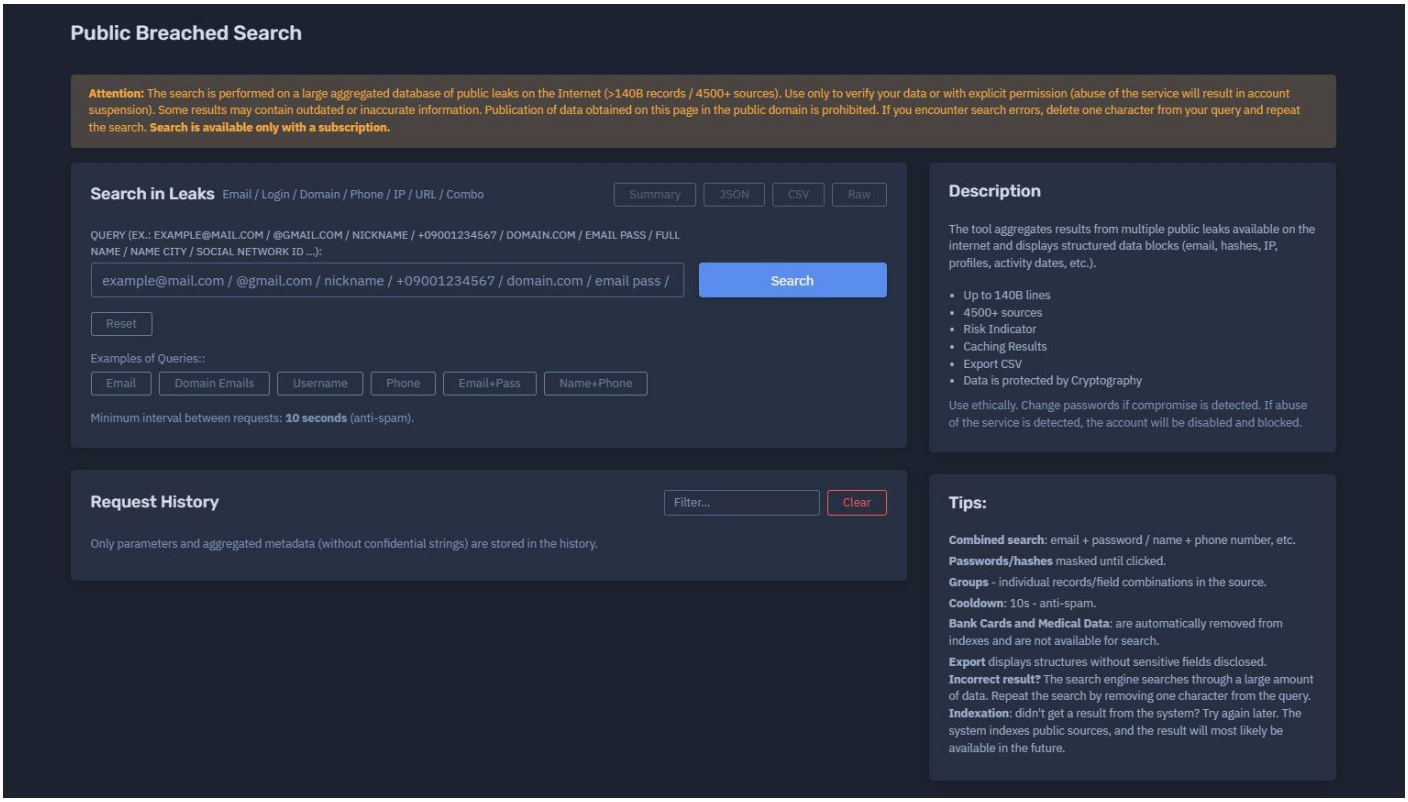
Public Breached Search | Public Breaches (140+ Billion Records)



Overview of the Service

The platform available at dash.niamonx.io/breaches_search is a professional-grade **Public Breached Data Search System** designed for verifying whether specific personal identifiers have appeared in any known public data leaks across the Internet.
It operates on an **aggregated dataset exceeding 140 billion records** collected from **over 4,500 public breach sources**, making it one of the most extensive publicly searchable breach databases in existence.

? How the Search Works

When a user enters a query — such as an **email address, username, phone number, IP, or domain** — the system performs a real-time lookup across its encrypted, indexed data clusters. The query is normalized, tokenized, and securely matched against hashed or pseudonymized datasets to locate potential breach entries.

The search engine uses **multi-vector indexing** optimized for text, numeric, and composite keys (e.g., *email* + *password*, *name* + *city*), allowing flexible combined searches.

To maintain integrity and performance:

- Each user request is subject to a **10-second cooldown** (anti-spam policy).
- Partial queries can improve recall; deleting one character may trigger a broader match.
- Cached results are used for frequent queries to improve response time.

? What Can Be Searched

You can look up:

- **Emails and logins**
- **Phone numbers** (international format)
- **Domains or URLs**
- **IP addresses**
- **Full names or social network identifiers**
- **“Combo” lines** (e.g., *email* + *password* pairs from public leaks)

The system structures results into logical “groups” that may include:

- Email or login identifiers
- Hashed or masked passwords
- IP and domain references
- Profiles and related metadata
- First/last seen activity dates

Sensitive fields like passwords remain **masked** until explicitly revealed by the user.

?? Security & Ethics

All stored data and query logs are **encrypted using modern cryptographic algorithms**.
Only **aggregated metadata** — not full confidential strings — is retained in request history for transparency and analytics.

Additional safeguards:

- **Bank card and medical information** are automatically excluded from indexing.
- **Publication of retrieved data** is strictly forbidden.
- Detected abuse leads to **account suspension and IP blocking**.

The service is intended for **ethical use only** — such as checking whether your credentials or company assets appear in public leaks and taking appropriate security measures (e.g., password changes, MFA setup).

? Extra Features

- **Risk indicator:** assesses the exposure level of each result.
- **Result caching:** speeds up repeated lookups.
- **CSV export:** allows structured export without revealing sensitive fields.
- **Ongoing index updates:** new sources are continuously crawled and normalized.

In summary, **NiamonX Breach Search** acts as a secure, encrypted intelligence platform that enables professionals and individuals to verify their exposure in public breaches responsibly. It prioritizes **data protection, cryptographic integrity, and ethical transparency**, providing actionable insights while maintaining user and data privacy.

? Contact Information

For any inquiries, users can contact the project team directly:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal Matters

An alternative contact channel is the official **Helpdesk**:

□□ https://support.niamonx.io/

Revision #3
Created 9 November 2025 05:08:26 by NiamonX Team
Updated 9 November 2025 05:27:44 by NiamonX Team