Cybersecurity Analysis of Password Managers

Milestone 2

Group 1
IT 4983
Section 01

Lita Massengale, Katie Shirilla, Caleb Fox,
Zack Rasheed, & Ruben Vazquez

03.26.2023

Milestone 2 Summary

- ☑ Met with our Industry Professional
- ☑ Researched how to perform a brute force attack
- ☑ Determined Bitwarden attack not possible
- ☑ Proved Chrome vulnerability
- ☑ Tested potential Firefox vulnerability
- ☑ Worked on research report and website

Our Targets

Milestone 1

- 1Password
- Bitwarden
- LastPass
- Google Chrome
- Firefox

Milestone 2

- Bitwarden
- Google Chrome
- Firefox

Bitwarden Attack Plan

When coming up with types of attack there were several options we looked into

- Brute force
- Keylogging
- Shell script to enable RDP

Bitwarden - Brute Force

Our main focus of attack for Bitwarden was to brute force the PIN that users create rather than the master password itself. We realized this would not work because after 5 failed attempts it would log the user out and make them use their main password to get back in. After the user is logged off, all PIN settings are reset and must be re-enabled by the user after logging back in with the master password. This is in place to mitigate brute force attempts and is why we were unsuccessful in breaching bitwarden.

Testing Environment:

- Tested on two devices (mobile phone, desktop)
- Tested with a Bitwarden account

Results:

- Unable to successfully brute force the password
- Kicked out of PIN option and forced to use main password to log back in
- To many possibilities for this approach to be successful

Google Chrome - ChromePass

ChromePass is a tool offered on the NirSoft website as a password recovery tool. It is intended to reveal URL data, username field, password field, and time created.

Testing Environment:

- Tested on two devices (laptop and desktop)
- Tested with and without Google Chrome account created

Results:

- Incompatible with Linux Ubuntu, only Windows OS
- Ran successfully
- Not flagged as a potential threat by Microsoft Defender
- On both devices, the application ran with no issue and immediately pulled on login data saved
- Logins file only available once signed into a Chrome profile using a Google account
- If multiple Google accounts are logged in under one Chrome profile, passwords from both accounts are stored in the same file
- Attempted to sign into a different Chrome profile and signed out of the previous profile/account. Passwords from both were still there, due to lack of differentiation

Firefox - Password Fox

PasswordFox is another tool offered on the NirSoft website as a password recovery tool. It is intended to reveal site data, username field, password field, record index, and Signons filename.

Testing Environment:

- Tested on two devices (laptop and desktop)
- Tested with and without Firefox Browser account created

Results:

- Incompatible with Linux Ubuntu, only Windows OS
- On both devices, Microsoft Defender flagged it as a potential threat
- On the laptop, the application would not run at all
- On the desktop, the application was unsuccessful (stating the operation could not be completed)
- Logins file only available once creating a Firefox account
- Logins are stored in a .JSON file. Attempted using other online tools specifically to decrypt .JSON files, however was unsuccessful
- All profile information is stored in Roaming files, rather than Local

Overall Findings

Bitwarden Status/ Failed attempt

- ➔ Brute force is not possible for bitwarden has mitigated risk by only allowing 5 attempts before lockout is enabled as well as allowing the user to use special characters within the simple passcode for desktop users. Even if bitwarden didn’t have a lockout feature a nine digit pin would have 10^9 = 1,000,000,000 different possibilities.

Google Chrome Status/ Successful attempt

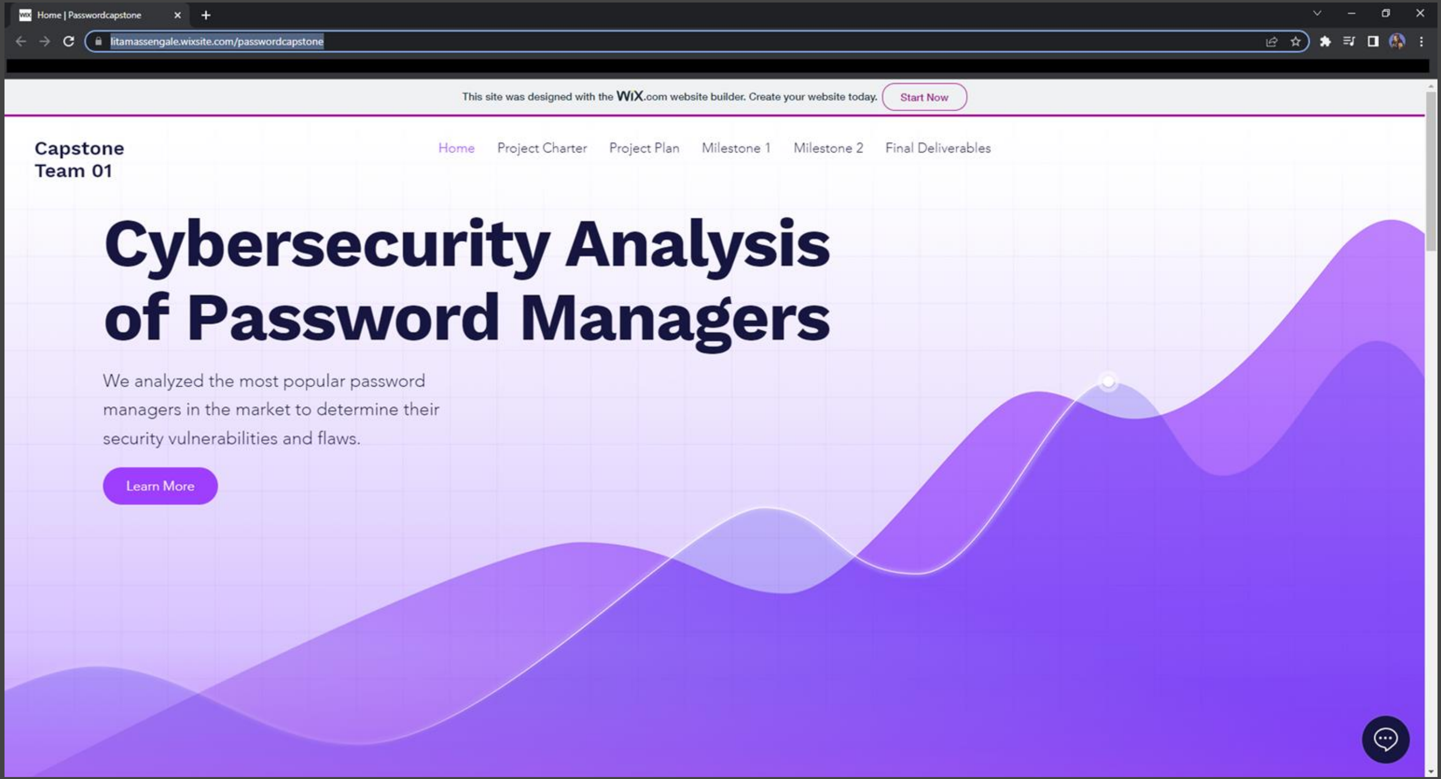
- ➔ We were able to find where the login data file was located on the local device. It was encrypted however chrome pass recovery tool is available to download and install to view the password file. This is a known tool that could be used to exploit users.

Firefox/ Failed attempt

- ➔ From the same website where we retrieved the chrome pass there was another tool that was unable to locate the file and un encrypt the data.

Website

https://litamassengale.wixsite.com/passwordcapstone



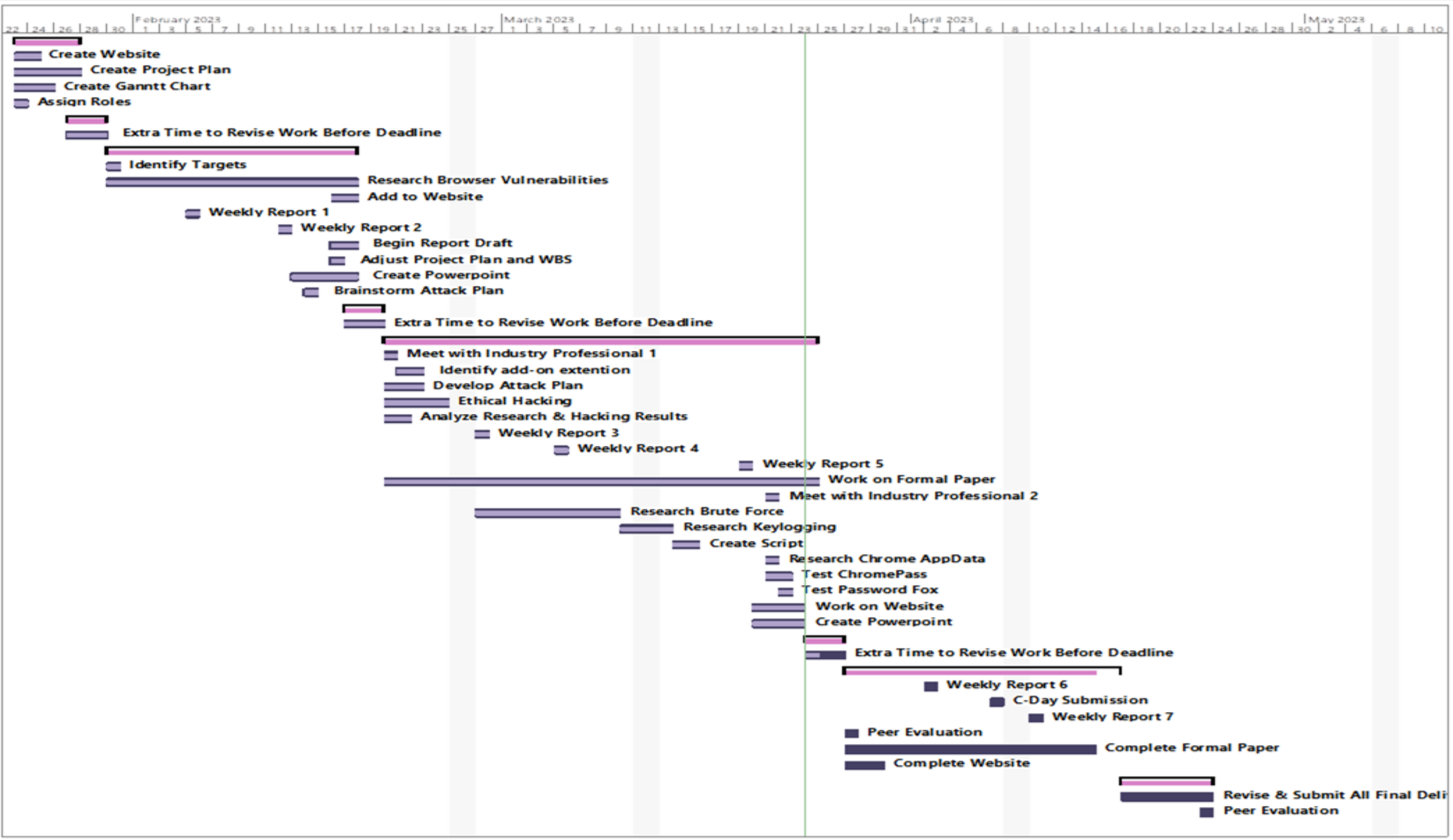
Cybersecurity Analysis of Password Managers

We analyzed the most popular password managers in the market to determine their security vulnerabilities and flaws.

Project Experience

- Adjustments to the project plan and WBS
- Addition of tasks as we began testing
- Good group communication
- Overall stayed on track with schedule

Updated Gantt Chart



Next Steps...

- Prepare for C-Day submissions
- Complete research report
- Complete project website

Thank You

- Lita, Katie, Caleb, Zack, & Ruben -