

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.

The Collaboration Platform for API Development

Simplify each step of building an API and streamline collaboration so you can create better APIs—faster.

[Learn More](#)

Get Started with Postman

Passwords need to be at least 7 characters long.

☐ Sign me up to get product updates, news, and other marketing communications.

Create Account

or



Sign Up With Google

Step 3: Sign in with a google account.

 Sign in with Google

Hi new

[Forgot password?](#)

Next

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

If You are agreeing to this EULA not as an individual but on behalf of your company, government, or other entity for which you are acting (for example, as an employee or government official) then "you" means your entity and You are binding your entity to this EULA. If you do not have such authority or if you do not agree with the terms of this EULA, do not accept this EULA and do not use the Product. The Product is not intended for and should not be used by anyone under the age of 16. You must ensure that all Users are at least 16 years old.

3. Use of the Product

[Privacy policy](#)

☒ Sign up to get product updates, news, and other marketing communications.

Decline Accept

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

Welcome to Postman!

Tell us a bit about yourself so we can help you get the most out of Postman.

What's your name?

Enter your name

Which of these roles is closest to yours?

Select an option

How do you plan to use Postman?

☐ API documentation ☐ Automated testing

☐ Debugging and manual testing ☐ Designing and mocking APIs

☐ Monitoring ☐ Publishing APIs

Continue

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

Bring your team to Postman and supercharge your API development

- ✓ Collaborate in real time to test and debug APIs faster
- ✓ Manage API changes with ease with built-in version control and API versioning
- ✓ Automatically generate API documentation to share with your team
- ✓ Integrate with code repos to keep API and software development lifecycles in sync
- ✓ Create powerful mocks to see how your API will run before it's in production

Create your own team

Team Name

Team URL

.postman.co

URL must have 6 - 64 characters, begin with a letter, and use only letters, numbers, and hyphens.

Continue

→ Continue Without a Team

Step 7: Click on create new.

Get started with Postman

Start with something new

Create a new request, collection or API, in a Workspace

Create New →

Import an existing file

Import any API schema file from your local drive or Github

Import file →

Explore our public network

Browse featured APIs, collections, and workspaces published by the Postman community.

Explore →

Work smarter with Postman

Learn how Postman can help you at every stage of the API development.

Learn →

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

Overview GET Untitled Request X + ...

Untitled Request

GET Enter request URL

Params Authorization Headers (5) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE	DESCRIPTION
Key	Value	Description

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

https://qxie58r0l.execute-api.us-east-1.amazonaws.com/default/ Save

GET https://qxie58r0l.execute-api.us-east-1.amazonaws.com/default/ Send

Params Authorization Headers (5) Body Pre-request Script Tests Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

Body Cookies Headers (7) Test Results Status: 403 Forbidden Time: 1557 ms Size: 326 B Save Response

Pretty Raw Preview Visualize JSON

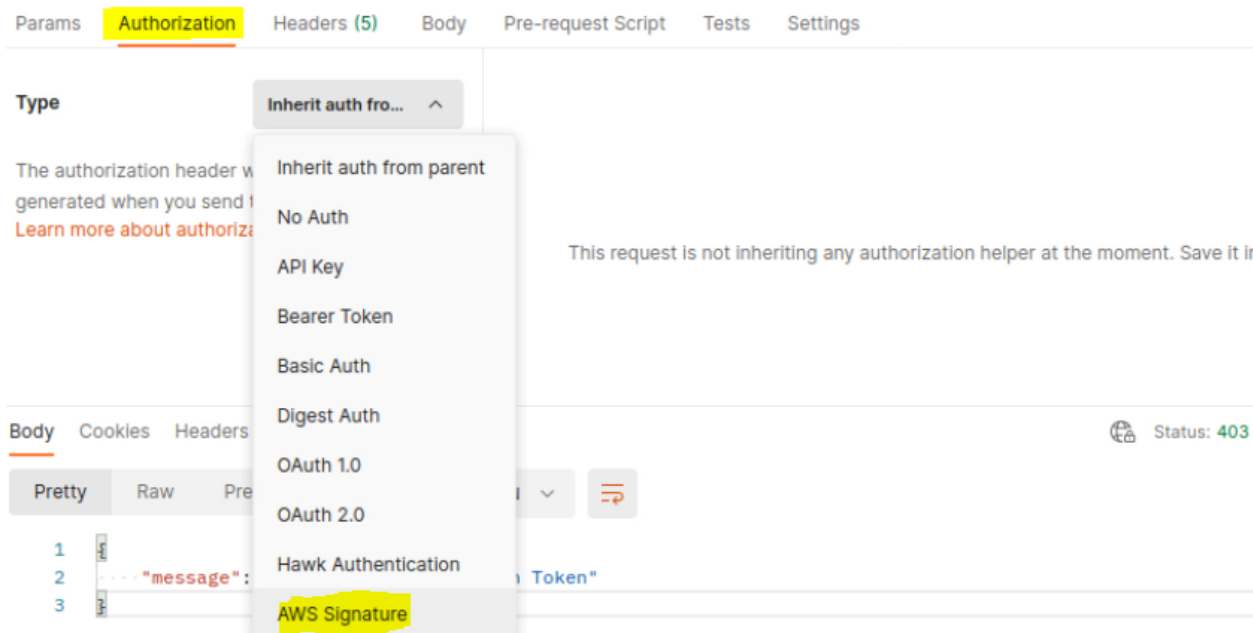
```

1 {
2   "message": "Missing Authentication Token"
3 }

```

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.

AccessKey AKIASBJXINNCDRKP546O

SecretKey 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|

▼ ADVANCED

These are advanced configuration options. They are optional. Postman will auto generate values for some fields if left blank.

AWS Region ⓘ e.g. us-east-1

SecretKey VCoCzWqwj6YL7msrn5ihfsC798rg+5m5WuN

▼ ADVANCED

These are advanced configuration options. They are optional. Postman will auto generate values for some fields if left blank.

AWS Region ⓘ us-east-1

Service Name ⓘ execute-api

Step 12: Send the request.

The screenshot shows the Postman interface for sending an AWS Signature request. The URL is `https://qxie58r0l.execute-api.us-east-1.amazonaws.com/default/`. The 'Authorization' tab is selected, showing the 'Type' as 'AWS Signature'. The 'AccessKey' is `AKIASBJXINNC DRKP5460` and the 'SecretKey' is `VCoCzWqwj6YL7msrn5lhfsC798rg+5m5WuN`. The 'Body' tab shows the response: `{\"Flag\": \"643a3866a6a360a70219f7e387a1e528\"}`. The status is 200 OK, Time: 809 ms, Size: 331 B.

FLAG: 643a3866a6a360a70219f7e387a1e528

Successfully retrieved flag in the API response.

References:

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