Crystal Vault Investigation — What We Found

A systematic OSINT sweep of an entire nation's government web infrastructure. Zero exploitation. Zero breaches. Just publicly served files that were never meant to be public.

The Numbers

- **38+ government organizations** compromised — ministries, military, agencies, state & municipal governments, election systems
- **30 unique database credential sets** — production logins to live government systems
- **7 complete source code repositories** reconstructed — 64,262 files of government application code
- **500,000+ security findings** catalogued across 1,700+ government domains
- **6,641+ domains** scanned using 5 custom-built OSINT tools
- **245 raw evidence files** (167 MB) downloaded directly from live servers as proof
- **Everything confirmed still live** as of February 22, 2026

What's Exposed

Credentials & Access

- [ ] 15+ environment files with plaintext database passwords — downloaded directly via browser
- [ ] 12 database credential sets from remote scanning alone — PostgreSQL, MySQL, Oracle
- [ ] 18 additional credential sets extracted from reconstructed source code
- [ ] 1 SMTP mail server credential — enables sending emails AS a government agency
- [ ] 1 SFTP production server credential — direct file system access to a live government server
- [ ] 2 active Telegram bot tokens — hardcoded in government source code
- [ ] 1 RSA 2048-bit private key — full PKCS#8 private key for a government deployment
- [ ] 6 Laravel application encryption keys — each enables remote code execution or session forging
- [ ] 1 Apache password hash — crackable, protects a state ID card system
- [ ] 1 Maps API key — embedded in water infrastructure mapping code
- [ ] Password `12345678` used on a system managing **pensions for every teacher in the country**
- [ ] Password `123456` on a postgres superuser account for social security data
- [ ] Password `password` on a ministry's WordPress database with phpMyAdmin on port 8080
- [ ] 3 municipal government systems sharing the exact same password across different applications
- [ ] Root MySQL with NO PASSWORD on a human resources system

Source Code

- [ ] 37,057 files from a national payroll system — zero parameterized SQL queries in the entire codebase
- [ ] 18,730 files from a youth employment platform — includes a hidden vote registration module
- [ ] 2,850 files from the national water utility — complete reservoir management system
- [ ] 1,788 files from a ministry — turns out to be a cemetery management system deployed on 6 subdomains
- [ ] 2,817 files from a waste management system — citizen records, family tracking, children's data
- [ ] SQL injection vulnerabilities in login pages — direct string concatenation, no sanitization
- [ ] Application-wide SQL injection — only defense is bypassable `addslashes()` across 37,000 files

Personal Data & PII

- [ ] 2,500+ government employee records with **bank account numbers** — directly downloadable CSV files
- [ ] National airline employee records with **home addresses**
- [ ] 298 judicial system employee records — cedulas, names, DOBs, addresses, marital status
- [ ] Payroll data with salary amounts linked to individual cedula numbers
- [ ] Salary declarations with corporate and individual tax ID (RIF) numbers
- [ ] 44 citizen ID numbers in a plaintext text file — sitting on a public web server
- [ ] A system that stores passwords in BOTH hashed AND plaintext — and displays them in an admin panel
- [ ] An API that returns any citizen's employment record and photo by entering their ID number — no login required
- [ ] Family group tracking — mapping family relationships, parentage, children's personal data
- [ ] Minor children's data collected through government aid applications

Database Dumps

- [ ] 150 MB of SQL database dumps from the national water utility — 14 files spanning 15 months
- [ ] 104 MB single production backup — the newest one, dated June 2025
- [ ] Complete water reservoir database — GPS coordinates, dam specifications, capacity data for every major reservoir
- [ ] User accounts table with bcrypt password hashes (cost factor 5 — trivially crackable)
- [ ] PostgreSQL backup files with accounting tables and balance sheets
- [ ] Monthly backup files showing the database growing over time — data archaeology

Photos & Documents

- [ ] 175 personal photos and scanned documents from a government ministry — still being served
- [ ] 52 event/attendance photos
- [ ] 123 government document scans
- [ ] Government ID card templates with source files (GIMP)
- [ ] Team profile photos of government workers

Election Infrastructure

- [ ] Full GraphQL API schema for the ruling party's election management system
- [ ] Mutations to **create admin accounts**, **record votes**, **open/close voting centers**
- [ ] Types including voting centers, voting tables, employees, vote reports
- [ ] Election system shares a server IP with the state's Docker/Kubernetes management panel
- [ ] Voter registration portal on the same infrastructure
- [ ] A "vote registration structure" module hidden inside a youth employment application

Critical Infrastructure — Water

- [ ] Two independent database access paths to the national water management system (MySQL + Oracle)
- [ ] GPS/UTM coordinates for every major water reservoir in the country
- [ ] Dam specifications — height, slope, crest length, spillway capacity, floodgate counts
- [ ] Operational water levels and storage volumes per reservoir
- [ ] Personnel contacts for reservoir operators — names, phone numbers, emails, cedula numbers
- [ ] 15 months of operational backups showing infrastructure state over time

Military & Defense

- [ ] 2 Ministry of Defense servers with web root set to user home directory
- [ ] Shell configuration files (.bashrc, .profile) from military servers — downloadable via browser
- [ ] This means `.ssh/`, `.bash_history`, `.gnupg/` are potentially web-accessible
- [ ] Military authentication system source code (Army Agroindustrial Brigade)
- [ ] Military deployment revealed through exposed git configurations

Internal Network Topology

- [ ] 15 internal IP addresses mapped across 10+ organizations
- [ ] LDAP Active Directory server for an entire government domain
- [ ] 3 internal GitLab servers — one with root user access
- [ ] Internal DNS names revealing backend architecture
- [ ] Zimbra email server configurations
- [ ] Docker/Kubernetes management panels accessible from the internet

Email & Identity

- [ ] 1,137 email addresses de-anonymized from encrypted Gravatar hashes
- [ ] 3,961 unique hashes collected across 162 government and media domains
- [ ] 142+ WordPress admin usernames enumerated from government sites
- [ ] 225+ government email addresses harvested from public sites
- [ ] 442+ personnel names extracted from document metadata (PDF/Office files)
- [ ] Government workers using personal Gmail accounts for official business
- [ ] A citizen's national ID number embedded in their email address on a government portal
- [ ] 71 Gravatar profiles enriched with biographical data (usernames, locations, bios)

Infrastructure Failures

- [ ] 40+ government domains with wildcard CORS — any website can make authenticated requests
- [ ] Central Bank of Venezuela exposing full PHP server configuration via phpinfo()
- [ ] A national bank exposing phpinfo()
- [ ] 222 Webmin instances across government domains
- [ ] 79 government Zimbra email login pages publicly accessible
- [ ] 5,008 WordPress sites identified across nearly 7,000 government domains
- [ ] 695,000+ archived URLs in the Wayback Machine dating back to 2004
- [ ] 69% of government infrastructure hosted on a single state-owned ISP

The Bottom Line

An entire nation's digital government — from the water that comes out of taps to the votes that determine who governs to the pensions that pay teachers to the airline that flies citizens — was recoverable from the open internet through basic URL requests.

No exploitation. No social engineering. No zero-days.

Just files that were never meant to be public, sitting on public web servers, waiting to be downloaded.

30 million citizens. 38+ organizations. 30 credential sets. 167 MB of raw proof.

All still live.

Crystal Vault Investigation — February 2026 Details available upon request.