[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@0edfe42b5fbc4a768699aaa348d59867?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Summary**

Cloud storage services facilitate web application and services to store and access objects in the storage service. Improper access control configuration, however, may result in sensitive information exposure, data being tampered, or unauthorized access.

A known example is where an Amazon S3 bucket is misconfigured, although the other cloud storage services may also be exposed to similar risks. By default, all S3 buckets are private and can be accessed only by users that are explicitly granted access. Users can grant public access to both the bucket itself and to individual objects stored within that bucket. This may lead to an unauthorized user being able to upload new files, modify or read stored files.

**Test Objectives**

* Assess that the access control configuration for the storage services is properly in place.

**How to Test**

First identify the URL to access the data in the storage service, and then consider the following tests:

* read the unauthorized data
* upload a new arbitrary file

You may use curl for the tests with the following commands and see if unauthorized actions can be performed successfully.

To test the ability to read an object:

curl -X GET https://<cloud-storage-service>/<object>

To test the ability to upload a file:

curl -X PUT -d 'test' 'https://<cloud-storage-service>/test.txt'

**Testing for Amazon S3 Bucket Misconfiguration**

The Amazon S3 bucket URLs follow one of two formats, either virtual host style or path-style.

* Virtual Hosted Style Access

https://bucket-name.s3.Region.amazonaws.com/key-name

In the following example, my-bucket is the bucket name, us-west-2 is the region, and puppy.png is the key-name:

https://my-bucket.s3.us-west-2.amazonaws.com/puppy.png

* Path-Style Access

https://s3.Region.amazonaws.com/bucket-name/key-name

As above, in the following example, my-bucket is the bucket name, us-west-2 is the region, and puppy.png is the key-name:

https://s3.us-west-2.amazonaws.com/my-bucket/puppy.jpg

For some regions, the legacy global endpoint that does not specify a region-specific endpoint can be used. Its format is also either virtual hosted style or path-style.

* Virtual Hosted Style Access

https://bucket-name.s3.amazonaws.com

* Path-Style Access

https://s3.amazonaws.com/bucket-name

Identify Bucket URL

For black-box testing, S3 URLs can be found in the HTTP messages. The following example shows a bucket URL is sent in the img tag in a HTTP response.

...  
<img src="https://my-bucket.s3.us-west-2.amazonaws.com/puppy.png">  
...

For gray-box testing, you can obtain bucket URLs from Amazon's web interface, documents, source code, or any other available sources.

Testing with AWS-CLI

In addition to testing with curl, you can also test with the AWS Command-line tool. In this case s3:// protocol is used.

List

The following command lists all the objects of the bucket when it is configured public.

aws s3 ls s3://<bucket-name>

Upload

The following is the command to upload a file

aws s3 cp arbitrary-file s3://bucket-name/path-to-save

This example shows the result when the upload has been successful.

$ aws s3 cp test.txt s3://bucket-name/test.txt upload: ./test.txt to s3://bucket-name/test.txt

This example shows the result when the upload has failed.

$ aws s3 cp test.txt s3://bucket-name/test.txt upload failed: ./test2.txt to s3://bucket-name/test2.txt An error occurred (AccessDenied) when calling the PutObject operation: Access Denied

Remove

The following is the command to remove an object

aws s3 rm s3://bucket-name/object-to-remove

**Tools**

* [AWS CLI](https://aws.amazon.com/cli/)