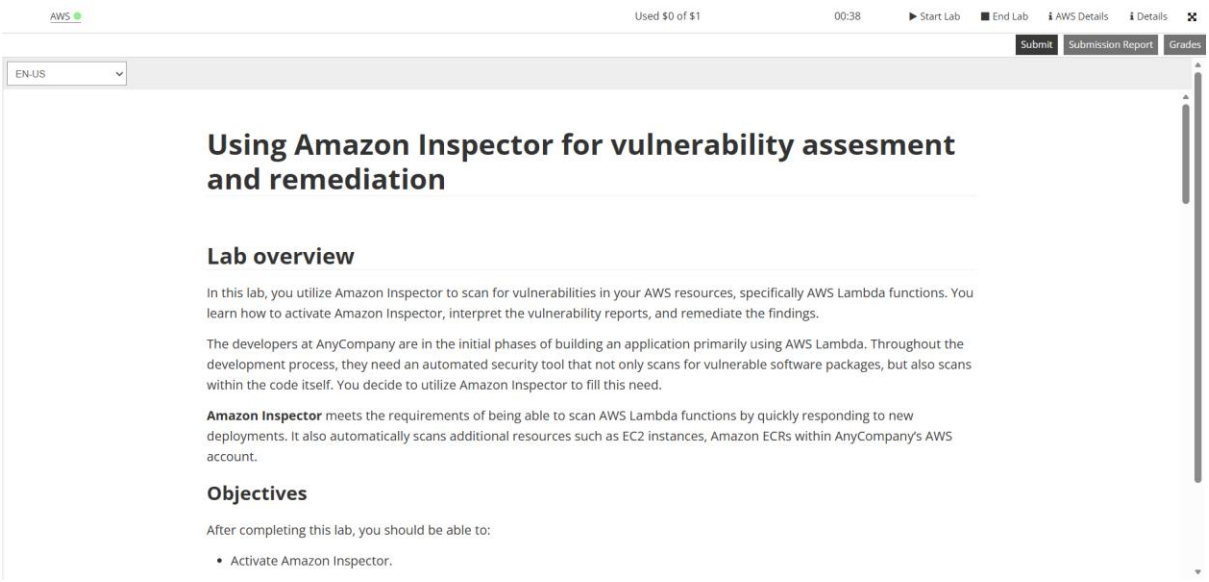
Using Amazon Inspector for vulnerability assesment and remediation



Objectives

After completing this lab, you should be able to:

- Activate Amazon Inspector.
- Analyze and interpret vulnerability findings.
- Remediate the vulnerabilities found by Amazon Inspector.

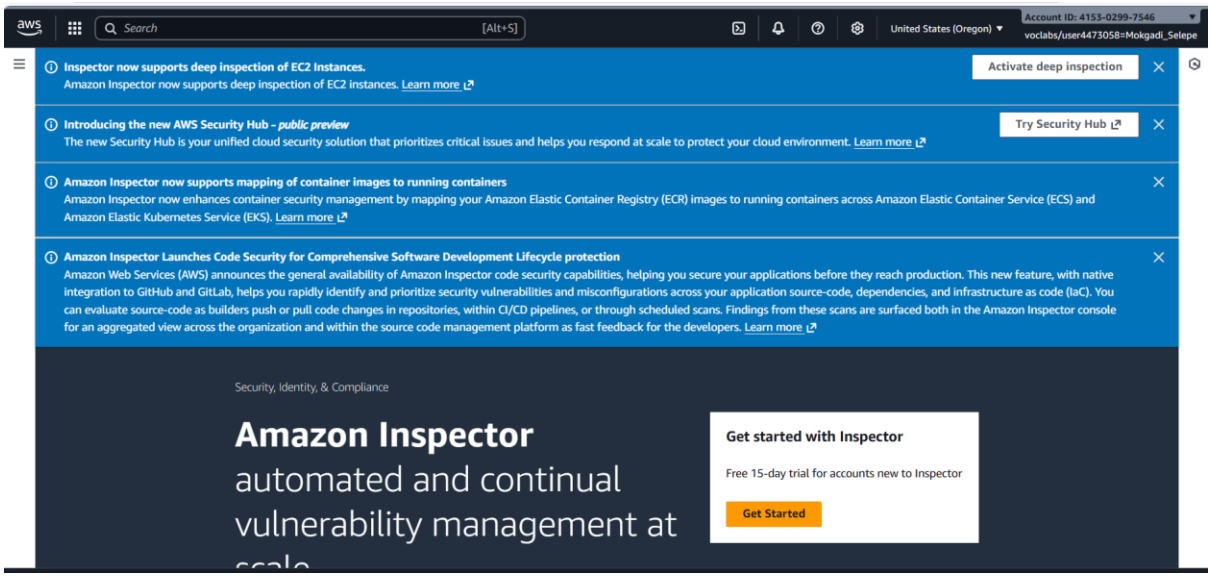
Duration

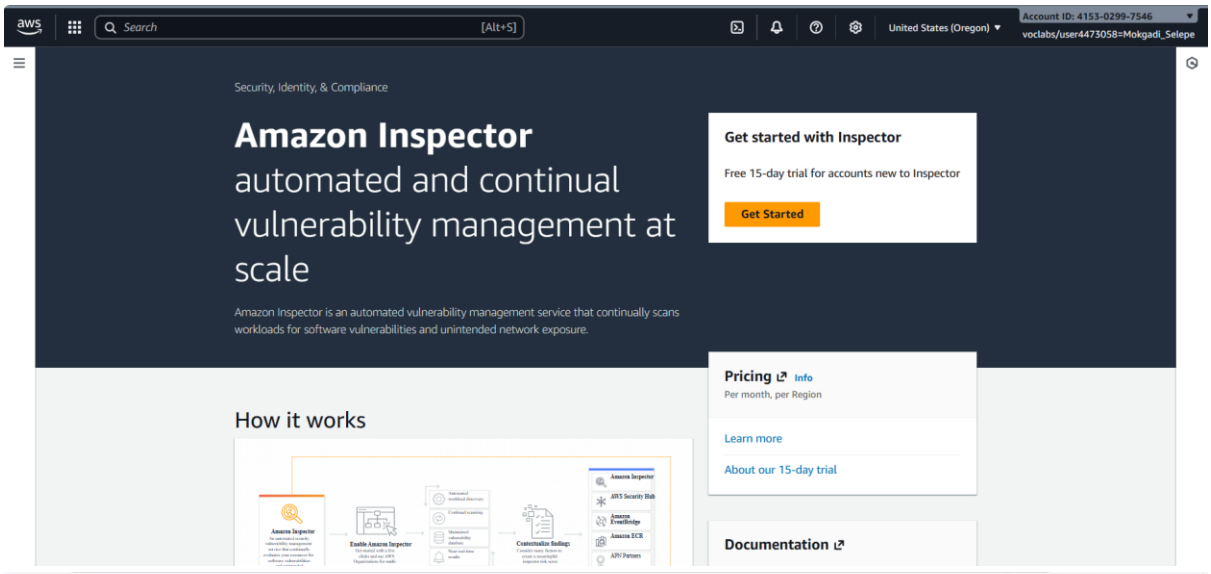
This lab requires approximately **30 minutes** to complete.

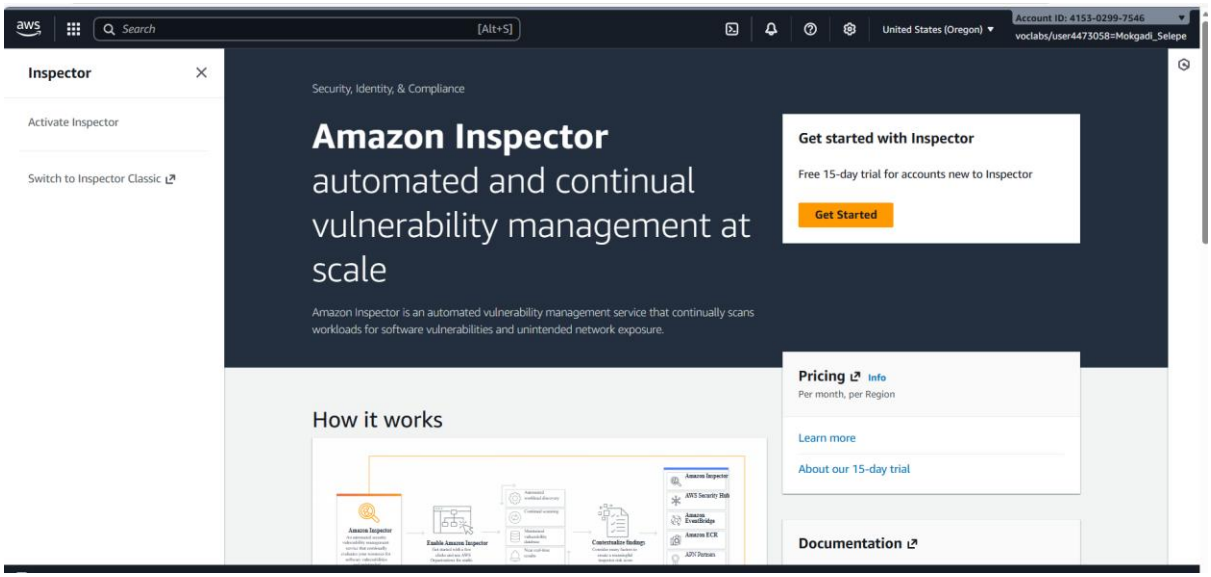
Lab environment

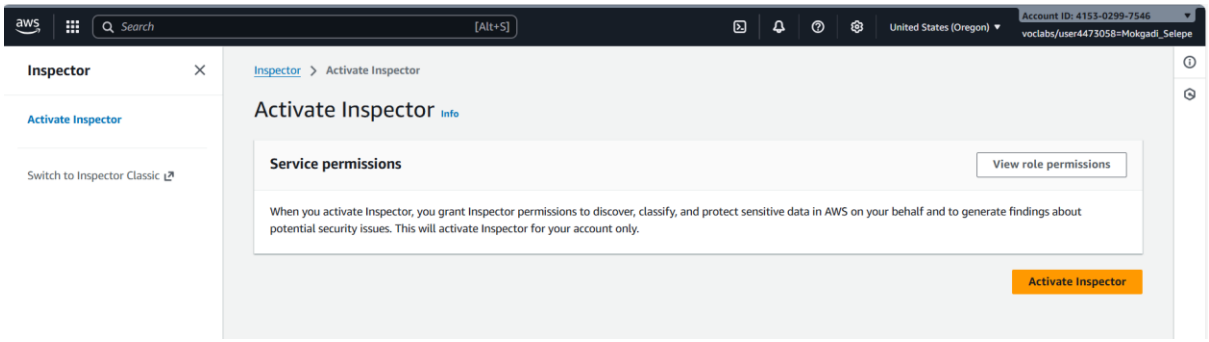
The environment has Lambda functions with vulnerabilities which will be subsequently scanned by Amazon inspector and reported as per severity.

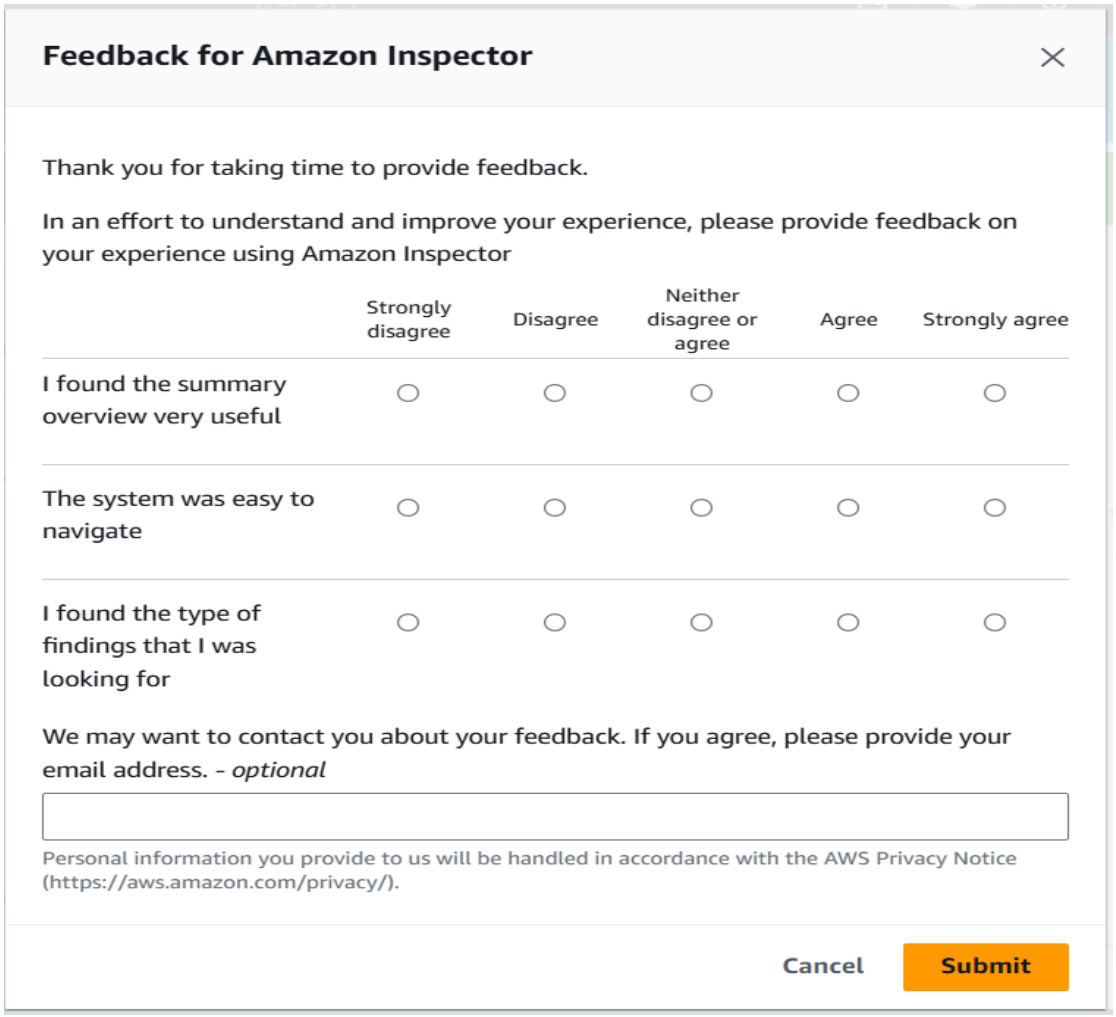
1: Activate the Amazon Inspector

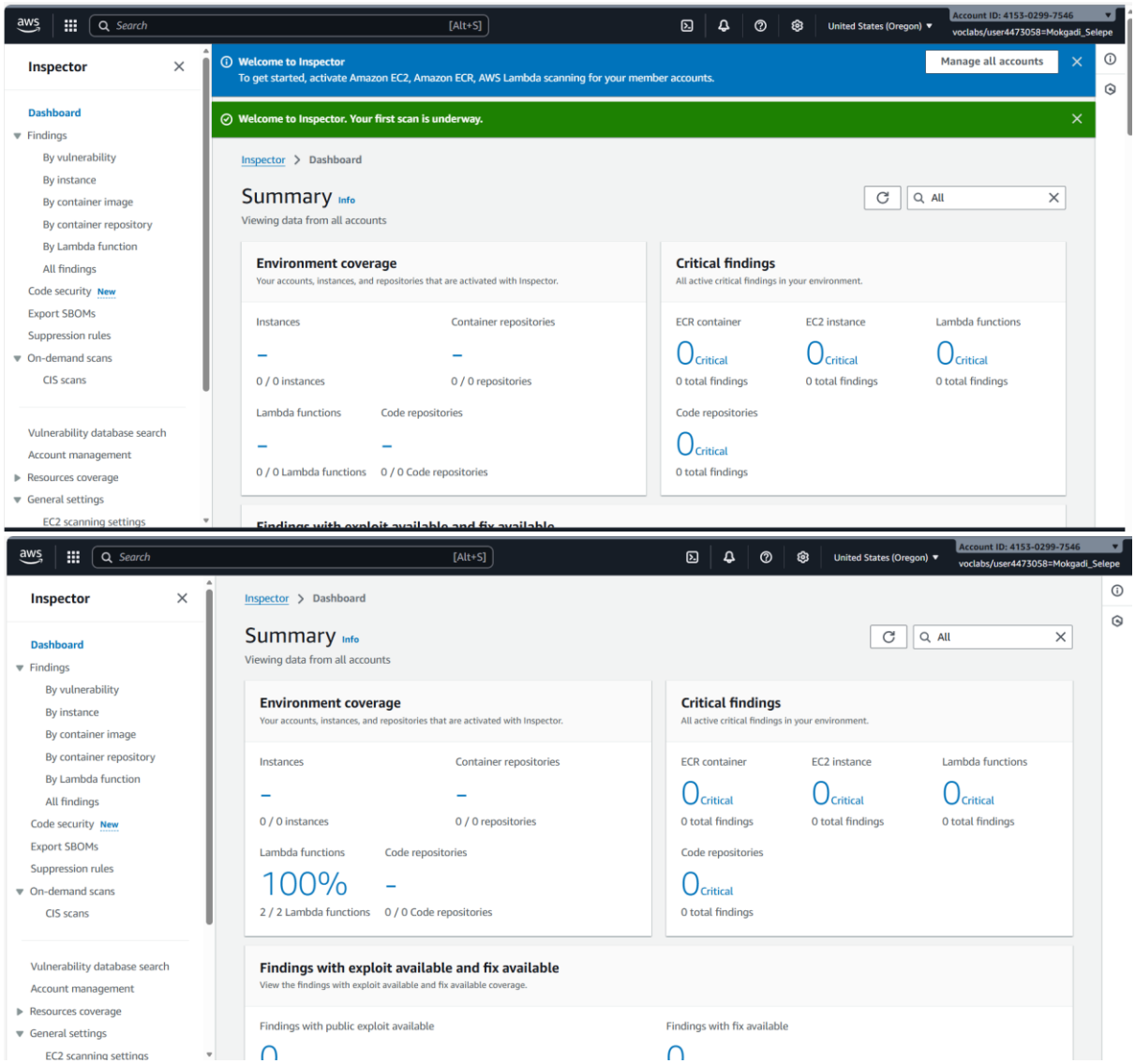

Search [Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Inspector now supports deep inspection of EC2 Instances.
Amazon Inspector now supports deep inspection of EC2 instances. Learn more
Activate deep inspection
Introducing the new AWS Security Hub – public preview
The new Security Hub is your unified cloud security solution that prioritizes critical issues and helps you respond at scale to protect your cloud environment. Learn more
Try Security Hub
Amazon Inspector now supports mapping of container images to running containers
Amazon Inspector now enhances container security management by mapping your Amazon Elastic Container Registry (ECR) images to running containers across Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Learn more
Amazon Inspector Launches Code Security for Comprehensive Software Development Lifecycle protection
Amazon Web Services (AWS) announces the general availability of Amazon Inspector code security capabilities, helping you secure your applications before they reach production. This new feature, with native integration to GitHub and GitLab, helps you rapidly identify and prioritize security vulnerabilities and misconfigurations across your application source-code, dependencies, and infrastructure as code (IaC). You can evaluate source-code as builders push or pull code changes in repositories, within CI/CD pipelines, or through scheduled scans. Findings from these scans are surfaced both in the Amazon Inspector console for an aggregated view across the organization and within the source code management platform as fast feedback for the developers. Learn more
Security, Identity, & Compliance
Amazon Inspector
automated and continual vulnerability management at scale
Get started with Inspector
Free 15-day trial for accounts new to Inspector
Get Started


Search [Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Security, Identity, & Compliance
Amazon Inspector
automated and continual vulnerability management at scale
Amazon Inspector is an automated vulnerability management service that continually scans workloads for software vulnerabilities and unintended network exposure.
Get started with Inspector
Free 15-day trial for accounts new to Inspector
Get Started
How it works
Pricing Info
Per month, per Region
Learn more
About our 15-day trial
Documentation


Search [Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Inspector
Activate Inspector
Switch to Inspector Classic
Security, Identity, & Compliance
Amazon Inspector
automated and continual vulnerability management at scale
Amazon Inspector is an automated vulnerability management service that continually scans workloads for software vulnerabilities and unintended network exposure.
Get started with Inspector
Free 15-day trial for accounts new to Inspector
Get Started
How it works
Pricing Info
Per month, per Region
Learn more
About our 15-day trial
Documentation


aws
Search
[Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Inspector
Activate Inspector
Switch to Inspector Classic
Inspector > Activate Inspector
Activate Inspector Info
Service permissions
View role permissions
When you activate Inspector, you grant Inspector permissions to discover, classify, and protect sensitive data in AWS on your behalf and to generate findings about potential security issues. This will activate Inspector for your account only.
Activate Inspector


Feedback for Amazon Inspector
Thank you for taking time to provide feedback.
In an effort to understand and improve your experience, please provide feedback on your experience using Amazon Inspector
Strongly disagree
Disagree
Neither disagree or agree
Agree
Strongly agree
I found the summary overview very useful
The system was easy to navigate
I found the type of findings that I was looking for
We may want to contact you about your feedback. If you agree, please provide your email address. - optional
Personal information you provide to us will be handled in accordance with the AWS Privacy Notice (https://aws.amazon.com/privacy/).
Cancel
Submit



I just turned on Amazon Inspector so it can keep checking my Lambda functions.

-First I typed “Inspector” in the console search bar and opened the service. In the left-hand menu I clicked “Activate Inspector” and then pressed the button to turn it on for my account – that’s only needed the first time.

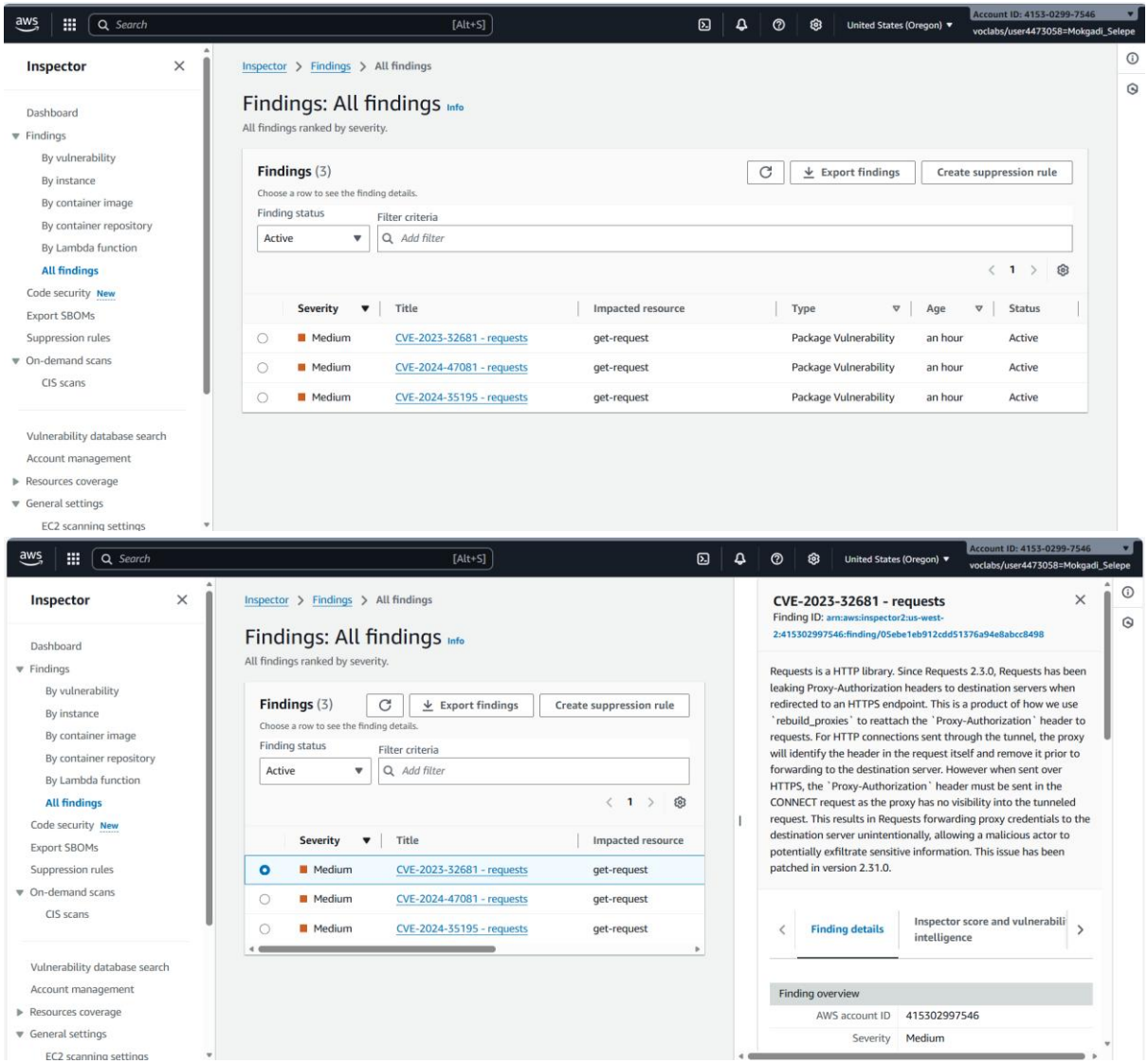
-After it started, a welcome message appeared and a scan began automatically.

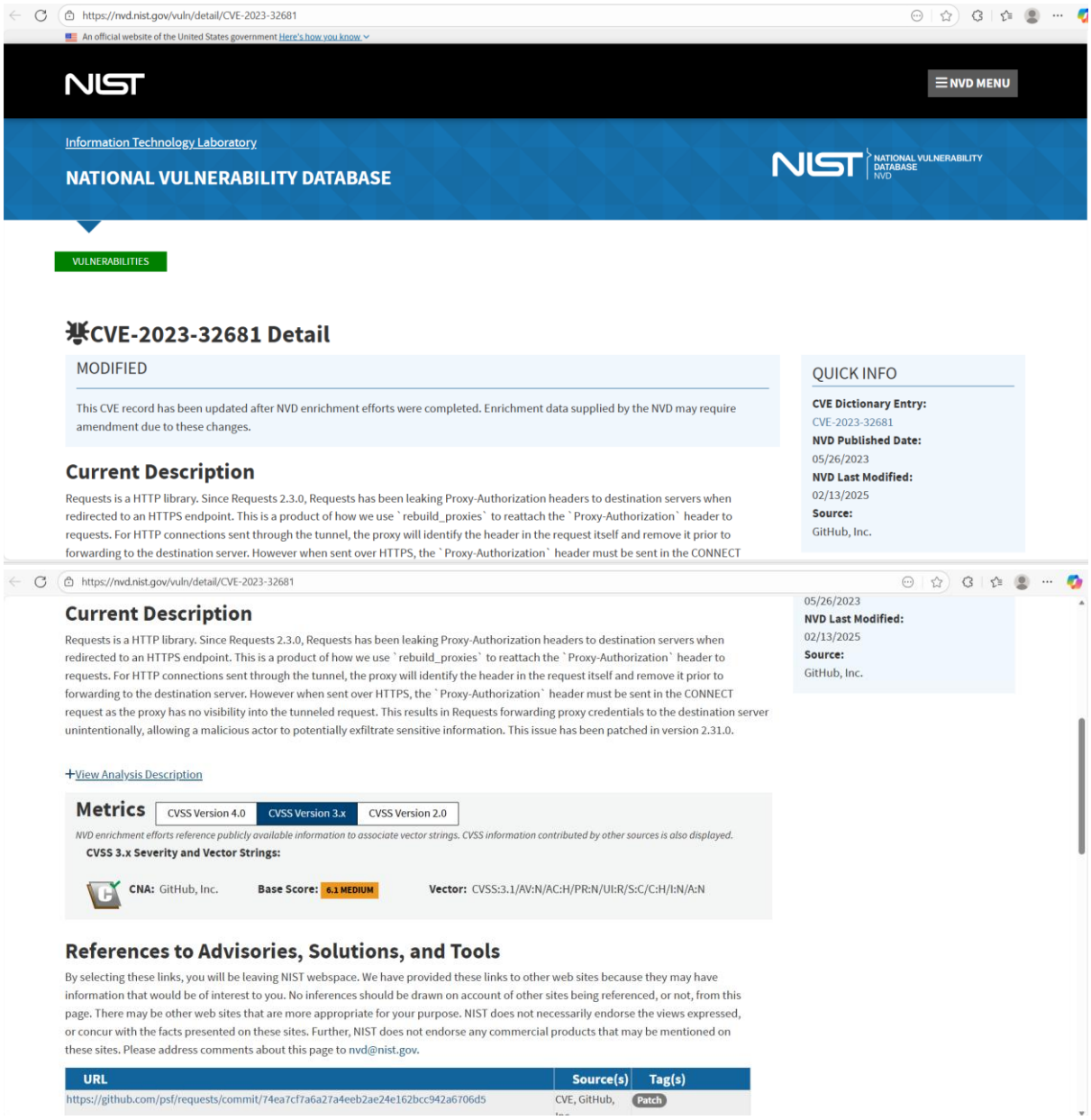
-I closed the survey prompt and any banner messages, then refreshed the page a few times until the dashboard showed that all my Lambda functions were covered (100 %).

The dashboard also shows my account number and that Inspector is now active, with standard scanning enabled for EC2, ECR and Lambda by default.

2: Reviewing the inspected resources

2.1: Reviewing your Lambda functions





I opened the “Findings” section on the left and clicked “All findings”.

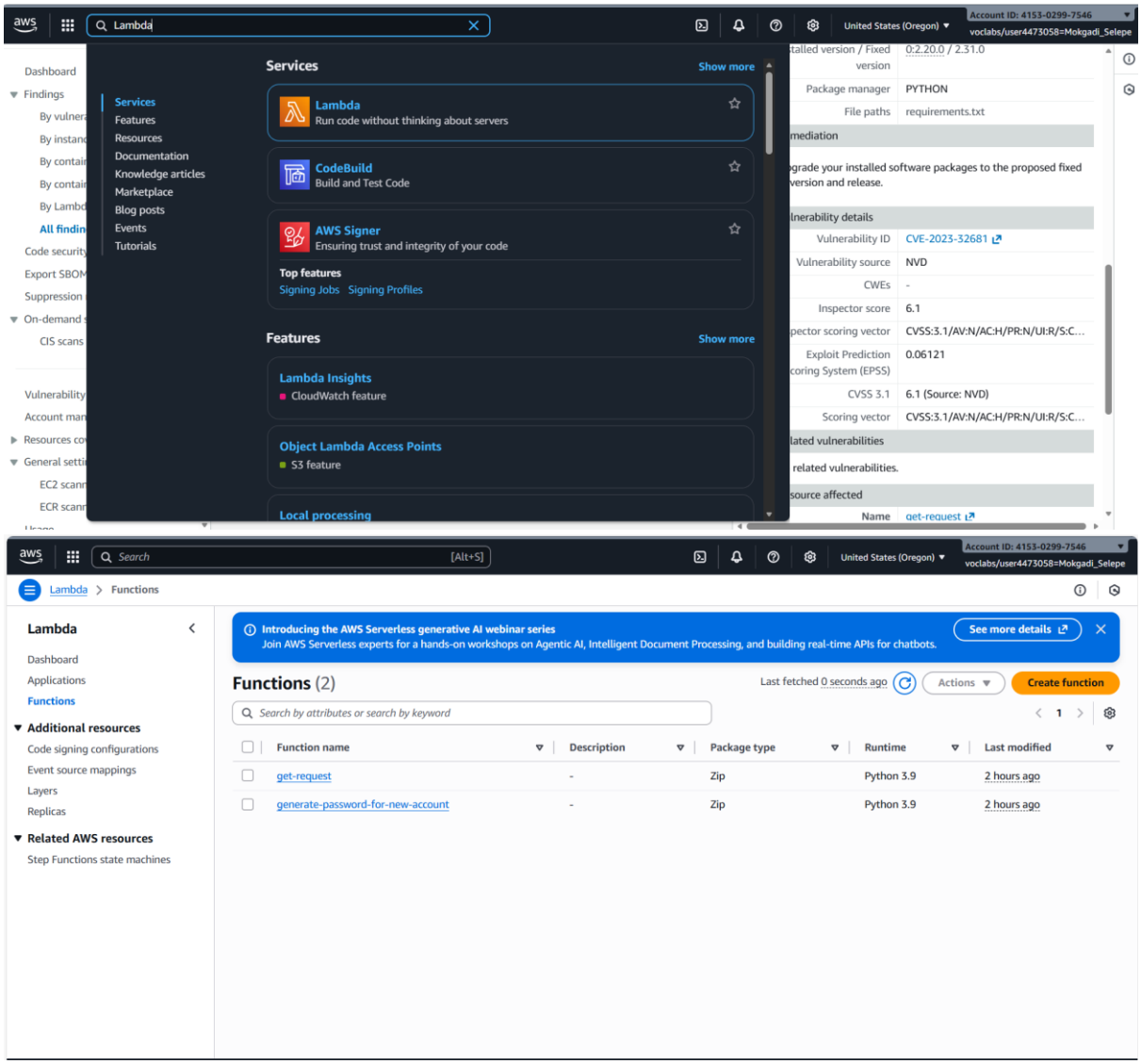
-Three rows showed up, one for each vulnerability that was found in my Lambda functions. Each row told me the severity (it was medium), which Lambda function was affected, and a short title explaining the issue.

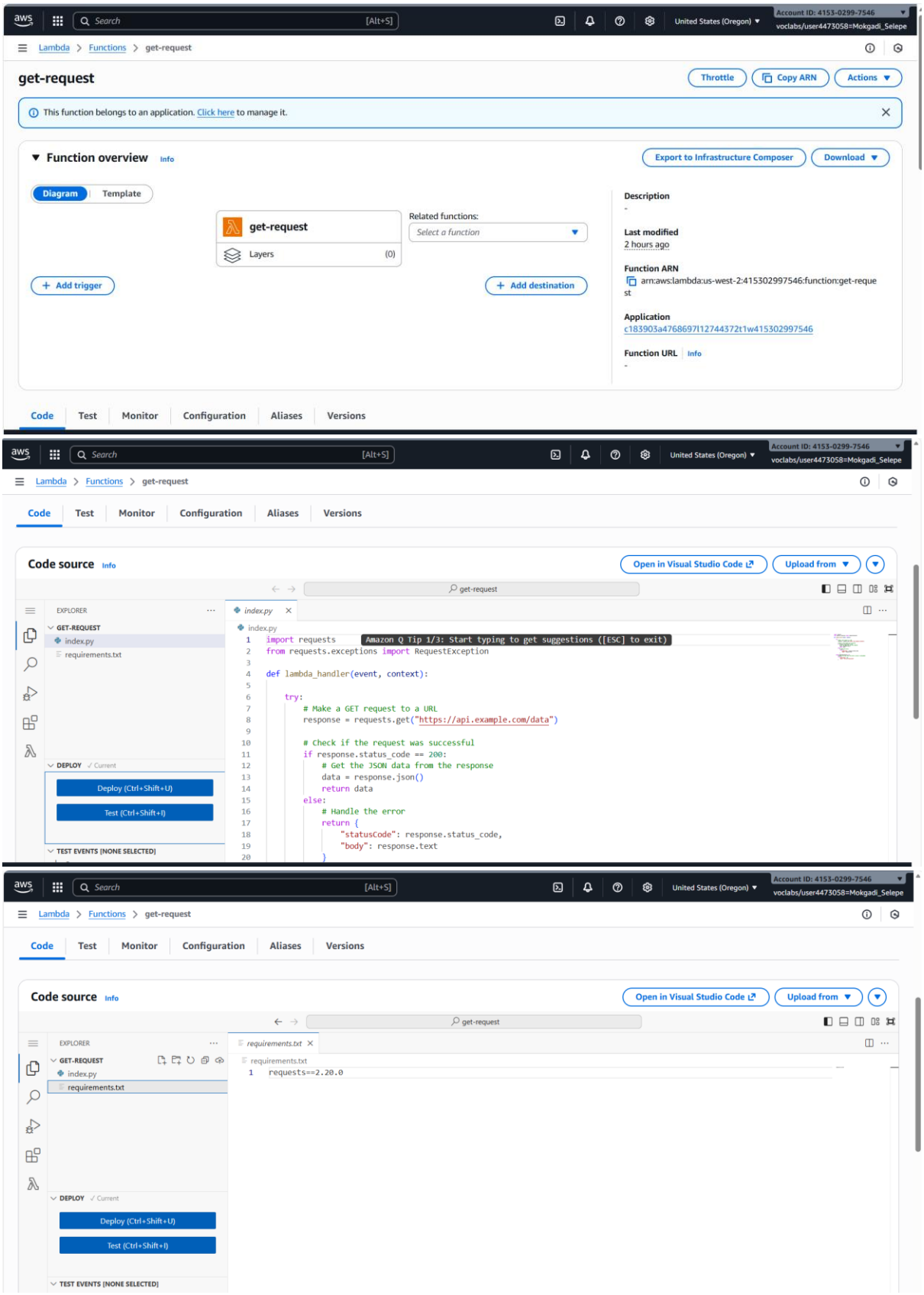
-I selected the radio button next to the finding titled “CVE-2023-32681 – requests”. That opened a side pane with more details about the vulnerability. In that pane I clicked the external link next to the Vulnerability ID, which took me to a page on the National Vulnerability Database (NVD) – a site run by NIST that lists standardized info about security flaws. That page gave me a deeper look at the problem.

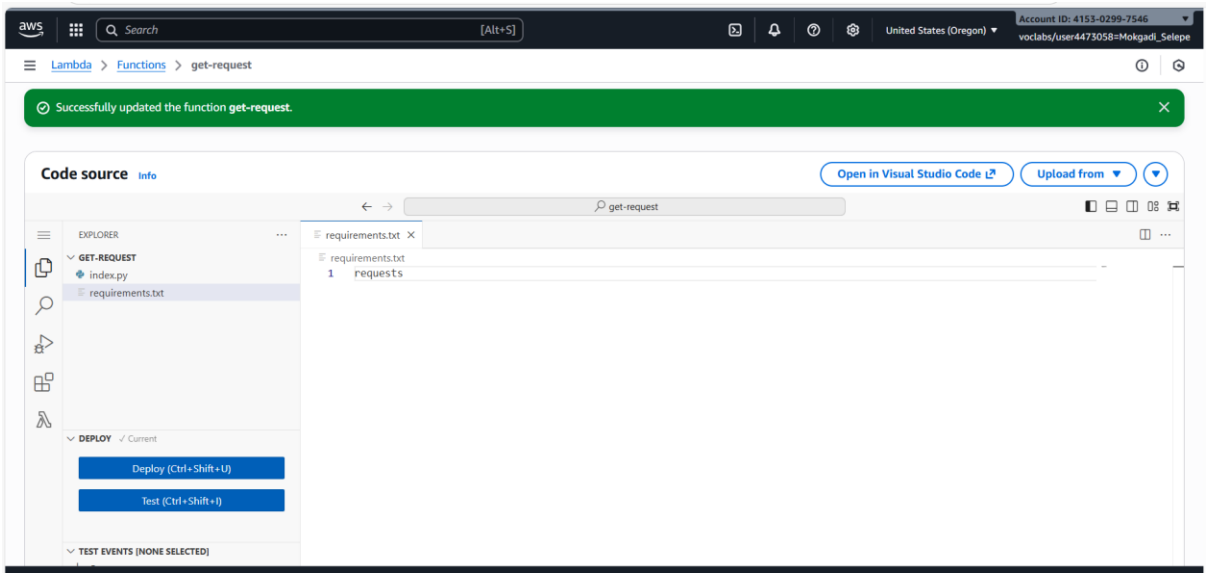
Back in the pane I saw the “Remediation” section, which said the requests package I was using is outdated and has a security hole, and that I should upgrade it. I’ll use that recommendation to fix the issue in my Lambda function.

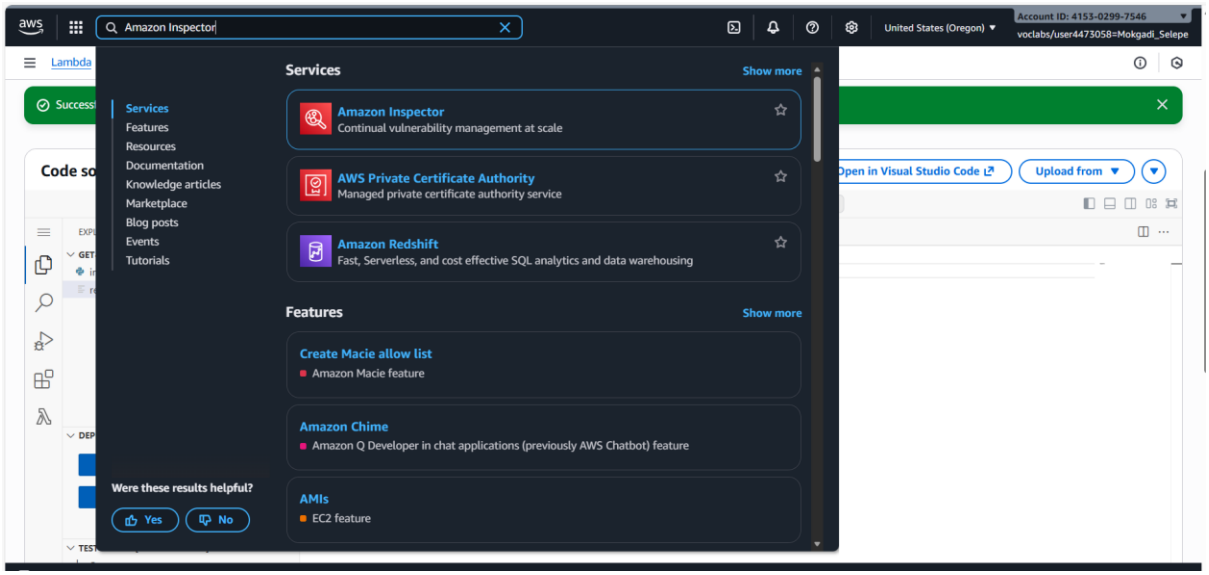
3: Remediating the vulnerabilities findings

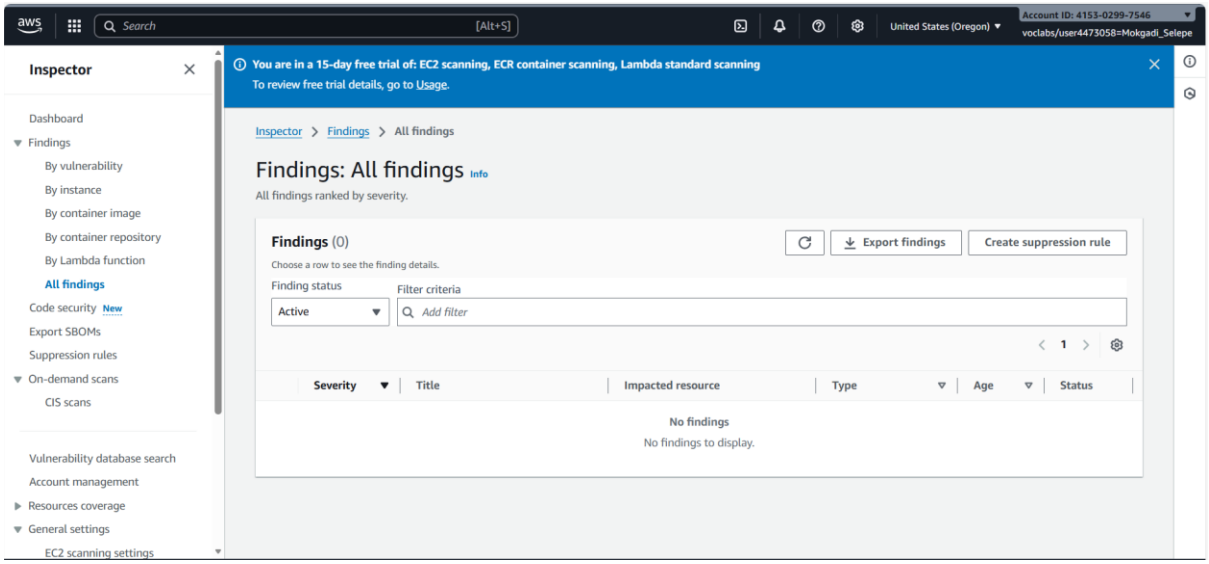
3.1: Remediating your Lambda function’s Package Vulnerabilities

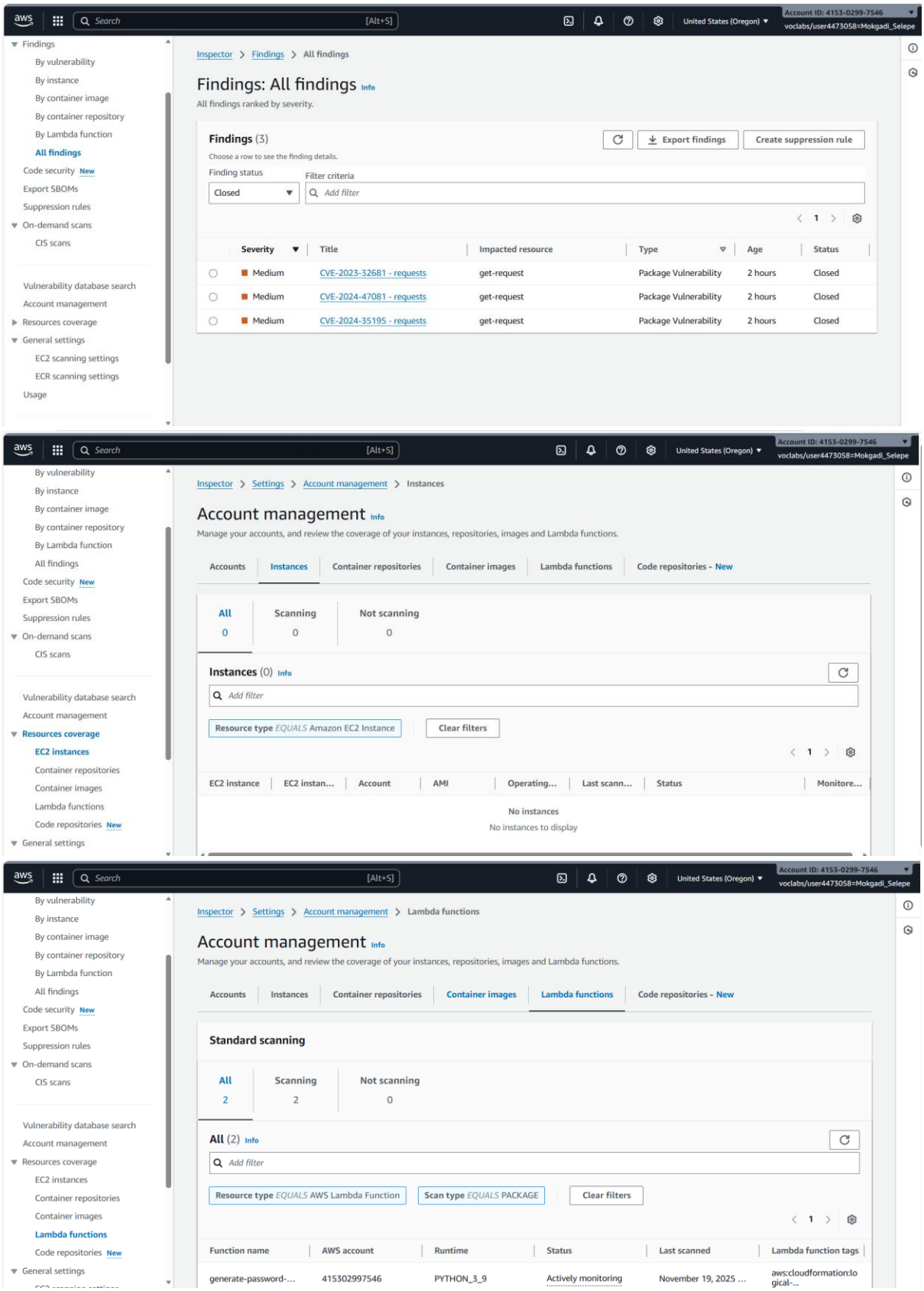


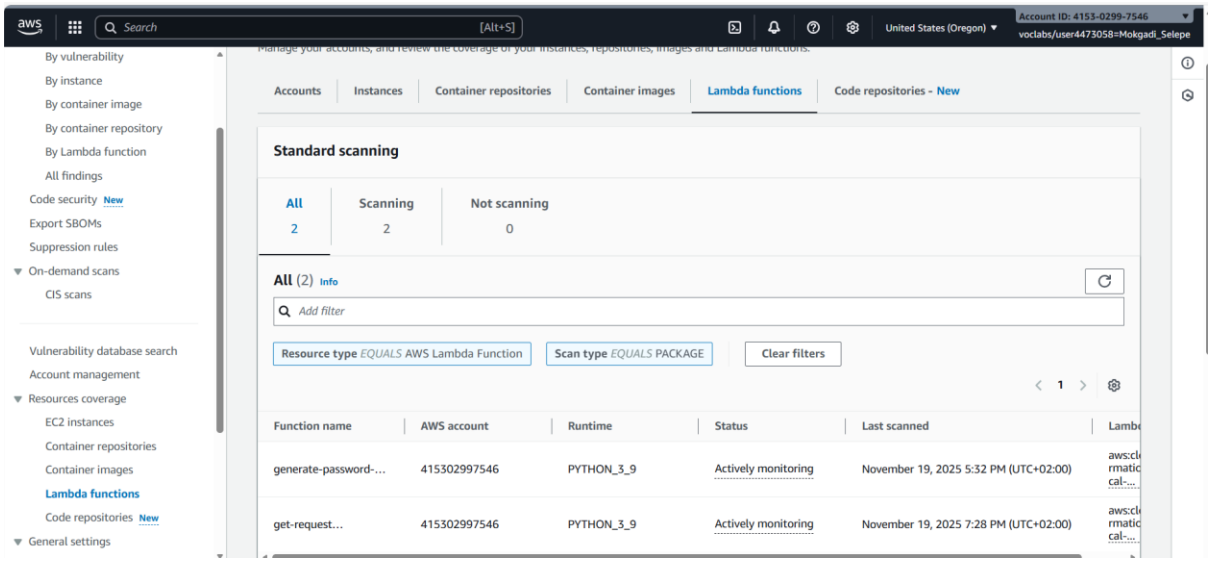

aws
Search
[Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Lambda > Functions > get-request
get-request
Throttle
Copy ARN
Actions
This function belongs to an application. Click here to manage it.
Function overview Info
Export to Infrastructure Composer
Download
Diagram
Template
get-request
Layers (0)
Related functions:
Select a function
Add trigger
Add destination
Description
Last modified
2 hours ago
Function ARN
arn:aws:lambda:us-west-2:415302997546:function:get-request
Application
c183903a4768697l12744372t1w415302997546
Function URL Info
Code
Test
Monitor
Configuration
Aliases
Versions
Code source Info
Open in Visual Studio Code
Upload from
EXPLORER
GET-REQUEST
index.py
requirements.txt
DEPLOY
Current
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
TEST EVENTS [NONE SELECTED]
Amazon Q Tip 1/3: Start typing to get suggestions ([ESC] to exit)
import requests
from requests.exceptions import RequestException
def lambda_handler(event, context):
try:
# Make a GET request to a URL
response = requests.get("https://api.example.com/data")
# Check if the request was successful
if response.status_code == 200:
# Get the JSON data from the response
data = response.json()
return data
else:
# Handle the error
return {
"statusCode": response.status_code,
"body": response.text
requests==2.20.0


Search [Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Lambda > Functions > get-request
Successfully updated the function get-request.
Code source Info
Open in Visual Studio Code
Upload from
EXPLORER
GET-REQUEST
index.py
requirements.txt
requirements.txt
1 requests
DEPLOY
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
TEST EVENTS [NONE SELECTED]


Amazon Inspector
Services
Features
Resources
Documentation
Knowledge articles
Marketplace
Blog posts
Events
Tutorials
Services
Show more
Amazon Inspector
Continual vulnerability management at scale
AWS Private Certificate Authority
Managed private certificate authority service
Amazon Redshift
Fast, Serverless, and cost effective SQL analytics and data warehousing
Features
Show more
Create Macie allow list
Amazon Macie feature
Amazon Chime
Amazon Q Developer in chat applications (previously AWS Chatbot) feature
AMIs
EC2 feature
Were these results helpful?
Yes
No


Search [Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Inspector
Dashboard
Findings
By vulnerability
By instance
By container image
By container repository
By Lambda function
All findings
Code security New
Export SBOMs
Suppression rules
On-demand scans
CIS scans
Vulnerability database search
Account management
Resources coverage
General settings
EC2 scanning settings
You are in a 15-day free trial of: EC2 scanning, ECR container scanning, Lambda standard scanning
To review free trial details, go to Usage.
Inspector > Findings > All findings
Findings: All findings Info
All findings ranked by severity.
Findings (0)
Export findings
Create suppression rule
Choose a row to see the finding details.
Finding status
Active
Filter criteria
Add filter
Severity
Title
Impacted resource
Type
Age
Status
No findings
No findings to display.


Search [Alt+S]
United States (Oregon)
Account ID: 4153-0299-7546
voclabs/user4473058=Mokgadi_Selepe
Findings
By vulnerability
By instance
By container image
By container repository
By Lambda function
All findings
Code security New
Export SBOMs
Suppression rules
On-demand scans
CIS scans
Vulnerability database search
Account management
Resources coverage
General settings
EC2 scanning settings
ECR scanning settings
Usage
Inspector > Findings > All findings
Findings: All findings Info
All findings ranked by severity.
Findings (3)
Export findings
Create suppression rule
Choose a row to see the finding details.
Finding status
Closed
Filter criteria
Add filter
Severity
Title
Impacted resource
Type
Age
Status
Medium
CVE-2023-32681 - requests
get-request
Package Vulnerability
2 hours
Closed
Medium
CVE-2024-47081 - requests
get-request
Package Vulnerability
2 hours
Closed
Medium
CVE-2024-35195 - requests
get-request
Package Vulnerability
2 hours
Closed
Inspector > Settings > Account management > Instances
Account management Info
Manage your accounts, and review the coverage of your instances, repositories, images and Lambda functions.
Accounts
Instances
Container repositories
Container images
Lambda functions
Code repositories - New
All
0
Scanning
0
Not scanning
0
Instances (0) Info
Add filter
Resource type EQUALS Amazon EC2 Instance
Clear filters
EC2 instance
EC2 instan...
Account
AMI
Operating...
Last scann...
Status
Monitore...
No instances
No instances to display
Inspector > Settings > Account management > Lambda functions
Account management Info
Manage your accounts, and review the coverage of your instances, repositories, images and Lambda functions.
Accounts
Instances
Container repositories
Container images
Lambda functions
Code repositories - New
Standard scanning
All
2
Scanning
2
Not scanning
0
All (2) Info
Add filter
Resource type EQUALS AWS Lambda Function
Scan type EQUALS PACKAGE
Clear filters
Function name
AWS account
Runtime
Status
Last scanned
Lambda function tags
generate-password-...
415302997546
PYTHON_3_9
Actively monitoring
November 19, 2025 ...
aws:cloudformation:logical-...



I opened the AWS console and searched for Lambda.

I picked the get-request function, opened its code editor, and found the requirements.txt file. I removed the version number (==2.20.0) from the line that said requests==2.20.0 so it just read requests. That tells Lambda to use the latest version of the package. I hit Deploy and a banner popped up saying the function was updated successfully.

Because the function changed, Amazon Inspector started a new scan automatically. I went back to the console, searched for Inspector, and opened the Findings page. I switched the filter from “Active” to “Closed” and saw that CVE-2023-32681 – requests now appears in the closed list, which means the vulnerability has been fixed.

Finally, I looked under Resources coverage → Lambda functions and saw that the last-scanned timestamp for the function was updated, confirming the new scan finished.

Conclusion

I turned on Amazon Inspector and set it up for my account, then I looked at the security problems it found in my Lambda function. After that, I fixed the issues by updating the vulnerable package, so the findings are now closed and my function is secure.