

School of Computer Science, UPES, Dehradun.

Lab 18

DevSecOps Lab

B.TECH. - V Semester

**Submitted to:**

Dr. Hitesh Kumar Sharma

**Submitted by:**

Name: Ishika Mehrotra

Batch: Devops B1

Sap Id: 500124411

Roll No.: R2142230281

**Lab Exercise 18- Scanning IaC Templates for Vulnerabilities**

# Objective

* Learn how to scan Infrastructure as Code (IaC) templates for security vulnerabilities.
* Use open-source IaC security tools to detect misconfigurations.
* Understand common risks such as public access, unencrypted resources, and insecure network rules.

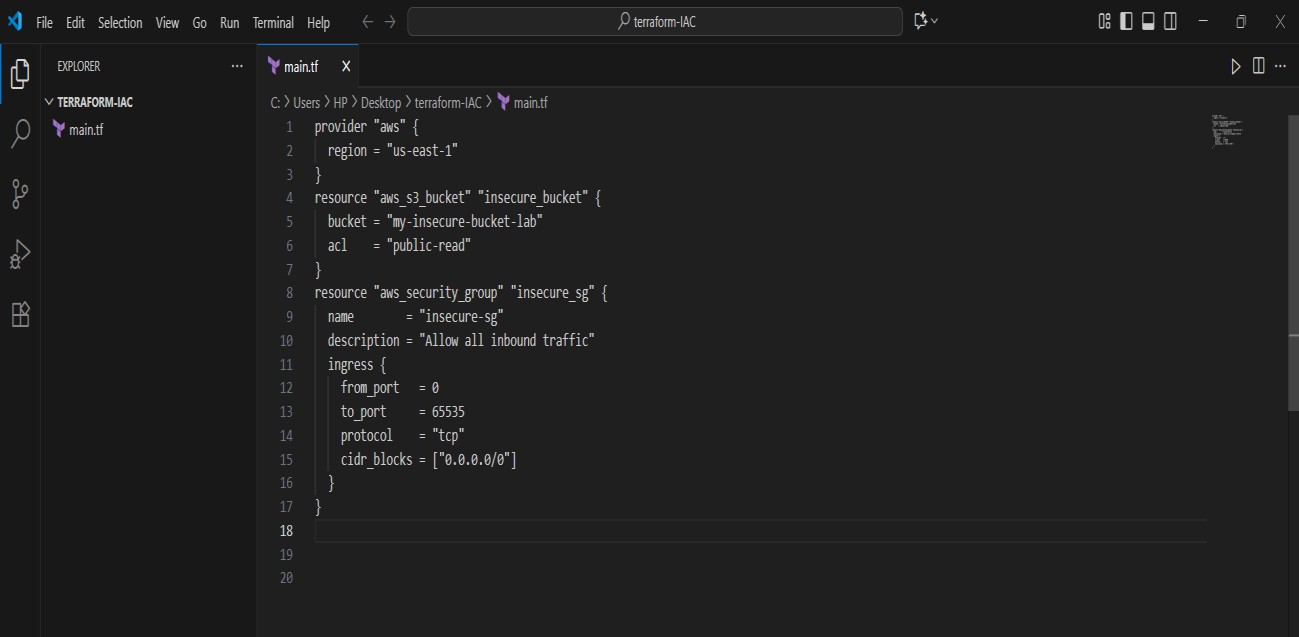
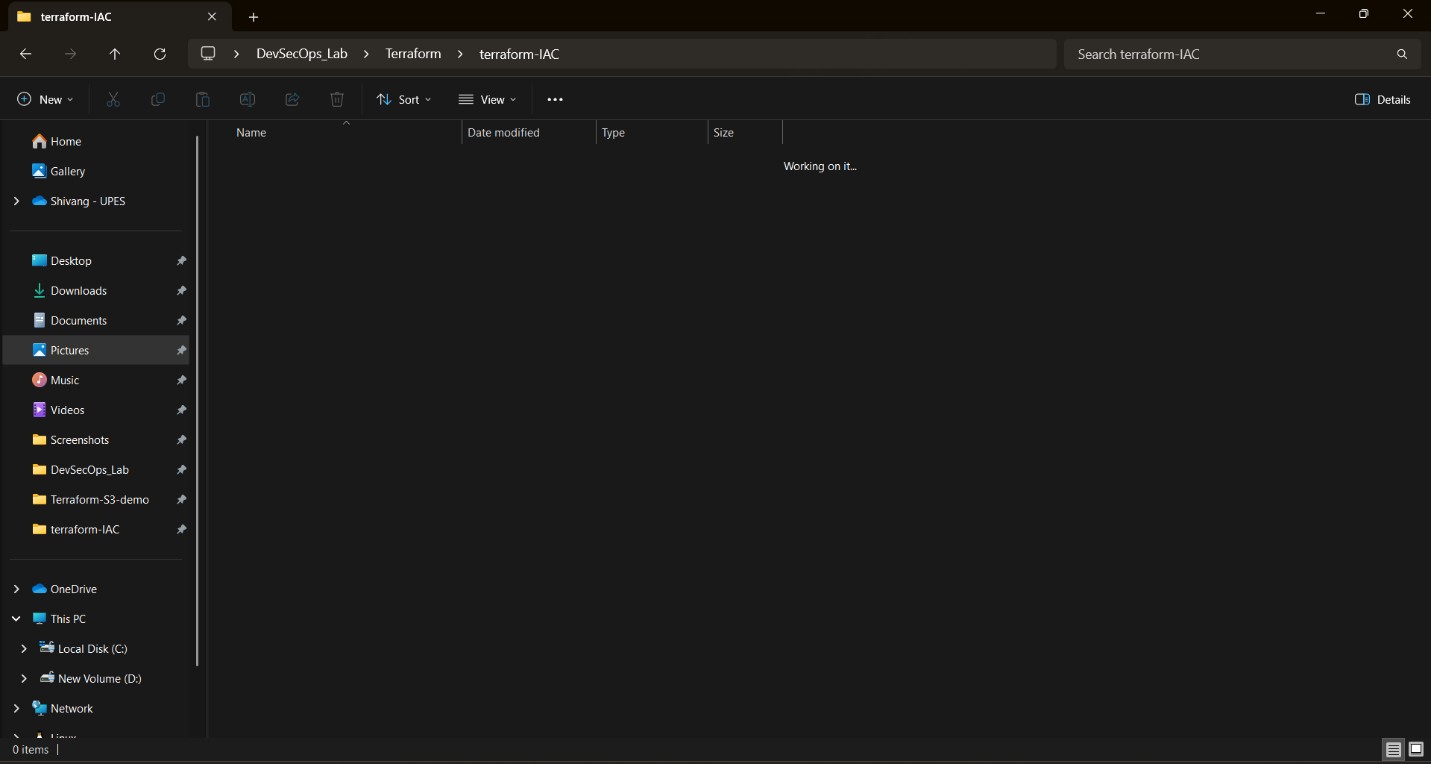
# Prerequisites

* A Linux/Windows/Mac machine with:
  + Terraform installed (for sample IaC)
  + **Checkov** (pip install checkov) or **tfsec** (brew install tfsec or binary download)
* Git installed (optional, for version control of IaC templates)

# Step 1: Create an Insecure IaC Template

Create a file named main.tf with the following Terraform code:

|  |
| --- |
| provider "aws" {  region = "us-east-1"  }  resource "aws\_s3\_bucket" "insecure\_bucket" { bucket = "my-insecure-bucket-lab"  acl = "public-read"  }  resource "aws\_security\_group" "insecure\_sg" { name = "insecure-sg"  description = "Allow all inbound traffic" ingress { from\_port = 0 to\_port = 65535 protocol = "tcp"  cidr\_blocks = ["0.0.0.0/0"]  }  } |



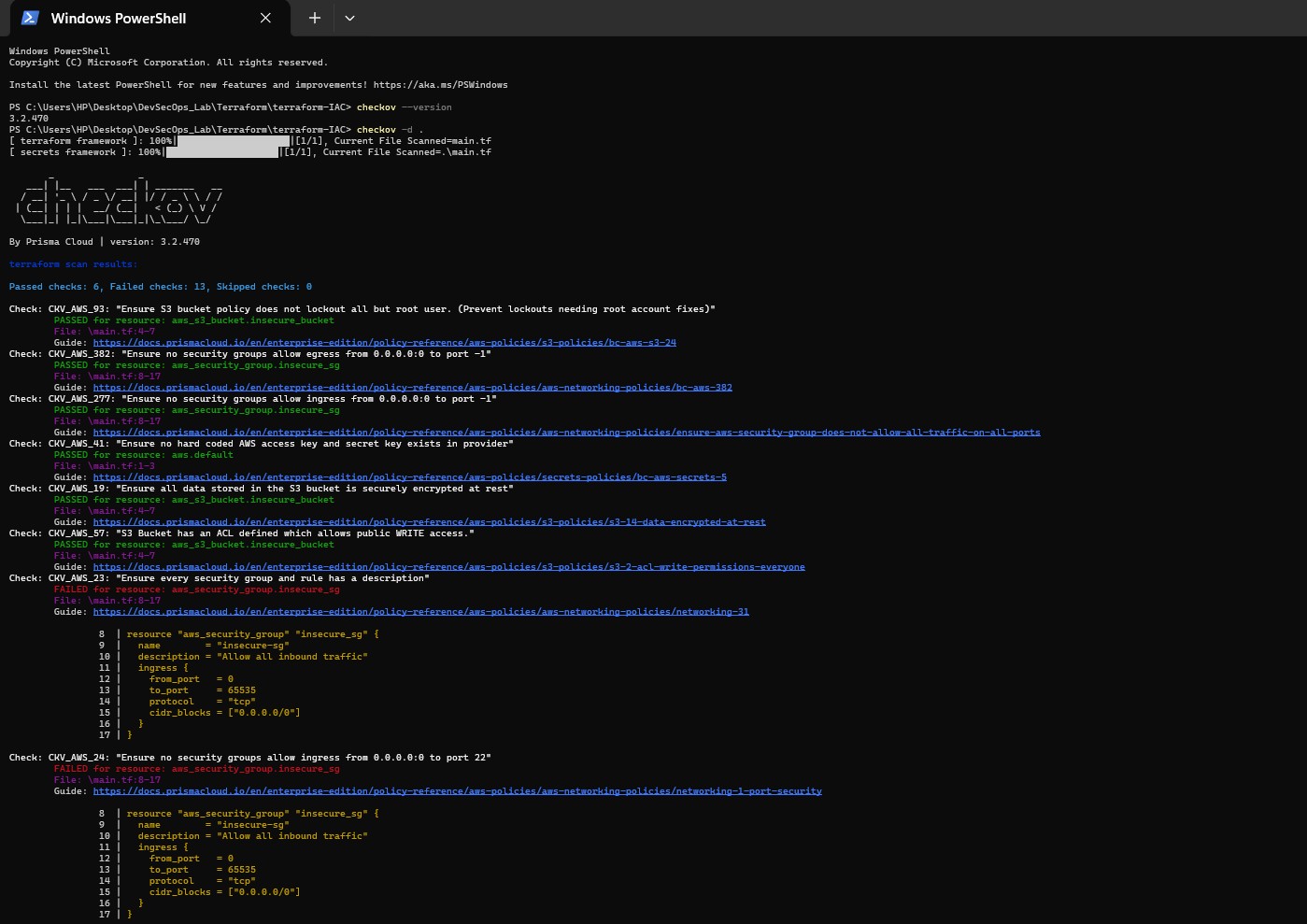
# Step 2: Scan the Template with Checkov

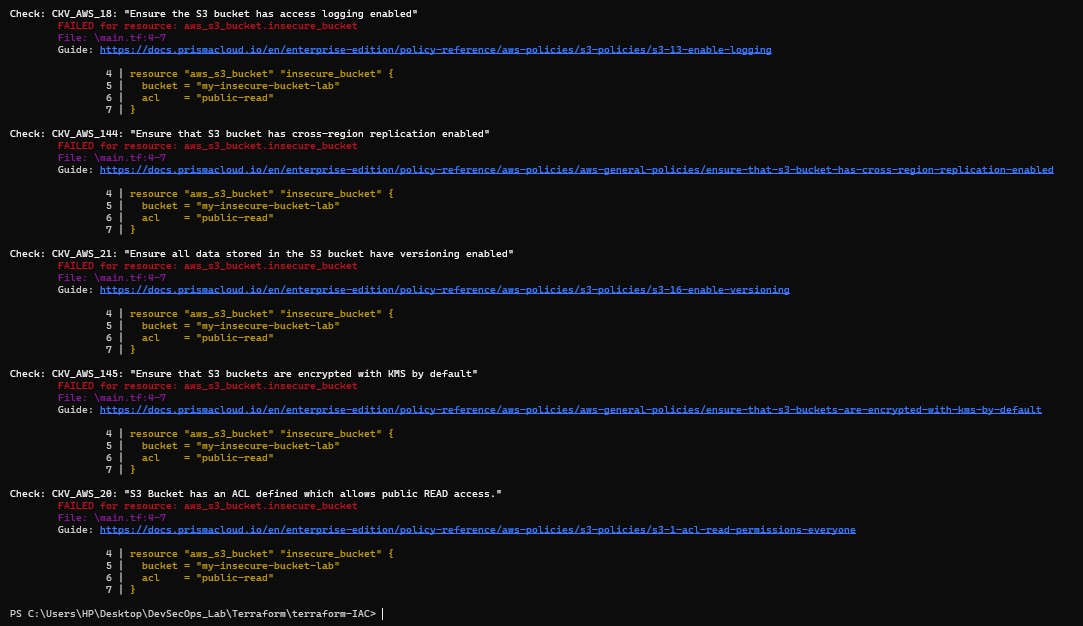
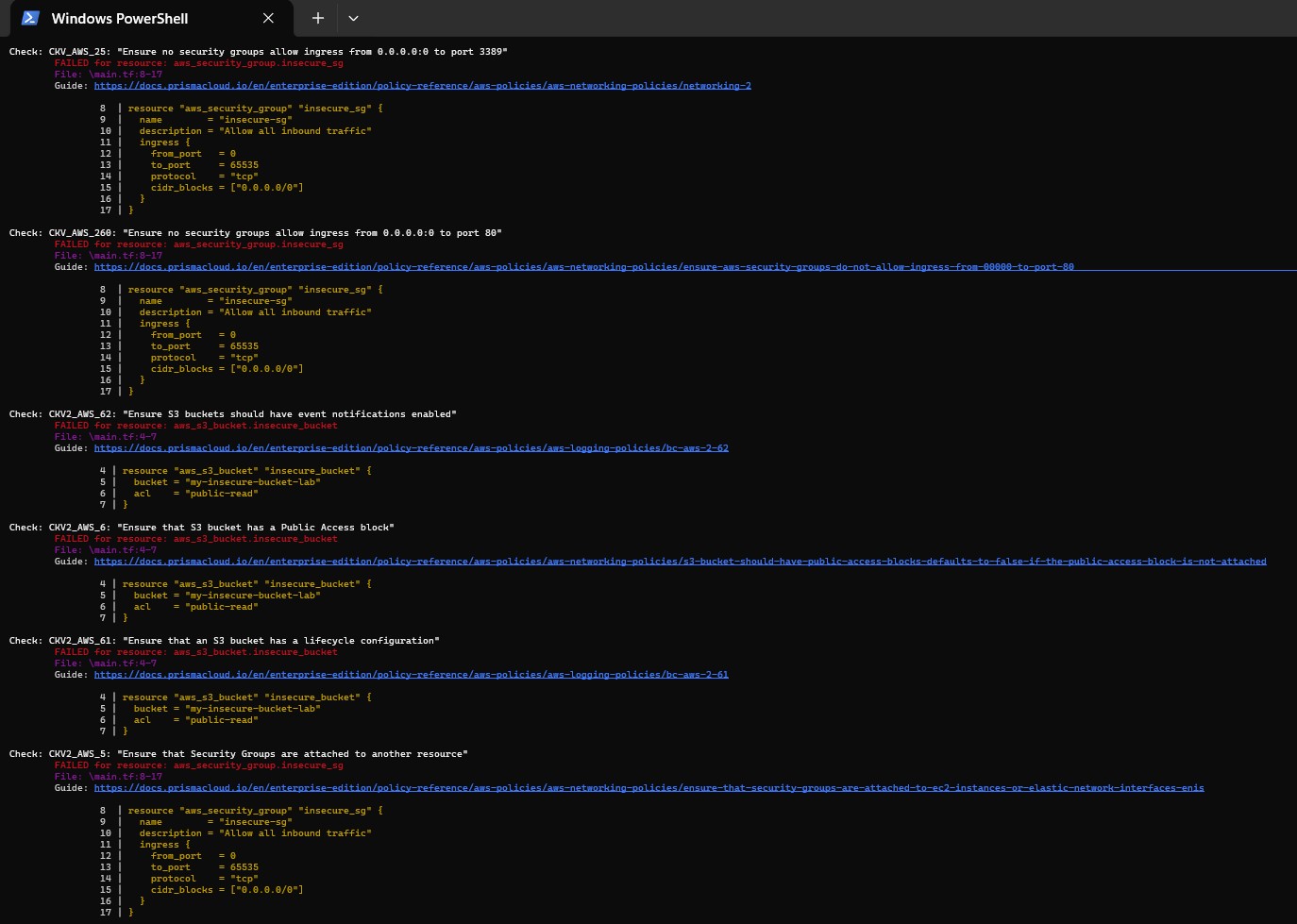
Run Checkov on the current directory:

checkov -d .

**Expected Findings:**

* Public S3 bucket access (public-read)
* Security group open to all inbound traffic **Expected Findings:**
* Warns about S3 bucket without encryption
* Flags open Security Group rules





# Step 3: Review the Report

Example output (Checkov):

Check: CKV\_AWS\_20: "S3 Bucket allows public read access"

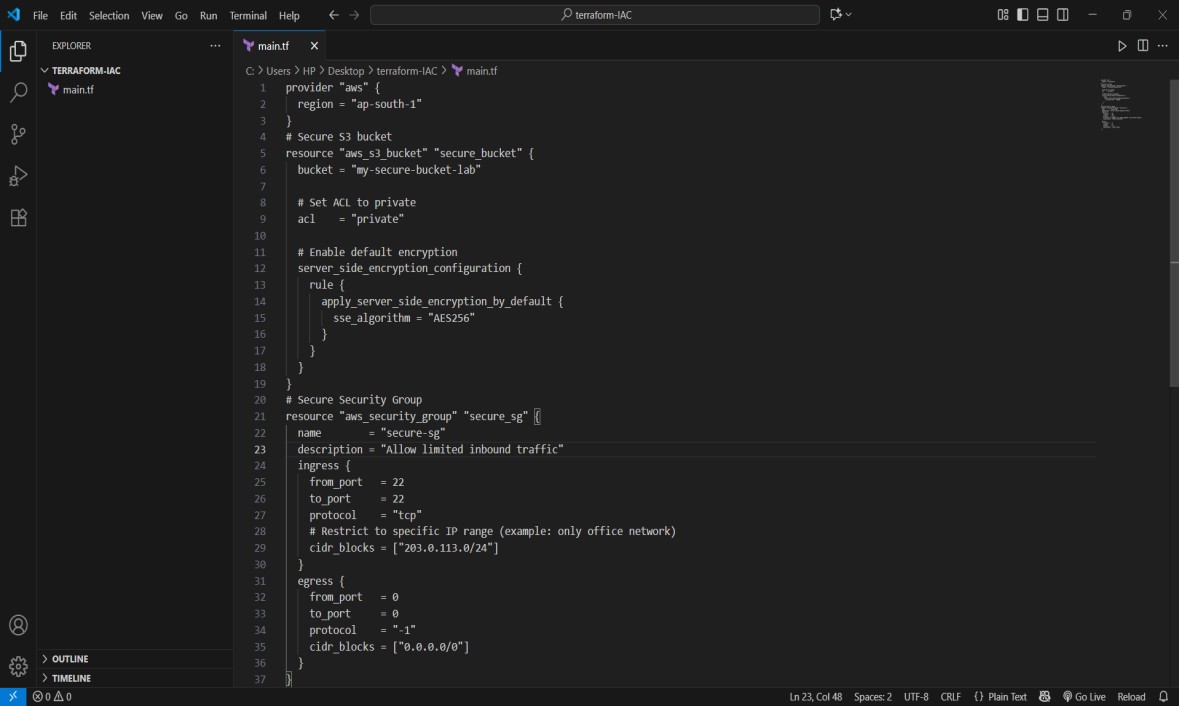
FAILED for resource: aws\_s3\_bucket.insecure\_bucket

Check: CKV\_AWS\_260: "Security group allows ingress from 0.0.0.0/0"

FAILED for resource: aws\_security\_group.insecure\_sg

**Step 4: Apply Fixes (Optional)** Modify the IaC template to:

* Set S3 bucket ACL to private
* Enable encryption (AES256)
* Restrict Security Group to specific IP ranges

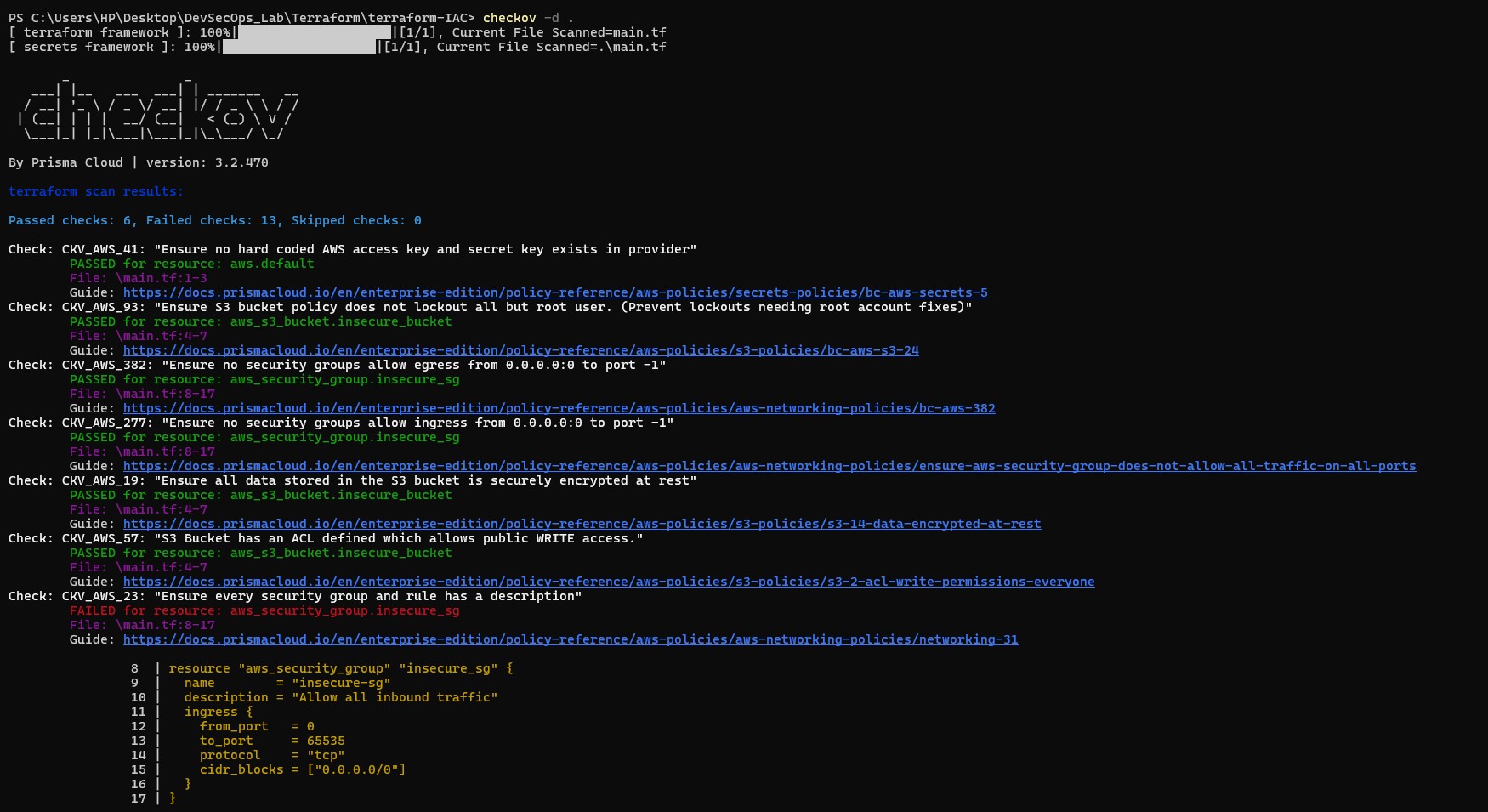


# Step 5: Rescan the Template

Run the scan again:

checkov -d .

Now the findings should be **resolved or reduced**.



# Step 6: Document Findings

Create a simple findings log:

**Findings Log – Terraform IaC**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Resource** | **Issue**  **Detected** | **Risk** | **Fix Applied** |
| 1 | aws\_s3\_bucket.insecure\_bucket | S3 bucket ACL set to  public-read | Public exposure of  data | Changed ACL to  private |
| 2 | aws\_s3\_bucket.insecure\_bucket | No encryption configured | Data at rest not protected | Enabled AES256  server-side encryption |
| **ID** | **Resource** | **Issue**  **Detected** | **Risk** | **Fix Applied** |
| 3 | aws\_security\_group.insecure\_sg | Ingress allows  0.0.0.0/0 on all TCP ports | Full internet  exposure  (critical risk) | Restricted ingress to specific CIDR  (203.0.113.0/24) and limited to port 22 |

