# CloudSploit Security Assessment Summary

Date: 2025-04-17 13:09:45

This document summarizes the findings from a CloudSploit security assessment.

## Summary of Findings

- Total Issues Found: 8  
- Critical: 1  
- High: 3  
- Medium: 2  
- Low: 2

## Detailed Findings and Recommendations

### IAM: Root Account Usage

Severity: Critical

Description: The root account was used for API calls. This is highly discouraged due to the unrestricted access it provides.

Recommendation: Create IAM users for daily tasks and restrict root account usage. Enable MFA for root.

### S3: Bucket Permissions - Public Access

Severity: High

Description: One or more S3 buckets are publicly accessible.

Recommendation: Use bucket policies to restrict access and block public access at the account and bucket levels.

### EC2: Unused Security Groups

Severity: High

Description: There are security groups not attached to any instance.

Recommendation: Remove unused security groups to reduce configuration sprawl and avoid confusion.

### IAM: Password Policy Weak

Severity: Medium

Description: The IAM password policy is too lenient and may allow weak passwords.

Recommendation: Enforce strong password requirements and enable password expiration policies.

### CloudTrail: Not Integrated with CloudWatch Logs

Severity: Medium

Description: CloudTrail is not configured to send logs to CloudWatch Logs.

Recommendation: Integrate CloudTrail with CloudWatch for real-time monitoring and alerting.

### RDS: Publicly Accessible Instances

Severity: Low

Description: Some RDS instances are publicly accessible.

Recommendation: Ensure RDS instances are not publicly accessible unless explicitly required.

### Lambda: Functions Without Timeout Set

Severity: Low

Description: Some Lambda functions have no timeout defined, risking indefinite execution.

Recommendation: Define appropriate timeout values for Lambda functions.

### CloudTrail: Not Enabled in All Regions

Severity: High

Description: CloudTrail is not enabled in all AWS regions.

Recommendation: Enable CloudTrail in all regions to ensure complete visibility into account activity.