SUPERVVISOR: AHMED HANIF

NARWAL AUTH API DELIVERABLE 1: STRENGTHS

MUHAMMAD NASEEM
SAMI NAEEM
HASSAAN FAROOQ

1) Protection and Security:
    - Server doesn't store password or hash, only public key Y
    - Each authentication attempt is unique
    - Protects against malicious servers misusing passwords.
    - Hard to attack due to randomized challenges
    - Immune to Man in the middle attacks
    - Protection against Phishing: As the actual password isn’t transmitted, phishing attacks are less effective
    - Immunity to Password Database Breaches
    - Cross-Site Password Reuse Mitigation: Even if a user reuses passwords across sites, the unique public keys generated for each site protect against cross-site vulnerabilities.
2) Scalability:
    - Reduced Server-Side Computational Load, As the majority of the cryptographic computations are performed on the client-slide, hence reducing the server load,
    - No Need for Secure Password Storage Techniques, As the server doesn’t need to implement complex password security strategies.
    - Facilitates Multi-Factor Authentication, As system can be easily extended to incorporate additional authentication factors.
    - Zero-Knowledge allows for easy auditing of the authentication process without exposing the sensitive information
    - Future-Proofing: The mathematical basis of the system (discrete logarithm problem) is believed to be resistant even to quantum computing attacks, providing some level of future-proofing.
3) Policy Compliance:
    - It compliance with privacy regulations, since it doesn’t store the user passwords
    - Narwal auth API is in-line with the regulations of a lot – if not all – of the security and protection standards and policies.