

**Finding Name: Information leakage (Email id & Database user id)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| DEV PATEL | PT | Project member | Ontrack | Nabiha Masood and Oliver Power |  |
|  |  |  |  |  |  |

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

**Finding Description**

Information leakage/ Inconsistent Masking: - The application was found to be masking sensitive fields inconsistently, such as email addresses and database user IDs, is being exposed in client-server communications during the web application's penetration testing. This sensitive data is contained in some server responses, which could be intercepted and used by attackers.

**Risk Rating**  
Impact: Significant  
Likelihood: Certain

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

Impacts like -

* Privacy Breach: - Email ID exposure can result in privacy violations and harm user privacy.
* Database security: - By disclosing user IDs, attackers may be able to target specific users through database infrastructure and obtain access without authorization or manipulating data.

**Affected Assets**

* User information stored in the application database.
* Database infrastructure and associated data.

**Evidence**

Steps guide on how to reproduce the vulnerability with screenshots

**Step 1: - Login with student user then select task from any current enrolled units (COS10001 – task 8.1P) and send message to tutor from right side of window.**

**A screenshot of a computer

Description automatically generated**

**Step 2: - Capture the request in burp-suite**

**A screenshot of a computer

Description automatically generated**

**Step 3: - Observe the response in which you will find the data consisting of user id and email id of tutor.**

**A screenshot of a computer

Description automatically generated**

**Step4: - Repeat same for another unit task (COS20007 – task 16) and will get the different tutor data.**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Step5: - So, it happens in every task of different units (COS30046 – task 2).**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Step6: - Can verify the user id with User base by login with admin user.**

**A screenshot of a computer

Description automatically generated**

**Remediation Advice**

* Mask Sensitive Data: -Implement data masking techniques to obfuscate sensitive information such as email IDs and database user IDs. This involves replacing actual data with placeholder characters or random values, ensuring that the original information is not exposed
* Minimize Data Exposure: -Review server responses and ensure that they do not include sensitive information that could be exploited. Minimize the amount of data exposed to the client.

**References**

Burp-suite

**Contact Details**

DEV PATEL – s222622553@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.