Generate and Store Strong Passwords: A Way to Manage Having a Multitude of Passwords

Teodor-Mihai CĂLUGĂREANU
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA of Bucharest,
Romania
teoclg@gmail.com

Abstract

In the current day it is difficult to have a strong password for each account that one someone makes. If an individual were to use similar simple passwords for all the accounts in his possession, then he would be very vulnerable to a brute force attack and other types of attacks. As such it is necessary to have difficult-to-guess, unique passwords for each account, even though it may be hard to remember all the passwords. A method to achieve this is by using a password manager and a password generator. By using a database management system like MySQL and a web framework such as Flask, based on Python, a solution can be made: a website which can generate and store passwords, as well as other information about the accounts, to make it easier to manage many passwords. This is beneficial to anybody that wants to improve the security of their accounts and does not want to be bothered to remember a large number of passwords.

Index terms: database, MySQL, password management, Python, secure passwords

References

[1]. How to help keep your Microsoft account secure, https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb.
[2]. How to Create a Strong Password, https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/.
[3]. Summers, Wayne & Bosworth, Edward. (2004). Password policy: The good, the bad, and the ugly. 1-6.
[4]. Oracle Cloud Infrastructure sign-up (OCI) https://www.oracle.com/cloud/.
[5]. Bitwarden Blog, How long should a password be?, https://bitwarden.com/blog/how-long-should-my-password-be/.
[6]. NordVPN Blog, Password entropy: Definition and formula, https://nordvpn.com/blog/what-is-password-entropy/.

[7]. DAS, Anupam, et al. The tangled web of password reuse. In: NDSS. 2014. p. 23-26.
[8]. M. Dell'Amico, P. Michiardi and Y. Roudier, "Password Strength: An Empirical Analysis," 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1-9, doi: 10.1109/INFCOM.2010.5461951.
[9]. Weir, Matt & Aggarwal, Sudhir & de Medeiros, Breno & Glodek, Bill. (2009). Password Cracking Using Probabilistic Context-Free Grammars. 391-405. 10.1109/SP.2009.8.
[10]. Garrison, C. P. (2008). An evaluation of passwords: Certified public accountant. The CPA Journal, 78(5), 70-71. Retrieved from https://www.proquest.com/scholarly-journals/evaluation-passwords/docview/212318354/se-2.
[11]. KESZTHELYI, András. About passwords. Acta Polytechnica Hungarica, 2013, 10.6: 99-118.
[12]. Chao Shen, Tianwen Yu, Haodi Xu, Gengshan Yang, Xiaohong Guan, User practice in password security: An empirical study of real-life passwords in the wild, Computers & Security, Volume 61, 2016, Pages 130-141, ISSN 0167-4048, https://www.sciencedirect.com/science/article/pii/S0167404816300657.
[13]. Number of e-mail users worldwide 2017-2026, https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/.
[14]. Average number of social media accounts per internet user from 2013 to 2018, https://www.statista.com/statistics/788084/number-of-social-media-accounts/.
[15]. Hussain, Hamzha. "Password Security: Best Practices and Management Strategies." Available at SSRN 4136333 (2022).
[16]. Bitwarden, World Password Day Global Survey Full Report, https://bitwarden.com/resources/world-password-day-global-survey-full-report/.
[17]. ALKALDI, Nora; RENAUD, Karen. Why do people adopt, or reject, smartphone password managers? In: 1st European Workshop on Usable Security-EuroUSEC 2016.
[18]. A. Morales, 8 Advantages of using MySQL in 2023, https://www.linkedin.com/pulse/8-advantages-using-mysql-2023-andrea-morales.