

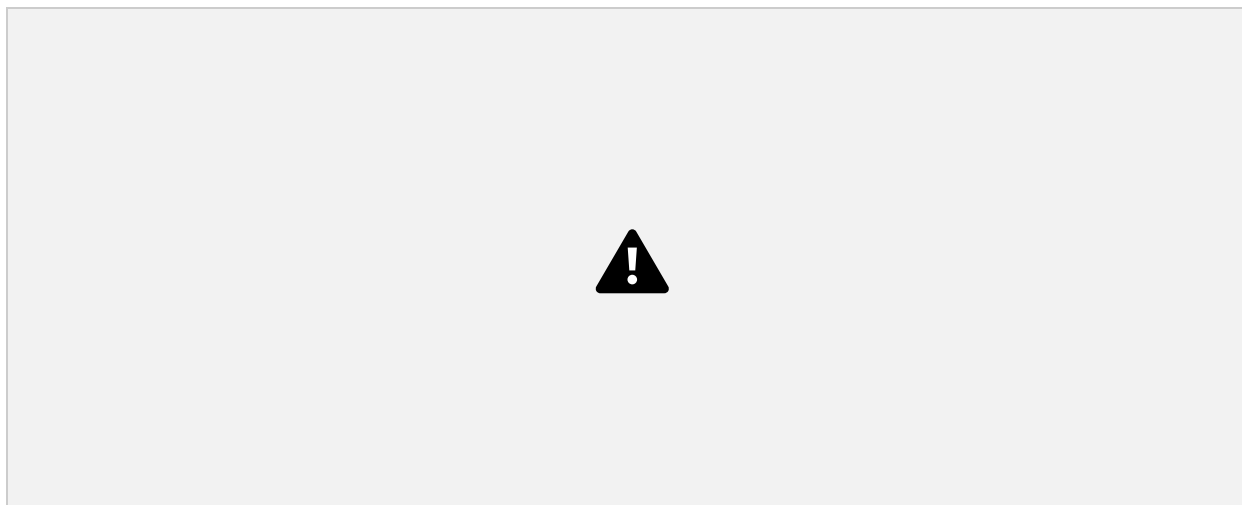
[illegible]

<b>Name</b>	Misconfigured Private API
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2277">https://attackdefense.com/challengedetails?cid=2277</a>
<b>Type</b>	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 access to AWS credentials.



**Step 2:** Sign-in into the AWS console.

## Sign in as IAM user

Account ID (12 digits) or account alias

108770978816

IAM user name

student

Password

●●●●●●●●●●●●●●●●

Sign in

[Sign in using root user email](#)

## Amazon DocumentDB (with MongoDB compatibility)

New role-based access control (RBAC) support helps you enforce least privilege access, and build multi-tenant applications

Get started »

### Step 3: Enumerate API details and resource policy.

APIs

Custom Domain Names

VPC Links

API: **private-api**

Resources

Stages

Authorizers

Gateway Responses

Models

**Resource Policy**

### Resource Policy

Configure access control to this private API using a Resource Policy. Access can be controlled by IAM condition elements, i Principal in the policy is set to \*, other authorization types can be used alongside the resource policy. If the Principal is set to resources. Changes to this policy require a deployment to take effect. [Learn more](#).

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": "*",  
7       "Action": "execute-api:Invoke",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

### Step 4: Check API stages.

APIs > private-api (6uo2game2h) > Stages > dev > /v1 > GET

Stages [Create](#) dev - GET - /v1

▼ dev  
▼ /  
▼ /v1  
GET

If Private DNS is enabled, use this URL: <https://6uo2game2h.execute-api.us-east-1.amazonaws.com/dev/v1>  
Otherwise, visit our documentation to learn about invoking private APIs

Use this page to override the dev stage settings for the GET to /v1 method.


Settings ☒ Inherit from stage  
☐ Override for this method

**Step 5:** Navigate to the ec2 dashboard and click on launch instance.

## Launch instance

Launch instance


Launch instance from template

**Launch instance** 

Note: Your instances will launch in the US East (N. Virginia) Region

**Step 6:** Use Amazon Linux 2 AMI.

### ▼ AMI Details

 **Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-047a51fa27710816e**

**Free tier eligible**

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance of the Amazon Linux AMI that is a...

Root Device Type: ebs    Virtualization type: hvm

**Step 7:** Use default VPC for instance.

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pri

Number of instances	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="text" value="vpc-ff1db382 (default)"/>	<a href="#">Create new VPC</a>
Subnet	<input type="text" value="No preference (default subnet in any Availability Zone)"/>	<a href="#">Create new subnet</a>
Auto-assign Public IP	<input type="text" value="Use subnet setting (Enable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="text" value="Open"/>	

**Step 8:** Launch the instance. Create a new key pair or use an existing one.

### Launch Status



#### Your instances are now launching

The following instance launches have been initiated: [i-043fca9a858fa34c7](#) [View launch log](#)



#### Get notified of estimated charges

[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount

**Step 9:** Connect to the instance in the instance dashboard.

## Instances (1/1) [Info](#)

search: i-043fca9a858fa34c7

<input checked="" type="checkbox"/>	Name ▾	Instance ID	Instance state ▾	Instance type ▾
<input checked="" type="checkbox"/>	–	i-043fca9a858fa34c7	Running	t3.micro

Launch instances

Launch instance from template

Connect

Stop instance

### Connect to instance [Info](#)

Connect to your instance i-043fca9a858fa34c7 using any of these options

**EC2 Instance Connect**

Session Manager

SSH client

Instance ID

i-043fca9a858fa34c7

Public IP address

34.232.65.73

User name

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

**Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

**Step 10:** Try accessing the API gateway using ec2.

```

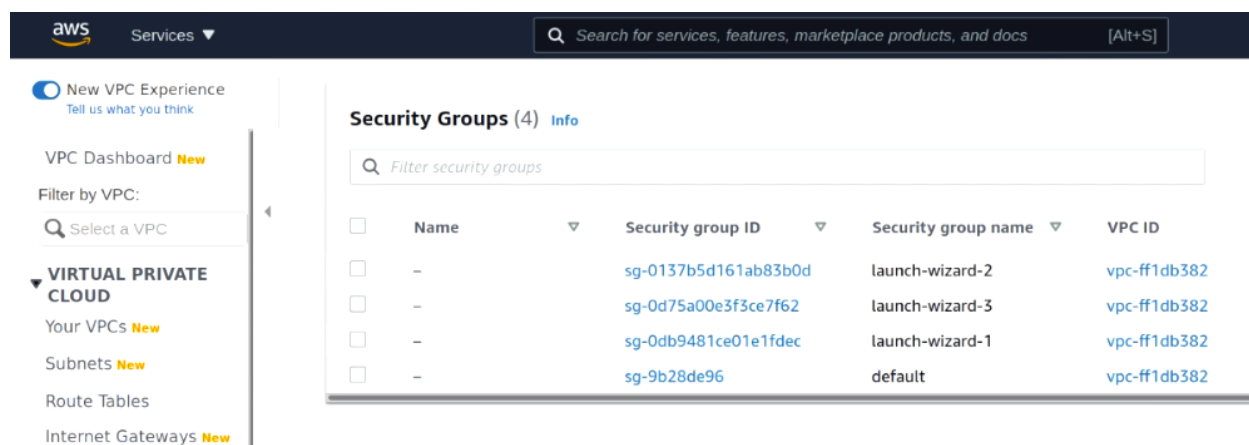
  _ | _ | _ | _ |
  _ | ( _ | _ | _ |
  _ | \ _ | _ | _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-60-1 ~]$ curl https://6uo2game2h.execute-api.us-east-1.amazonaws.com/dev/v1
curl: (6) Could not resolve host: 6uo2game2h.execute-api.us-east-1.amazonaws.com
[ec2-user@ip-172-31-60-1 ~]$
```

The request fails.

**Step 11:** Navigate to the VPC dashboard in another tab and navigate to the security group panel.



**Step 12:** Create a new security group with the following details.



VPC > Security Groups > sg-08e3da73846109b19 - all-access

## sg-08e3da73846109b19 - all-access

### Details

Security group name

all-access

Security group ID

sg-08e3da73846109b19

Description

Full Access

Owner

838431069332

Inbound rules count

2 Permission entries

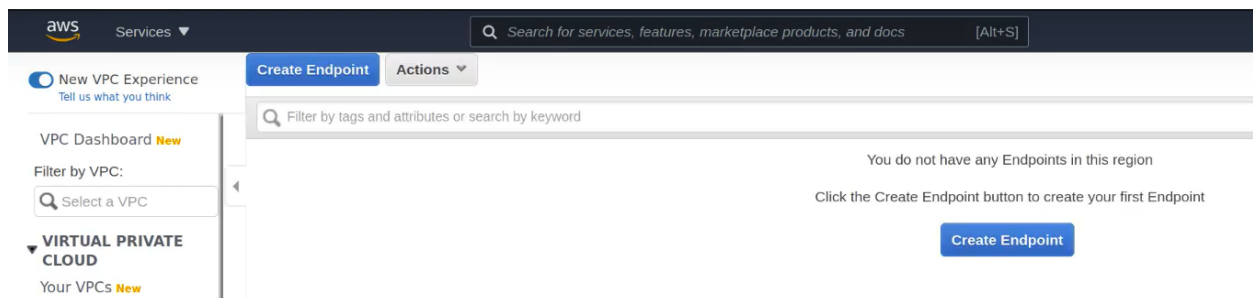
Outbound rules count

2 Permission entries

**Step 13:** Navigate to the endpoint services and create a new endpoint with the following details.

**Service Name:** com.amazonaws.us-east-1.execute-api

Select all availability zones.





Service Name com.amazonaws.us-east-1.execute-api ⓘ

51 to 100 of 113

Service Name	Owner	Type
<input type="radio"/> com.amazonaws.us-east-1.elasticbeanstalk	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.elasticbeanstal...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.elasticfilesystem	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.elasticfileyste...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.elasticloadbala...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.elasticmapred...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.email-smtp	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.emr-containers	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.events	amazon	Interface
<input checked="" type="radio"/> com.amazonaws.us-east-1.execute-api	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.frauddetector	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.git-codecommit	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.git-codecommi...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.glue	amazon	Interface

VPC\* vpc-ff1db382 ⓘ ⓘ


Subnets subnet-d9ee73bf ⓘ subnet-206cf401 ⓘ subnet-f71538ba ⓘ subnet-edba24b2 ⓘ subnet-4d59f87c ⓘ (+1 subnets) ⓘ


Availability Zone	Subnet ID
<input checked="" type="checkbox"/> us-east-1a (use1-az1)	subnet-d9ee73bf ▼
<input checked="" type="checkbox"/> us-east-1b (use1-az2)	subnet-206cf401 ▼
<input checked="" type="checkbox"/> us-east-1c (use1-az4)	subnet-f71538ba ▼
<input checked="" type="checkbox"/> us-east-1d (use1-az6)	subnet-edba24b2 ▼
<input checked="" type="checkbox"/> us-east-1e (use1-az3)	subnet-4d59f87c ▼
<input checked="" type="checkbox"/> us-east-1f (use1-az5)	subnet-d65e09d8 ▼





le DNS name ☒ Enable for this endpoint ⓘ

To use private DNS names, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS Support' are set to 'true' for your VPC (vpc-ff1db382). [Learn more](#).

**Step 14:** Use the newly created security group.



Security group **sg-08e3da73846109b19** [Create a new security group](#) 

Select security groups 

Filter by tags and attributes or search by keyword 						
 1 to 5 of 5  						
<input type="checkbox"/>	Group ID	Group Name	VPC ID		Description	Owner ID
<input type="checkbox"/>	sg-0137b5d1...	launch-wizard-2	vpc-ff1db382	EC2-VPC	launch-wizar...	838431069332
<input checked="" type="checkbox"/>	sg-08e3da73...	all-access	vpc-ff1db382	EC2-VPC	Full Access	838431069332
<input type="checkbox"/>	sg-0d75a00e...	launch-wizard-3	vpc-ff1db382	EC2-VPC	launch-wizar...	838431069332
<input type="checkbox"/>	sg-0db9481c...	launch-wizard-1	vpc-ff1db382	EC2-VPC	launch-wizar...	838431069332
<input type="checkbox"/>	sg-9b28de96	default	vpc-ff1db382	EC2-VPC	default VPC s...	838431069332

Use 'Full Access' policy after choosing the security group.

**Step 15:** Wait for the endpoint to become active and connect to the ec2 terminal.

 Endpoint ID : vpce-001db9ac1f94ed9fc  Add filter						
<input checked="" type="checkbox"/>	Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status
<input checked="" type="checkbox"/>		vpce-001db9ac1f9...	vpc-ff1db382	com.amazonaws.us-east-1.exe...	Interface	available

### Connect to instance [Info](#)

Connect to your instance i-043fca9a858fa34c7 using any of these options

**EC2 Instance Connect**

Session Manager

SSH client

Instance ID

i-043fca9a858fa34c7

Public IP address

34.232.65.73

User name

ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

**Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect

**Step 16:** Try accessing the API gateway using ec2.

```

  _ | ( _ | _ )
  _ | ( _ | _ ) Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-60-1 ~]$ curl https://6uo2game2h.execute-api.us-east-1.amazonaws.com/dev/v1
Flag: 43a3866a6a360a70219f7e387a1e528
[ec2-user@ip-172-31-60-1 ~]$
```

**FLAG:** 43a3866a6a360a70219f7e387a1e528

Successfully accessed API gateway and retrieved flag.

**Note:** VPC Endpoints cost 0.01 \$ per hour and similarly the EC2 instances also have hourly charge, please terminate them after usage otherwise unattended resources can incur unnecessary charges.