBT .bank.in Security Investigation** (2026) — Discovery of 33+ unauthenticated API endpoints on the IDRBT Domain Registration Portal exposing bcrypt password hashes for 5,576 bank employees, documented in this report. The daily security audit feed [10] and live uptime monitor [11] are published as open data.
- **Fintech Governance RTI Program** (2018–ongoing) — Systematic RTI-based investigations filed with the RBI, NPCI, SEBI, and other financial regulators to track enforcement actions, payment system operator compliance, and consumer protection mechanisms [12].
- **Certificate Transparency Monitoring** (ongoing) — Tracking SSL certificate issuance for Indian banking and government domains to identify phishing infrastructure and mis-issued certificates.

References

1 CashlessConsumer about page: https://www.cashlessconsumer.in/about/

2 CashlessConsumer disclaimers: https://www.cashlessconsumer.in/about/disclaimers/

3 KillerLoanApps investigation: https://www.cashlessconsumer.in/post/killerloanapps

4 Fake lending apps database (Medium): https://medium.com/cashlessconsumer/fake-digital-lending-apps-database-b5de323f6d1b

5 KillerLoanApps at Hasgeek: https://hasgeek.com/cashlessconsumer/killerloanapps-detecting-fake-fintech-apps

6 @CyberDost engagement on predatory lending — see CashlessConsumer's referenced work with Ministry of Home Affairs' cyber awareness initiative.

7 BFIL Consent Scam — Citizens' Report (March 2022): https://www.cashlessconsumer.in/uploads/BFILConsentScamReport.pdf

8 Internet Freedom Foundation explainer on BFIL consent scam: https://internetfreedom.in/bfil-consent-scam

9 DigitalLending WatchTower at Hasgeek: https://hasgeek.com/cashlessconsumer/digital-lending-watchtower

10 bank-in-domains daily audit (GitHub): https://github.com/CCAgentOrg/bank-in-domains

11 Banking domain uptime monitor: https://uptime.cashlessconsumer.in

12 RTI filings list: https://www.cashlessconsumer.in/post/rtilist

Report by Srikanth L, CashlessConsumer. June 2026.