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.

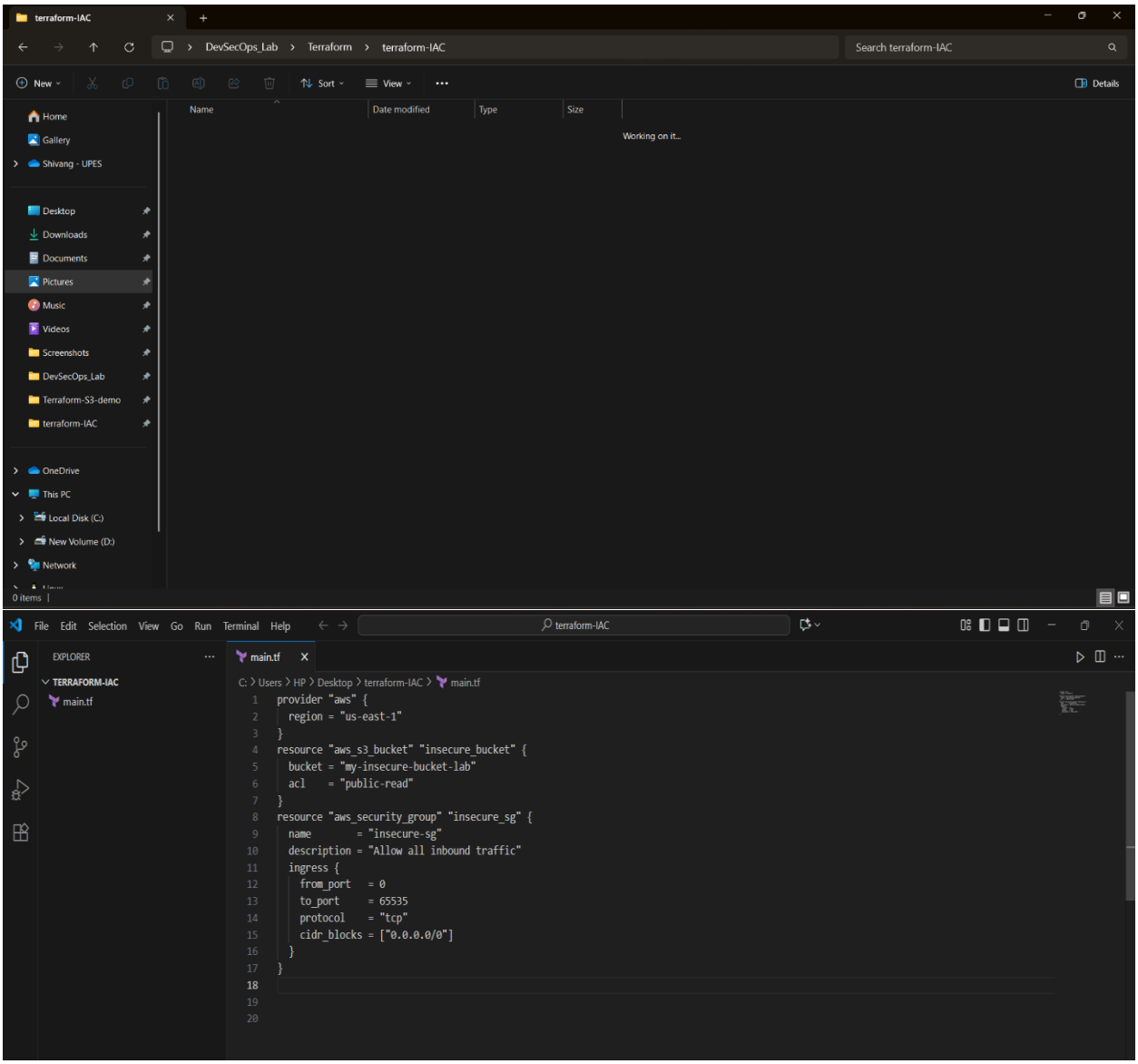
Prerequisites

- 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 .
```

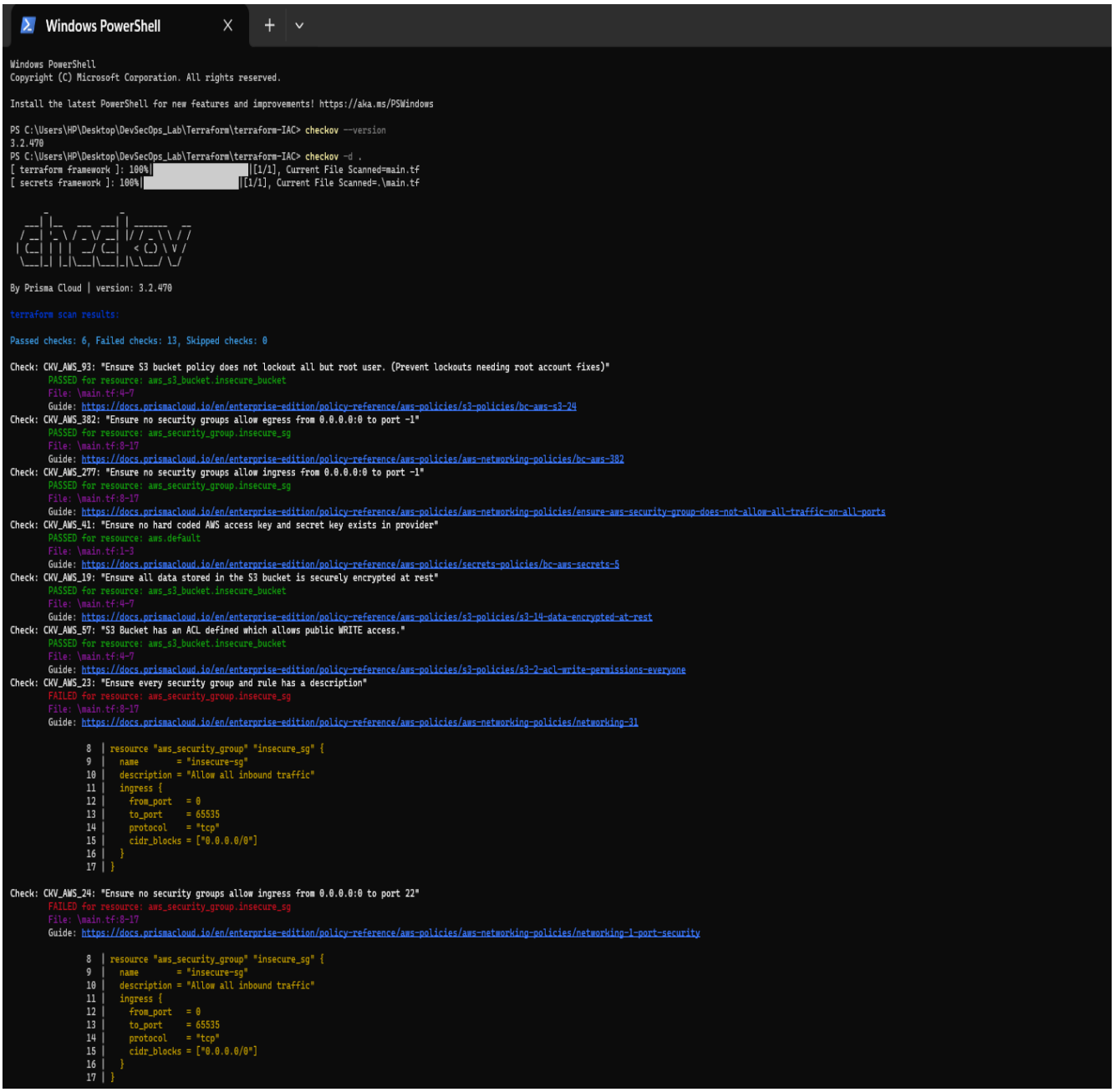
Expected Findings:

- 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




Windows PowerShell
Check: CKV_AWS_25: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 3389"
FAILED for resource: aws_security_group.insecure_sg
File: \main.tf:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/networking-2
8 | resource "aws_security_group" "insecure_sg" {
9 | name = "insecure-sg"
10 | description = "Allow all inbound traffic"
11 | ingress {
12 | from_port = 0
13 | to_port = 65535
14 | protocol = "tcp"
15 | cidr_blocks = ["0.0.0.0/0"]
16 | }
17 | }
Check: CKV_AWS_260: "Ensure no security groups allow ingress from 0.0.0.0:0 to port 80"
FAILED for resource: aws_security_group.insecure_sg
File: \main.tf:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-aws-security-groups-do-not-allow-ingress-from-00000-to-port-80
8 | resource "aws_security_group" "insecure_sg" {
9 | name = "insecure-sg"
10 | description = "Allow all inbound traffic"
11 | ingress {
12 | from_port = 0
13 | to_port = 65535
14 | protocol = "tcp"
15 | cidr_blocks = ["0.0.0.0/0"]
16 | }
17 | }
Check: CKV2_AWS_62: "Ensure S3 buckets should have event notifications enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/bc-aws-2-62
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV2_AWS_6: "Ensure that S3 bucket has a Public Access block"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/s3-bucket-should-have-public-access-blocks-defaults-to-false-if-the-public-access-block-is-not-attached
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV2_AWS_61: "Ensure that an S3 bucket has a lifecycle configuration"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-logging-policies/bc-aws-2-61
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV2_AWS_5: "Ensure that Security Groups are attached to another resource"
FAILED for resource: aws_security_group.insecure_sg
File: \main.tf:8-17
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-networking-policies/ensure-that-security-groups-are-attached-to-ec2-instances-or-elastic-network-interfaces-enis
8 | resource "aws_security_group" "insecure_sg" {
9 | name = "insecure-sg"
10 | description = "Allow all inbound traffic"
11 | ingress {
12 | from_port = 0
13 | to_port = 65535
14 | protocol = "tcp"
15 | cidr_blocks = ["0.0.0.0/0"]
16 | }
17 | }
Check: CKV_AWS_18: "Ensure the S3 bucket has access logging enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-13-enable-logging
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV_AWS_144: "Ensure that S3 bucket has cross-region replication enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-s3-bucket-has-cross-region-replication-enabled
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV_AWS_21: "Ensure all data stored in the S3 bucket have versioning enabled"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-16-enable-versioning
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV_AWS_145: "Ensure that S3 buckets are encrypted with KMS by default"
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/aws-general-policies/ensure-that-s3-buckets-are-encrypted-with-kms-by-default
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
Check: CKV_AWS_20: "S3 Bucket has an ACL defined which allows public READ access."
FAILED for resource: aws_s3_bucket.insecure_bucket
File: \main.tf:4-7
Guide: https://docs.prismacloud.io/en/enterprise-edition/policy-reference/aws-policies/s3-policies/s3-1-acl-read-permissions-everyone
4 | resource "aws_s3_bucket" "insecure_bucket" {
5 | bucket = "my-insecure-bucket-lab"
6 | acl = "public-read"
7 | }
PS C:\Users\HP\Desktop\DevSecOps_Lab\Terraform\terraform-IAC>

Step 3: Review the Report

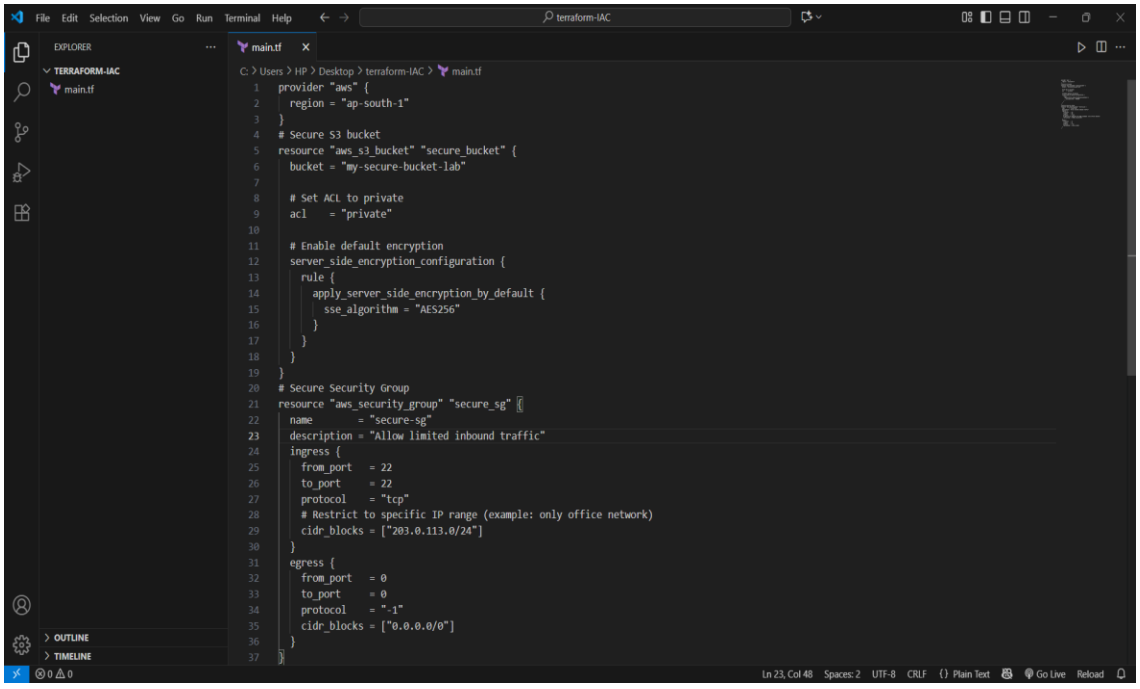
Example output (Checkov):

```
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

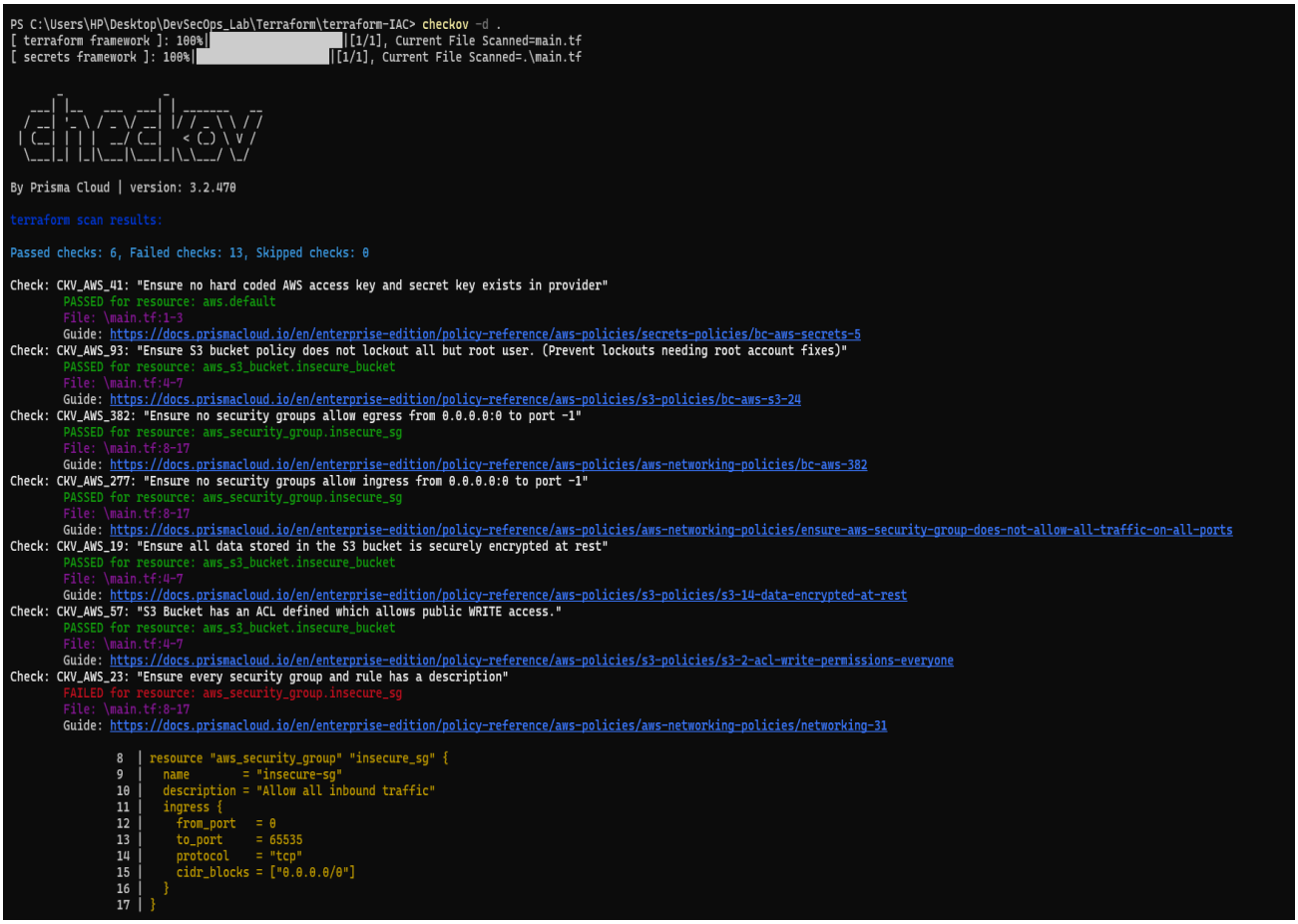


Step 5: Rescan the Template

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