

**Finding Name: privilege escalation**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Byeongnam Choe | SCR | Project Member | Ontrack | Nabiha Masood |  |
|  |  |  |  |  |  |

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

**Finding Description**

Privilege escalation is an attack designed to gain unauthorized privileged access to a system. The OnTrack app generates an 'auth\_token' every time a user logs into the web app. The 'auth\_token' should not be used on different accounts however, OnTrack fails to block users from reusing the auth\_token. Moreover, an 'auth\_token' generated under a student account can be used on an admin account, which could cause a privilege escalation attack. OnTrack checks the username aligned with the auth\_token when accessing web pages on the admin account, but certain pages, including 'teaching period' and 'activity\_types,' fail to check the auth\_token.

**Risk Rating**  
Impact: Major  
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**

This vulnerability could allow a threat actor to access and take advantage of the system by escalating their privileges. The threat actor could manipulate data, access user information, and compromise the entire system, as they can gain entry into the admin account. This could damage the company's reputation and have a serious impact on both users and the company itself.

**Affected Assets**

User information

Web application

Web data

**Evidence**

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

Step1.

**Launch the Burp Suite to capture the tokens**

**A screenshot of a computer

Description automatically generated**

**Click “next” to create a project**

**A screenshot of a computer

Description automatically generated**

**Click “start Burp” to start the Burp Suite**

**A screenshot of a computer

Description automatically generated**

**Go to “proxy tab” and click “open browser” to open OnTrack.**

**A screenshot of a computer

Description automatically generated**

**Step 2: Log into “student\_1” account to capture the “auth\_token”**

Student token: 7nJocd4sDwsfebKzFa\_o

A screenshot of a computer

Description automatically generated

**Step3:**

**Then log into “aadmin” account to capture its “auth\_token” and verify that app generate different “auth\_token”**

**A screenshot of a login form

Description automatically generated**

Admin token: puF1\_dt49pUnyrfn4sUz

A screenshot of a computer

Description automatically generated

**Step4:**

**Go to “teaching period” page to capture source code and send it to repeaterA screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated**

A screenshot of a computer

Description automatically generated

**Confirm that OnTrack fail to block the request as I use student auth\_token**

**Activity\_types:**

A screenshot of a computer

Description automatically generated

**Normal response:**

A screenshot of a computer

Description automatically generated

**Remediation Advice**

Implement an authentication system to ensure that the system verifies the "auth\_token" against the corresponding account. Also, verify the "auth\_token" to ensure that low privilege accounts cannot access high privilege resources

**References**

Burp Suite

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

Thanks for your submission.

Please write up in detail about more on Remediation Advice (one-liner isn’t enough).

Format the report nicely, make it presentable and easy to read.

Elaborate more on each step and the evidence screenshot attached. For example, Step1: Launch Burpsuit, Step2: Login, Step3: Retreive authentication token and so on... while also adding one or two-liners to the steps to explain.