Task 1:

A screenshot of a computer

Description automatically generated

Task 2.1 b:

To retrieve Alice's record from the web page using a SQL injection attack, one could exploit the vulnerability in the authentication process by manipulating the input fields to inject malicious SQL code. Since we know Alice's birthday is 9/20 and that the SQL query likely includes a clause for querying by the 'birth' field, we can input a payload that alters the query to retrieve Alice's record. For instance, by inputting a payload in the Employee ID field like ' OR birth='9/20' -- and any value in the Password field, we can manipulate the query to check if the birth date matches '9/20', thus retrieving Alice's record. Upon executing this injection attack and capturing the results, we would demonstrate the successful exploitation of the SQL injection vulnerability to retrieve Alice's record without requiring her ID or password. This underscores the importance of robust input validation and SQL query parameterization to mitigate such vulnerabilities in web applications.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Task 2.2 b:

Step 1: Craft the SQL Injection Payload

1. We want to retrieve Alice's information based on her birthday, which is 9/20.
2. We'll inject a condition into the SQL query to match Alice's birthday.

Step 2: Craft the Curl Command

curl 'www.SEEDLabSQLInjection.com/unsafe\_credential.php?eid=10000' --data-raw 'password=%27%20OR%20birth=%279/20%27%20--'

1. Construct a curl command with the appropriate URL and parameters, including the SQL injection payload.
2. Include Alice's Employee ID in the URL.
3. Use the --data-raw flag to specify the payload for the POST request.
4. Inject a condition OR birth='9/20' to match Alice's birthday in the payload.
5. Encode special characters like single quotes (') using URL encoding.

Step 3: Execute the Curl Command

Run the curl command to send the request to the web application.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Task 3.1 b:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Task 3.2: