Password manager

EERO KAINULAINEN

Password manager

- User is able to add, edit and remove credentials for sites
  - Accessed using a master password
  - User can copy stored passwords to clipboard, which is cleared after 30-second time window unless pasted
  - User can also import/export vaults
- User can also generate a random password with a length of their choosing
  - Min. 8 characters
- Implemented using Python
  - Most important libraries: cryptography, secrets
- UI is implemented using Tkinter
  - Quite basic → future improvement plans

Main secure programming methods

- The master password is hashed using PBKDF2-HMAC-SHA256 with 200,000 iterations
  - Keeps the passwords stored in the vault secure
- Salts, nonces and file restrictions are used to protect the vault from brute forcing
  - Nonce: number used once, a password won't look the same when encrypted twice using this
- 7/10 OWASP top 10 implemented
  - Others were not relevant to a local password manager
  - A02, A03, A04, A05, A06, A07, and A09 implemented

Known issues and future possibilities

- Memory dump can expose some stored values
- 30-second clipboard erasure is not guaranteed to stop other processes from accessing it
- The clipboard won't be erased if the user pastes the copied password within the 30-second timeframe

- In the future:
  - Logging access/modification attempts with timestamps
  - Backup/recovery options

Demo time!