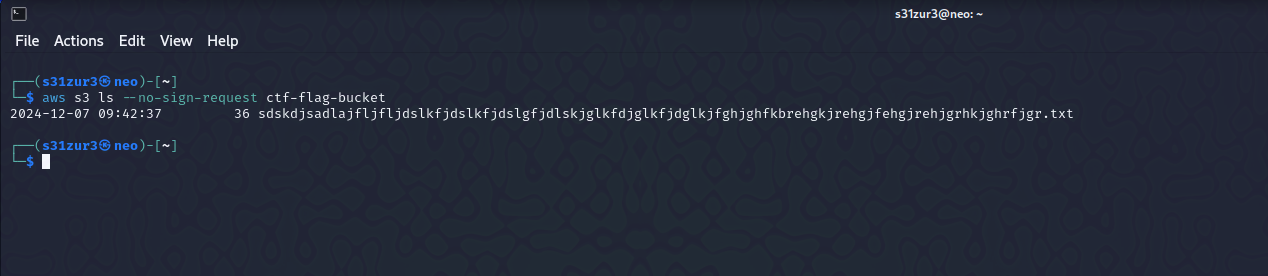
**Misconfigured Bucket**

**Tools used:**

Awscli

**Steps:**

1. Use the cmd “aws s3 ls –no-sign-request ctf-flag-bucket” to list the contents.



1. aws s3 buckets have a specific url structure https://<bucket>.<region>.s3.amazonaws.com/<key>, so I just put in the bucket name and the obtained file name and ended up with this <https://ctf-flag-bucket.s3.amazonaws.com/sdskdjsadlajfljfljdslkfjdslkfjdslgfjdlskjglkfdjglkfjdglkjfghjghfkbrehgkjrehgjfehgjrehjgrhkjghrfjgr.txt>.

**Flag:** r00t@localhost{wh0\_st0le\_my\_c00kies}

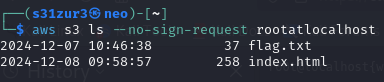
**S3crets**

**Tools Used:**

awscli

**Steps:**

1. Use the cmd “aws s3 ls –no-sign-request rootatlocalhost” to get the contents.



1. Substitute flag.txt in place of index.html and we end up with <https://rootatlocalhost.s3.us-east-1.amazonaws.com/flag.txt> .

**Flag:** r00t@localhost{s3\_bucket\_leaked\_data}