EXP:- 02

Date:- 21/01/2025

ROLLNO:- A009

Aim:- Implementing authentication using any library

What is authentication?
Authentication is the process of verifying the identity of a user, device, or system to ensure that they are who they claim to be. It typically involves checking credentials, such as password, fingerprint or security token, to confirm that the user has permission to access specific resources or services.

* Types Of Authentication:-

1) Password-Based Authentication :
The user is required to provide a password to gain access to an account or system. it's the most common and basic method.

Example:- Logging into a website using a username and password

2] Multi-Factor Authentication (MFA):
MFA requires the user to provide two or more different factors to verify identity. These factors typically include something you know (password) something you have (phone or token) and something you are (biometric data).

Example:- A user entering a password and then receiving a one-time-code on their phone.

3] Two-Factor Authentication (2FA):-
MFA requires the user to provide two or more different factors to verify identity. these factors typically include something you know, combining a password with something else (like a code sent via sms, an app or email)

Example:- Logging into a Google account with a password and a one-time code sent to your phone.

4) Biometric Authentication:- This types uses unique physical characteristics for identification such as fingerprints, Facial recognition, voice recognition or retina scans.

Example:- Unlocking a smartphone using fingerprint scanning or facial recognition.

5] Token-Based Authentication:-
Involves generating a token, that grants access to a system or service. Tokens can be short-lived or revoked when no longer needed.

Example:- Using an OAuth token to authenticate a user with a third-party service.

6) Smart Card Authentication:-
Uses a physical smart card that contains embedded credentials or cryptographic keys to verify the user's identity. Often used in corporate environments for secure access.

Example:- Employess using an ID badge with an embedded chip to access restricted areas.

7) Certificate-Based Authentication:-
Relies on digital certificates to authenticate users or devices. This method ensures that both parties can trust the other's identity.

Example:- Websites using SSL/TLS certificates to authenticates to their identity to users and ensure secure connections.

* Readline Sync :- It refers to using synchronous input mechanism in program often seen in command-line tools or scripts. while convenient for interactive user input it can pose security risk.

1) BufferFlow
ii) Input validation Issue
iii) keylogging Risk
iv) Dos Attacks
v) Sanitizing input and avoiding sensitive data exposure, mitigate these risk.

* Bcrypt :- is a password-hashing tool used to securely store passwords. Instead of saving plain passwords, it converts them into a scrambled format using an algorithm Even if someone steals the database, the hashed passwords are hard to crack.

1) Hashing
2) salt
3) slow by design

* Flask :- is a lightweight and simple web framework for python. It helps developers Create web-applications quickly and easily.

Key Features:-

I) Lightweight
II) Flexible
III) Built-in-tools
IV) Extensible

9 Werkzeug security :- It refers to the security utilities provided by Werkzeug, a WSGI, library commonly used with Flask. It includes tools to handle tasks like password hashing and managing cryptographic operations securely.

Key Features:-

I) Password Hashing
II) Request validation
III) Cryptographic helpers

Developers can build web applications with robust protection against common vulnerabilities like insecure password storage and replay attacks.

Conclusion :- Hence, we learned how to do authentication using any library.