SQL Injection Challenge – Step-by-Step Guide (Up to Flag Submission)

> **Scope**: This document contains **only the step guide from attacker perspective** for a basic SQL Injection login-bypass challenge, ending at **flag discovery and submission**. Intended for **authorized labs / CTFs only**.

Step 1: Open the Challenge Page

- Navigate to the provided challenge URL
- Identify a **login form** with:
- `username`
- `password`

Step 2: Confirm Injection Point

Input Test: - Username: `'` - Password: `'`

Expected Result: - SQL error message OR abnormal response (blank page / crash / redirect)

➡️Confirms the input is directly used in an SQL query.

Step 3: Determine Attack Objective

- Goal: **Bypass authentication**
- Assumption: Backend query follows this pattern:

```
SELECT * FROM users WHERE username = '<input>' AND password = '<input>';
```

Step 4: Craft the Injection Payload

Use an always-true condition with a comment:

```
' OR '1'='1' --
```

Payload logic: - Closes the username string - Forces TRUE condition - Comments out password validation

Step 5: Execute the Injection

Enter the payload:

Field	Value
Username	`' OR '1'='1' --`
Password	anything

Click **Login / Submit**.

Step 6: Verify Successful Bypass

Success indicators: - Redirect to dashboard / profile page - Access to restricted content - Session cookie created

➡️Authentication bypass confirmed.

Step 7: Locate the Flag

After login, attacker checks: - Dashboard page - Profile page - Admin panel - Hidden message banner

Typical flag formats: - `FLAG{...}` - `CTF{...}` - `flag: ...`

Step 8: Capture the Flag

Example:

```
FLAG{sql_injection_login_bypass}
```

Copy the full flag **exactly as shown**.

Step 9: Submit the Flag

- Return to the challenge platform
- Paste the flag into the **flag submission field**
- Click **Submit / Check**

Step 10: Challenge Completed

- Platform confirms correct flag
- Challenge marked as **Solved**
- Points awarded

End of Step Guide (Up to Flag Submission)

⚠️This guide is for **legal, educational security labs only**.