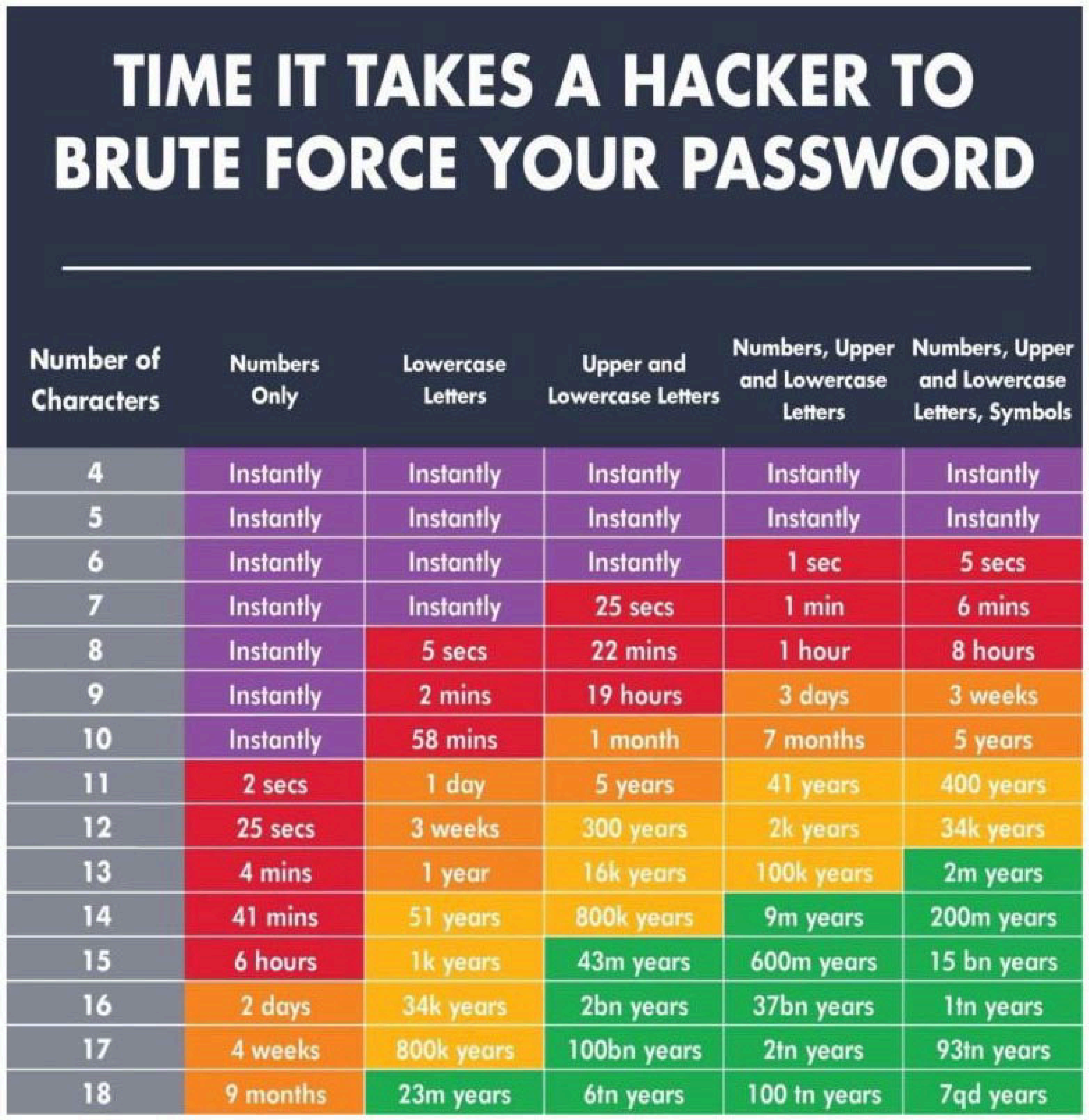
CS 482- Cybersecurity

Encryptonite: Built to Encrypt. Designed to Endure.

By Zahra Amini and Mollie McDonald

Quick Stats:

- 30% of internet users have experienced a data breach due to a weak password.
- Two-thirds of Americans use the same password across multiple accounts. A Google poll found that 1 in 8 US adults used the same password for every single one of their online accounts
- The most commonly used password is “123456.”
- 59% of US adults use birthdays or names in their passwords.
- Approximately one million passwords are compromised each week.
- Brute-force hacking attempts, where hackers try various combinations of characters, happen every 39 seconds.
- Poor passwords contribute to 81% of corporate data breaches
- 70% of weak passwords can be cracked in less than one second using brute-force attacks
- Password reuse creates a domino effect, where compromising one account can lead to multiple accounts being compromised

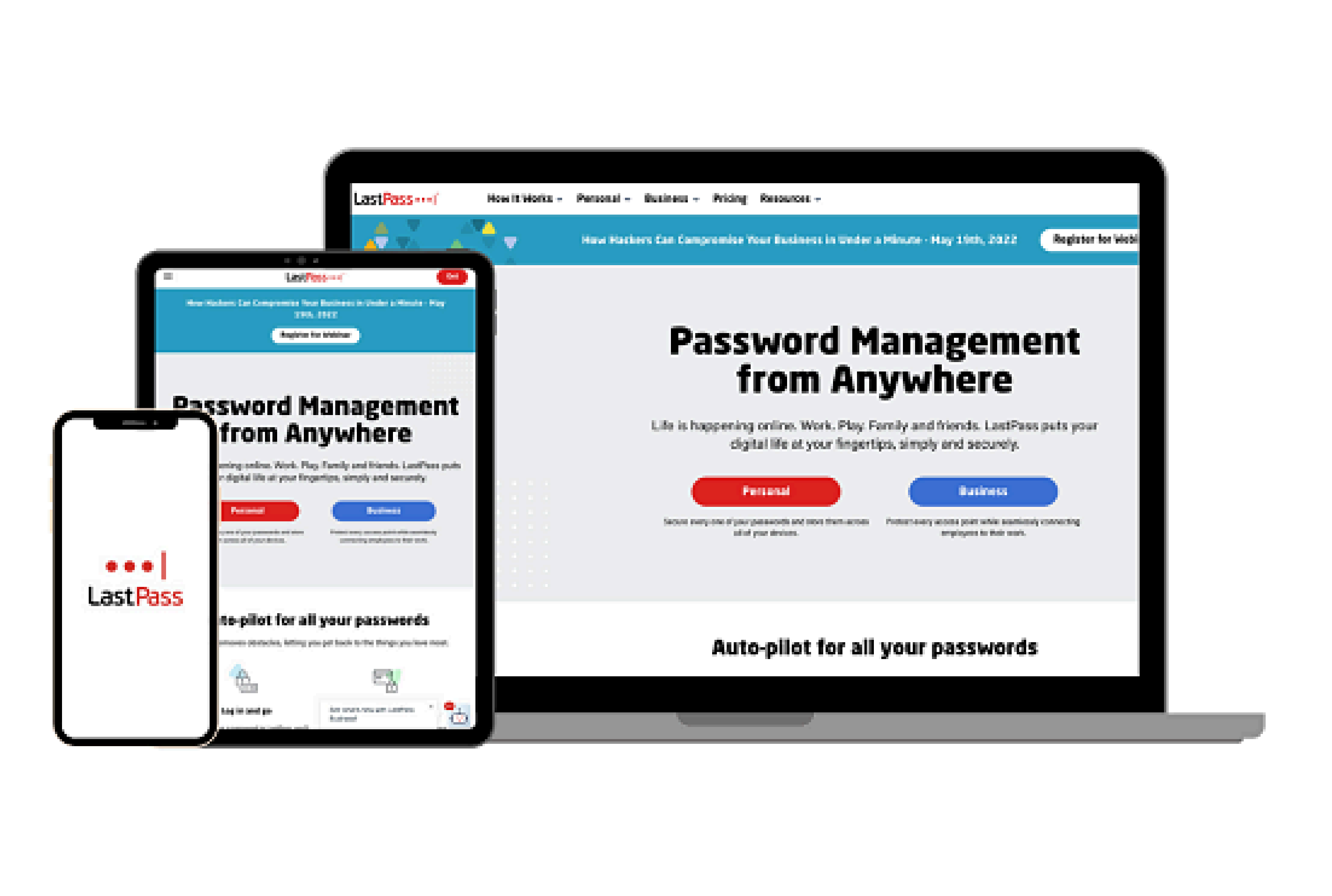


TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Intro:

- In December 2022, LastPass, America's most popular password management tool experienced a data breach. A single compromised credential caused exposure of its development environment to unauthorized actors.
- The breach affected 30 million users
- These stolen passwords are bought, sold, and later used in credential-stuffing attacks. Stolen credentials account for 80% of password-hacking incidents
- In 2019, 27% of hackers tried to guess other people's passwords, and 17% made accurate guesses.
- Multi-factor authentication can stop 96% of bulk phishing attacks and 76% of targeted attacks


LastPass
How Hackers Can Compromise Your Business in Under a Minute - May 19th, 2022
Password Management from Anywhere
Life is happening online. Work. Play. Family and friends. LastPass puts your digital life at your fingertips, simply and securely.
Personal
Business
Auto-pilot for all your passwords

Project Deliverables

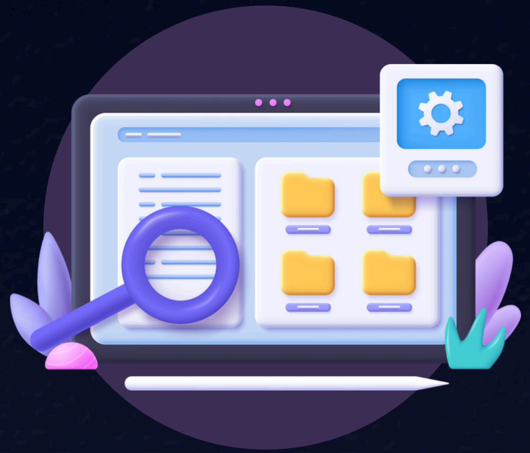
Passwork Checker

Checks password strength and gives feedback based on length, complexity, and rating of poor, fair, moderate, and strong.

Strong Password: pR!Xg78@FnA9o%!

Password Generator

Generates password based on length, captitilization, numbericals, special characters/symbols that you input.



Password Vault

Stores passwords in an SQLite database for easy retrieval.

Password Encryption

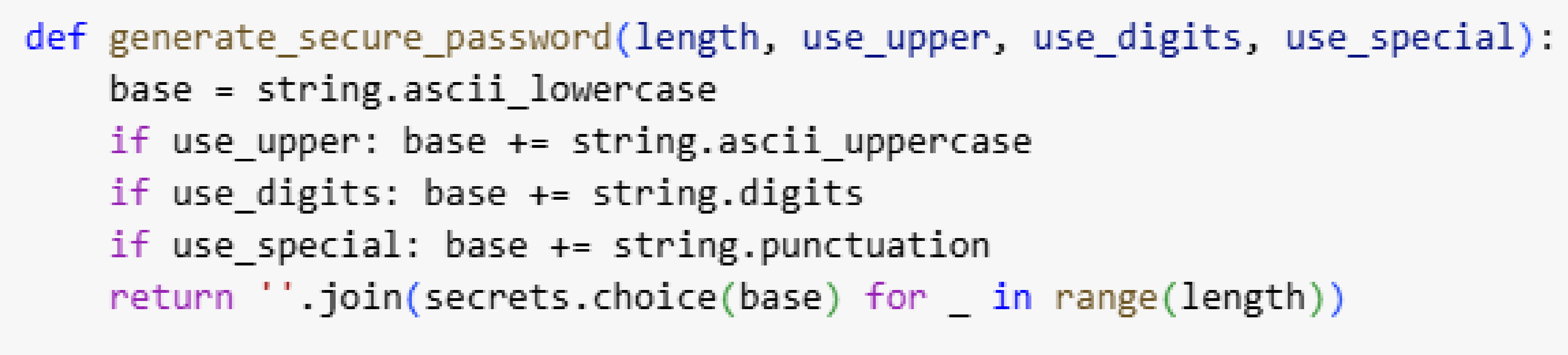
Encrypts and decrypts passwords using AES for secure storage.

Password Checker:

- Requirements:
  - At least 12 characters
  - Includes a capital letter
  - Includes a lowercase letter
  - Includes a number
  - Includes a special character
- Password ratings:
  - Weak
  - Moderate
  - Strong

Password Generator:

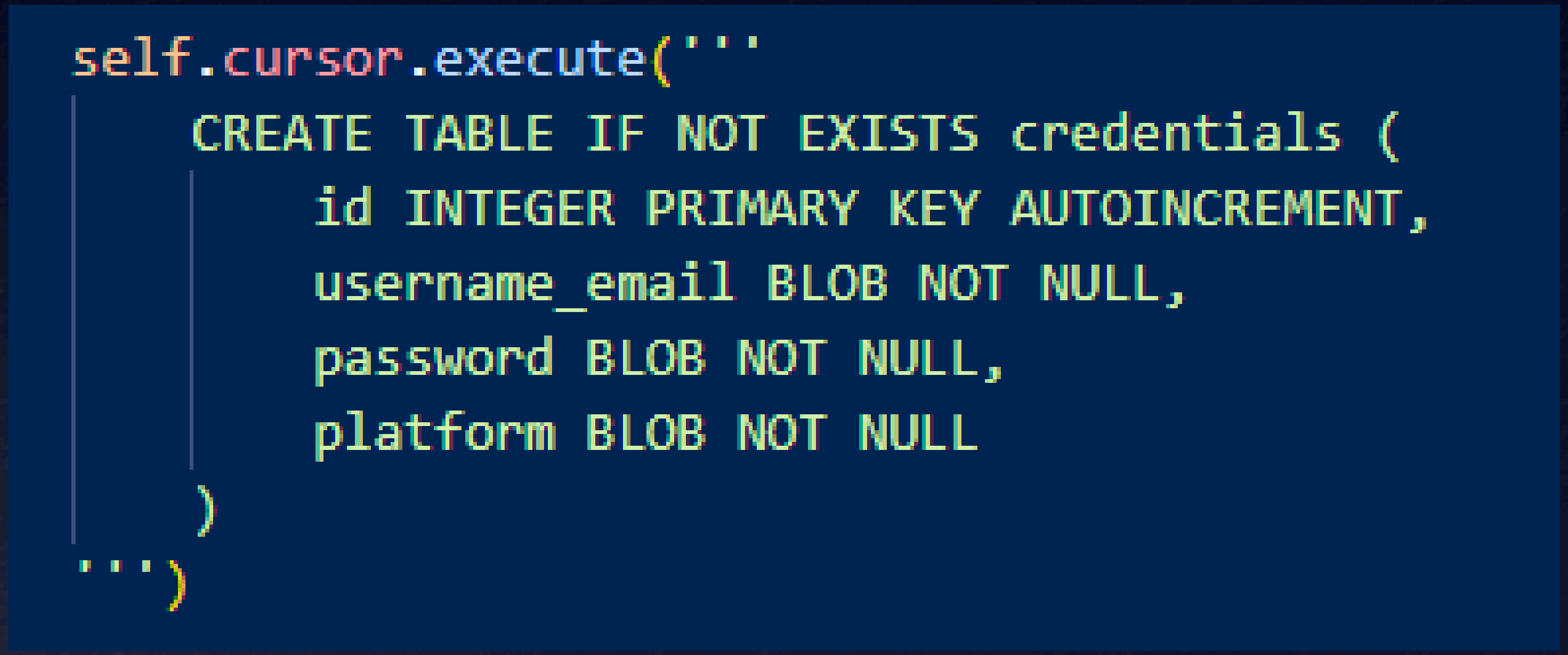
- Creates a random secure password
  - Length chosen by user, must be at least 8
  - User can choose whether to include special characters
  - Contains uppercase and lowercase letters, numbers



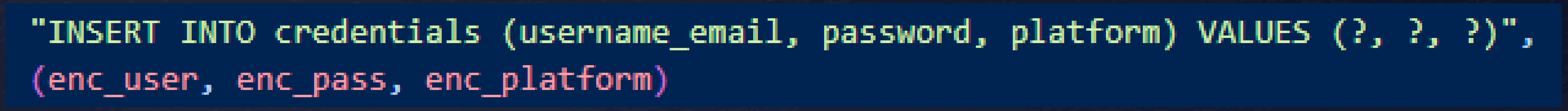
```python
def generate_secure_password(length, use_upper, use_digits, use_special):
    base = string.ascii_lowercase
    if use_upper: base += string.ascii_uppercase
    if use_digits: base += string.digits
    if use_special: base += string.punctuation
    return ''.join(secrets.choice(base) for _ in range(length))
```

Password Vault:

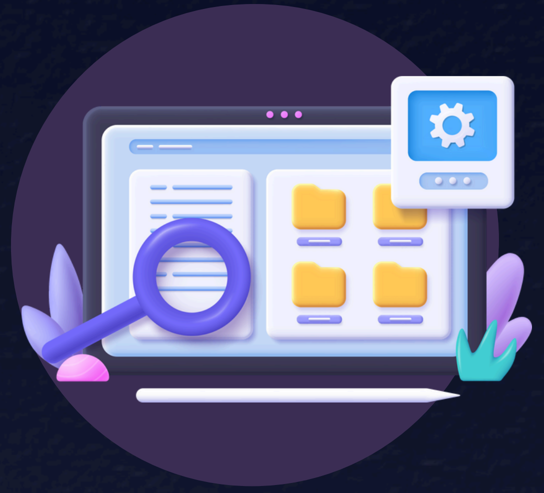
- Stores passwords in an SQLite Database
  - Columns: id, platform, username, password
- User can retrieve full password list, or search based on platform name



```
self.cursor.execute('''
    CREATE TABLE IF NOT EXISTS credentials (
        id INTEGER PRIMARY KEY AUTOINCREMENT,
        username_email BLOB NOT NULL,
        password BLOB NOT NULL,
        platform BLOB NOT NULL
    )
''')
```



```
"INSERT INTO credentials (username_email, password, platform) VALUES (?, ?, ?)",
(enc_user, enc_pass, enc_platform)
```



Encryption:

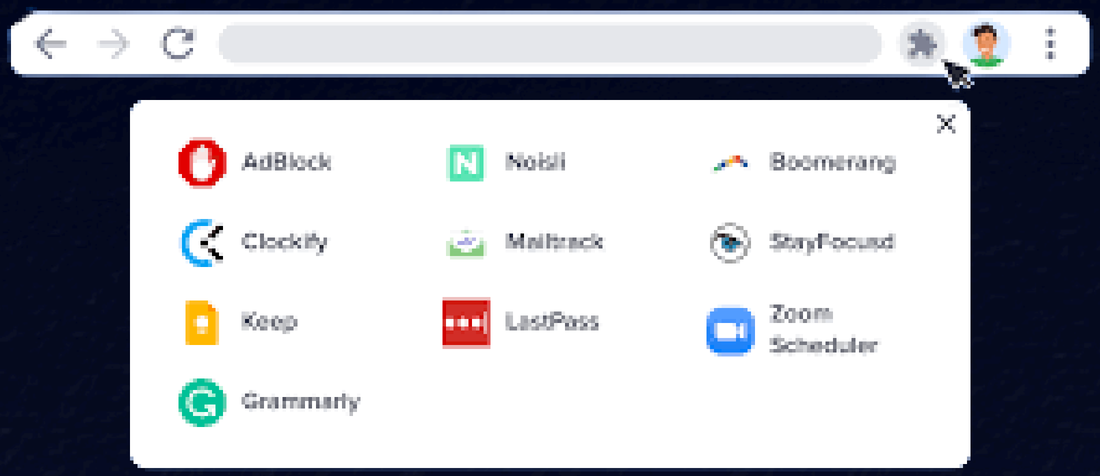
- Pycryptodome library
  - Crypto.Cipher
  - Crypto.Util
  - Crypto.Protocol
- AES Encryption/Decryption
- SHA-256 Hash Algorithm
- scrypt
  - created by Colin Percival, described in the paper “Stronger key derivation via sequential memory-hard functions”
  - derives key from a password
  - Computationally expensive and memory intensive, therefore more secure against attacks using custom hardware

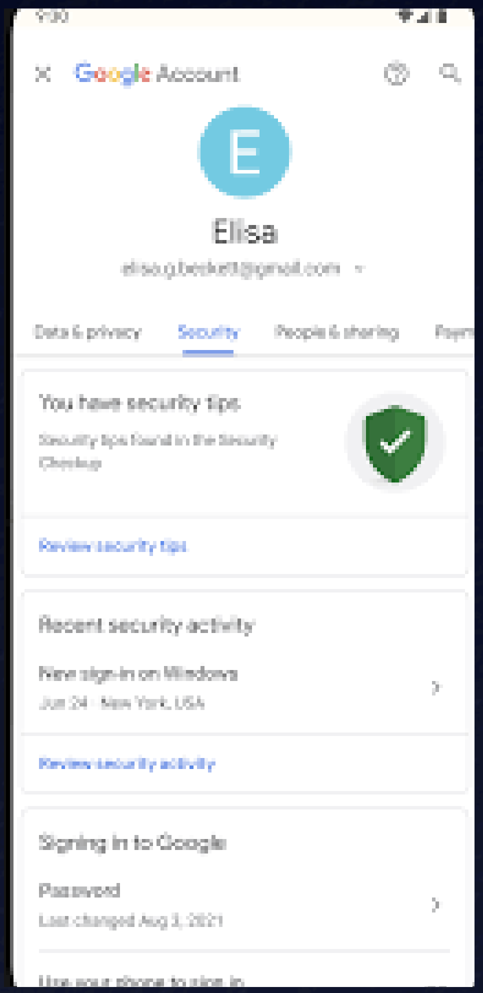
Additional Features

- Main password for access
  - Requires upper/lowercase letter, special character, number
  - At least 8 characters
  - 3 attempts
- 2-factor authentication
  - requires app such as Microsoft or Google Authenticator
- Erase/backup database
- Tkinter UI for usability

Future Work:

- More 2-step verification options
- Account recovery (reset password)
- Breach alerts
- Browser extention
- Cloud sync/multi-device access
- Biometric access





Elisa

elisa.g.beckett@gmail.com

You have security tips

Security tips found in the Security Checkup

Review security tips

Recent security activity

New sign-in on Windows

Jun 24 · New York, USA

Review security activity

Signing in to Google

Password

Last changed Aug 3, 2021

Use your phone to sign in

Conclusion:

What We Built

- Password Strength Checker – Validates input against entropy-based rules
- Secure Password Generator – User-driven, randomized, compliant passwords
- Encrypted Vault – AES-secured local database with SHA-256 + scrypt
- User Access Layer – Master password + 2FA + Tkinter UI

Class Concepts Applied in Practice

- Cryptography: AES encryption, hashing, memory-hard key derivation
- Software Architecture: Modular design with secure abstraction layers
- Data Management: Encrypted SQLite integration with CRUD operations
- Human-Centered Security: Usability meets best practices in auth design

REFERENCES:

- Palatty, N. J. (2025, February 6). 30+ Password statistics you need to know in 2025. Astra Security. https://www.getastra.com/blog/security-audit/password-statistics/
- Percival, C. (2009, January). Stronger key derivation via sequential memory-hard ... https://www.tarsnap.com/scrypt/scrypt.pdf
- Howarth, J. (2024, October 31). 50+ Password statistics: The state of password security in 2024. Exploding Topics. https://explodingtopics.com/blog/password-stats#mfa-and-passwordless-security-statistics
- Knutsson, K. (2025, May 24). 19 billion passwords have leaked online: How to protect yourself. Fox News. https://www.foxnews.com/tech/19-billion-passwords-have-leaked-online-how-protect-yourself
- Cybernews. (2025, May 7). Major password breach sees over 19 million leaked – here's how to check if yours is compromised. New York Post. https://nypost.com/2025/05/07/tech/major-password-breach-sees-over-19-million-leaked/
- Bitwarden. (2025). The State of Password Security 2025 Report. Bitwarden. https://bitwarden.com/resources/the-state-of-password-security/
- Scoop Market. (2025). Multi-factor authentication statistics. https://scoop.market.us/multi-factor-authentication-statistics/?utm_source=chatgpt.com
- The Business Research Company. (2023, April 13). Multi factor authentication market size, share, revenue, trends and drivers for 2023–2032. https://www.thebusinessresearchcompany.com/report/multi-factor-authentication-global-market-report?utm_source=chatgpt.com

Thank You!