# **SECURE API ACCESS USING**

LAMBDA Logo

Description automatically generated

Hello! folks its awesome to have you here working towards understanding how to secure your APIs using **LAMBDA**. So, let’s get started right away with this tutorial.

To know why do we need to use a Lambda Authorizer click [ [here](https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html) ]

Chart

Description automatically generated

Before we get started you need to know when you use a custom authorizer such as Lambda the pattern would be that once the authorizer get the token it then read it and verifies it with another data provider if the user is legit or not and then a decision would be taken in the authoriser to return policy document [string] which would be like this

Graphical user interface, text, application, email

Description automatically generated

**Let’s Build a REST API**

Go to AWS console and search for API Gateway and then choose to build REST API. Then in a similar fashion create new resources, methods, Lambda function and stage. Follow it up by testing your API. So once your API is ready, you’d have a similar screen.

Graphical user interface, application

Description automatically generated

Now let’s create another Lambda function which would act as our Authorizer.

Graphical user interface, application

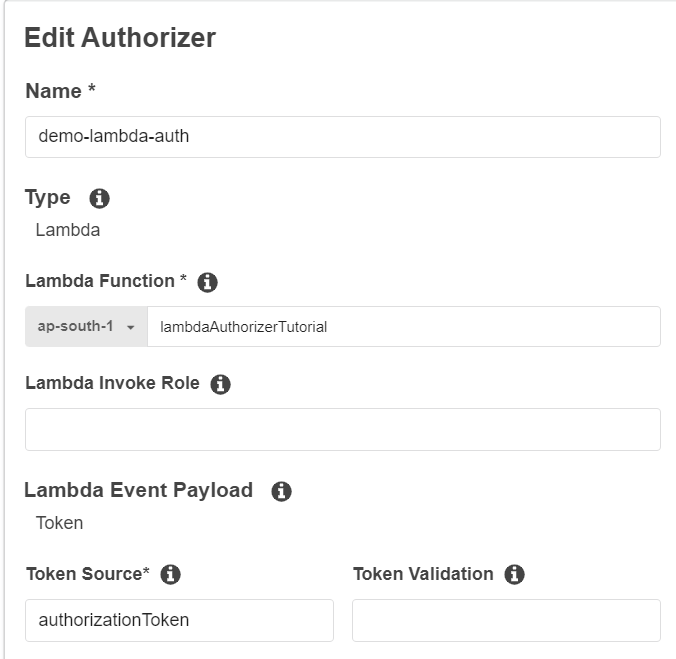
Description automatically generated

Now for the code paste the code given in **authorizerLambdaCode.txt** file, In that you’ll understand that initially we are just logging the event and later when it comes to validating the user if the token sent is valid then we give him access to the all the resources we have created in that API that’s why at the end of URL you’d find **/\*/\*** All resources and methods and generate a policy document if the auth variable that we have created states “**Allow**”.

Conclusion: If the token is **abc123** then it will allow or else it will deny.

Now Deploy the authorizer.

Now come to Authorizer section in our REST API. Create a new authorizer



Automatically AWS would grant and create the invoke role. Accept it and the **CREATE** the authorizer.

Now test the authorizer by giving the token i.e. **abc123**

Now go to the resources section and refresh the page so that our authorizer would now be shown in the **method request** of the resource.

Graphical user interface, text, application

Description automatically generated

Then **Deploy the API**.

**TESTING THE API**

Use Postman to test, add a header **authorizationToken** and give the value **abc123** and invoke the URL.

Graphical user interface, text, application, email

Description automatically generated

In case you give wrong token

Graphical user interface, text, application, email

Description automatically generated

This marks the end of the tutorial, thank you for sticking till the end and finishing the tutorial, hope you understood the concepts of using custom authorizer and how to implement and integrate with an API. **Happy Learning!!**

References:

* <https://docs.aws.amazon.com/>
* https://www.youtube.com/watch?v=al5I9v5Y-kA&t=174s