Tresor-Berichte

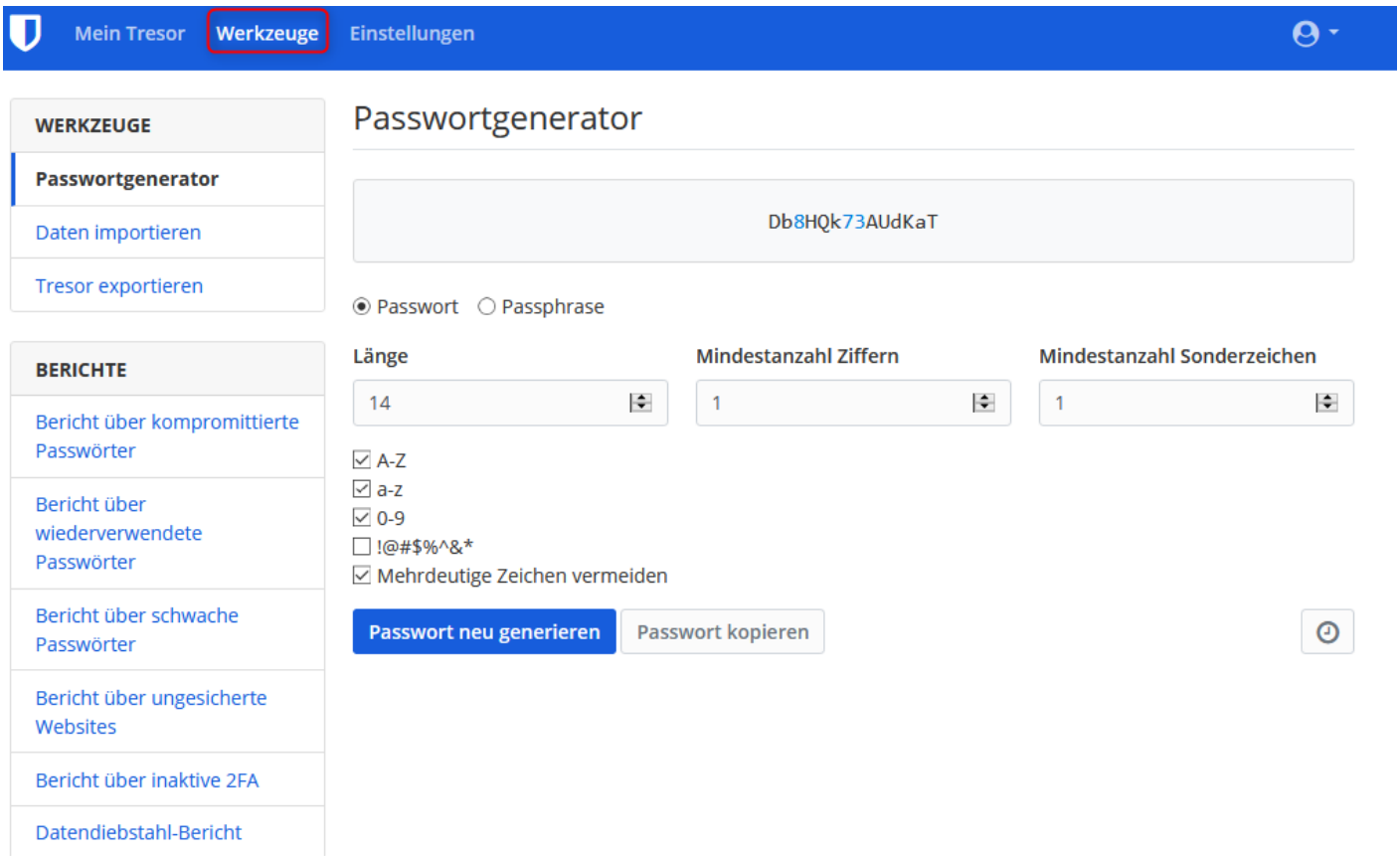
> **STATUS: VALID**

Berichte aufrufen

Mit Sylencer-Password kann der Benutzer auf eine Reihe von Berichtswerkzeugen zugreifen, um den Gesamtzustand ihres persönlichen Tresors wie folgt zu bewerten:

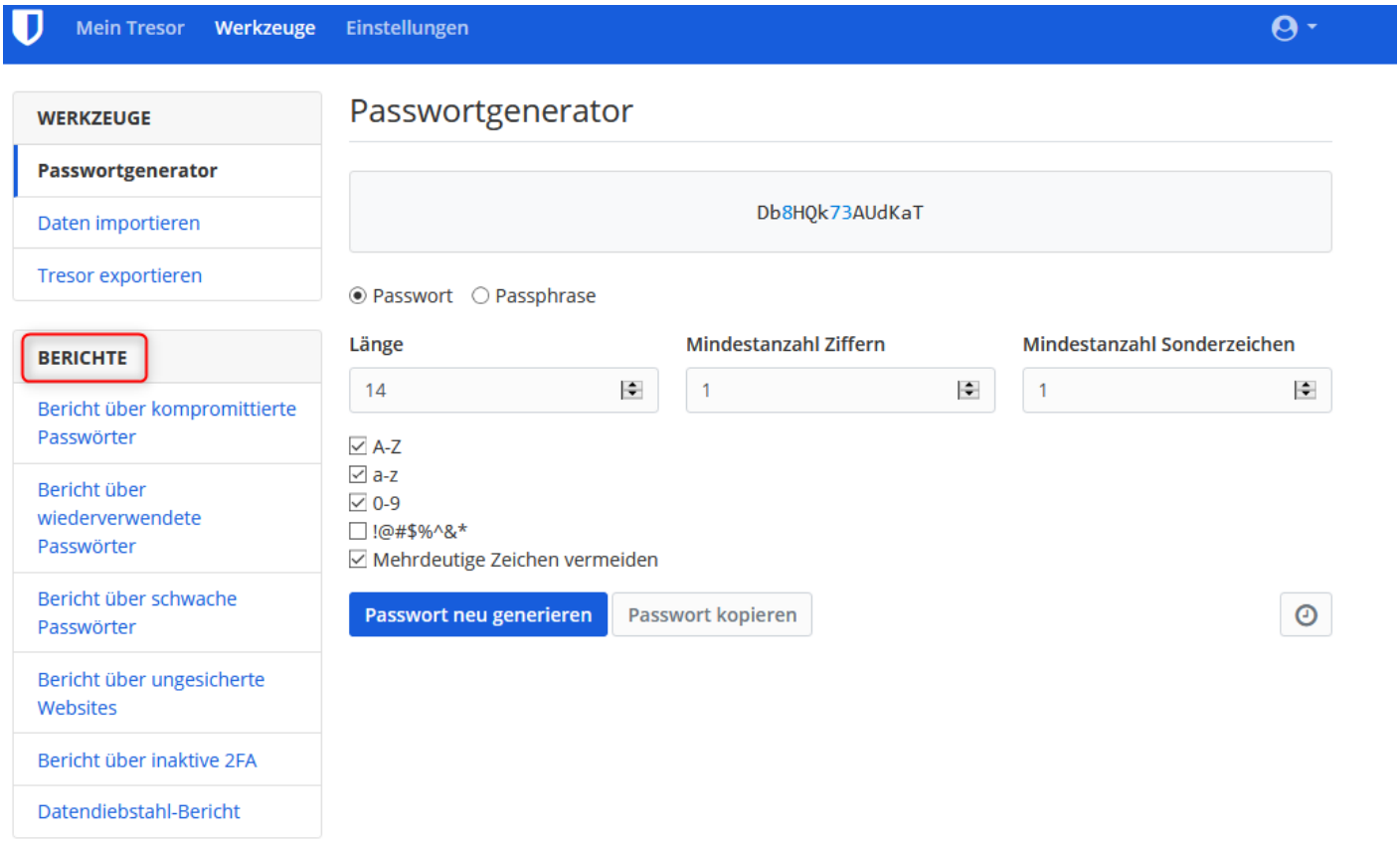
01. Logge Dich in den Web-Tresor unter dem URL ***[s. Zugangsdaten]*** ein.

02. Klicke in der oberen Navigationsleiste auf ***Werkezuge***.



---

03. Suche den Abschnitt ***Berichte***.



04. Wähle den gewünschten Bericht aus.

Verfügbare Berichte

Bericht über kompromittierte Passwörter

Dies sind Passwörter, die in bekannten Datenschutzverletzungen aufgedeckt wurden, die öffentlich veröffentlicht oder im Dark Web verkauft wurden.

Der Bericht verwendet einen vertrauenswürdigen Webdienst, um die ersten 5 Ziffern des Hashes alle Deiner Passwörter in einer Datenbank mit bekannten geleakten Passwörtern zu suchen. Die zurückgegebene übereinstimmende Liste von Hashes wird dann lokal mit dem vollständigen Hash Deiner Kennwörter verglichen. Dieser Vergleich wird nur lokal durchgeführt, um Deine ***k-Anonymität*** zu wahren.

Aber warum verwenden wir nur die ersten 5 Ziffern des Hashwerts Deiner Kennwörter? Wenn der Bericht mit Deinen tatsächlichen Passwörtern durchgeführt wird, ist es egal, ob diese offengelegt

werden oder nicht, Du würdst sie freiwillig an den Dienst weitergeben.

Und auch wenn das Ergebnis dieses Berichts nicht bedeutet, dass Dein individuelles Konto kompromittiert wurde, sondern nur, dass Du ein Kennwort verwendest, das in diesen Datenbanken mit exponierten Kennwörtern gefunden wurde, solltest Du es vermeiden, durchgesickerte und nicht eindeutige Kennwörter zu verwenden.

Bericht über wiederverwendete Passwörter

Wenn ein von Dir genutzter Dienst kompromittiert wurde, kann die Wiederverwendung desselben Passworts an anderer Stelle Hackern den Zugriff auf weitere Deiner Online-Konten erleichtern. Du solltest für jedes Konto oder jeden Dienst ein eindeutiges Kennwort verwenden. Der Bericht ***Wiederverwendete Passwörter*** hilft Dir, diese missbräuchlichen Passwörter leicht zu identifizieren.

Bericht über schwache Passwörter

Schwache Kennwörter können leicht von Hackern und automatisierten Tools erraten werden, die zum Knacken von Kennwörtern verwendet werden. Verwende den ***Bericht über schwache Passwörter***, um diese Passwörter schnell zu isolieren. Der Sylencer-Passwortgenerator kann Dir helfen, stärkere Passwörter zu erstellen.

Bericht über ungesicherte Websites

Die Verwendung ungesicherter Websites mit dem ***http://*** Schema kann gefährlich sein. Wenn die Website es erlaubt, solltest Du immer mit dem ***https://*** Schema zugreifen, damit Deine Verbindung verschlüsselt ist.

Bericht über inaktive 2FA

Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dazu beiträgt, Deine Konten zu schützen. Wenn die Website dies anbietet, solltest Du die Zwei-Faktor-Authentifizierung immer aktivieren. Der Inactive 2FA Report sucht in Deinem Tresor nach Objekten, bei denen Du keinen TOTP-Authentifizierungsschlüssel hinterlegt hast und vergleicht diese dann mit Daten von ***https://twofactorauth.org/***.

Datendiebstahl-Bericht (nur für einzelne Tresore)

Ein ***Bruch*** ist ein Vorfall, bei dem die Daten einer Website illegal von Hackern eingesehen und dann öffentlich veröffentlicht wurden. Mit dem ***Datendiebstahl-Bericht*** kannst Du die Arten von Daten überprüfen, die bei diesen Brüchen kompromittiert wurden (E-Mail-Adressen, Kennwörter, Kreditkarten usw.) und entsprechende Massnahmen ergreifen, wie z. B. das Ändern von Kennwörtern.

> **Done! Herzlichen Glückwunsch! Du hast soeben Deine Passwörter auf die Sicherheit überprüft und Gegenmassnahmen ergriffen.**

Version #3
Erstellt: 7 November 2023 19:51:16 von Sylencer
Zuletzt aktualisiert: 6 Mai 2024 21:54:47 von Sylencer