| **ID** | **Description** | **Impact** | **Risk Score** |
| --- | --- | --- | --- |

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | Passwords are stored in plain text in the database. | High (Data exposure) | 8/10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **2** | No email validation during registration (invalid email format allowed). | Medium | 6/10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **3** | Duplicate usernames can be registered without any restriction. | Medium | 6/10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **4** | Username-only login is allowed without a password. | High (Unauthorized) | 8/10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | No password validation (weak passwords like "a" are accepted). | Medium | 5/10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **6** | Register endpoint returns 200 OK even for incomplete data (Invalid Data). | Low (Incorrect status) | 4/10 |

|  |  |  |  |
| --- | --- | --- | --- |
| **7** | Login returns correct error message for incorrect credentials, but 200 OK. | Low (Incorrect status) | 4/10 |