

**Finding Name: Database Credentials stored in clear text**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Natalia Khobotova | SCR | CSR Junior Lead | Ontrack |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
|  |

**Finding Description**

The MariaDB credentials, including the root password, database name, username, and password, are stored in clear text within the .devcontainer\devcontainer.env

**Risk Rating**  
Impact: Major  
Likelihood: Minor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

Storing database credentials in clear text poses a significant risk to the company and the application. If an unauthorised individual gains access to these credentials, they could potentially compromise the integrity, confidentiality, and availability of the company's data. This could lead to data breaches, unauthorised access to sensitive information, and potential financial and reputational damage to the company.

**Affected Assets**

* MariaDB database
* Application data stored in the MariaDB database

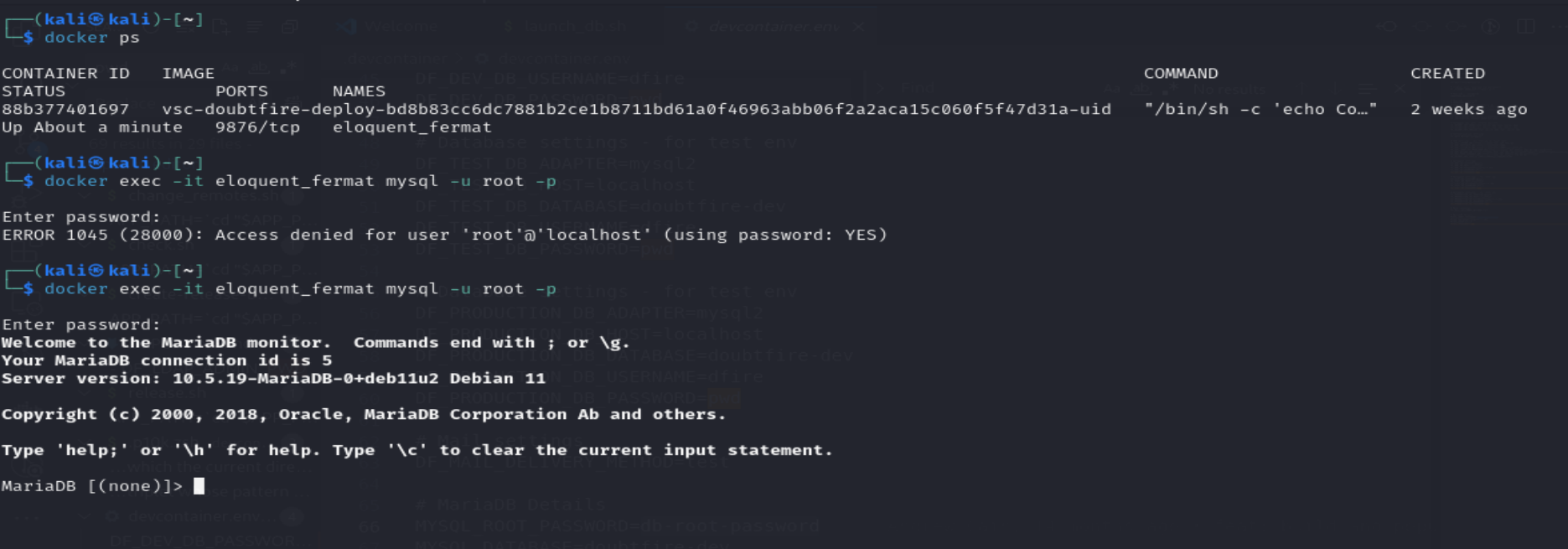
**Evidence**

**Step 1**. Navigate to .devcontainer\devcontainer.env (line 66)A screenshot of a computer

Description automatically generated

**Step 2.** List running docker containers, to get the name of the container (docker ps)

**Step 3.** Use the name (eloquent\_fermat) and access MariaDB using the credentials in the devcontainer.dev (password: db-root-password)

You can now perform any queries – list and delete or add users

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

**Remediation Advice**

**Encrypt Database Credentials**:

Encrypt the MariaDB credentials. Use a secure and trusted encryption mechanism to encrypt the credentials. Only decrypt the credentials when necessary for database access.

**Secure Access to Credentials:**

Restrict access to the .devcontainer\devcontainer.env file. Ensure that only authorised personnel can access this file by using file system permissions to restrict access.

**Implement Secrets Management with Docker:**

Utilise Docker secrets to securely manage and store sensitive information, such as database credentials. Docker secrets provide a built-in way to manage sensitive data in Docker Swarm clusters or services. Using Docker secrets, sensitive information is securely passed to Docker services without exposing the data in the compose file or environment variables.

**References**

*Manage sensitive data with Docker secrets*. (n.d.). Retrieved from docs.docker.com: https://docs.docker.com/engine/swarm/secrets/

*Securing Passwords in Docker*. (2023, November 6). Retrieved from www.baeldung.com/: https://www.baeldung.com/ops/docker-securing-passwords

**Contact Details**

• Natalia Khobotova

• s223011356@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.