Task 4: Questions and Analysis:

- What additional architectural change can be made to reduce the internet-facing attack surface of the web application instance.

* Assuming the IAM permissions for the S3 bucket are still insecure, would creating VPC private endpoints for S3 prevent the unauthorized access to the secrets bucket.

**Best Practice**: Using VPC end Points: with VPC endpoints, the data between the VPC and S3 is transferred within the amazon network, and protects from internet traffic. VPC endpoints for S3 adds additional security control to help limit access to S3 buckets. You can control what buckets, requests, users, or groups are allowed through a specific VPC endpoint.

* Will applying default encryption setting to the s3 buckets encrypt the data that already exists?
* No encrypting the S3 bucket will not encrypt the already existing data.
* The changes you made above were done through the console or CLI; describe the outcome if the original cloud formation templates are applied to this environment?
* When we go back to cloud formation and check the stack info, the drift status is drifted. All manual changes will be lost.