Finding Name: Privilege Escalation, tutor accessing admin sites

Name	Team	Role	Project	Quality Assurance	Is this a re-tested Finding?
Jackson Anton Bouwman	AppAttack	Pen-Tester	OnTrack Web App	Darryl Ooi	No

Was this Finding Successful?
Yes

Finding Description

Issue: The admin institution settings pages are accessible to unauthorized users. This is a result of inadequate access control mechanism for sensitive URLs.

How: From the home page as a tutor, manually entering the path in the browsers URL and gained access. Through this, authentication can be bypassed granting access to administrator pages.

Risk Rating

Impact: Minor
Likelihood: High

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

Administrative actions were unsuccessful not allowing access to any sensitive data. The Broken Access Control allowing lower-level users to access administrative endpoints presents both an operational and representative risk. If an attacker can chain this vulnerability with others or if further authentication bypasses are discovered, the attacker would then be able to access and modify sensitive data. This data includes that of user information which if accessed will have a detrimental effect on user trust in the application and Deakin, with the risk of Personally Identifiable Information being exposed which would result in likely legal implications.

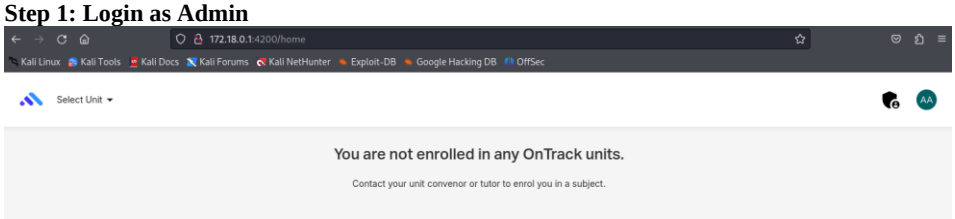
Affected Assets

OnTrack Web API:

- Endpoint: http://172.18.0.1:4200/admin/units
- Endpoint: http://172.18.0.1:4200/admin/institution-settings
- Endpoint: http://172.18.0.1:4200/admin/users
- Role: Tutor

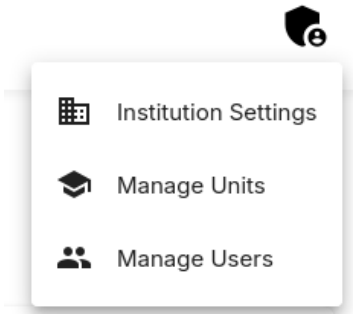
Evidence

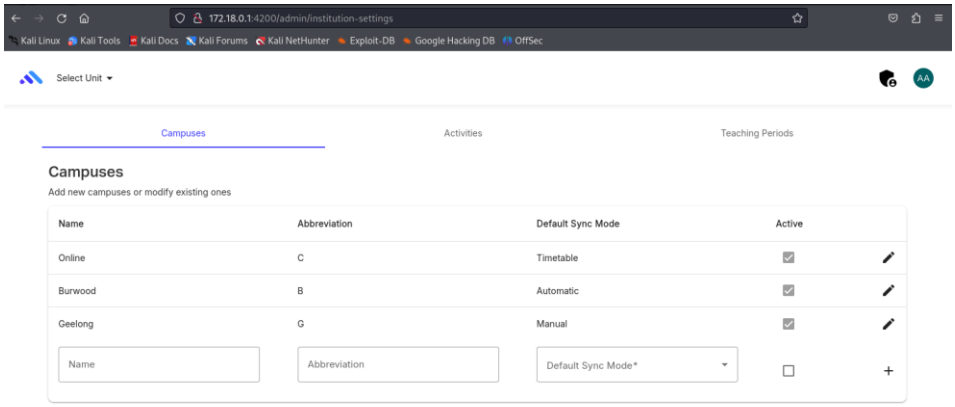
Step 1: Login as Admin



Enter the login credentials for the admin being aadmin and password, then you will be redirected to the home page.

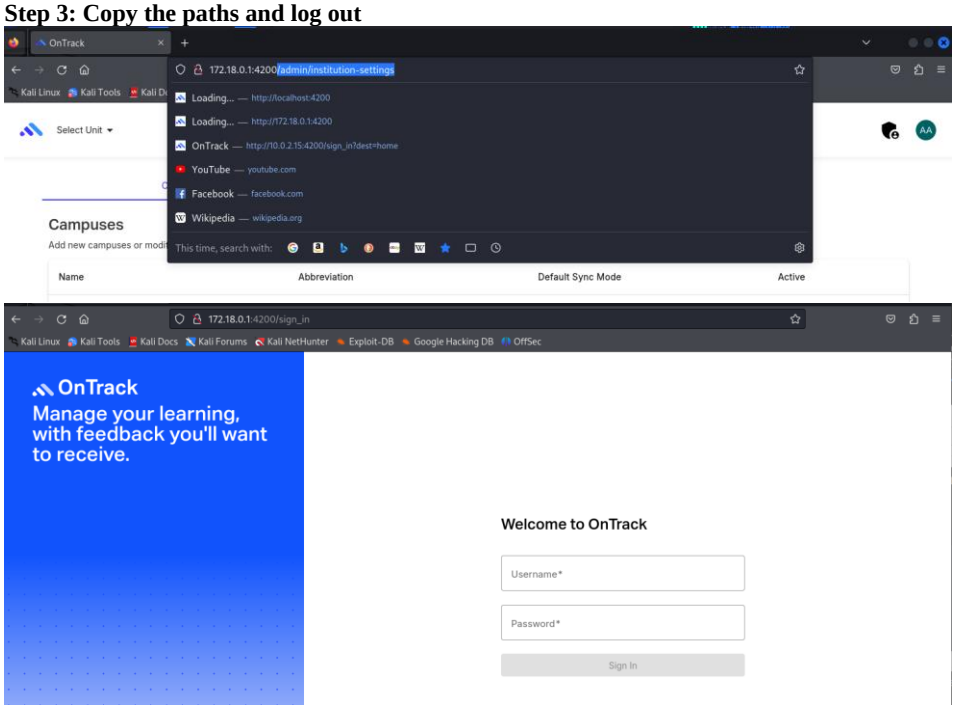
Step 2: Navigate to the sensitive pages





Click the 1st icon on the top right and click on institution settings, then the same for manage units and manage users

Step 3: Copy the paths and log out



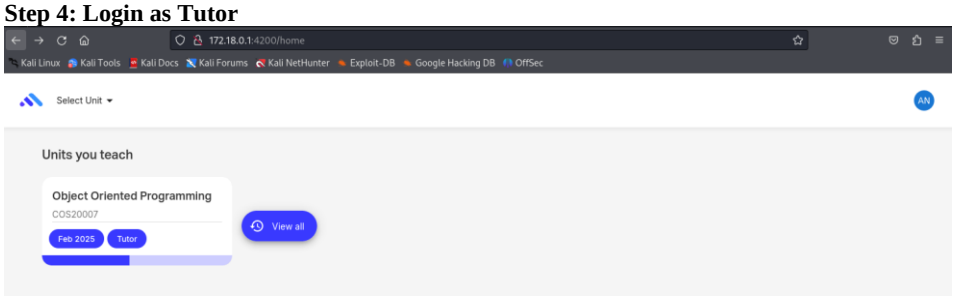
Keep the window open and open a new ontrack page in another tab then log out. You should have the following links.

http://172.18.0.1:4200/admin/units

http://172.18.0.1:4200/admin/institution-settings

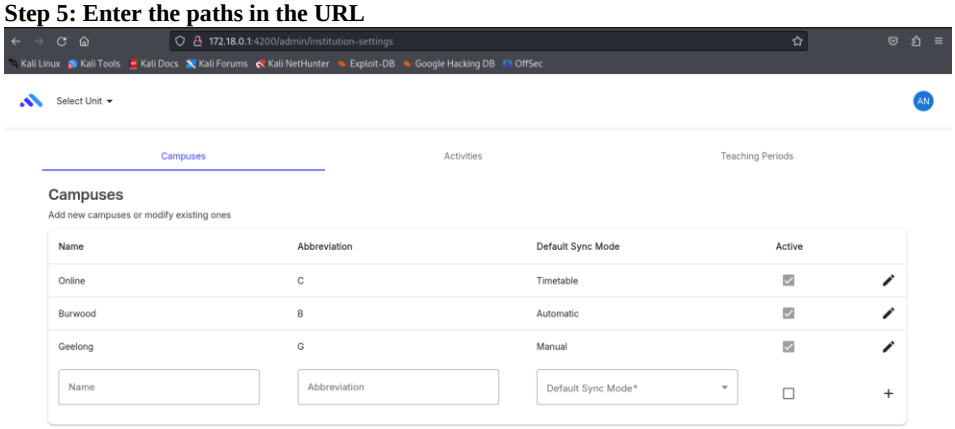
http://172.18.0.1:4200/admin/users

Step 4: Login as Tutor



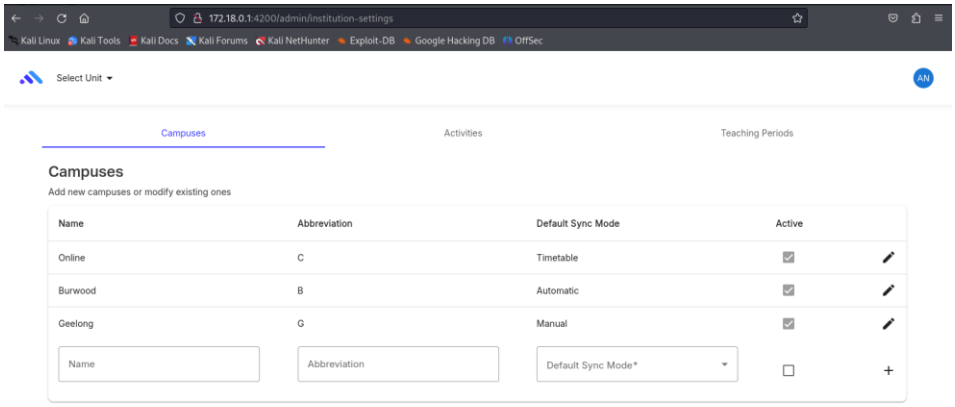
Enter the login credentials for the tutor being atutor and password, then you will be redirected to the home page.

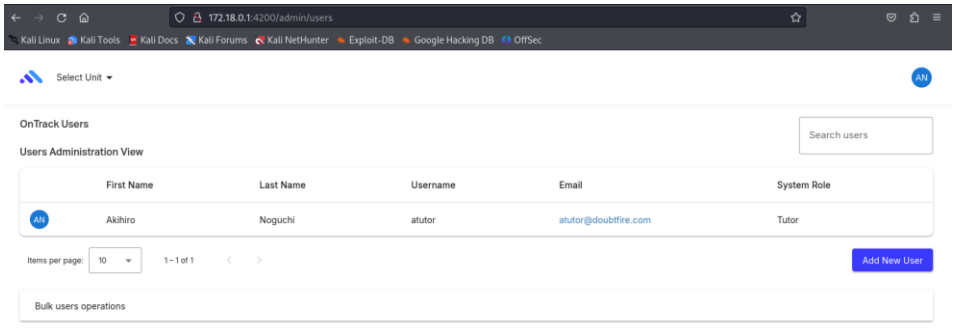
Step 5: Enter the paths in the URL

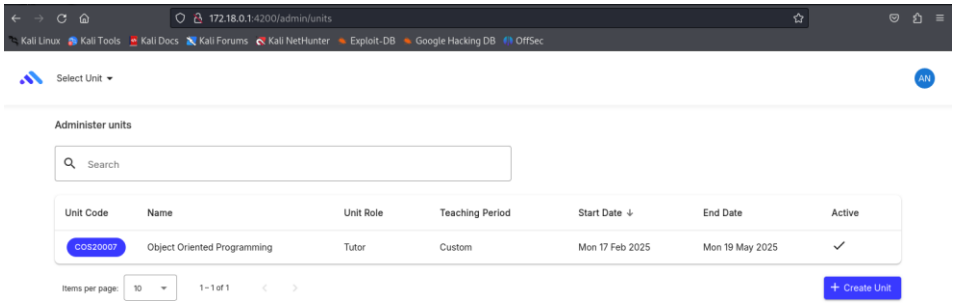


Enter the path to the admin path in the URL being /admin/institution-settings etc then be redirected

Step 6: Be redirected to the admin pages







Although there isn't any sensitive data and no modifications can be applied to the page, the tutor account has elevated privileges enabling the access to the admin pages.

Remediation Advice

The vulnerability arises due to inadequate access control measures, in this case a tutor was able to manually access the admin institution settings page via the URL.

To avoid this specifically, input validation must be implemented on URL paths, verifying user roles against the URL request. Another action that can be taken is the implementation of multi-factor authentication for administrative users accessing privileged pages. Using HTTP 403 Forbidden for unauthorised attempts to access sensitive URLs with minimal information displayed in these messages is another action that can be taken to keep sensitive information secure.

References

No tools required:
Login atutor , password
Path to enter admin/institution-settings

Contact Details

Jackson Anton Bouwman
Student, Deakin university
S222238893@deakin.edu.au

Pentest Leader Feedback.

- Please rename the document to follow the naming conventions outlined in the findings workflow document.
- Please change all the blue text to black.
- Role and project were incorrect, which I have fixed for you.
- Provide more information and details in your finding description. Also mention the specific URL/endpoints.
- In the risk rating section, impact and likelihood should just be single words as shown below:

- In the evidence section, demonstrate how you were able to find the /admin/institution-settings endpoint to be used for privileged access.
- Please demonstrate successful modification of the Campuses, Activities, and Teaching Periods which you claimed possible in the evidence description. I was unable to do this in my testing. Thus, if it is not possible to modify these, please adjust all sections of your report to reflect this and reassess your impact risk rating.
- Don't use localhost address use one of the other two external network addresses and using localhost provides higher access. Use the 10.0.01 or the other
- @JACKSON ANTON BOUWMAN

Commented [DO1]: @JACKSON ANTON BOUWMAN