Slide Me A Fiddy
Script

Intro
Good Morning ladies and gentlemen. Today we will be discussing a new password manager called “Fiddy Manager.” If you will give me your attention for just a few moments, we will explain the importance of having a password manager, the steps that went into the wire framing and Research & Development of it and finally the actual product and show you the behind the scenes E! True Hollywood Story of how we made this incredibly helpful tool.
But first, let’s meet the team behind Fiddy Manager. We have Brooke Braham, Samantha Brown, Ryan Cook, Reza Nosrati, Dylan Terrazas and myself Ricky Foust. Together we will all be speaking with you today, so strap in and hold on while we dive deeper into the exciting world of password management.

Part 1
So what’s a password manager and “why would I need this anyways?”
According to a 2023 study by Goodfirms, 3 in 10 users have been victims of data breaches due to weak passwords and this number is growing rapidly.
The HIPAA journal reported that data breaches soared from 45.9 million in 2021 to 133 million in 2023. This has led to a 278% increase in ransomware attacks during the same period. This is a huge problem which has led companies to start using password management services.
And that is where Fiddy Manager comes in. With one master password, you’ll be able to log into Fiddy Manager and create secure new passwords, see the health of current passwords, and store passwords inside of a locked ‘vault.’
It provides enhanced security by generating and storing strong unique passwords for each account, as well as enforcing a strong password policy such as minimum length, complexity requirements and password expiration dates.
Ultimately Fiddy Manager was crafted with your security in mind, offering a simple solution to safeguard your passwords with utmost reliability and confidentiality.

Here’s Ryan to tell you how we facilitated this process.

Part 2
In the initial phase of our project, we embarked upon the task of wireframing, the architectural blueprint of our web page.
Our team utilized Jamboard, which allowed us the opportunity to collectively brainstorm. Through this collaborative endeavor we identified all the aspects of the wireframe.

This included a sign on screen and then a main page with a sidebar and the actual password log.
We also decided upon buttons we wanted to create (such as the choice of a password or passphrase button option), a timer (to log-out when inactivity occurs), sorting options of passwords, and recording each password's creation and expirations dates.
Once this task was completed it was time to start writing code.
Our team used CodePen as our collaborative workspace where everyone was able to individually type out HTML, CSS and JavaScript code.
We allocated specific tasks - ranging from designing action buttons, to creating the inactivity timer, to password and passphrase creation rules, and to table creation.
CodePen allowed us to work simultaneously without stepping on each other's toes but as we progressed, consolidating our individual contributions occasionally presented challenges.

Here's Dylan to tell you more.

Part 2.5
Merge errors and unexpected CSS adjustments occasionally confused us.
Recognizing the need for a more robust environment to finalize our work, we transitioned to Visual Studio Live Share. In this environment, we transferred the most recent code iterations from CodePen and began adding the final touches and working out the error codes. This allowed us to save, test, and carefully update parts of our code until we got everything working together.

We then used Firebase for our account creation and storing. Firebase handled our account creation, storing hashed passwords, account disabling, and password resets. Additionally, it also offered analytics insights, reliable hosting solutions, and efficient storage capabilities.

With Fiddy Manager your passwords, usernames and corresponding sites are highly secured through a defense in depth approach. Here is Brooke to walk you through what we implemented.

Part 3
First, we've implemented User Authentication, ensuring secure access to our application for specific users. Through the creation of a login page, we've strengthened our system, safeguarding password data from unauthorized access.

Second, we implemented password hashing. When storing these passwords, it's crucial for us to uphold strict security measures to protect the user's passwords. Whenever a new account is created, Firebase hashes the passwords using their internal hashing script. These hash parameters include a hash key and password salting. Password

salting, which adds a random piece of data to user passwords before it is hashed, creates additional protections for the password and mitigates the risk of password cracking through techniques like rainbow table attacks.

Third, we implemented shoulder surfing prevention by incorporating a blur effect over the passwords listed on the log to prevent unwanted viewership by potential internal threats.

Fourth, we created an automatic timeout feature to occur once a minute of inactivity occurs. This will initiate a 60 second countdown that once finished, will blur the entire screen until logged out - in order to prevent shoulder surfing or unwarranted access to your personal Fiddy Manager Account.

And lastly we've implemented Cross-Site Scripting protections by ensuring that user input is properly sanitized before being rendered in the HTML. This prevents malicious scripts from being injected into the page, thereby mitigating the risk of XSS attacks.

Additionally, the code employs Content Security Policy headers to restrict the sources from which resources can be loaded, further fortifying the application against XSS vulnerabilities.

Now it's time to show you how it works, here's *Samantha* for a walkthrough.

Part 4

Here is our first screen featuring the ability to enter your username and password to login
We also provide a link to Create an Account. These fields are all required. (RETURN TO LOGIN)
If needed, we have an automated Reset Password service.
Once you login you will see we have the ability to review and add passwords
(Add Passphrase) We can choose between a password and passphrase
Password Expiration Dates are set automatically at 180 days to remind you to change passwords twice a year.
As a reminder, the passwords are blurred to prevent Shoulder surfing
We provide the ability to delete a password (CLICK ABOUT ME)
This page tells users a little more about the Fiddy Manager team including how to connect with them on LinkedIn (RETURN TO DASHBOARD)
When you're finished, use the Logout button.
For demonstrations, our Inactivity timer is set to 5 seconds but will reset with any user input.
Once the timer reaches 0:00, we are logged out.

That concludes our walk through, now here's Reza to tell you what else we have in store for Fiddy Manager.

Part 5

When looking at the future for Fiddy Manager we would love to expand eventually and create more features to enhance our security for our users.

Our main idea that we would like to add would be a ‘Hardware Token,’ that you would use in conjecture with your password when logging into your Fiddy Manager. This increases further security because now the single factor authentication to log in will be transformed into a multi-factor authentication log in.

When talking about the different factors in authentication - there are 5 commonly used ones: Something you know (which is a knowledge factor), something you have (which is a possession factor), something you are (which is an inherence factor), something you do (which is an action factor) and somewhere you are (which is a location factor).

So by introducing a hardware token - we would be adding on a ‘something you have’ factor - since someone would need a physical object in their possession to access their Fiddy Manager - in addition to the ‘Something you know factor’ - which the user will already know - which is their master password to their account. So by doing that we would be introducing a multi-factor authentication which would amplify the security for our users.

Going to pass it back now to Dylan.

Conclusion

We hope you enjoyed our presentation today and learned a little bit more about what a password manager can do for you. And if you’re one of the 33% Americans who use their pet’s names extensively in their password choices, it may be time to consider ‘Fiddy Manager.’ Thank you for watching.