
ATTACK
DEFENSE
by PentesterAcademy

Name	IAM based Authentication
URL	https://attackdefense.com/challengedetails?cid=2278
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.

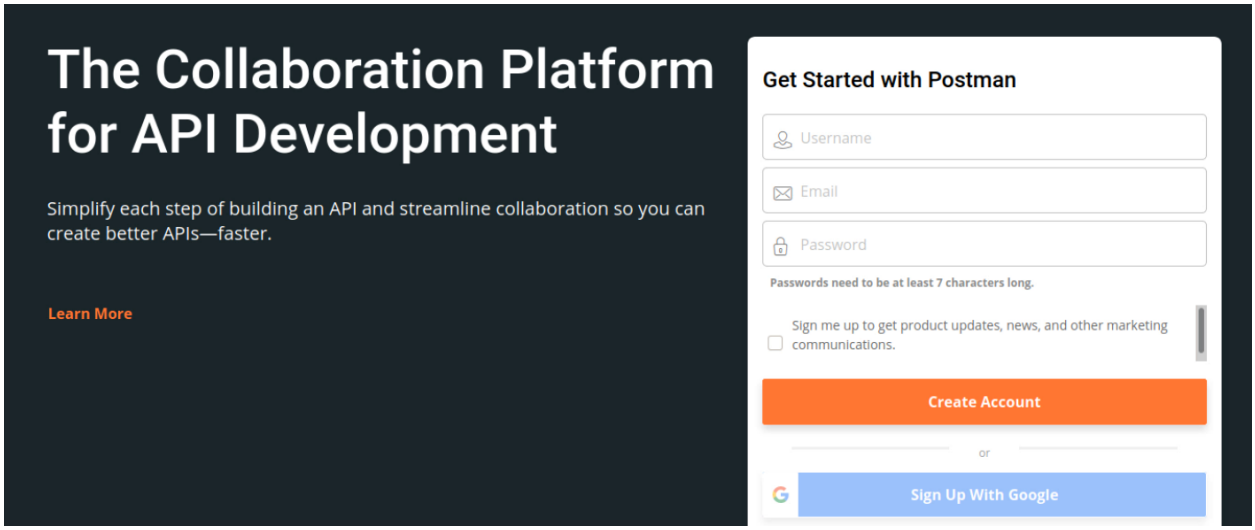
Solution:

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

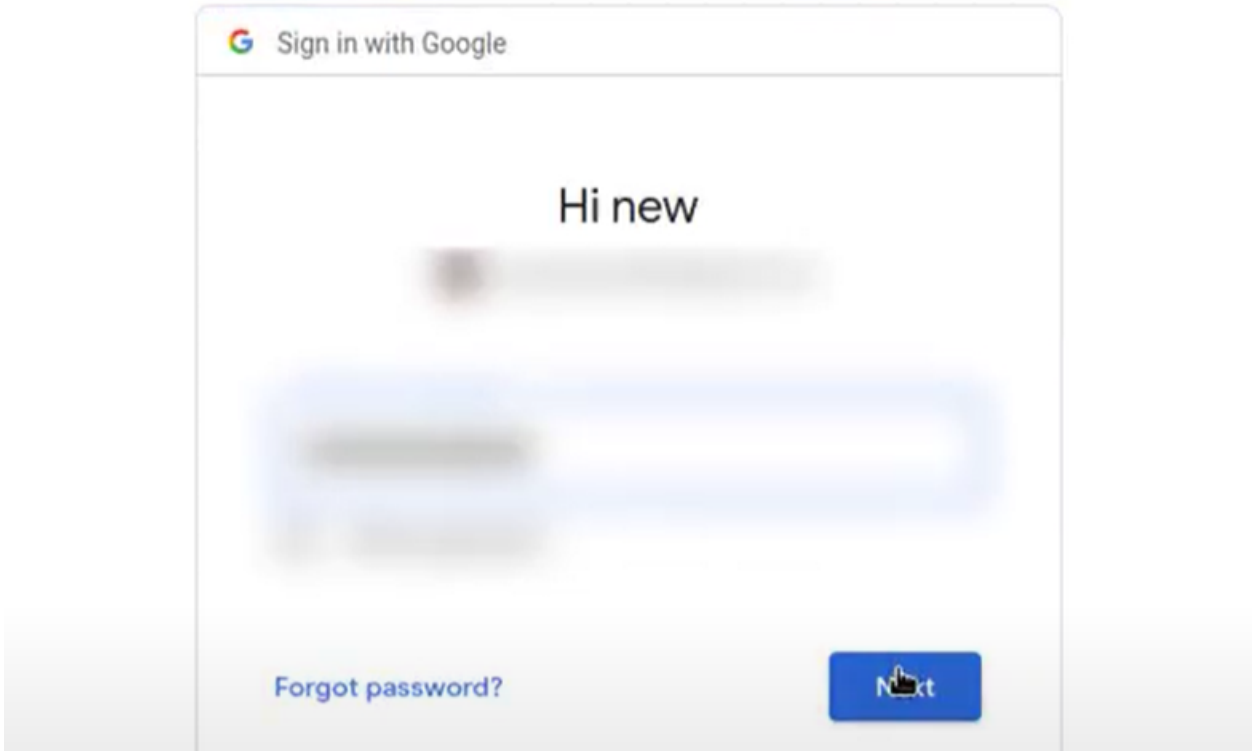
Access Credentials to your AWS lab Account

Login URL	https://140239203140.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad4f8JHpB3kb06UX
Access Key ID	AKIASBJXINNCDRKP546O
Secret Access Key	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

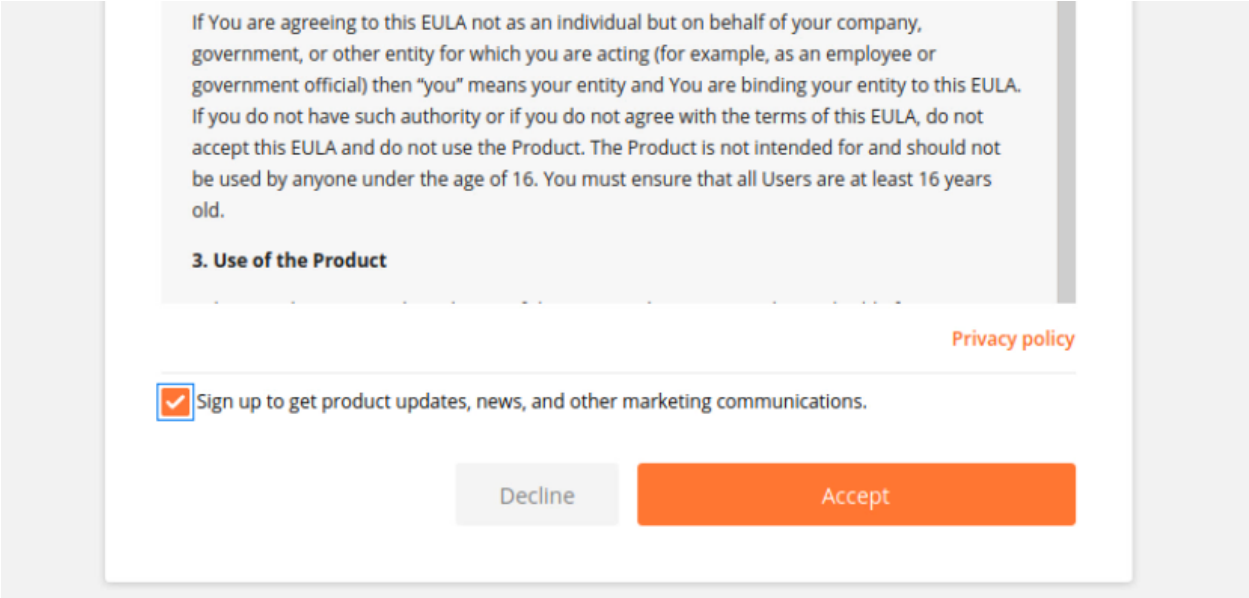
Step 2: Navigate to https://postman.com and sign in using google.



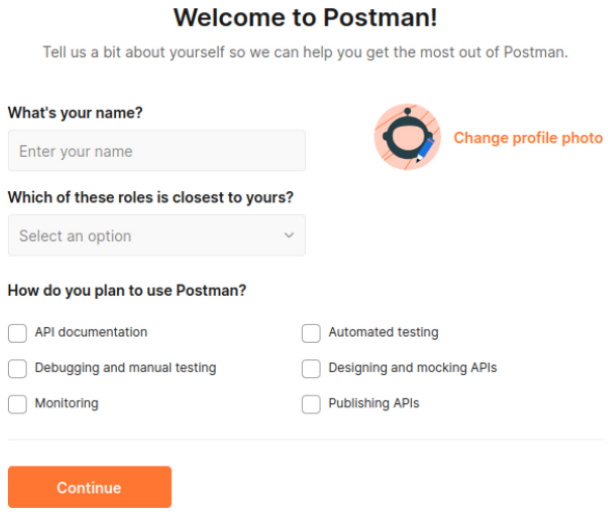
Step 3: Sign in with a google account.



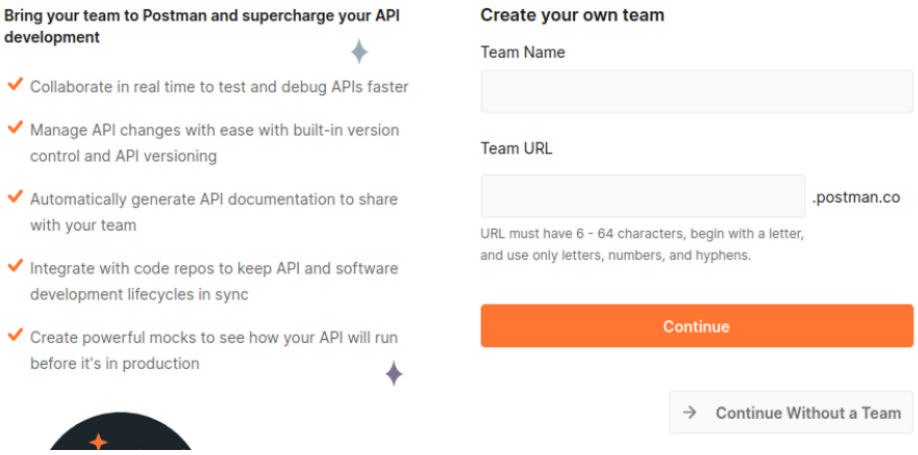
Step 4: Read and accept user licence terms and agreements.



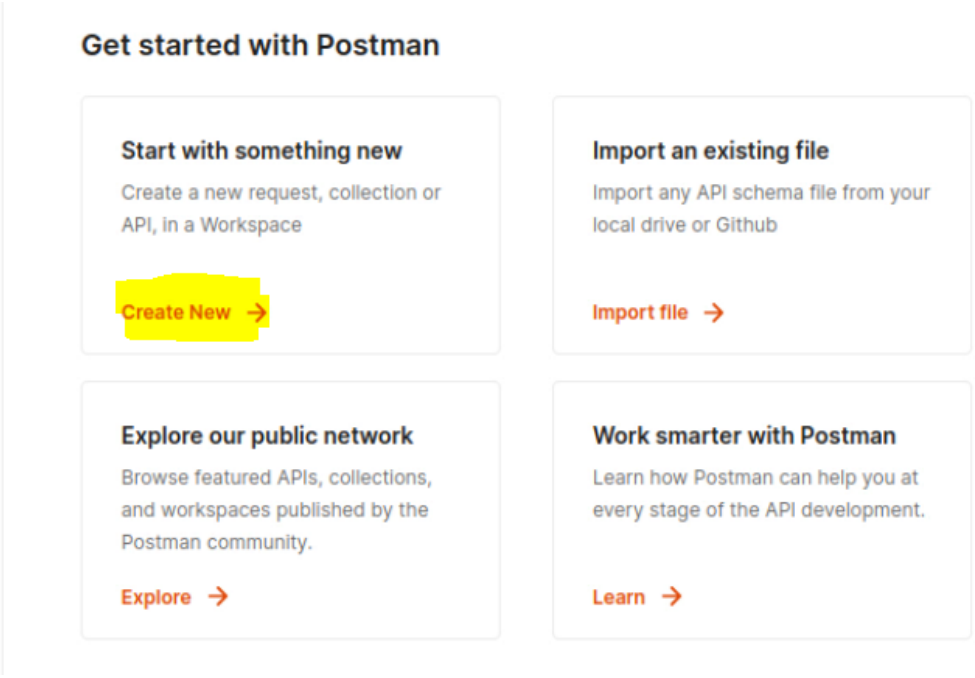
Step 5: Fill dummy values in the next tutorial steps.



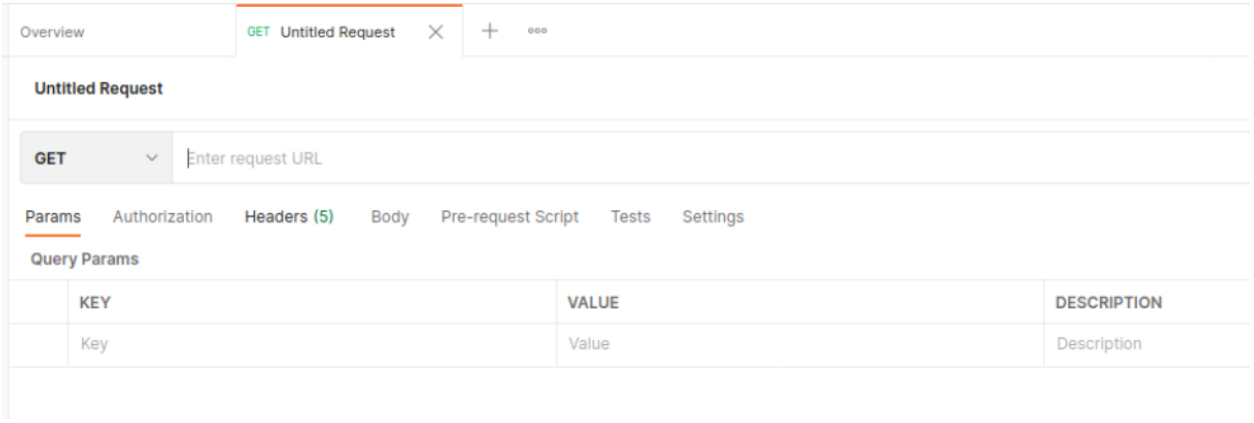
Step 6: Click on continue without a team on the next screen.



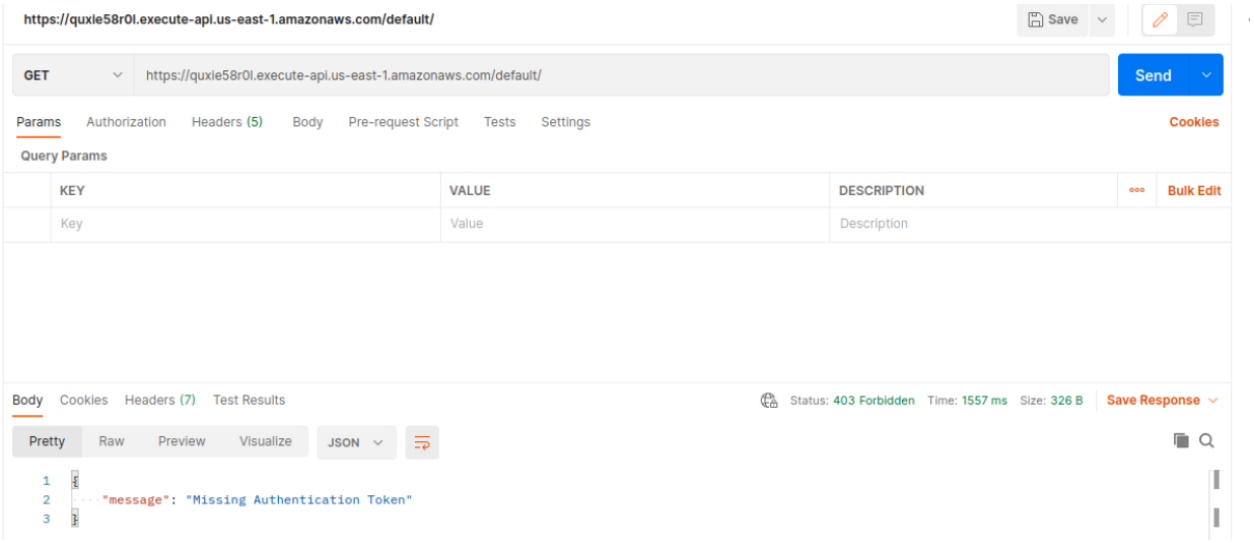
Step 7: Click on create new.



Step 8: Create a new request in the workspace by clicking the “+” button next to the overview tab.

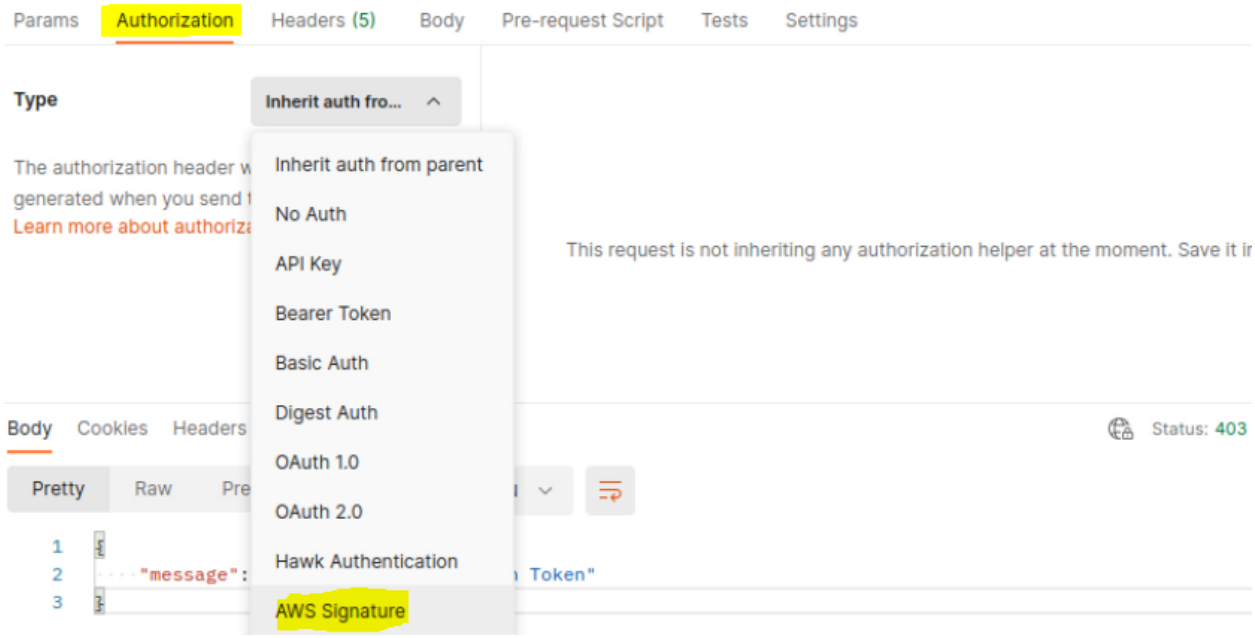


Step 9: Enter the URL on the top bar and send a GET request to the target API.

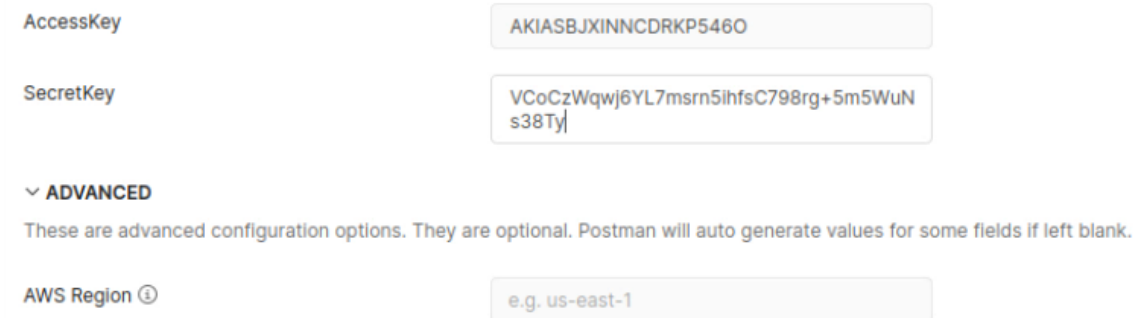


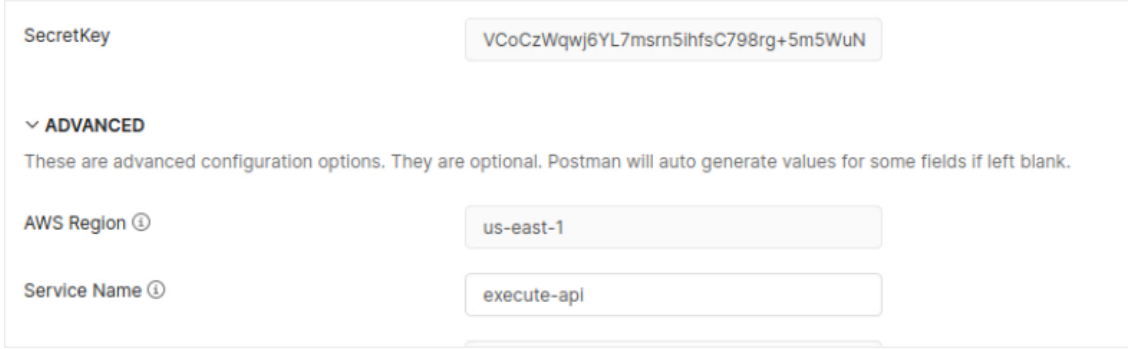
API returns missing authentication token message.

Step 10: Click on the authorization tab and select the AWS signature option.

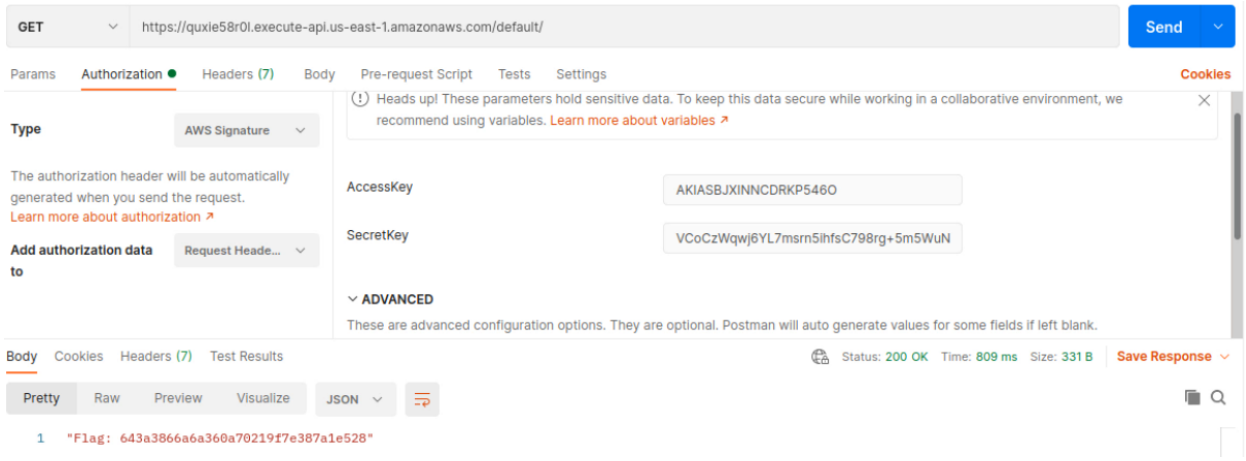


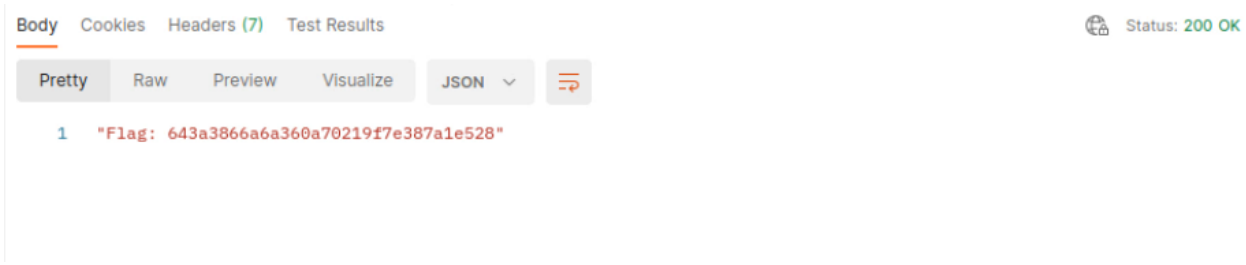
Step 11: Enter access keys and AWS region in the panel on the right and use “execute-api” as the service name.





Step 12: Send the request.





FLAG: 643a3866a6a360a70219f7e387a1e528

Successfully retrieved flag in the API response.

References:

1. Postman (https://www.postman.com/)