Relevanz und Sicherheit von Passwortmanagern

junk_rat

Wie können Passwortmanager Datensicherheit gewährleisten und welche Risiken bieten Sicherheitslücken?

CVE-2024-44276

- Sicherheitslücke in Apples „Passwords“
- Verwendete Passwörter werden in Datenleaks gesucht
- Wenn positiv, Link zum Ändern des Passworts

  → Problem: Link war standardmäßig HTTP

[1]

CVE-2024-44276

- **Wenn Nutzer sein neues Passwort über HTTP Link vergibt, kann es ein Angreifer dieses abfangen (Bspw. Öffentliches WLAN)**
- **Apple behob die Lücke erst mehrere Monate später**
- **Sicherheitsforscher wurden nicht belohnt**

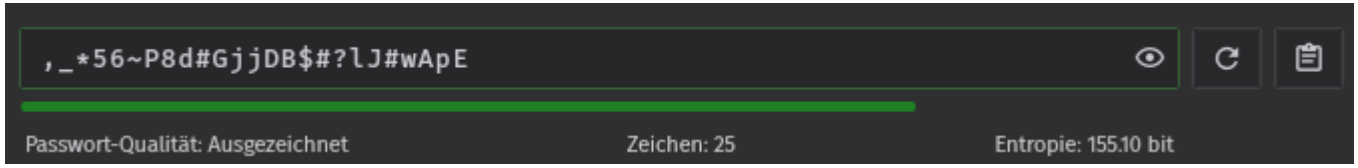
[1]

Warum ist Passwortsicherheit so wichtig?

Relevanz der Passwortsicherheit

- **Häufigstes Problem: Menschen benutzen das gleiche Passwort mehrmals (Stand 2019)**
- **Gute Passwörter kann man sich sehr schlecht merken**

  Beispiel:



- **Herausforderung: Sichere Passwörter für alle Webseiten benutzen** [2, 3]

Relevanz der Passwortsicherheit

[2, 3]

- **Meist werden Passwörter gewählt, die auf persönlichen Informationen basieren und einfach zu merken sind**

→ Anfällig für Social Engineering und Dictionary Attacken

```
it$ more rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
```

```
hannah
amanda
loveyou
pretty
basketball
andrew
angels
tweety
flower
playboy
hello
elizabeth
hottie
tinkerbell
charlie
samantha
barbie
chelsea
lovers
teamo
jasmine
brandon
666666
shadow
```

```
888888
adriana
cutie
james
banana
prince
friend
jesus1
crystal
celtic
zxcvbnm
edward
oliver
diana
samsung
freedom
angelo
kenneth
master
scooby
carmen
456789
sebastian
```

Beispiel:

Generierung einer Wortliste mit Wörtern der Hochschul-Webseite:

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo cewl -d 2 -m 5 -w itsecurityhsalbsig.txt https://www.hs-albsig.de/studienangebot/bachelorstudiengaenge/it-security-studium/
[sudo] Passwort für kali:
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
^CHold on, stopping here ...

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ wc -l itsecurityhsalbsig.txt
6756 itsecurityhsalbsig.txt
```

```
Hochschule
Engineering
Forschung
Management
Sigmaringen
Lehre
Albstadt
Business
Propädeutikum
Studium
Studieren
Bewerbung
Science
Studierende
Informatik
Unternehmen
Wintersemester
Sciences
Digital
Ansprechpartner
Personen
Teilzeit
Angewandte
Zertifikate
WebUntis
individueller
```

Lösung des Problems: Passwortmanager

Grundlagen von Passwortmanagern

- Speichert Passwörter verschlüsselt in „Vault“
- Vault kann idR mit Masterpasswort geöffnet werden
- Integrierter Passwortgenerator
- IdR Autofill-Feature
- IdR Warnung, wenn Passwort in Datenleak gefunden wurde

[4]

Sicherheitsaspekte von Passwortmanagern

- Besonders hohe Sicherheitsanforderungen wegen Single-Point-of-Failure
- Gute Verschlüsselung
- Backupmöglichkeit (Server- o. Clientseitig)
- Integrierter Passwortgenerator
- Mechanismus zum Warnen vor schlechten Passwörtern

[4]


LastPass

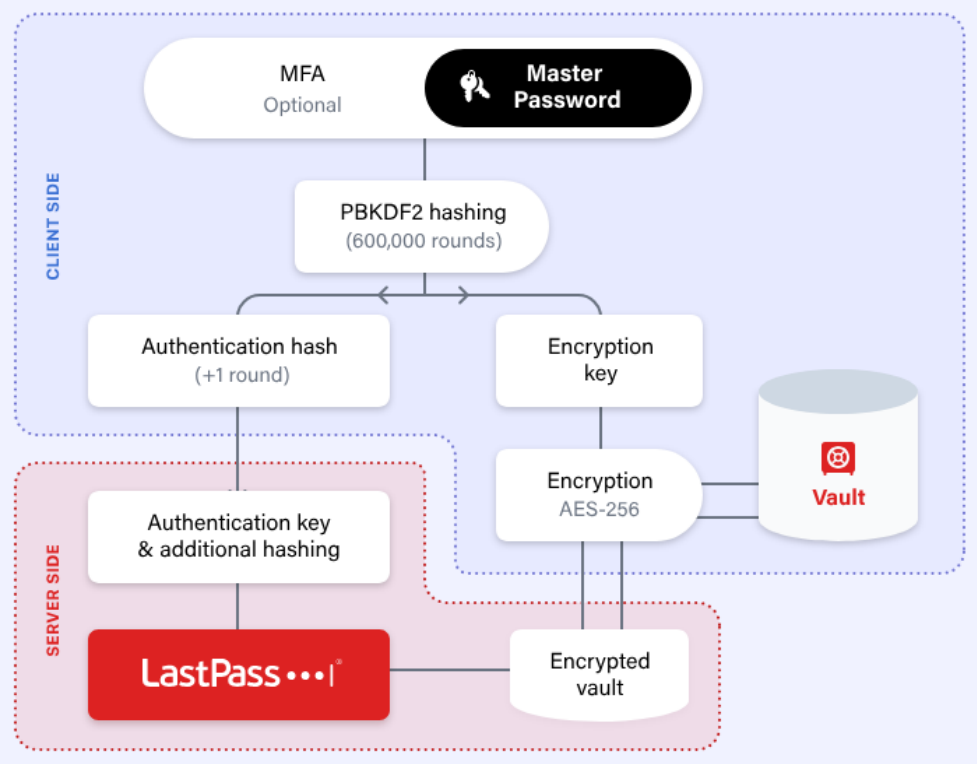
LastPass

- > 33 Mio. Nutzer (2025)
- Große OS u. Browser Unterstützung
- OTP-Generierung → Nutzbar für 2FA

[5, 6, 8]

LastPass

- **Zero-Knowledge Prinzip**



[7]

LastPass Hack 2022

- **Hacker hackten LastPass Server**

  → Zugang zu Quellcode, Nutzerdaten, verschlüsselte Passwordvaults

- **Passwordvaults konnten bei schlechten Masterpassworten geknackt werden**

- **Hexadezimale URLs (KEINE VERSCHLÜSSELUNG) an LastPass geschickt**
  → Widerspruch zu Zero-Knowledge Prinzip **[9, 10, 11]**

Apple Passwords

Apple Passwords

- **Wenige Funktionen**
- **Nur auf Apple Geräten verfügbar**
- **Hat kein Masterpasswort**
  → iCloud Account / Gerät gehackt → Passwortmanager gehackt → Single-Point-of-Failure

  => Passwortmanager sollte nicht teil eines Ökosystems sein

[3, 12, 15]


KeePass

KeePass

- Open Source, standardmäßig nur clientseitig
- Unterstützt mehrere Verschlüsselungsalgorithmen (AES256, ChaCha20, TwoFish)
- Varianten für Betriebssysteme (KeePassDX: Android, KeePassXC: Mac u. Linux)

[13, 14]

Sicherheitslücken bei KeePass

- **CVE-2023-24055: Angreifer mit Nutzerrechten kann Standardkonfiguration so verändern, dass KeePass einen unverschlüsselten Export der Datenbank anlegt, ohne dass Nutzer das Masterpasswort eingeben muss**
- **CVE-2023-32784: Angreifer konnte Masterpasswort aus Memory Dump des Systems auslesen**

→ Für Beides ist zum Ausnutzen Systemzugriff notwendig

[15, 16, 17]

KeePass Klone mit Malware

- Jeder kann Open Source Software klonen und neu verbreiten
- KeePass Versionen mit Malware werden durch Webseiten-Klone zum Download angeboten

→ Ein Passwortmanager allein reicht nicht aus. Nutzer müssen ihr System sauber halten und gegen Social Engineering geschult werden

[17]

Fazit

Fazit

- **PW-Manager essentielles Werkzeug gegen schlechte Passwörter, trotz Single-Point-of-Failure**
- **Keine Software kann zu 100 % sicher sein**
- **Richtige Nutzung: Starkes Masterpasswort, Software aktuell halten**

→ Ein Passwortmanager ist trotz seiner Risiken besser als kein Passwortmanager

Quellen

- [1] Golem.de: IT-News für Profis (n.d.): [online] https://www.golem.de/news/unsicheres-http-ios-nutzer-durch-phishing-luecke-in-passwords-app-gefaehrdet-2503-194452.html [abgerufen am 23.04.2025]
- [2] Mitnick, Kevin/Robert Vamosi (2017): The art of invisibility, First Back Bay international mass market edition, November 2018, Back Bay Books, vol. ISBN 978-0-316-52692-0
- [3] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," Conf. Res. Pract. Inf. Technol. Ser., Vol. 98, No. Aisc, pp. 71-78, 2009
- [4] Usability, security and trust in password managers: A quest for user-centric properties and features (2019): Sciencedirect, https://www.sciencedirect.com/science/article/pii/S1574013718302533#sec4 [online] [abgerufen am 17.05.2025]
- [5] TechRepublic Staff (2025): LastPass Review: Is it Still Safe and Reliable in 2025?, TechRepublic, [online] https://www.techrepublic.com/article/lastpass-review/ [abgerufen am 19.05.2025]
- [6] Wise, Jason (2025): How Many People Use LastPass in 2025? (Statistics), Earthweb, [online], https://earthweb.com/blog/lastpass-users/ [abgerufen am 25.05.2025]

- [7] Zero-Knowledge Encryption & Security Model – LastPass (n.d.): [online] https://www.lastpass.com/security/zero-knowledge-security [abgerufen am 25.05.2025]
- [8] Li, Zihwei/Warren He/Devdatta Akhawe/Dawn Song/University of California, Berkeley (2014): The Emperor's New Password Manager: Security Analysis of Web-based Password Managers, Usenix, August 20–22, 2014, San Diego, CA, ISBN 978-1-931971-15-7, [online] https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-li-zhiwei.pdf [abgerufen am 25.05.2025]
- [9] Toubba, Karim (n.d.): Security incident December 2022 update - LastPass - The LastPass blog, [online] https://blog.lastpass.com/posts/notice-of-recent-security-incident [abgerufen am 25.05.2025]
- [10] Gentles, Jessica/Mason Fields/Garrett Goodman/Suman Bhunia/Department of Computer Science and Software Engineering, Miami University (n.d.): Breaking the Vault: A Case Study of the 2022 LastPass Data Breach, Oxford, USA 45056 Ohio, United States of America: Miami University, [online] https://arxiv.org/pdf/2502.04287 [abgerufen am 25.05.2025]
- [11] User, Concerned LastPass (2017): PSA: LastPass does not encrypt everything in your vault, HackerNoon, [online] https://hackernoon.com/psa-lastpass-does-not-encrypt-everything-in-your-vault-8722d69b2032 [abgerufen am 25.05.2025]

- [12] Hackappcom (n.d.): GitHub - hackappcom/ibrute: AppleID bruteforce p0c, GitHub, [online] https://github.com/hackappcom/ibrute [abgerufen am 25.05.2025]
- [13] Reichl, Dominik (n.d.): Security – KeePass, [online] https://keepass.info/help/base/security.html#secencrypt [abgerufen am 25.05.2025]
- [14] Novak, Janette (2025): KeePass Review, Forbes Advisor, [online] https://www.forbes.com/advisor/business/software/keepass-review/ [abgerufen am 25.05.2025]
- [15] Team, KeePassXC (2025): KeePassXC Password Manager, [online] https://keepassxc.org/#project [abgerufen am 25.05.2025]
- [16] NVD - CVE-2023-24055 (n.d.): [online] https://nvd.nist.gov/vuln/detail/CVE-2023-24055 [abgerufen am 25.05.2025]
- [17] Knop, Dirk (2023): Passwort-Manager: Umstrittene Sicherheitslücke in KeePass beseitigt, in: Security, 09.02.2023, [online] https://www.heise.de/news/Umstrittene-KeePass-Schwachstelle-mit-Update-geschlossen-7489944.html [abgerufen am 25.05.2025]
- [18] Long, Emily (2025): Apple Passwords password manager review, Tom's Guide, [online] https://www.tomsguide.com/computing/password-managers/apple-passwords-review [abgerufen am 25.05.2025]

Teil 2 – Deep Dive

junk_rat

Open Source vs. Closed Source Passwortmanager

- **Open Source: Jeder kann Quellcode auf Sicherheit überprüfen und Sicherheitslücken melden**
- **Closed Source: Sicherheitslücken werden durch Sicherheitsforscher u. Bug-Bounty Progranne gefunden**

  → Liegt an der Firma, wie mit gefundenen Sicherheitslücken umgegangen wird


1Password

1Password

- **Cloudbasiert**
- **Schlüsselmaterial wird aus 2 Faktoren abgeleitet:**
  1. Masterpasswort
  2. Clientseitiger Secret Key (nicht im kryptografischen Sinne)

  → Hacker kann Vault nicht entschlüsseln, selbst wenn er das Masterpasswort kennt

1Password

- Vermischung von symmetrischer u. asymmetrischer Krypto
- Symmetrisch: 256-Bit AES im GCM
- 1Password speichert private Key in der Cloud (!)
- Private Key wird mit AES verschlüsselt
  → Dieser AES Schlüssel wird zufällig aus Account-Passwort und lokal gespeichertem Secret Key generiert

1Password

- **Secret-Key wird bei Registrierung clientseitig generiert**

  → Aktuelle 1Password Version + Account ID + 26 zufälligen Zeichen = 2^{18} mögliche Kombinationen

- **Masterpasswort erraten nicht möglich, da Secret Key fehlt**
- **Bei Gerätedefekt ohne Secret-Key Passwort-DB nicht mehr zugreifbar → Emergency-Kit-PDF**

1Password CVE-2024-42219

- Sicherheitslücke betraf MacOS Client für 1Password
- Ermöglichte es, Interprozess-Kommunikation auszulesen

  → Inhalte des Vaults konnten ausgelesen werden
- Patch wurde schnell veröffentlicht

Bitwarden

- Open Source
- Self-Hostable
- 0-Knowledge Prinzip
- Clientseitige Verschlüsselung des Vaults (AES 256-Bit)

Bitwarden Sicherheitslücke

- Sicherheitslücke im Auto-Fill Mechanismus
- Passwörter wurden auch in externe HTML Iframes eingefüllt
- Iframe kann eingegebene Daten an 3rd Party Webseite weiterleiten

  → Low-Risk, da sehr wenige Webseiten Iframes mit Input Formularen einbinden

Bitwarden Sicherheitslücke

- Bitwarden wusste seit 2018 von der Iframe Lücke
- Wurde absichtlich nicht behoben
- Behebung würde auch legitime Nutzung verhindern

→ Apple bindet z.B. bei icloud.com ein legitimes Iframe von apple.com ein

Bitwarden Sicherheitslücke

- **Logindaten wurden auch bei Subdomains ausgefüllt, wenn Hauptdomain der hinterlegten Domain entsprach**

  login.beispiel.com
  angriffsvektor.beispiel.com

  → Kritisch wenn Webseite Usercontent auf Subdomains hostet

Quellen

- 1Password (2025): About the 1Password security model | 1Password Support, 1Password
  https://support.1password.com/1password-security/
- Winder, Davey (2024): Critical 1Password security flaw could let hackers steal unlock key, Forbes
  https://www.forbes.com/sites/daveywinder/2024/08/07/critical-1password-security-flaw-could-let-hackers-steal-unlock-key/
- https://www.bleepingcomputer.com/news/security/bitwarden-flaw-can-let-hackers-steal-passwords-using-iframes/
- https://keepass.info/help/base/security.html#secencrypt
- https://www.heise.de/news/Umstrittene-KeePass-Schwachstelle-mit-Update-geschlossen-7489944.html
- https://cyberinsider.com/password-manager/reviews/bitwarden/
- https://www.tomsguide.com/computing/password-managers/apple-passwords-review
- https://robfreeman.com/should-you-use-the-apple-passwords-app/