Password Vault

Dikshitha Rathore[1], Kathera Bhavita[2], Challa Kavya Reddy[3]

[1]Student of Department of Computer Science and Engineering – Cybersecurity, Geethanjali College of Engineering and Technology, Hyderabad, Telangana
[2]Student of Department of Computer Science and Engineering – Cybersecurity, Geethanjali College of Engineering and Technology, Hyderabad, Telangana
[3]Student of Department of Computer Science and Engineering – Cybersecurity, Geethanjali College of Engineering and Technology, Hyderabad, Telangana

---***---

Abstract - Let's be real, keeping track of passwords for every online account is a pain. Most folks just recycle the same flimsy passwords everywhere, which is basically inviting trouble. That's what pushed me to create this Password Vault. It's built to keep your passwords safe and make your digital life a whole lot easier. Here's the deal, the vault locks down your passwords using solid AES encryption. Only you can unlock them with your master password. Once you're in, everything stays private. All the complicated key management stuff happens in the background, so you never have to mess with it. But this thing does more than just stash your passwords. It checks how strong they are and scans to see if any have popped up in data breaches. If it finds something weak or compromised, you get an instant heads-up—time to fix it. There's even a phishing detector. If you're about to log in somewhere shady, it throws up a warning before you get caught. I put the whole thing together in Python with a simple Tkinter interface. It's easy to use, even if you're not super tech-savvy. By combining strong encryption, smart checks, breach alerts, and phishing protection, this Password Vault actually cuts through the chaos of online security. It's not just a tool—it's a way to build better password habits, one login at a time.

Key Words: Password Vault, Cyber Security, Encryption, Authentication, Password Management, Breach Detection, Phishing Detection

1. INTRODUCTION

These days, it's almost impossible to get through daily life without using online platforms. People and organizations depend on things like email, online banking, social media, cloud storage, shopping sites, and all sorts of work or school portals. Every one of these places asks for a username and password. The more accounts you have, the harder it gets to keep track of all those passwords—and to keep them safe. That's why password security has become such a huge deal in cybersecurity.

Passwords are still the go-to method for logging in, mostly because they're easy to use and cheap to set up. But let's be honest, passwords are also the weak spot in most systems. A lot of people pick simple passwords so they don't forget them, or they use the same password everywhere, or they stash their passwords in places that are not secure at all like text files, browsers, or even sticky notes. Stuff like this just makes it easier for someone to break in, steal data, or commit fraud.

We see all sorts of cyberattacks now brute-force attacks, dictionary attacks, credential stuffing, phishing, and big data breaches. The sad truth is, hackers don't always need to break fancy security measures. Most of the time, they just take advantage of weak, reused, or already stolen passwords. When huge data leaks happen, millions of usernames and passwords end up out in the wild, and because people reuse passwords, one leak can open the door to a bunch of your accounts. That's why managing passwords securely matters more than ever.

This is where password vaults or password managers step in. They're apps that keep all your login credentials locked up in an encrypted vault. Instead of remembering a dozen passwords, you only need to remember one master password to get into the vault. Everything inside stays encrypted, so even if someone gets their hands on the storage, your data's still safe. Good password managers can also help you create strong, unique passwords for every site, making password reuse a thing of the past.

There are lots of commercial password managers out there, but they're not perfect. Some make you pay monthly fees, some force you to use their cloud, some aren't open about how they work, and a lot of them feel way too complicated if you're not tech-savvy. And if a password manager stores everything in one place without top-notch security, that just gives hackers a bigger target. So, it's really important to build password vaults that are not only secure, but also easy to use and trustworthy.

This Password Vault project takes on those challenges head-on. It gives you a secure space for all your credentials, protected by strong encryption and tough authentication only the right person gets in. It uses advanced encryption to lock down your passwords and manages the keys carefully so nobody else can decrypt your stuff.

But it doesn’t stop there. The vault checks how strong your passwords are and helps you create better ones. It looks out for your credentials in known data breaches, warning you right away if something’s been leaked. There’s even phishing detection, so if you try to log in somewhere sketchy, it lets you know.

The app’s built in Python and comes with a simple interface made with Tkinter, so anyone can use it, even if they don’t know much about tech. It works offline, so you don’t have to worry about losing access if the internet goes down, and it doesn’t trade off security for convenience. Plus, the way it’s built means new features can be added later like using biometrics, syncing with the cloud, or handling credentials for a whole company.

To sum it up, this Password Vault is all about making digital life safer by fixing the usual password problems people face. By bringing together strong encryption, smart authentication, password checks, breach alerts, and phishing protection, it helps people use better password habits and keeps them more aware of online risks. It’s a practical, hands-on tool for anyone who wants to take control of their digital security.

2. LITERATURE REVIEW

Back in 2007, Florencio and Herley dug into how people actually use passwords online. They looked at a massive pile of real authentication records and found something pretty concerning most folks pick short, simple passwords and just reuse them all over the place. It turns out, this habit makes it way easier for attackers to pull off credential stuffing and dictionary attacks. Basically, relying on people to come up with good passwords isn’t working. The researchers pushed for automated password managers tools that generate and store strong, unique passwords for each site to cut down on human mistakes and make things safer overall.

A year earlier, Gaw, Felten, and Fernandez-Kelly tried to figure out how regular people deal with managing a bunch of passwords in daily life. Through interviews and user studies, they saw the same patterns over and over: people write passwords down, reuse them, or just tweak a familiar one because it’s hard to remember so many. Usability problems are at the heart of why people behave this way. The team suggested that password managers, if they’re actually easy to use, can take the pressure off and make security better. Their work really set the stage for the user-friendly password vaults we see now, where security and convenience finally meet.

Then, in 2012, Kelley, Komanduri, Mazurek, and Shay took a closer look at how we judge password strength. Instead of just counting characters or looking for a mix of letters and numbers, they used probabilistic models and pattern recognition to estimate how easy a password would be to guess in real life. They found that a lot of passwords marked “strong” by old-school rules were still sitting ducks for targeted attacks. Their research showed that when you give people honest, detailed feedback on password strength, they actually pick better passwords. This makes a strong case for building smarter, more accurate strength meters right into password vaults.

Fast forward to 2018, and Li, Wang, and Sun built a password manager focused on rock-solid security. Their system used strong encryption, smart key management, and solid hashing and salting to keep stored credentials safe from offline attacks. They tested it against brute-force and data leakage threats and proved that encrypted password vaults make it a lot tougher for attackers to break in. Their findings hammered home the need for tight cryptographic protection in any serious password vault.

In 2019, Hunt and McMillan shook things up by introducing breach detection for users. Basically, they let people safely check if their passwords were exposed in any known data breaches without ever sending those passwords to outside servers. When someone’s credentials turned up in a breach, the system warned them so they could change their password right away. This kind of breach alert stopped people from sticking with leaked passwords, which are a huge risk for account takeovers. Their work showed how critical it is to bake breach detection right into password vaults.

By 2021, Wang, Zhang, and Chen pulled everything together. They designed a password vault that handled encrypted storage, password strength checks, and breach detection all under one roof. Their system gave users real-time feedback and security alerts, and it worked: people started choosing stronger passwords and stopped reusing compromised ones. The research made it clear that bundling all these tools into a single, user-friendly app makes a huge difference for security. That’s exactly the direction modern password vaults are heading making things safer and easier at the same time.

3. EXISTING SYSTEM

Most people handle their passwords with a mix of old-school habits and whatever tools are easiest to grab. Some folks just scribble passwords in a notebook, stash them in a plain text file, or dump them into a notes app without a second thought. It feels simple, but there’s zero encryption or protection. If someone gets hold of your phone or laptop, well, your passwords are just sitting there, wide open.

Then you've got browser password managers the ones built into Chrome, Safari, or whatever you use. They definitely make life easier, filling in passwords automatically. But they lean hard on your browser and device security. If someone else uses your computer or it gets hacked, your saved logins aren't exactly safe. Plus, most browser managers don't give you much control over things like encryption or advanced security features. Forget about real breach detection or warnings about sketchy websites.

Third-party password managers like LastPass, Dashlane, or KeePass step things up with encrypted storage and password generators. They're way better than handwritten notes, no question. But they aren't perfect. Everything hinges on one master password if that's weak or gets leaked, you're in trouble. And because a lot of these managers use cloud sync, you have to trust their servers with your data and stay connected to the internet. That opens the door to privacy worries and the risk of big breaches.

A lot of password tools tack on simple "strength" meters, too. But most only check for things like length, numbers, or special characters. They miss the point. You can still end up with "Password123!" labeled as strong, which is laughable. People end up feeling safe when they shouldn't.

On top of all that, most password managers don't warn you if your logins show up in a data breach or if you're about to hand over your credentials to a phishing site. So, you're often the last to know if something's gone wrong and by then, it's too late.

Most password management options force you to pick between convenience and real security. Either you get something easy to use but risky, or you lock things down and deal with a headache. The lack of smart password checks, built-in breach alerts, phishing protection, and offline access just shows how much we need a better, safer, and more user-friendly way to protect our passwords.

4. PROPOSED SYSTEM

This system is all about giving people a safer, smarter way to manage their passwords without making things complicated. The Password Vault puts security first but keeps things simple, so you don't have to jump through hoops just to keep your logins safe. It mixes tough cryptography with clever security tools, so your credentials stay locked down, organized, and you're always up to speed about any password risks.

Here's how it works, every password you save gets encrypted with strong algorithms like AES. Even if someone grabs the storage file or database, they're just looking at unreadable data unless they have your decryption key. You unlock everything with a master password, so only you (or someone you trust) can see or change anything inside. The system takes key management seriously, too, blocking any sneaky attempts to break in or steal your keys.

Instead of the same old password rules, this vault checks the strength of your passwords in real time. It actually looks at patterns, unpredictability, and all that nerdy stuff then gives you instant feedback. You end up making stronger, unique passwords, and that shuts down most brute-force and guessing attacks.

There's more. The vault keeps an eye out for data breaches. If any of your passwords show up in a known breach, you get an alert right away. You can swap out that password before anyone uses your leaked info against you. That way, you're not left in the dark, and you avoid things like credential stuffing and account takeovers.

Worried about phishing? The vault's got your back. If you try to save or use a password on a fishy website, it'll warn you. It scans URLs and looks for patterns that match known phishing tricks, so you're less likely to hand over your info to the wrong people.

Everything runs on Python, using Tkinter for the interface, so it's straightforward even if you're not a tech expert. No need to stay online all the time, either. You can access your passwords securely, even offline. Plus, the whole thing's built to handle upgrades down the line think multi-factor authentication, biometric logins, syncing with the cloud, and managing credentials for businesses.

In short, this Password Vault blends strong protection, smart features, and ease of use. It's a practical answer to today's password headaches, built for real people who just want to stay safe online.

5. TECHNOLOGIES USED IN PROJECT

Modern password managers lean on a mix of smart programming, strong cryptography, and easy-to-use interfaces. With the Password Vault, all of these come together. Each piece of tech matters whether it's storing passwords, checking their strength, authenticating users, spotting breaches, or blocking phishing attempts.

1. Python Programming Language

Python is at the heart of the Password Vault. It's simple to read, packed with security libraries, and just makes development fast. With Python, you get smooth cryptography integration, database management, password analysis, and easy API connections. Plus, it runs everywhere Windows, Linux, macOS. That means users and developers don't have to fuss about compatibility or maintenance.

2. Tkinter (Graphical User Interface)

Tkinter builds the visual side of the Password Vault. You'll see windows, buttons, input fields, pop-up alerts all the stuff you actually interact with. Tkinter keeps things light and responsive, so you're not waiting around. It also takes security seriously, especially when handling master passwords or saved credentials.

3. Cryptography Libraries for Encryption and Hashing

Security here isn't just a checkbox. Three main libraries do the heavy lifting:
Fernet handles encrypting and decrypting stored passwords. Credentials get locked up before storage and only unlock for users who've logged in.
hashlib deals with hashing think SHA-256 and other strong algorithms to make sure data stays unchanged and secure.
bcrypt is for hashing the master password. It salts and adapts, so even if someone gets their hands on the data, cracking the original password is nearly impossible.
Put together, these tools keep your credentials safe from offline attacks and prying eyes.

4. Password Strength Evaluation Library (zxcvbn)

zxcvbn checks how strong your passwords really are. Instead of just nagging about "uppercase letters," it looks at patterns, dictionary words, and how easy a password is to guess. You get live feedback, nudging you to pick something safer and more unique.

5. Breach Detection API

Nobody wants to reuse a password that's floating around the dark web. That's where the Have I Been Pwned (HIBP) API steps in. The app checks if your password has shown up in any known breaches, without exposing your actual password. If it's compromised, you find out right away and can swap it out. That's a big step towards keeping your accounts safe from credential stuffing.

6. Phishing Detection Technologies

Phishing is always a threat. The Password Vault fights back in two ways:
Google Safe Browsing API checks website links against Google's massive threat list and blocks the bad ones.
If you're offline or Google isn't an option, a custom rule-based filter looks for sketchy domains using keywords and patterns linked to phishing.
Both keep you from saving or using passwords on fake websites.

7. SQLite Database

For local storage, SQLite does the job. It's fast, lightweight, and doesn't need a server running in the background. Pair it with encryption, and you've got a solid, secure place to stash sensitive credentials on your desktop.

8. Secure Key Management and Key Derivation Techniques

The Password Vault doesn't skimp on key security. It generates and manages encryption keys carefully, using key derivation to turn user input into strong cryptographic keys. Only authorized users can unlock and access what's stored.

9. Operating System and Deployment Environment

This app runs on pretty much anything Windows, Linux, macOS hanks to Python. It works as a standalone desktop program, so you don't need to be online all the time. That means you get privacy, reliability, and access, no matter where you are.

6. WORKFLOW

Here's how the password vault works, from the second you log in to the moment you leave. The whole thing is designed to keep your info locked down without slowing you down. You've got features like password search, a built-in generator, auto timeouts, lockouts after failed logins, and clear indicators showing how strong your passwords are. All of it's there to make things safer and simpler.

Step 1: Register and Log In

You start by making an account or signing in with your master password. When you register, the system locks away your master password using hashing and salting. When you log in, it checks your password against what's stored. Get your password wrong twice in a row and you're locked out for a minute just to keep out brute-force attacks.

Step 2: Key Generation

After you're in, the system creates encryption keys based on your master password using a key derivation function. These keys only exist in memory during your session they never sit around unprotected.

Step 3: Add Passwords and Check Strength

When you add a new password, you can type it in yourself or let the password generator handle it. The vault checks how long, complex, and varied your password is, and then tells you how strong it is so you know if you've picked a good one.

Step 4: Real-Time Strength Check

Every password whether you made it or the generator did goes through a strength check as you type. If the password's weak, you'll know right away and can fix it before saving.

Step 5: Breach Check

Right after the strength test, the system checks if your password has ever shown up in a data breach, but it does it privately. If your password's out there, you get an instant warning and a chance to pick something safer.

Step 6: Encrypt and Store

Once your password passes all the checks, the system encrypts it with strong algorithms and stores it in a local database. Even if someone gets into the database, all they'll see is a bunch of scrambled data.

Step 7: Search and Retrieve

If you need to find a password, you just search by service name or whatever tag you used. Pick the one you want and the vault decrypts it for you on the spot nothing gets exposed.

Step 8: Update or Delete

You're always in charge. If you want to update or delete a password, it's easy. For updates, the system runs through all the same checks again before saving.

Step 9: Auto Timeout

Forget to log out? No big deal. The vault shuts itself down after you've been inactive for a while, locking everything up so nobody else can get in.

Step 10: End Session

When you log out or the session times out, the system wipes all temporary data, keys, and sensitive info from memory. Nothing gets left behind.

In short, you get strong passwords, locked-down data, and a smooth ride from start to finish.

7. IMPLEMENTATION

Now comes the real work actually building the password vault. Here's where everything gets serious: secure logins, encrypted storage, password strength checks, and even breach detection all come together. The team goes with Python and its libraries for this job they're solid, secure, and honestly, pretty easy to work with. This section breaks down how each part of the vault takes shape and how we tie all these security features together for smooth, safe password management.

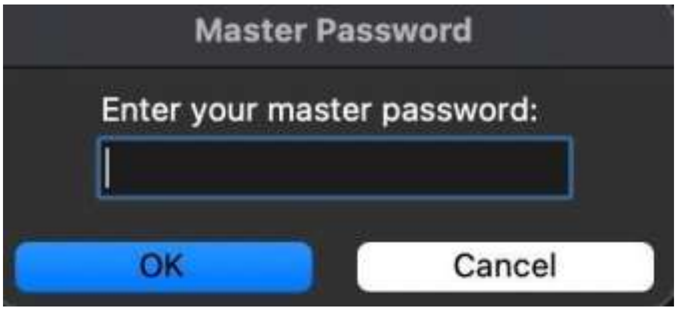
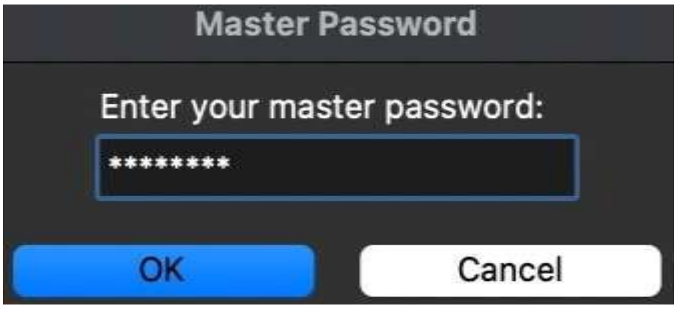


Fig 1 : Master Password Entry Screen

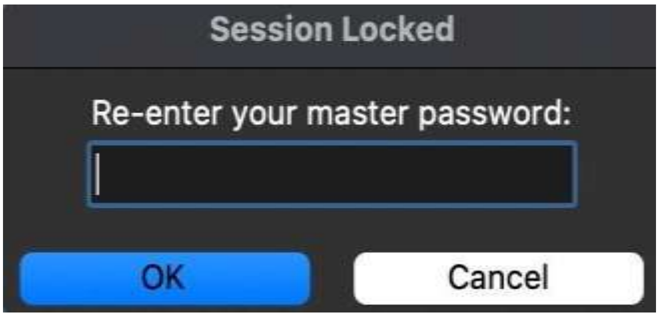
This image displays the interface where the master password is entered for user authentication. It asks the user to input their master password in order to gain access to the password vault, thereby maintaining secure access control.



****

Fig 2 : Master Password Authentication Interface

This image displays the master password authentication interface of the password vault system. It asks the user to input the master password, which is hidden to safeguard sensitive information. The entered password is securely checked before access is granted to the encrypted vault, ensuring that only authorized individuals can view stored credentials.

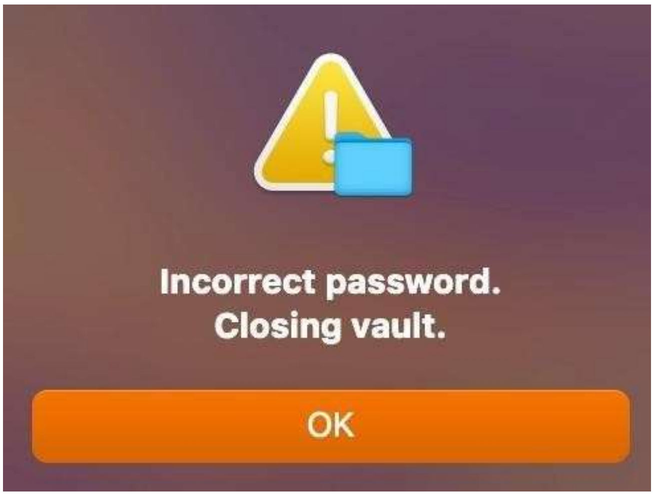


Session Locked

Re-enter your master password:

Fig 3 : Session Lock Authentication Interface

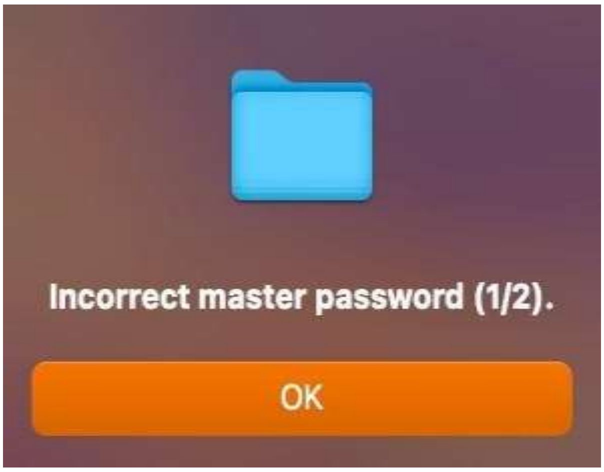
This image displays the session lock screen of the password vault system, where the user must input the master password again to restore access. It improves security by blocking unauthorized access following periods of inactivity or several unsuccessful login attempts.



Incorrect password.
Closing vault.

Fig 4 : Incorrect Master Password Alert

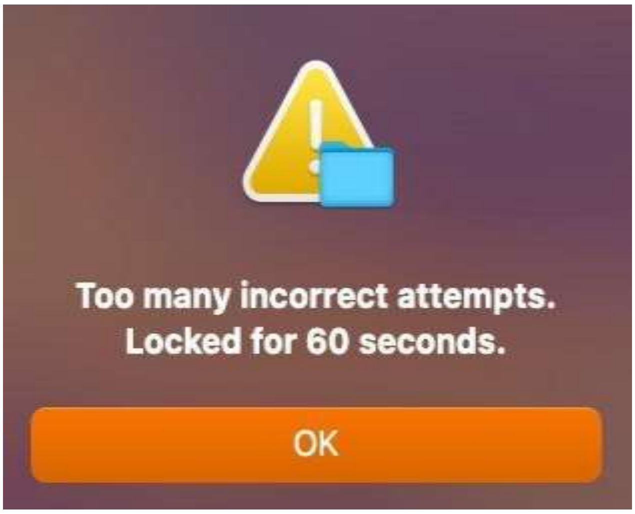
This image shows the warning message that appears when the wrong master password is entered. The system automatically closes the password vault to stop unauthorized access and improve security.



Incorrect master password (1/2).

Fig 5 : Failed Login Attempt Notification

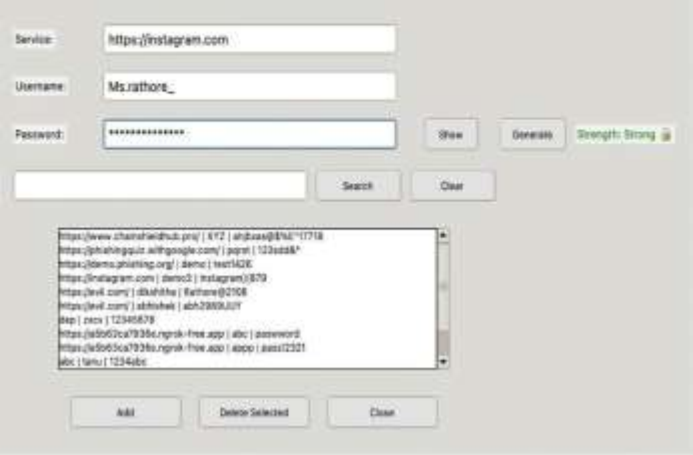
This image displays the alert that appears following an incorrect entry of the master password, showing how many failed attempts have been made. It supports security by restricting multiple unauthorized access tries.



Too many incorrect attempts.
Locked for 60 seconds.

Fig 6 : Account Lockout Warning Message

This image shows the lockout warning that appears following several failed attempts to enter the master password. To protect against brute-force attacks and improve security, the system briefly restricts access for one minute.



Service: https://instagram.com

Username: Ms.rathore_

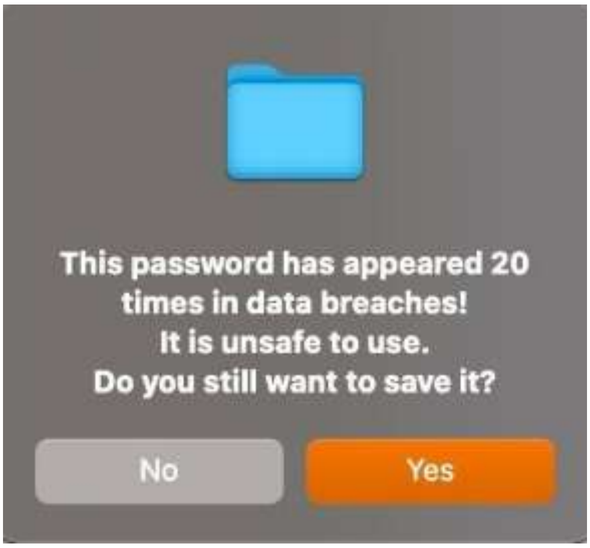
Password: ***************

Strength: Strong

https://www.chainsfieldhub.pro/ | XYZ | ahjbzas@$%^'17718
https://phishingquiz.withgoogle.com/ | pqrst | 123sdd&*
https://demo.phishing.org/ | demo | test1426
https://instagram.com | demo3 | instagram)(879
https://evil.com/ | dikshitha | Rathore@2108
https://evil.com/ | abhishek | abh2989JUY
dep | zxcv | 12345678
https://a5b63ca7936e.ngrok-free.app | abc | password
https://a5b63ca7936e.ngrok-free.app | appp | pass12321
abc | tanu | 1234abc

Fig 7 : Password vault Dashboard

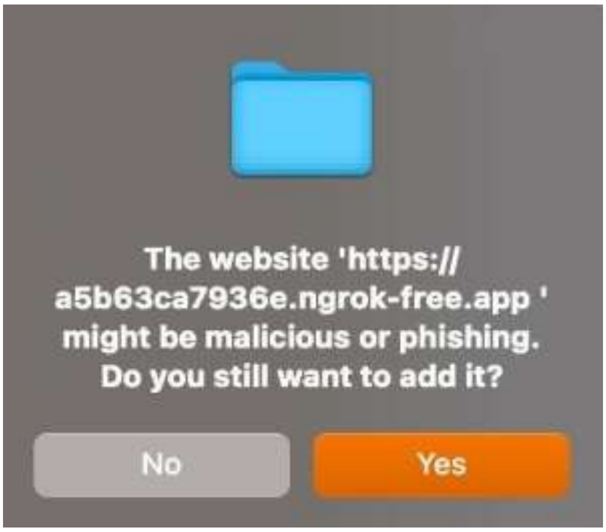
This image presents the primary password vault interface, allowing users to add, create, search for, and manage saved login information. It shows service details, hidden passwords, and a password strength meter, supporting secure and effective password management.



This password has appeared 20 times in data breaches!
It is unsafe to use.
Do you still want to save it?

Fig 8 : Password Breach Detection Warning

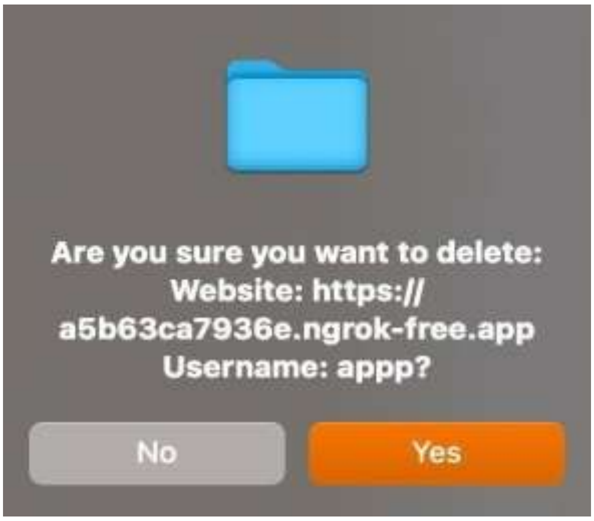
This image displays the alert that appears when a password is identified as part of a known data breach. It alerts the user to the security risk and asks them to make a choice before storing the affected password.



The website 'https://a5b63ca7936e.ngrok-free.app ' might be malicious or phishing. Do you still want to add it?

Fig 9 : Malicious Website Warning Alert

This image shows a security alert that appears when a website is recognized as possibly harmful or designed for phishing. It notifies the user and asks for confirmation before permitting the addition of login details, which improves overall safety.



Are you sure you want to delete:
Website: https://a5b63ca7936e.ngrok-free.app
Username: appp?

Fig 10 : Password Deletion Confirmation Dialog

This image displays the confirmation message that appears prior to deleting saved credentials. It helps prevent users from unintentionally removing significant password entries from the vault.

8. CONCLUSION

We built a secure, smart password vault because, honestly, dealing with passwords the old way just sucks. Everyone's got too many logins to remember, and that's how people end up reusing weak passwords or scribbling them on sticky notes. Our vault puts everything in one encrypted spot, so your credentials stay safe and you don't have to mess with clunky spreadsheets or risky shortcuts. It’s real protection that actually keeps hackers out.

But this vault isn’t just a simple lockbox. We packed it with strong cryptography—hashing, salting, encryption, secure key derivation, all of it. Your passwords stay private and untouched. The system checks how strong your passwords are and gives you a nudge if you’re slacking off. If any of your info shows up in a data breach, you get an alert right away. We thought about the little things too—locking accounts after too many failed attempts, closing the vault if you go idle, and actually deleting stuff when you hit delete. Breaking in? Good luck with that.

We also made sure it’s easy to use. The vault can whip up strong passwords for you, help you find your logins fast, and the interface just clicks. You don’t need a manual. We wanted something people would actually stick with, so it’s simple, not bloated, and works for both solo users and teams.

At the end of the day, this vault proves you don’t have to pick between tight security and real-world usability. You get encryption, smart password checks, breach alerts, and session controls all in one place. It helps people kick bad password habits and stop putting their info at risk. Down the line, we’re thinking about syncing across devices, adding multi-factor authentication, or even using biometrics. Security’s always changing, and we’re ready to keep up.

REFERENCES

1. Florencio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: Proceedings of the 16th International World Wide Web Conference (WWW). ACM Press (2007) 657–666
2. Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, Flagging, and Paranoia: Adoption Criteria in Password Selection. In: Proceedings of the Symposium on Usable Privacy and Security (SOUPS). ACM Press (2006) 1–12
3. Bonneau, J.: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: IEEE Symposium on Security and Privacy. IEEE Press (2012) 553–567
4. Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R.: Guess Again (and Again and Again): Measuring Password Guessability Empirically. In: IEEE Symposium on Security and Privacy. IEEE Press (2012) 523–537
5. Hunt, T., McMillan, C.: Protecting Passwords Using Breach Detection Techniques. IEEE Security & Privacy Magazine 17(3) (2019) 34–42
6. Wang, D., Zhang, Z., Chen, P.: A Comprehensive Study of Password Managers and Their Security. Computers & Security 87 (2019) 101–115
7. Li, X., Wang, Y., Sun, L.: Secure Password Vault Design Using Encrypted Storage and Key Derivation Functions. Journal of Information Security and Applications 41 (2018) 78–89
8. Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L.: Measuring Password Reuse and Synchronization between Users. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS). ACM Press (2014) 175–186
9. Ganesan, R., Shanmugapriya, D.: Secure Password Management Using Cryptographic Techniques. International Journal of Computer Applications 179(7) (2018) 25–30
10. Chiasson, S., van Oorschot, P.C., Biddle, R.: A Usability Study and Critique of Two Password Managers. In: Proceedings of the 15th USENIX Security Symposium. USENIX Association (2006) 1–16
11. Sommer, R., Paxson, V.: Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In: IEEE Symposium on Security and Privacy. IEEE Press (2010) 305–316
12. Kahn Academy Research Group: Best Practices for Secure Password Storage and Management. ACM Computing Surveys 52(4) (2019) 1–36
13. Bishop, M.: Computer Security: Art and Science. Addison-Wesley Professional, Boston (2003)
14. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
15. Green, M., Smith, M.: Cryptopals Crypto Challenges: Practical Cryptography for Developers. Journal of Cryptographic Engineering 8(2) (2018) 89–102
16. Kahn, A., Gupta, R.: A Survey on Password Authentication and Password Vault Systems. International Journal of Cyber Security and Digital Forensics 10(2) (2021) 45–56