**SHAIR Defect Report**

* **Defect ID**: 0006
* **Summary**: Database information is leaked in the API response in case of exceptions
* **Defect Type:** Security
* **Priority**: Medium
* **Severity**: Critical
* **Defect Complexity**: Medium
* **Description**:

User cannot create new notes if the input data entered for the notes is lengthy (more than 255 characters). The backend API fails with Sql exception.

* **Pre-Requisites:**

1. Some notes should be created in the in the application already
2. At-least one of the notes should have ‘test’ keyword within it
3. Open the browser’s Dev Tools and navigate to the Network tab to check the APIs triggered during UI operations

* **Steps To Reproduce**:

1. Open a web-browser
2. Launch URL <https://master.hiring-assignment.qa.c66.me/login>
3. Login into the application using valid username & password
4. Navigate to Profile tab
5. In the Note Content text area, enter a length string with more than 255 characters
6. Click on Submit button
7. In the browser Dev tools, check the API with name ‘note’

* **Expected Results**:

1. The API response should indicate the reason of the failure ,however, without sharing any technical details of the backend database

* **Actual Results**:

1. The API fails with 500 exception because its unable to handle more than 255 characters sent in request.
2. The API response shows all vital information about the database e.g. Table name and its column names

\*\*(Please refer the ‘Additional Information’ section shared below)

* **Reported By**: Priyanka
* **Reported On**: 9th Nov 2022
* **Assigned To**: <Developer1>
* **Current Status**: Open
* **Environment**: Test
* **Build Version**: <Not Available>
* **OS:** Windows 10
* **Browser:** Chrome v107.x.x
* **Additional Information:**

The backend is not functioning correctly

Request URL :

Post : https://master.hiring-assignment.qa.c66.me:3001/v3/note

Request Payload :

{"userId":"4601760c-a44f-45d5-9593-28944875f17d","text":"If you want to create robust, browser-based regression automation suites and tests, scale and distribute scripts across many environments, then you want to use Selenium WebDriver, a collection of language specific bindings to drive a browser the way it is done by"}

Response : 500

{"name":"QueryFailedError","message":"Data too long for column 'text' at row 1","query**":"INSERT INTO `note`(`id`, `text`, `createdAt`, `updatedAt`, `userId`)** VALUES (?, ?, DEFAULT, DEFAULT, ?)","parameters":["93f5d9d8-138f-4997-bc01-cf1f14a71128","If you want to create robust, browser-based regression automation suites and tests, scale and distribute scripts across many environments, then you want to use Selenium WebDriver, a collection of language specific bindings to drive a browser the way it is done by","4601760c-a44f-45d5-9593-28944875f17d"],"driverError":{"code":"ER\_DATA\_TOO\_LONG","errno":1406,"sqlState":"22001","sqlMessage":"Data too long for column 'text' at row 1","sql":"INSERT INTO `note`(`id`, `text`, `createdAt`, `updatedAt`, `userId`) VALUES ('93f5d9d8-138f-4997-bc01-cf1f14a71128', 'If you want to create robust, browser-based regression automation suites and tests, scale and distribute scripts across many environments, then you want to use Selenium WebDriver, a collection of language specific bindings to drive a browser the way it is done by', DEFAULT, DEFAULT, '4601760c-a44f-45d5-9593-28944875f17d')"},"code":"ER\_DATA\_TOO\_LONG","errno":1406,"sqlState":"22001","sqlMessage":"Data too long for column 'text' at row 1","sql":"INSERT INTO `note`(`id`, `text`, `createdAt`, `updatedAt`, `userId`) VALUES ('93f5d9d8-138f-4997-bc01-cf1f14a71128', 'If you want to create robust, browser-based regression automation suites and tests, scale and distribute scripts across many environments, then you want to use Selenium WebDriver, a collection of language specific bindings to drive a browser the way it is done by', DEFAULT, DEFAULT, '4601760c-a44f-45d5-9593-28944875f17d')"}

**Screenshot :**

Note api failing

