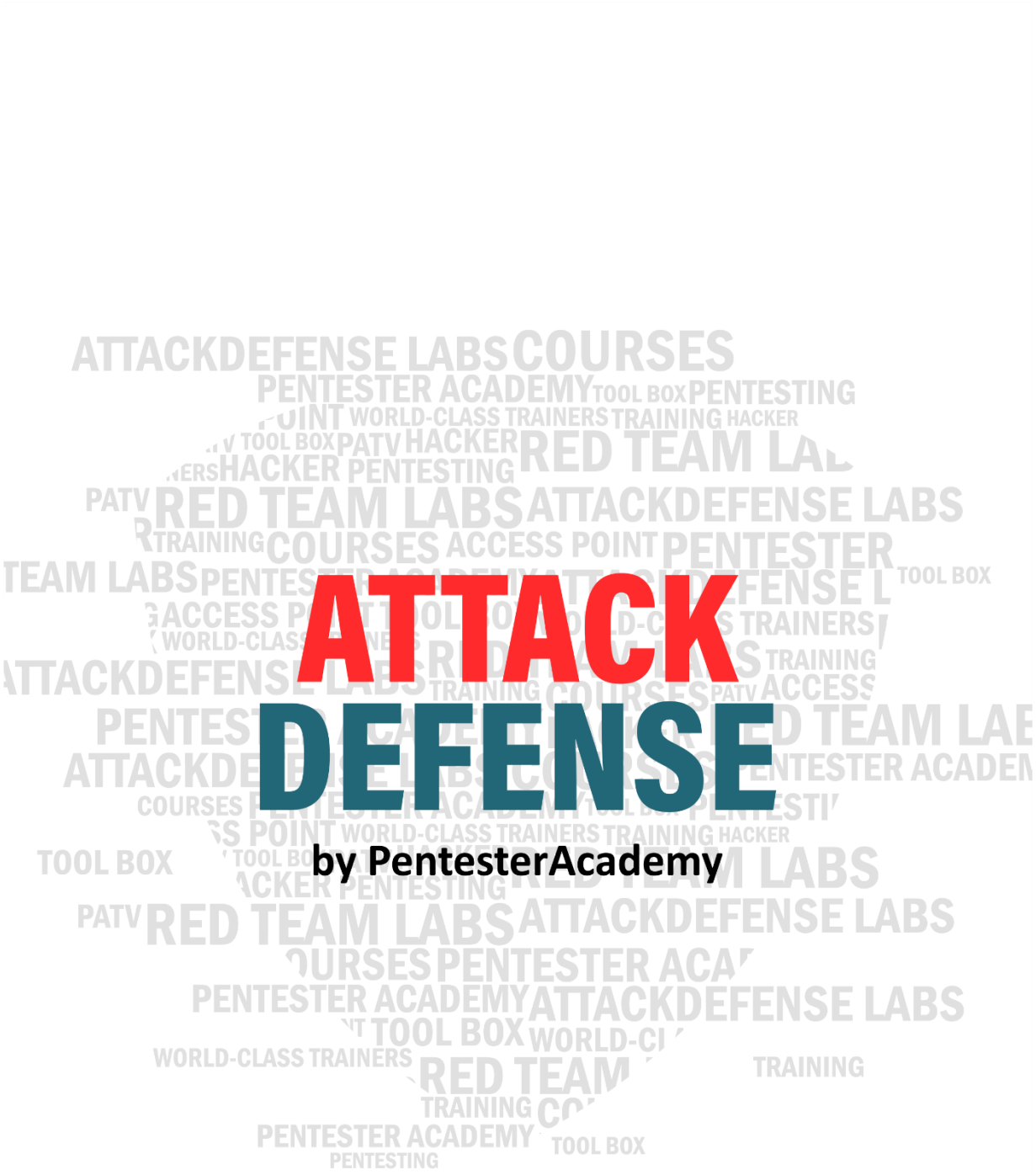

ATTACK
DEFENSE
by PentesterAcademy

Name	DynamoDB : SQL Injection
URL	https://attackdefense.com/challengedetails?cid=2292
Type	AWS Cloud Security : Databases

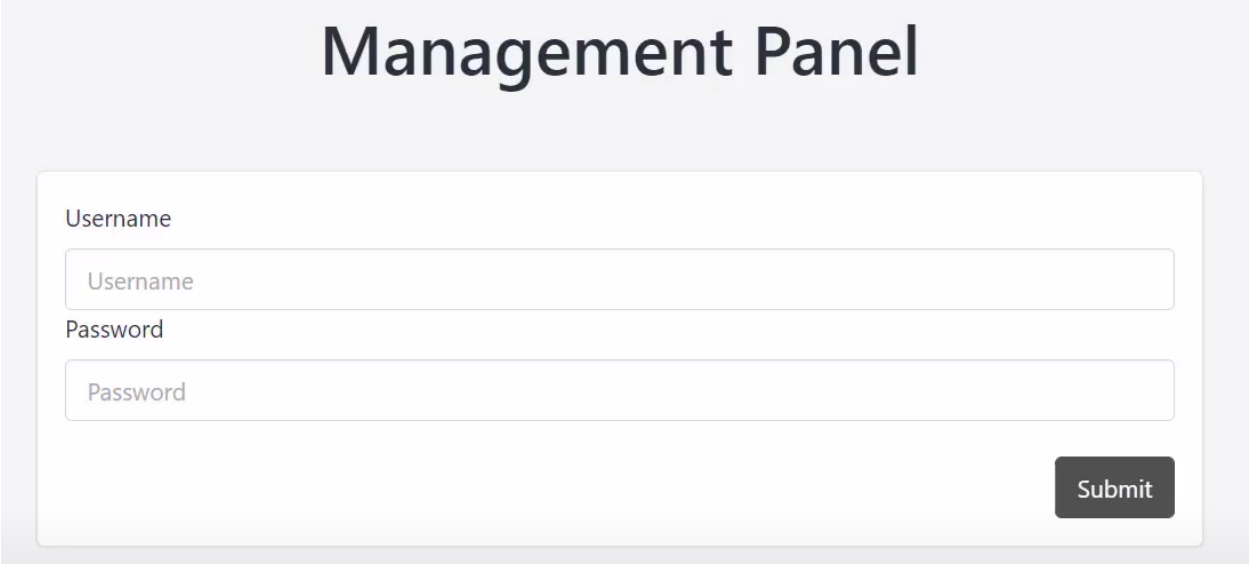
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

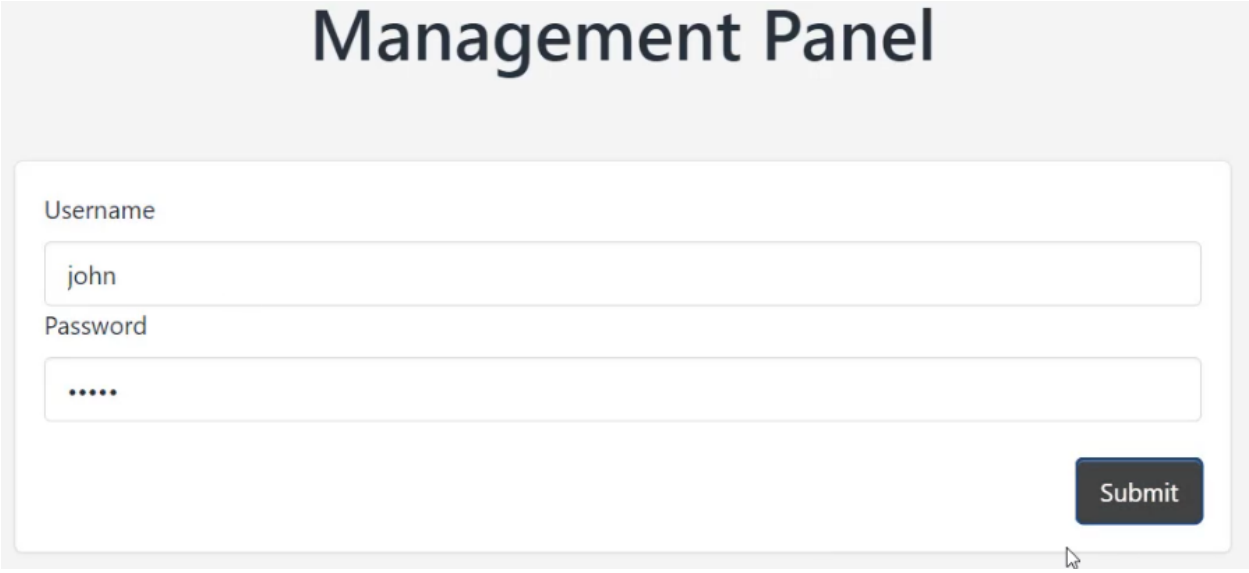
Vulnerability: **SQL injection**

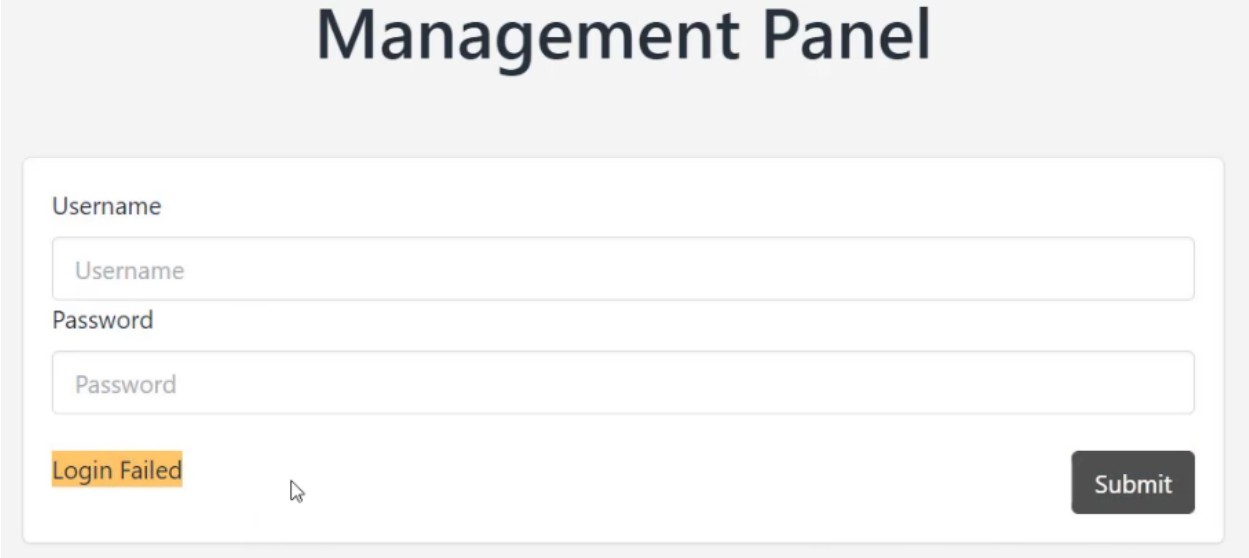
Step 1: Inspect the web application.

URL: https://yscpye9z66.execute-api.us-east-1.amazonaws.com/dev/



Step 2: Fill dummy values and try to login.



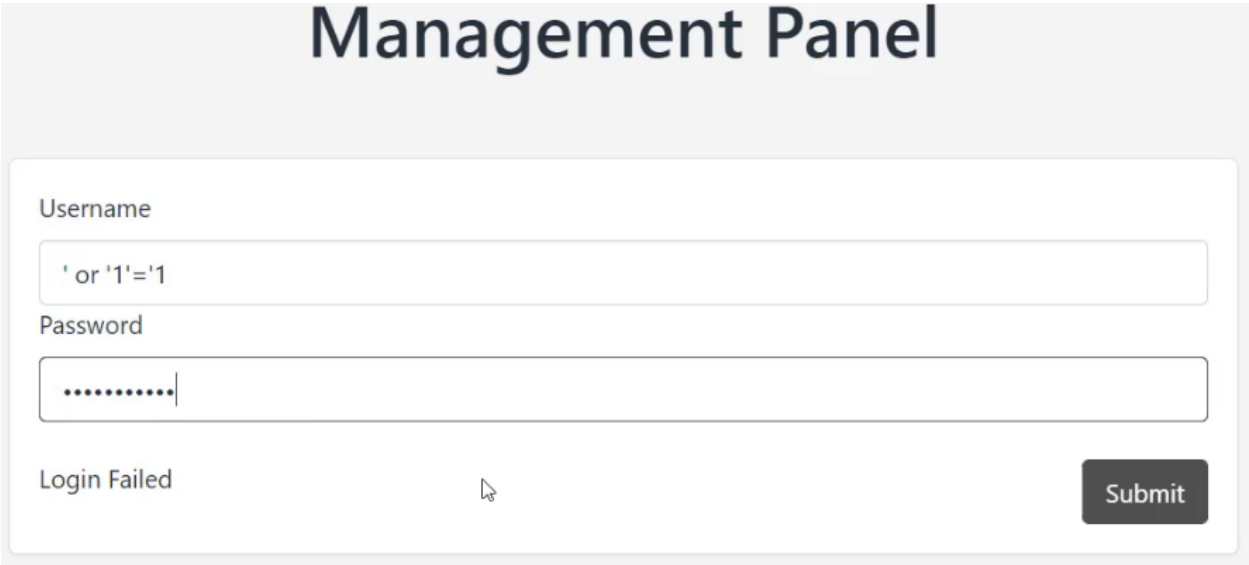


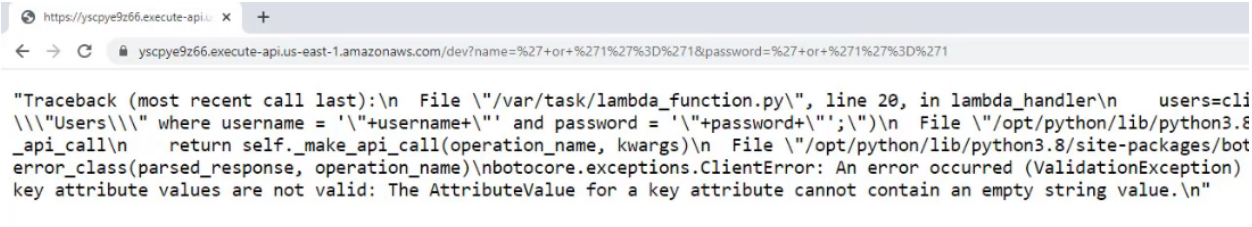
Login failed.

Step 3: Try simple SQL injection payload.

Payload:

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





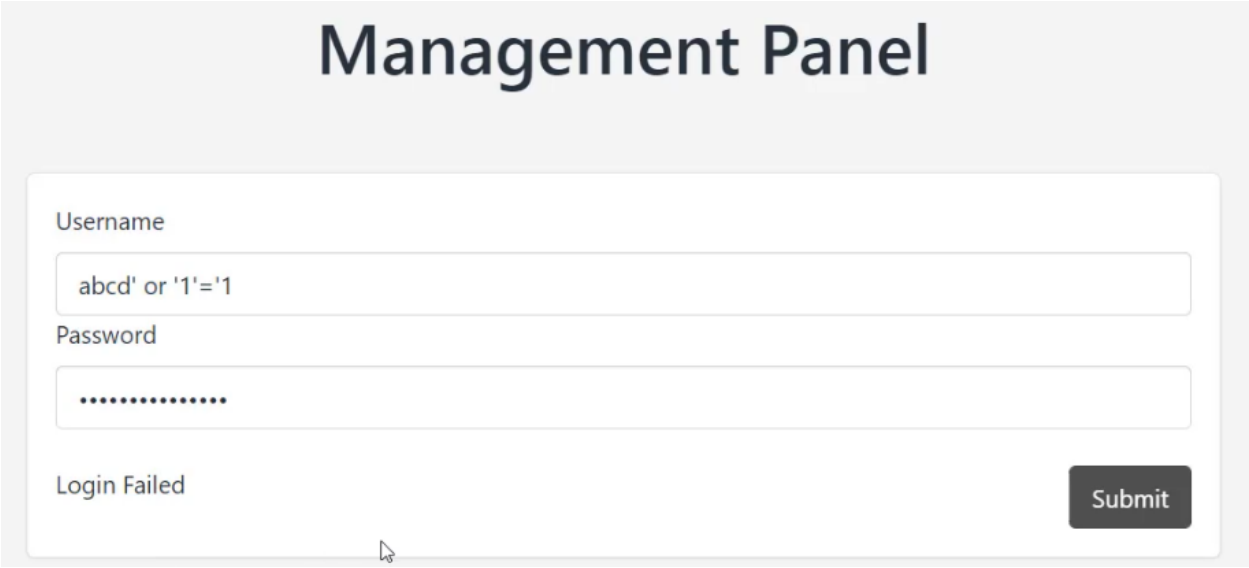
Got an error, this hints that SQL injection is working.

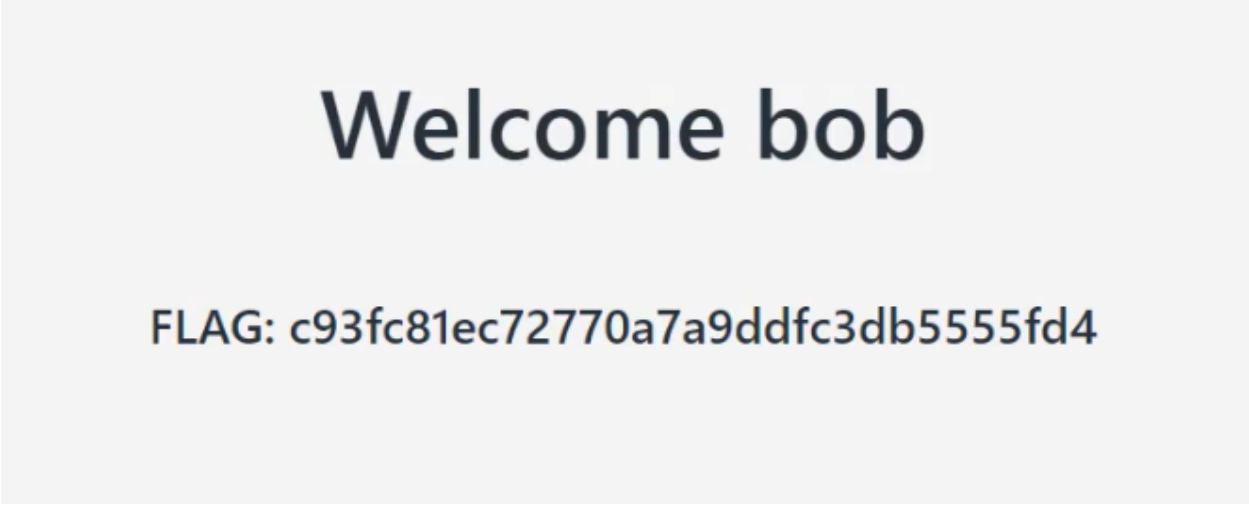
Since the payload started with single quotes, the attribute values became empty.

Step 4: Try inserting any string before payload so that attribute value doesn't become empty.

Payload:

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





FLAG: c93fc81ec72770a7a9ddfc3db5555fd4

Successfully logged in and retrieved the flag.