NAME:- Samarth khedekar

Id :- 161

Tool Name:

LeakPeek

History:

LeakPeek is a web-based OSINT (Open Source Intelligence) tool that gained traction among cybersecurity professionals for identifying exposed credentials across multiple breached databases by just using an email address.

Description:

LeakPeek is a data breach lookup tool that allows users to check whether a specific email ID appears in any known data breaches. It returns password leaks, associated metadata, and breach origin—useful for reconnaissance and threat profiling.

What Is This Tool About?

LeakPeek helps security researchers and investigators determine if email accounts have been compromised in past data breaches. It scrapes breached database dumps and aggregates leaked credentials to provide quick, actionable insight.

Key Characteristics / Features:

1. No login required
2. Email-based breach check
3. Displays partial passwords (masked)
4. Shows breach sources (website/databases)
5. Fast and intuitive interface
6. Supports bulk email checking (via API or paid options)

7. IP logging to monitor abuse
8. Provides metadata like date/time of breach
9. TOR accessible for anonymous browsing
10. Publicly visible breach intelligence
11. Can be used for phishing campaign defense
12. Identifies reused passwords
13. Supports username-based search
14. Linked social media data (if exposed)
15. Updated breach database

Types / Modules Available:

Email Lookup

Username Search

Domain Search

IP Lookup (limited use)

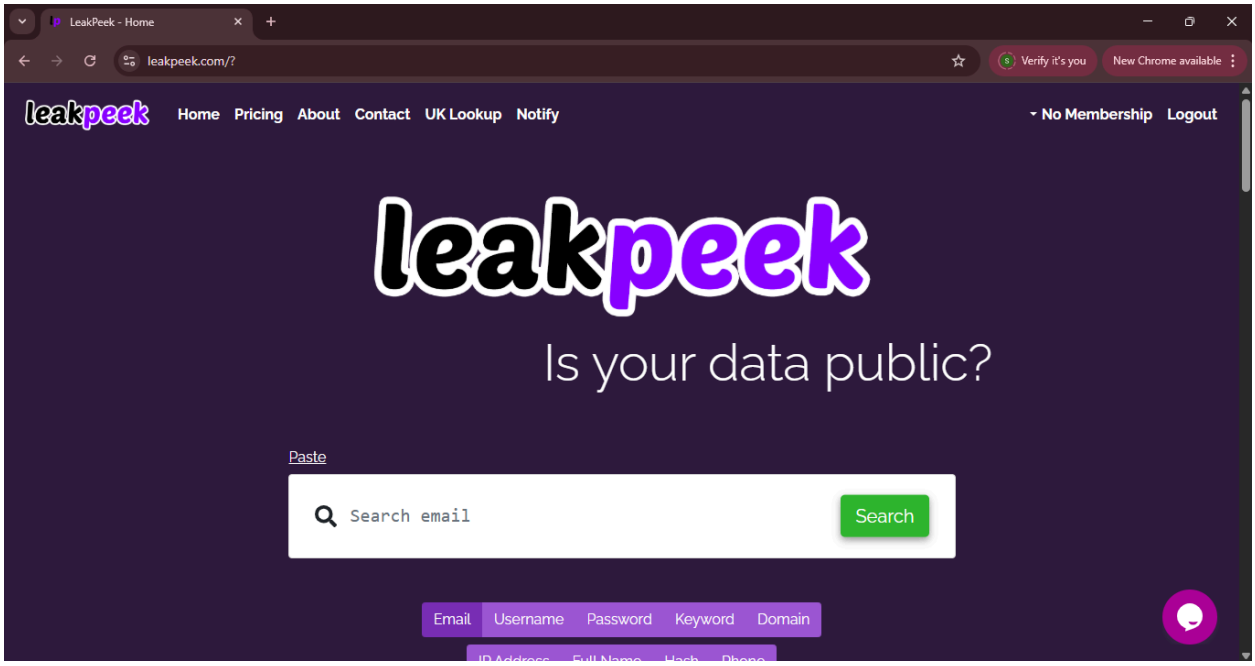
Pastebin & Leak Indexing

How Will This Tool Help?

- Identify compromised user credentials
- Validate insider threats
- Gather threat intelligence during OSINT phase
- Detect reused or weak passwords
- Understand threat actor targeting
- Assist red teams in crafting more authentic phishing campaigns (ethically)

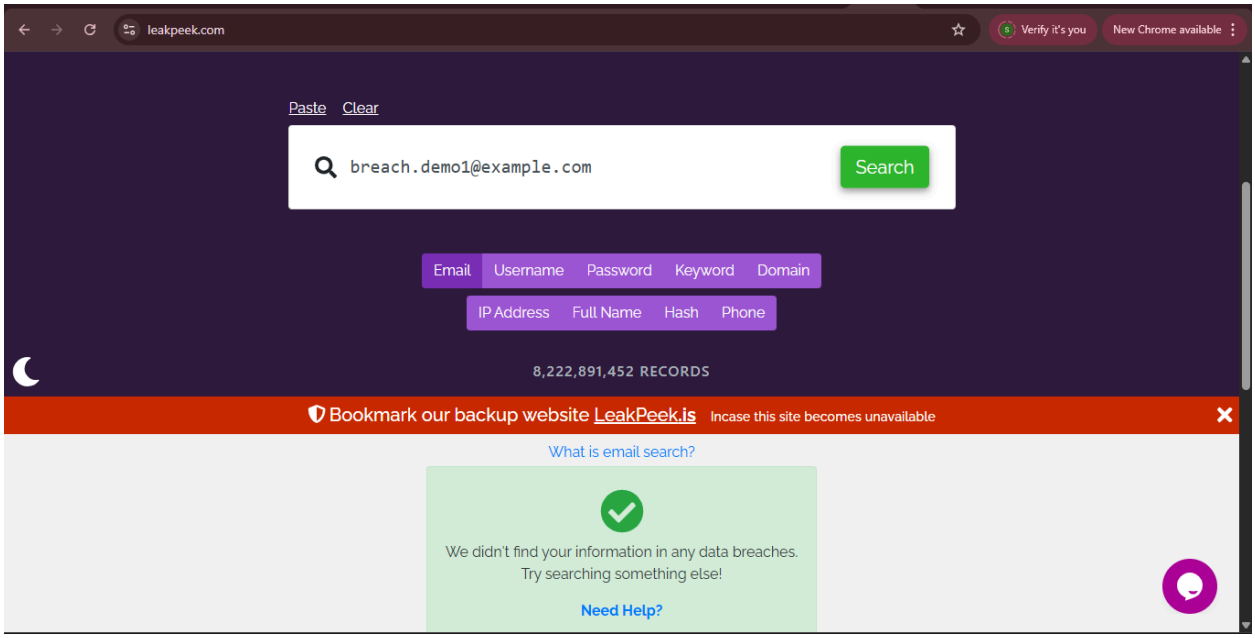
Proof of Concept (PoC) Images:

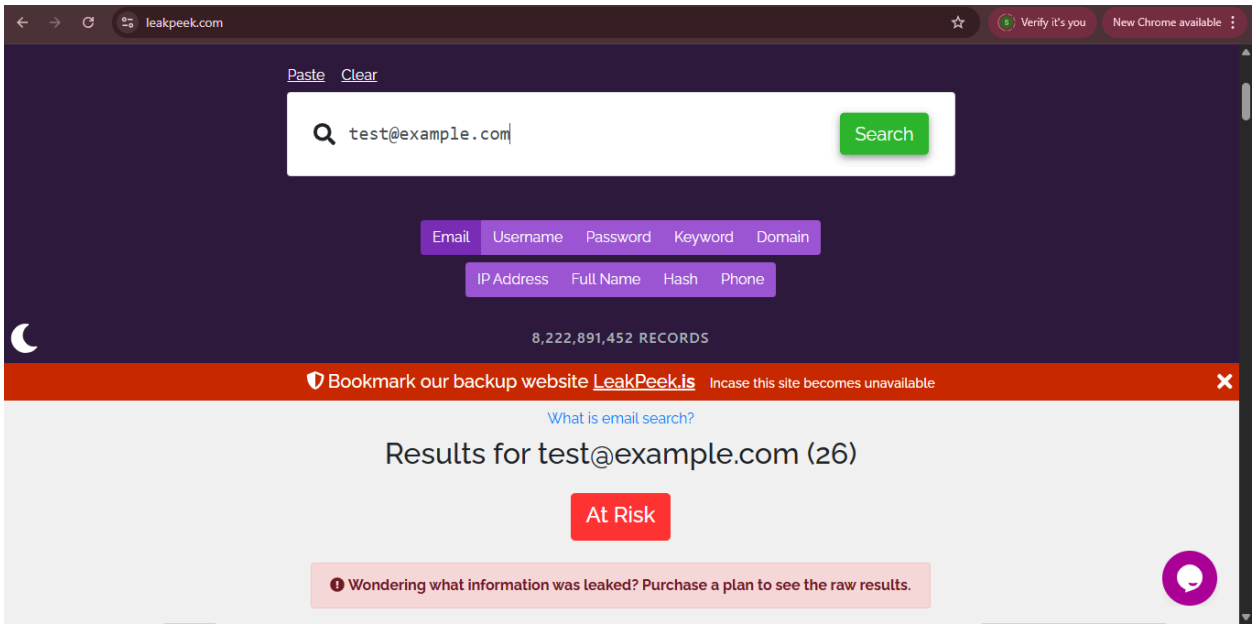
1. Homepage of Leak



Peek

2. Search email safe and risky





3. List of breached sites
4. Timestamp of breach events
5. Domain lookup result

6. Username result page
7. Associated metadata view
8. Social media leakage results
9. Reused password indicator
10. TOR version landing page

🗒️ 15-Liner Summary:

1. Web-based breach data lookup
2. Simple email/username interface
3. Lists masked leaked credentials
4. Public and free (basic version)
5. Reveals source of breach
6. No registration needed
7. Supports OPSEC via TOR
8. Ideal for investigators and pentesters
9. Can flag reused credentials
10. Shows date/time of breach

Time to Use / Best Case Scenarios:

- During email breach investigation
- Before engaging phishing assessments
- Recon phase of red team ops

- For security awareness reporting
- Credential stuffing analysis

When to Use During Investigation:

- Pre-breach reconnaissance
- During credential exposure validation
- Dark web monitoring
- Phishing incident response
- User training & awareness demo

Best Person to Use This Tool & Required Skills:

Best User: OSINT Investigator / Red Teamer / Threat Intelligence Analyst
Required Skills:

- Basic OSINT techniques
- Understanding breach database indicators
- Ethical use of leaked credential data
- Familiarity with email/social enumeration

Flaws / Suggestions to Improve:

- No API access in free version
- Limited result detail (for privacy)
- Can’t verify hash integrity
- No integration with SIEM or SOC tools
- No export options in free tier

Good About the Tool:

- Fast and free
- Simple interface
- No login needed
- Continuously updated leak sources
- TOR support enhances anonymity
- Great for quick credential exposure checks