ACIT 4630 – Assignment 1 – Keep Secrets Secret!

Note: This is an individual assignment

Use `docker-compose` to create a WordPress stack:

https://github.com/docker/awesome-compose/tree/master/official-documentation-samples/wordpress/

Steps

1. Set-Up

Use the above tutorial to create your `docker-compose`

Take note of your docker- compose file, particularly the environment variables.

Run `docker-compose up -d` and then navigate to `localhost:80` to view your WordPress installation.

If you see WordPress configuration your setup is complete! (You don't need to continue further for this assignment)

2. Explore

Bash into your running WordPress container. (You need to find the id of the container that's running the WordPress image first by `docker ps`)

```
docker exec -it <container_id> bash
```

or alternatively, use docker desktop to get CLI access to the container and run /bin/bash

Using bash, print off your environment variables. Hint: printenv

Questions:

- Include screenshots of:
  - Your running docker containers (i.e., docker ps)
  - Your running Wordpress application in your browser
- As you've noticed we've put some credentials in the docker-compose file using environment variables. Imagine that this file ends up in source control. What is the potential security risk?
- List three good development practices that GitGaurdian has suggested to avoid leaking credentials with this docker setup.
- Go through this link https://docs.docker.com/compose/environment-variables/ and explain how we can use an environment file instead of exposing credentials in the docker-compose file given above? (Provide code snippet and commands)

Submission:

Submit your report, with the screenshots and answers to the questions above, to the Assignment 1 drop box on the Learning Hub before Week 5 class.