

**Finding Name: Broken Access Control**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Shayne Dawson | PT | Team member | Ontrack | Natalia Khobotova | Yes |
|  |  |  |  |  |  |

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

**Finding Description**

Broken Access Controls allows student accounts to view admin pages that should be restricted to admin account only access. The student access can’t modify anything inside the pages but can view the pages which is an exploit called broken access control.

**Risk Rating**  
Impact: Minor  
Likelihood: Moderate

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

Broken Access Controls are policies that stop users from accessing resources outside of their intended audience. This discloses information that a regular user account should not have access to and should be locked behind the administrator panel. The information exposed can be used in mapping a website and seeing what information is locked behind administrative access. The student account can’t modify anything but if an attacker was to gain access to an account that could, it knows two access points it can test.

**Affected Assets**

**Web application - OnTrack**

<http://localhost:4200/#/admin/teaching-periods>

http://localhost:4200/#/admin/institution-settings

**Evidence**

Provide a step by step guide on how to reproduce the vulnerability with screenshots

**Step 1. Login as a regular student account.**

A screenshot of a computer

Description automatically generated

**Step 2. Access the above URLs.**

A screenshot of a computer

Description automatically generated

**Step 3.**

**Webpage loads.**

**Remediation Advice**

* Deny any access to this website and only allow admin accounts to even view it. They should be locked behind an admin panel.
* Log when users outside of the administrator group access these webpages.

**References**

https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/

**Contact Details**

SHAYNE DAWSON

dawsonsh@deakin.edu.au

**Pentest Leader Feedback.**

HI Shayne, great job! The instructions are straightforward to follow, and the exploit is easy to replicate. Could you please review your affected assets section? It should include components or parts on the app vulnerable to the finding