UC-339

Cybersecurity Analysis of Password Managers

INTRO/ABSTRACT

Our objective is to analyze the cybersecurity framework of popular password managers by researching vulnerabilities and exploring potential exploits. We chose to analyze five of the most popular password managers on the market: 1Password, BitWarden, LastPass, Google Chrome, and Firefox. After researching we determined our focus would be Bitwarden's PIN feature, Google Chrome, and Firefox. We were unsuccessful at brute-forcing Bitwarden or its PIN feature due to a 5-attempt full lockout feature. Using a password recovery tool, ChromePass, we were able to successfully decrypt the local Login Data file for Google Chrome. We attempted to use a similar tool to decrypt the local passwords file for Firefox, however it was unsuccessful due Microsoft Defender flagging the application.

METHODS

Bitwarden

- Shell Script &Brute Force

Google Chrome

- Python scripts masked as password recovery Tool (ChromePass)

Firefox

- Python scripts masked as password recovery tool (PasswordFox)

RESULTS

Bitwarden/ Failed attempt

- Brute-force was not successful, due to their mitigation policy that allows 5 attempts before user lockout. At which point, the user's PIN is disabled and they are required to re-enter their master password before proceeding and enabling the PIN option again.

Google Chrome/ Successful attempt

- ChromePass was successful at decrypting the login data file. Through more thorough testing, we found it is possible to access the login data file of other users on the local machine if their Windows login password is obtained.

Firefox/ Failed attempt

- PasswordFox was unsuccessful, because it was flagged by Microsoft Defender as potentially containing a virus, so we were unable to launch the tool.

Resources:

https://commons.wikimedia.org/wiki/File:Bitwarden_logo.svg
https://logos-world.net/chrome-logo/
http://www.stickpng.com/img/icons-logos-emojis/tech-companies/firefox-logo
http://www.nirsoft.net/utils/chromepass.html
http://www.nirsoft.net/utils/passwordfox.html

This capstone project aims to evaluate the cybersecurity framework of popular password managers, identify vulnerabilities, and explore possible exploit opportunities. The project is important because a secure and reliable password manager is crucial in protecting sensitive data from breaches, which are becoming more common and complex. Passwords can unlock various websites with private information that can lead to severe consequences if accessed by bad actors.

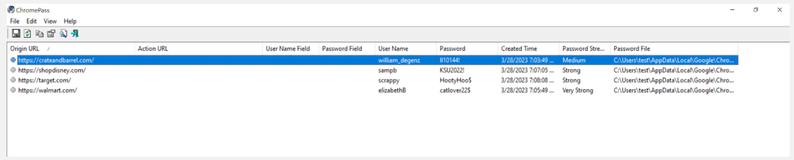

Figure 1: Above displays the plaintext Google Chrome logins in the ChromePass interface after the application is launched.

Visit our website for more information:

Figure 2: Above is the encrypted login data file when opened using Notepad.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s): Lita Massengale, Katie Shirilla, Zack Rasheed, Ruben Vazquez, Caleb Fox
Advisors(s): Donald Privitera