



Dark Web ID + vPenTest

Dark Web ID Integration

The Dark Web ID Integration enables vPenTest to use compromised credentials from the dark web during penetration tests, revealing how stolen passwords can lead to unauthorized access. It helps MSPs and organizations understand the risks of weak credentials, validate controls like 2FA, and strengthen defenses against real-world attacks.

SEE HOW FAR STOLEN CREDENTIALS CAN TAKE AN ATTACKER

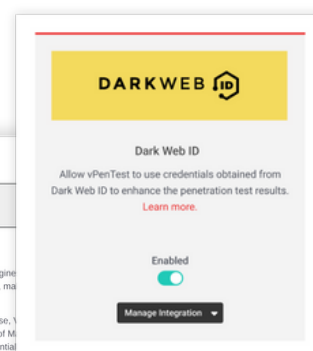
Organizations often underestimate the risks of weak or reused passwords. Without understanding the impact of compromised credentials, they can't effectively prioritize stronger password policies. The Dark Web ID Integration helps demonstrate the real-world consequences of poor password hygiene, driving awareness and improving security practices to reduce the risk of security breaches.

With this integration, vPenTest will:

- Confirm whether exposed credentials are still valid.
- Use those credentials to access systems and identify sensitive data.
- Report how dark web credentials were leveraged during the assessment.

HOW IT WORKS

- 1 **Enable Integration:** Turn on Dark Web ID in Global Settings > Integrations tab.
- 2 **Map Organizations:** Link your Dark Web ID and vPenTest accounts.
- 3 **Run Tests:** Use compromised credentials in internal or external tests.
- 4 **View Results:** Findings appear in vPenTest reports automatically.



vPenTest

CRITICAL Compromised Users

Observation

The dark web is a part of the internet that is not indexed by traditional search engine activities. It requires specific software, configurations, or authorization to access, making it a prime location for stolen data, including compromised user account credentials.

During the Open Source Intelligence (OSINT) scan conducted in the testing phase, 100 compromised email addresses associated with The Ministry of Magic that some user accounts may have been exposed in a data breach and are potential targets for unauthorized access.

Recommendation

Given the serious nature of this finding, we recommend the following actions to protect your organization and its users:

1. **Reset Compromised Passwords:** Immediately instruct users whose credentials have been compromised in the evidence section to change their passwords. Ensure that the new passwords are strong, unique, and adhere to security best practices.
2. **Implement Multi-Factor Authentication (MFA):** Enhance security by requiring two or more verification methods to gain access to user accounts, thus adding an extra layer of defense against unauthorized access.
3. **Conduct Regular Security Audits:** Regularly review and audit your security policies and controls. This includes checking for vulnerabilities, outdated software, and ensuring that security patches are applied promptly.
4. **Educate Users:** Conduct security awareness training to educate users about the importance of using strong, unique passwords for different services and the dangers of password reuse.
5. **Monitor for Suspicious Activity:** Continuously monitor systems and accounts for unusual activities that may indicate unauthorized access or attempts to access.
6. **Review and Update Security Policies:** Ensure that your security policies are up-to-date and comprehensive, covering aspects like password management, data protection, and incident response.

Evidence

The following table displays a list of up to ten (10) compromised email addresses associated with The Ministry of Magic that were identified during the dark web scan:

Email Address	Source	Password	Breach Date
db1@test.com	id theft forum	Test1234	02/22/2025
db1@test.com	id theft forum	Test1234	02/22/2025
db1@test.com	id theft forum	Test1234	02/22/2025
albus.dumbledore@test.com		Admin1234	02/19/2025
albus.dumbledore@test.com		Admin1234	02/19/2025
sinus.black000@test.com	PDP file	myOnlySecret	02/17/2025
sinus.black000@test.com	PDP file	AzkabanPrison3r	02/16/2025
sinus.black000@test.com	PDP file	AzkabanPrison3r	02/12/2025
sinus.black000@test.com	PDP file	AzkabanPrison3r	02/22/2025
sinus.black000@test.com	PDP file	my000Secret!	02/22/2025

Demo Company | Project: Internal Network Penetration Test

Confidential | Page 6 of 40

Enable the Integration today to uncover the impact of stolen credentials & strengthen your security posture!

Schedule a Demo Today!