

## S3 Public Access Scanner (Moto-Compatible)

**Author:** Daniel Chisasura

**Version:** 1.0

**License:** MIT






**Platform:** Python 3.x

**Dependencies:** boto3, botocore, Moto (for local testing)

### Overview

This Python script scans all S3 buckets in an AWS account (or Moto mock environment) and identifies buckets with public access granted via Access Control Lists (ACLs). It's designed to help developers and security teams detect misconfigured buckets that may expose sensitive data.

### Features

-  Lists all S3 buckets and checks their ACLs
-  Flags buckets with public access (AllUsers group)
-  Compatible with Moto for safe local testing
-  Handles access errors gracefully
-  Provides a clear summary of findings

### Usage

#### 1. Install Dependencies:

```
pip install boto3 botocore moto
```

#### 2. Start Moto Server:

```
moto_server s3 -p 5000
```

### 3. Run the Script:

```
python s3_public_access_scanner.py
```

#### Configuration

The script is preconfigured to use Moto's local endpoint:

```
endpoint_url='http://127.0.0.1:5000'
```

```
aws_access_key_id='testing'
```

```
aws_secret_access_key='testing'
```

```
region_name='us-east-1'
```

To use with real AWS credentials, remove the `endpoint_url` and replace with valid credentials or use IAM roles.

#### Sample Output

```
🔍 Starting scan for public S3 buckets...
```

```
Checking bucket: example-bucket...
```

```
Checking bucket: public-bucket...
```

-----

```
✅ Scan complete.
```

```
🚨 The following S3 buckets are PUBLICLY ACCESSIBLE:
```

```
- public-bucket
```

---

## Lessons Learned

- **ACLs can expose data:** Always audit bucket permissions.
- **Moto is great for testing:** Avoids accidental changes in production.
- **Error handling matters:** AccessDenied errors are common in real-world audits.
- **Automation improves security hygiene:** Regular scans help catch misconfigurations early.

## Disclaimer

This script is intended for educational and administrative use. Always verify flagged buckets before taking action to avoid disrupting legitimate access.