

**Finding Name: Use of Hardcoded Credentials**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Shamail Haider | SCR | Senior Team Member | Ontrack | Jaspriya Kaur and Payas Paul |  |
|  |  |  |  |  |  |

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

**Finding Description**

Hardcoded credentials (CWE 798) are a security flaw in which critical authentication credentials (e.g., usernames, passwords, API keys) are integrated directly into an application's source code, making them easily available to anybody with code access. This is a major security risk that can result in unauthorised access, data breaches, and other security problems.

**Risk Rating**  
Impact: Minor  
Likelihood: Unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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**

**Affected Assets**

Identify assets that are affected by this vulnerability.

doubtfire-web\src\app\api\services\spec\user.service.spec.ts

**Evidence**

**A screen shot of a computer

Description automatically generated**

**Remediation Advice**

Avoid hardcoding sensitive data such as usernames and passwords straight into the source code. This method improves security and flexibility by isolating configuration data from application logic.

+ host: mysqlconfig.host,

user: mysqlconfig.username,

**References**

CWE-798: Use of Hard-coded Credentials, <https://cwe.mitre.org/data/definitions/798.html>

<https://owasp.org/www-community/vulnerabilities/Use_of_hard-coded_password>

**Contact Details**

Shamail Haider

S222408241@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.