Full Citation

URL

https://www.computer.org/csdl/proceedings-article/sp/2021/893400b626/1t0x9vjv8Z2

Abstract

Password managers are tools to support users with the secure generation and storage of credentials and logins used in online accounts. Previous work illustrated that building password managers means facing various security and usability challenges. For strong security and good usability, the interaction between password managers and websites needs to be smooth and effortless. However, user reviews for popular password managers suggest interaction problems for some websites. Therefore, to the best of our knowledge, this work is the first to systematically identify these interaction problems and investigate how 15 desktop password managers, including the ten most popular ones, are affected. We use a qualitative analysis approach to identify 39 interaction problems from 2,947 user reviews and 372 GitHub issues for 30 password managers. Next, we implement minimal working examples (MWEs) for all interaction problems we found and evaluate them for all password managers in 585 test cases.Our results illustrate that a) password managers struggle to correctly implement authentication features such as HTTP Basic Authentication and modern standards such as the autocomplete-attribute and b) websites fail to implement clean and well-structured authentication forms. We conclude that some of our findings can be addressed by either PWM providers or web-developers by adhering to already existing standards, recommendations and best practices, while other cases are currently almost impossible to implement securely and require further research.