

DIGISURAKSHA PARHARI FOUNDATION

Intern name : Prateek

Intern ID : 166

Tool name : deHashed (<https://dehashed.com/>)

e-mail : prateek18yarnale@gmail.com

DeHashed: A Breach Intelligence and OSINT Platform

1.0 Executive Summary

DeHashed is an advanced online breach intelligence and investigative platform designed to aggregate, analyze, and provide access to billions of records of compromised data. Functioning as a powerful search engine, DeHashed enables users to query and trace leaked credentials, personal identifiers, and sensitive data across the clear web, deep web, and dark web. Its vast and continually updated database makes it a crucial tool for professionals engaged in cybersecurity, digital forensics, open-source intelligence (OSINT), and law enforcement investigations.

With support for querying a wide range of identifiers—such as emails, usernames, IP addresses, phone numbers, and hashed passwords—DeHashed offers unparalleled visibility into the extent and history of data breaches. The platform empowers investigators to map relationships between data points, identify reused credentials, detect account compromises, and monitor digital assets for future exposure.

This report presents a comprehensive overview of DeHashed, outlining its origin, functionality, core features, and various use-case scenarios. It also evaluates the tool's strengths in terms of usability, scalability, and investigative value, while highlighting certain limitations such as legal ambiguities, data freshness, and interface optimization. Overall, DeHashed stands out as a high-utility tool for organizations and individuals seeking to improve their cyber hygiene, respond to breaches, and enhance situational awareness in an increasingly data-compromised world.

2.0 History and Development

DeHashed was developed with the mission of making breach intelligence accessible, aiming to empower individuals and organizations to understand and mitigate risks associated with data exposures. Unlike some platforms that have faced legal issues, DeHashed strives to operate within legal frameworks, differentiating itself from "hack tools" and focusing on legitimate security and investigative use cases. Its continuous development focuses on expanding its database of compromised data, incorporating new private datasets, and enhancing search functionalities to provide rapid and comprehensive results. The platform emphasizes transparency in pricing and user privacy, while actively working to prevent misuse of its data.

3.0 Description: What Is This Tool About?

DeHashed is a powerful search engine designed to uncover and analyze cybersecurity data breaches and leaked information. It maintains a vast database of sensitive data, including usernames, email addresses, IP addresses, names, and even hashed or plaintext passwords, that have been publicly exposed or traded online. The platform's primary purpose is to allow individuals, security analysts, journalists, and law enforcement agencies to search this compromised data to:

- **Determine personal exposure:** Check if their own credentials or personal information have been compromised.
- **Assess organizational risk:** Identify if company data, including employee or customer information, is present in breaches.
- **Aid in investigations:** Provide crucial intelligence for fraud prevention, identity theft investigations, and broader OSINT inquiries.

DeHashed focuses on providing a "full disclosure" of data where possible, informing users precisely what information has been leaked.

4.0 Key Characteristics and Features

Feature	Description
Comprehensive Data Aggregation	Collects sensitive data from a wide range of sources across the clear web, deep web, and dark web, offering one of the largest databases of breach information in the industry.
Multi-Parameter Search	Allows users to search for various data types, including usernames, email addresses, IP addresses, names, and more. Supports advanced queries with wildcard, regex, and search operators for precise results.
Breach Monitoring & Alerts	Provides ongoing monitoring services for sensitive information. Users can set up alerts via email, text message, or webhooks to receive real-time notifications when their monitored data appears in new breaches.
API Access	Offers a clean, fast, and flexible API for programmatic access to its breach intelligence data. This enables developers and organizations to integrate DeHashed's capabilities into their own applications and automated workflows.
WHOIS Data Intelligence	Includes a newly launched feature for domain and IP data intelligence, providing access to historical WHOIS data, Reverse WHOIS, and other essential information for robust OSINT.
Focus on Privacy	Claims to prioritize user privacy by not logging exact searches (only the number of searches), using state-of-the-art security technology, and avoiding excessive data collection or sharing of user data.
Affordability and Transparency	Aims to make security accessible by offering many services for free and providing transparent pricing for paid features, distinguishing itself from competitors perceived as overcharging.
Rapid Incident Response	Known for being among the first to respond to and integrate new security incidents and data breaches, providing timely intelligence to users.

Anti-Scraping Measures	Employs a "leaky bucket algorithm" to prevent large-scale scraping of its data, mitigating misuse and the creation of "combo lists" by malicious actors.
------------------------	--

5.0 Types / Modules Available

DeHashed primarily operates as a consolidated search and monitoring platform, with its core functionalities structured around:

- **Search Engine Module:** The central interface for querying compromised data using various input types (email, username, IP, name, etc.) with advanced filtering options.
- **Monitoring Service:** Enables users to set up alerts for specific emails, phone numbers, usernames, or domains, receiving notifications when these assets are found in new breaches.
- **API Integration:** Provides a robust API for enterprises and developers to integrate DeHashed data directly into their security information and event management (SIEM) systems, vulnerability management platforms, and other security tools (e.g., Splunk ES, SentinelOne, Proofpoint, Palo Alto Networks Firewall).
- **WHOIS Data Module:** A specialized tool for retrieving current and historical domain and IP registration information, valuable for domain investigations and identifying ownership changes.

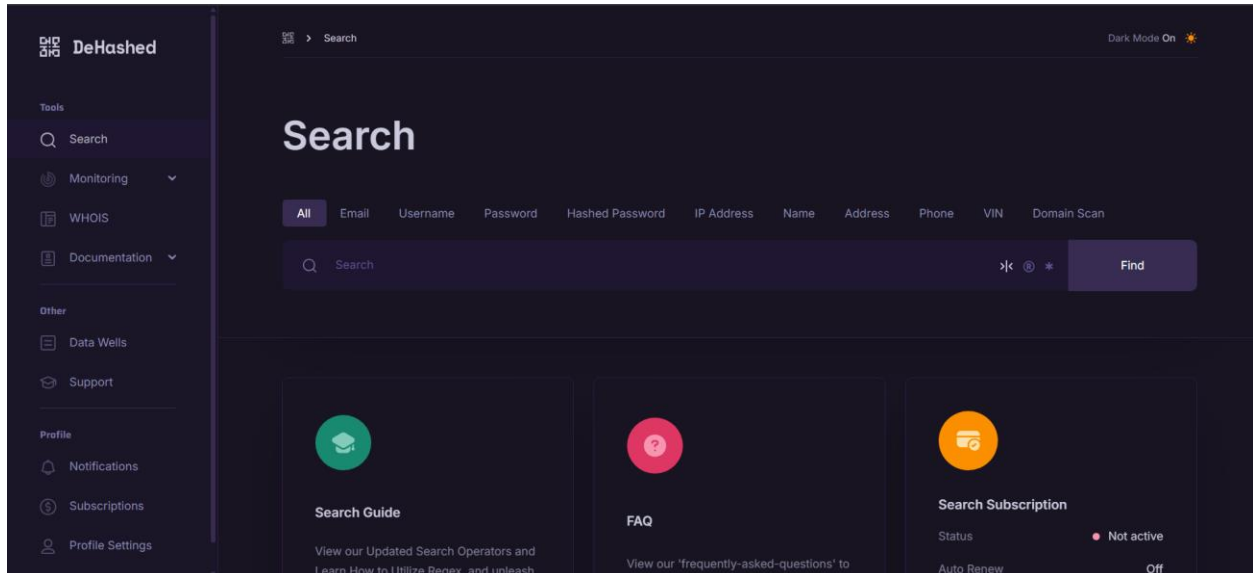
6.0 Operational Benefits

DeHashed offers significant operational benefits for various stakeholders:

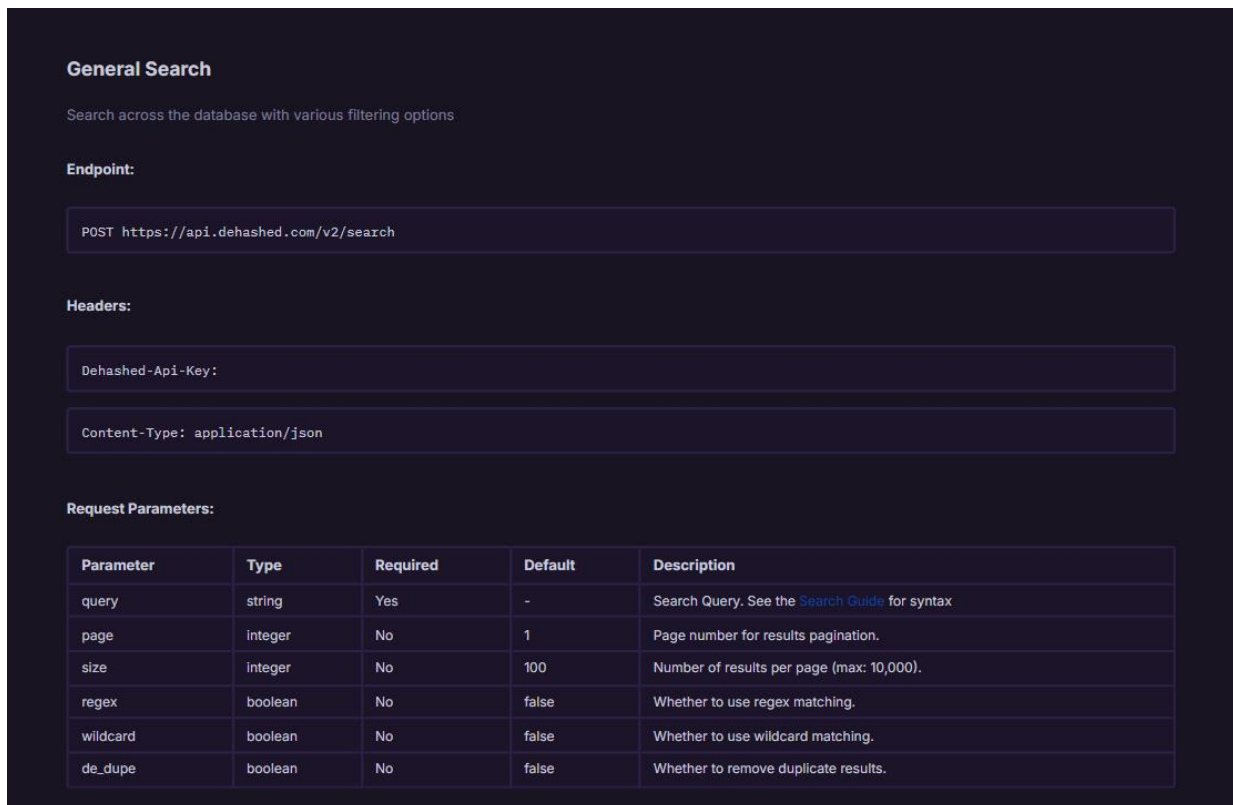
- **Proactive Threat Intelligence:** Enables organizations to identify compromised credentials and data exposures that could lead to account takeover, credential stuffing, or identity fraud, allowing for proactive mitigation.
- **Enhanced Security Posture:** Helps individuals and enterprises assess their risk exposure to data breaches, reinforcing their overall cybersecurity posture.
- **Accelerated Incident Response:** Provides rapid access to breach data, significantly reducing the time required to investigate suspicious activity and respond to security incidents.
- **Streamlined OSINT Investigations:** Serves as a critical resource for OSINT practitioners to enrich intelligence, identify associations, and verify information related to individuals or entities.
- **Fraud Prevention:** Supports efforts to prevent identity fraud by allowing for the quick identification of leaked personal identifiable information (PII).

- **Cost-Effective Security:** Offers a free tier and competitively priced paid plans, making advanced breach intelligence accessible to a wider audience, including smaller firms and individuals.

7.0 Proof of Concept (PoC) Visuals



Search feature



Response:

The response includes an array of entries with available information. Attributes will be omitted if they are empty.

```
{
  "balance": 100,
  "entries": [
    {
      "id": "5603802198",
      "email": ["test@example.com"],
      "ip_address": ["127.0.0.1"],
      "username": ["username@example.com"],
      "password": ["examplepassword"],
      "hashed_password": ["password:salt|passwordhash"],
      "name": ["name"],
      "dob": ["01/02/60"],
      "license_plate": ["123456"],
      "address": ["example address"],
      "phone": ["+18006551234"],
      "company": ["example company"],
      "url": ["url.com"],
      "social": ["social username"],
      "cryptocurrency_address": ["@cryptocurrencyaddress"],
      "database_name": "Example Database Name",
      "raw_record": {
        "le_only": true,
        "unstructured": true
      }
    }
  ],
  "took": "179µs",
  "total": 5
}
```

Search and response shown.

Code Examples:

python

golang

nodejs


curl

```
import requests

api_key = "API-KEY"

def v2_search(query:str,page:int,size:int,wildcard:bool,regex:bool,de_dupe:bool) -> dict:
    res = requests.post("https://api.dehashed.com/v2/search", json={
        "query": query,
        "page": page,
        "size": size,
        "wildcard": wildcard,
        "regex": regex,
        "de_dupe": de_dupe,
    }, headers={
        "Content-Type": "application/json",
        "DeHashed-API-Key": api_key,
    })
    return res.json()

if __name__ == '__main__':
    response = v2_search("testing", 1, 1, False, False, True)
    print(response)
```

 DeHashed

Tools

Search

Monitoring

WHOIS

Documentation

Other

Data Wells

Support

Profile

Notifications

Subscriptions

Profile Settings

Log Out

Data Wells



1-20 of 23869

Search Data Wells

Q

Sort By: Name (A-Z)

Show Per Page: 20

Logo	Website	Date	Count	
	000Webhost	2015-03-01	15,241,933	—
<div><div>Description</div><div>In March 2015, 000webhost, a free web hosting provider, experienced a significant data breach impacting nearly 15 million customer records. The compromise included exposure of full names, email addresses, plain text passwords, and IP addresses.</div><div>Exposed Data Notably Includes<ul style="list-style-type: none">name_fullemailip_addresspassword</div></div>				
	0059.co.kr (Cit0day)	2020-11-04	3,139	—
<div><div>Description</div><div>This breach is a part of the Cit0day breach collection. In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches.</div><div>Exposed Data Notably Includes<ul style="list-style-type: none">emailpassword</div></div>				

1

2

3

4

...

1194

>

8.0 Optimal Usage Scenarios

DeHashed is particularly valuable in the following scenarios:

- **Post-Breach Analysis:** Immediately following a reported data breach, to determine the extent of personal or organizational exposure.
- **Credential Stuffing Prevention:** Regularly monitoring employee or customer credentials to identify if they have appeared in breaches, preventing account takeover attempts.
- **Due Diligence:** Conducting background checks or vetting new hires/partners to identify potential security risks from past data exposures.
- **Identity Theft Investigation:** Assisting individuals or law enforcement in tracing compromised PII for identity fraud cases.
- **Cyber Threat Intelligence:** Enriching threat intelligence feeds by identifying trends in leaked data and understanding attacker methodologies.
- **OSINT Investigations:** Gathering foundational intelligence on targets by identifying associated emails, usernames, and other leaked data.
- **Domain Ownership Research:** Utilizing the WHOIS module to uncover historical domain ownership and related entities.

9.0 Application in Investigations

DeHashed is a pivotal tool across multiple phases of cybersecurity and OSINT investigations:

- **Reconnaissance:** Quickly gathering initial intelligence on an individual, organization, or domain by searching for their presence in breach databases.
- **Vulnerability Assessment:** Identifying exposed credentials that could be used to gain unauthorized access to systems or accounts.
- **Incident Response:** During an active incident, to determine if the compromise stemmed from publicly available leaked credentials.
- **Digital Forensics:** Providing context to forensic investigations by linking observed malicious activity to known data breaches.
- **Threat Hunting:** Proactively searching for organizational assets or employee data within newly disclosed breaches to identify potential attack vectors.
- **Legal and Compliance:** Demonstrating due diligence in data protection by actively monitoring for and responding to data exposures.

10.0 Target User Profile and Skill Requirements

Ideal Users:

- Cybersecurity Analysts
- Security Operations Center (SOC) Teams
- Incident Responders
- Forensic Investigators
- Open-Source Intelligence (OSINT) Analysts
- Journalists investigating data breaches
- Law Enforcement Agencies
- Individual users concerned about their personal data security

Skill Requirements:

- **Basic Understanding of Cybersecurity Concepts:** Familiarity with terms like data breaches, credentials, hashing, and PII.
- **Search Logic:** Ability to formulate effective search queries, potentially utilizing boolean operators, wildcards, and regular expressions for advanced searches.
- **Data Interpretation:** Skill in interpreting and contextualizing search results from breach data.
- **No Coding Required for Basic Use:** The web interface is user-friendly. However, programming skills (e.g., Python) are beneficial for leveraging the API for automation and integration.

11.0 Identified Areas for Improvement

Flaw	Suggestion for Improvement
User Support Responsiveness	Some user feedback indicates inconsistent or delayed responses from customer support, particularly for paid or LE accounts. Suggestion: Enhance customer support infrastructure, provide clear SLAs for response times, and offer multiple support channels (e.g., live chat, dedicated phone lines for enterprise users) to ensure timely assistance.
Clarity on Data Scope/Quality	While claiming a comprehensive database, detailed information on data sources, update frequency, and methodology for deduplication or false positive reduction is not always transparent. Suggestion: Publish a detailed whitepaper or knowledge base articles on their data collection methodology, data quality assurance processes, and explicit scope of data covered.
Pricing Model Transparency	While general pricing is mentioned, a clearer breakdown of free vs. paid tier limitations and specific feature comparisons could be improved. Suggestion: Provide a more explicit feature comparison matrix on the pricing page, detailing the exact benefits and limitations of each subscription tier, including credit usage or query limits.
Historical Data Timelines	While DeHashed collects historical data, specific features for visualizing changes or timelines of data over time within its own interface could be enhanced. Suggestion: Develop a graphical timeline view for individual records or domains, showing when data first appeared and any subsequent updates, to aid in tracking evolution of exposure.
Integration Documentation for API	While an API exists, comprehensive and developer-friendly documentation with code examples for various languages could improve adoption. Suggestion: Provide expanded API documentation, including use cases, common integration patterns, and code samples in popular programming languages (e.g., Python, Java, Node.js).

12.0 Strengths of the Tool

- **Extensive Database:** Possesses one of the largest and most comprehensive databases of compromised credentials and leaked information, crucial for broad intelligence gathering.

- **Powerful Search Capabilities:** Offers advanced search functionalities including wildcard, regex, and operator support, allowing for highly targeted and precise queries.
- **Proactive Monitoring:** The real-time breach monitoring and alert system is a significant advantage for both personal and organizational security, enabling immediate response to new exposures.
- **Valuable for Various Professionals:** Highly beneficial for cybersecurity analysts, OSINT investigators, law enforcement, and journalists due to its specific focus on breached data.
- **API for Automation:** The availability of a robust API allows for seamless integration into existing security tools and automated workflows, enhancing enterprise security operations.
- **Commitment to Accessibility:** Aims to keep security accessible through free services and transparent, competitive pricing, differentiating itself from more expensive enterprise solutions.
- **WHOIS Data Integration:** The inclusion of historical and reverse WHOIS data adds another valuable layer for comprehensive OSINT investigations.