Logical and Security testing task

## SQL Injection Vulnerability

Description: The code concatenates user inputs directly into SQL queries without proper parameterization. This is present in both the client\_registration and client\_login functions.

Impact: An attacker could manipulate the input to execute arbitrary SQL commands, potentially leading to data leakage or complete database compromise

Risk Score: 9.5 (Critical)

## Weak Password Storage

Description: The application stores user passwords in plain text without hashing

Impact: If the database is compromised, all user passwords would be exposed.

Risk Score: 8.0 (High)

## JWT Secret Exposure

Description: The JWT secret key is hardcoded as plain string

Impact: If the source code is exposed, attackers can easily guess and retrieve the secret key. Allowing them to forge valid JWT tokens

Risk Score: 7.5 (High)

## Improper JWT Decoding

Description: The decodeNoneJwt function decodes the JWT without verifying the signatures

Impact: An attacker can forge a valid JWT without a valid signature

Risk Score: 9.0 (Critical)

## Lack of Input Validation

Description: The application does not validate the format of the phone number, email, username during registration and login

Impact: This could lead to unexpected behavior or allow attackers to exploit the system with malformed input

Risk Score: 5.0 (Medium)

## Error Handling and Information Leakage

Description: The application returns generic error messages that do not provided specific feedback on which input was incorrect

Impact: This could lead to bad user experience and does not provide information for users to correct their mistakes

Risk Score: 4.0 (Medium)

## Inadequate Rate Limiting and Lockout Mechanism

Description: There is no mechanism to limit the number of login attempts or to lock accounts after multiple failed attempt

Impact: This could lead to brute-force attacks where an attacker could guess user credentials without restriction

Risk Score: 7.0 (High)

## Potential for Cross-Site Scription (XSS)

Description: User Inputs are not sanitized before being used in the application

Impact: If these inputs are reflected back to the user without sanitization it could lead to XSS attacks

Risk Score: 6.0 (Medium)

## Missing Password Complexity Check

Description: The client\_registration endpoint does not enforce any password complexity requirements

Impact: Weak passwords can easily be guessed or hackers

Risk Score: 6.0 (Medium)