Security Assessment:

# Assessment date: 03/08/24

# Results

Success: Attack did not work (Good)

Fail: Attack did work (Bad)

# SQL Injections:

| Route | Field | Queries Used | Result |
| --- | --- | --- | --- |
| users/register | Username | “ or “”=”  \” or \”\”=\”  ‘ or ‘’=’  \’ or \’\’=\’  test‘);Drop TABLE User; -- | Success  Success  Success  Success  Success |
| users/login | Email | “ or “”=”  \” or \”\”=\”  ‘ or ‘’=’  \’ or \’\’=\’  test‘);Drop TABLE User; -- | Success  Success  Success  Success  Success |
| challenge/add | Query | “ or “”=”  \” or \”\”=\”  ‘ or ‘’=’  \’ or \’\’=\’  test‘);Drop TABLE User; -- | Success  Success  Success  Success  Success |
| challenge/:id | param | “ or “”=”  \” or \”\”=\”  ‘ or ‘’=’  \’ or \’\’=\’  test‘);Drop TABLE User; -- | Success  Success  Success  Success  Success |

## Status: Passed

# Packet capture:

Encryption has not been applied to the system, so it is vulnerable to packet sniffing.

Example of captured packet:  
A computer code on a white background

Description automatically generated

## Security Impact:

* Account hijacking
* Unauthorized account creation

## Remediation:

* Enable https encryption

## Status: Not implemented

# Directory Traversal

| Methods used | Result |
| --- | --- |
| ../ | Success |
| %2E%2E%2F | Success |
| %2E%2E/ | Success |

## Status: Passed

# XSS

| Location | Query | Result |
| --- | --- | --- |
| First name injected on dashboard page | <script>alert(‘xss’)</script> | Success |

## Status: Passed

# Vulnerable Dependencies:

| Package name | Vulnerability | CVSS | Severity to Project |
| --- | --- | --- | --- |
| Frontend/Semver | REGEX DOS | 7.5 (High) | Low |

## Status: Needs attention