Markus Afonso
Set C
January 30, 2024

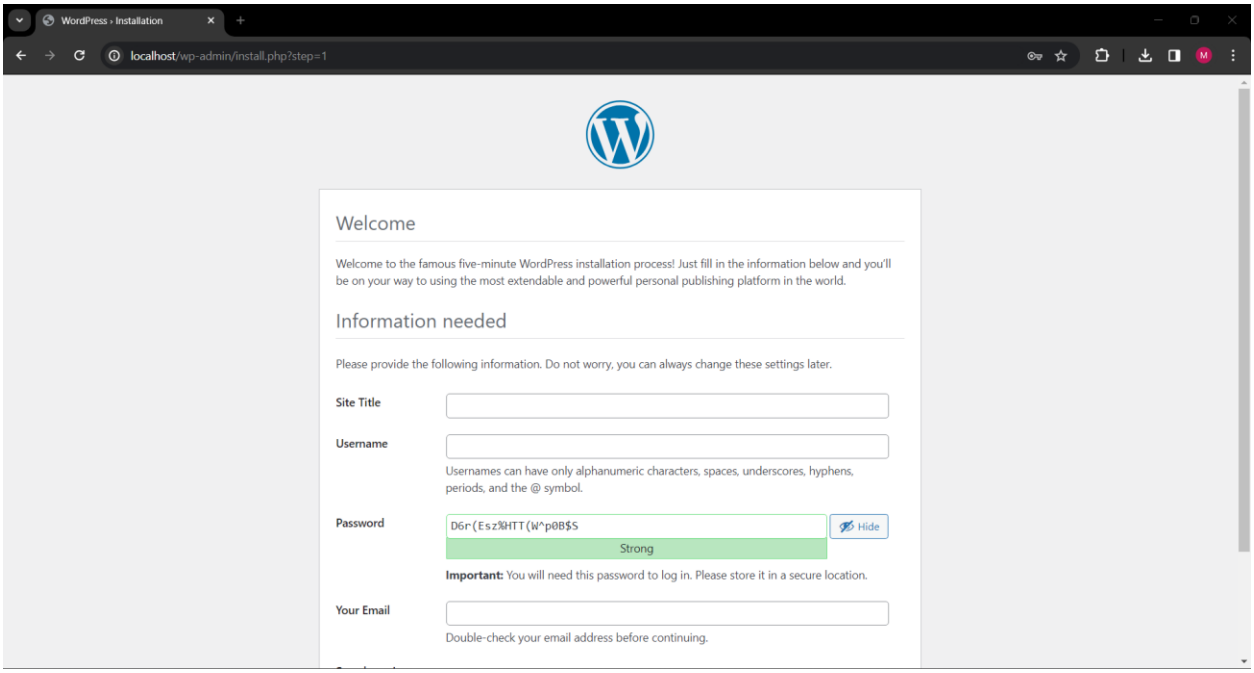
Questions:

Screen shot of docker containers:

```
~\OneDrive - BCIT\Desktop on  (us-west-1)
❯ docker ps -a
CONTAINER ID   IMAGE                COMMAND                  CREATED         STATUS         PORTS                  NAMES
6c2a90ef4f6d   mariadb:10.6.4-focal   "docker-entrypoint.s…"   6 minutes ago   Up 6 minutes   3306/tcp, 33060/tcp    my_wordpress-db-1
fa18cfb62b2c   wordpress:latest       "docker-entrypoint.s…"   6 minutes ago   Up 6 minutes   0.0.0.0:80->80/tcp     my_wordpress-wordpress-1

~\OneDrive - BCIT\Desktop on  (us-west-1)
❯
```

Screenshot of Wordpress application in 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?

There is a high security risk with having secrets contained within the docker-compose file. If this ends up in source code, anyone with access to the source code can also gain access to the SQL container we created. Any individuals gain that have access to the source code repository, can retrieve the Docker Compose file and obtain the sensitive credentials. Or, if the repository is public, an attacker could easily gain unauthorized access to the SQL container and compromise the database, leading to data breaches, unauthorized modifications, or other malicious activities.

Three development practices that GitGaurdian has suggests

1. Name sensitive files in .gitignore and .npmignore

   In our case, we would add the docker-compose file in the .gitignore, so it is not added to the repository.

2. Store your secrets in a safer place

GitGaurdian recommends using local environment variables, storing secrets encrypted in a git repository, or using a "secrets as a service" solution like Hashicorp's Vault or Square's Keywhiz.

3. Whitelist your Ips

   In our case, we could attach the docker containers to a network and only allow communication to the SQL container from the wordpress container by only allowing the IP of the wordpress container.

Using an environment file

We can protect our secrets by using a .env file. We can store our secrets here, and reference them in our docker-compose file using ${variable}. Then, we can add the .env file to our .gitignore so that it's not included in the code repository. By doing this, we can keep the secrets private on our local machine. Notice the difference in the docker-compose file and the new .env file:

.env file:

```
❯ cat .env
MYSQL_ROOT_PASSWORD=somewordpress
MYSQL_DATABASE=wordpress
MYSQL_USER=wordpress
MYSQL_PASSWORD=wordpress
WORDPRESS_DB_HOST=db
WORDPRESS_DB_USER=wordpress
WORDPRESS_DB_PASSWORD=wordpress
WORDPRESS_DB_NAME=wordpress
```

New docker-compose file:

```
❯ cat docker-compose.yml
services:
  db:
    # We use a mariadb image which supports both amd64 & arm64 architecture
    image: mariadb:10.6.4-focal
    # If you really want to use MySQL, uncomment the following line
    #image: mysql:8.0.27
    command: '--default-authentication-plugin=mysql_native_password'
    volumes:
      - db_data:/var/lib/mysql
    restart: always
    environment:
      - MYSQL_ROOT_PASSWORD=${MYSQL_ROOT_PASSWORD}
      - MYSQL_DATABASE=${MYSQL_DATABASE}
      - MYSQL_USER=${MYSQL_USER}
      - MYSQL_PASSWORD=${MYSQL_PASSWORD}
    expose:
      - 3306
      - 33060
  wordpress:
    image: wordpress:latest
    volumes:
      - wp_data:/var/www/html
    ports:
      - 80:80
    restart: always
    environment:
      - WORDPRESS_DB_HOST=${WORDPRESS_DB_HOST}
      - WORDPRESS_DB_USER=${WORDPRESS_DB_USER}
      - WORDPRESS_DB_PASSWORD=${WORDPRESS_DB_PASSWORD}
      - WORDPRESS_DB_NAME=${WORDPRESS_DB_NAME}
volumes:
  db_data:
  wp_data:
```

The commands to run the docker-compose file stays the same, and the containers boot up the same as before:

```
ACIT-4630-Info-Assurance-and-Security\as1\my_wordpress on  main [!?] on  (us-west-1)
❯ docker compose up -d
[+] Running 33/33
 ✓ db 10 layers [##########]      0B/0B      Pulled                                                                    39.9s
   ✓ 7b1a6ab2e44d Pull complete                                                                                       13.1s
   ✓ 034655750c88 Pull complete                                                                                       10.8s
   ✓ f0b757a2a0f0 Pull complete                                                                                       11.8s
   ✓ 5c37daf8b6b5 Pull complete                                                                                       12.6s
   ✓ b4cd9409b0f6 Pull complete                                                                                       12.2s
   ✓ dbcda06785eb Pull complete                                                                                       12.8s
   ✓ a34cd90f184c Pull complete                                                                                       12.9s
   ✓ fd6cef4ce489 Pull complete                                                                                       13.1s
   ✓ 3cb89a1550ea Pull complete                                                                                       17.0s
   ✓ df9f153bd930 Pull complete                                                                                       13.5s
 ✓ wordpress 21 layers [####################]      0B/0B      Pulled                                                    55.5s
   ✓ 2f44b7a888fa Pull complete                                                                                        6.4s
   ✓ 3a95dcec6035 Pull complete                                                                                        0.4s
   ✓ e22afa33f327 Pull complete                                                                                       17.1s
   ✓ 1aa61ea11ee8 Pull complete                                                                                        0.8s
   ✓ ea67ae2bde33 Pull complete                                                                                        2.4s
   ✓ ff5356c6468f Pull complete                                                                                        2.7s
   ✓ 5e91cb51e886 Pull complete                                                                                        3.1s
   ✓ 935e88b21d5f Pull complete                                                                                        4.6s
   ✓ 8202e883ada1 Pull complete                                                                                        5.0s
   ✓ be40d3507d33 Pull complete                                                                                        6.3s
   ✓ 5fac4c1a6ab6 Pull complete                                                                                        6.6s
   ✓ 03fcb105f703 Pull complete                                                                                        6.8s
   ✓ 87c6b0d7fa4d Pull complete                                                                                        7.0s
   ✓ 7b595acbbcdc Pull complete                                                                                       10.6s
   ✓ 9097ed91daa0 Pull complete                                                                                       10.3s
   ✓ 4796aa9f1a89 Pull complete                                                                                       10.2s
   ✓ 8edd6604ce7d Pull complete                                                                                       10.5s
   ✓ 9b37f9713fe2 Pull complete                                                                                       10.7s
   ✓ 581954acac8f Pull complete                                                                                       12.4s
   ✓ 6073502d7819 Pull complete                                                                                       10.9s
   ✓ 879585ec90c2 Pull complete                                                                                       11.0s
[+] Running 3/3
 ✓ Network my_wordpress_default        Created                                                                          0.0s
 ✓ Container my_wordpress-wordpress-1  Started                                                                          0.3s
 ✓ Container my_wordpress-db-1         Started                                                                          0.3s

ACIT-4630-Info-Assurance-and-Security\as1\my_wordpress on  main [!?] on  (us-west-1) took 56s
❯ docker ps -a
CONTAINER ID   IMAGE                COMMAND                  CREATED              STATUS              PORTS                  NAMES
81e0989ca761   wordpress:latest     "docker-entrypoint.s…"   About a minute ago   Up About a minute   0.0.0.0:80->80/tcp     my_wordpress-wordpress-1
51242ab713fc   mariadb:10.6.4-focal "docker-entrypoint.s…"   About a minute ago   Up About a minute   3306/tcp, 33060/tcp    my_wordpress-db-1
```