Finding Name: Insecure Direct Object Reference (IDOR) – Unauthorized Access to Staff Information

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

Was this Finding Successful?
Yes

Finding Description

An **IDOR vulnerability** was discovered in the OnTrack web application, which allows a student-level authenticated user to access sensitive staff information by manipulating API request parameters. The endpoint /api/units/{unit_id} returns full details of the academic staff members associated with any unit, including their:

- Full names
- Email addresses
- Roles (Convenor, Tutor)
- Usernames and nicknames

This data is returned without any access control or role-based filtering, violating the principle of least privilege.

Risk Rating

Impact: **Major**

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

The exposure of personally identifiable information (PII) like staff email addresses and usernames increases the risk of targeted phishing, identity theft, and social engineering attacks. It undermines user privacy, breaks compliance with data protection laws (e.g., GDPR), and could erode user trust in the platform, especially from academic staff.

Affected Assets

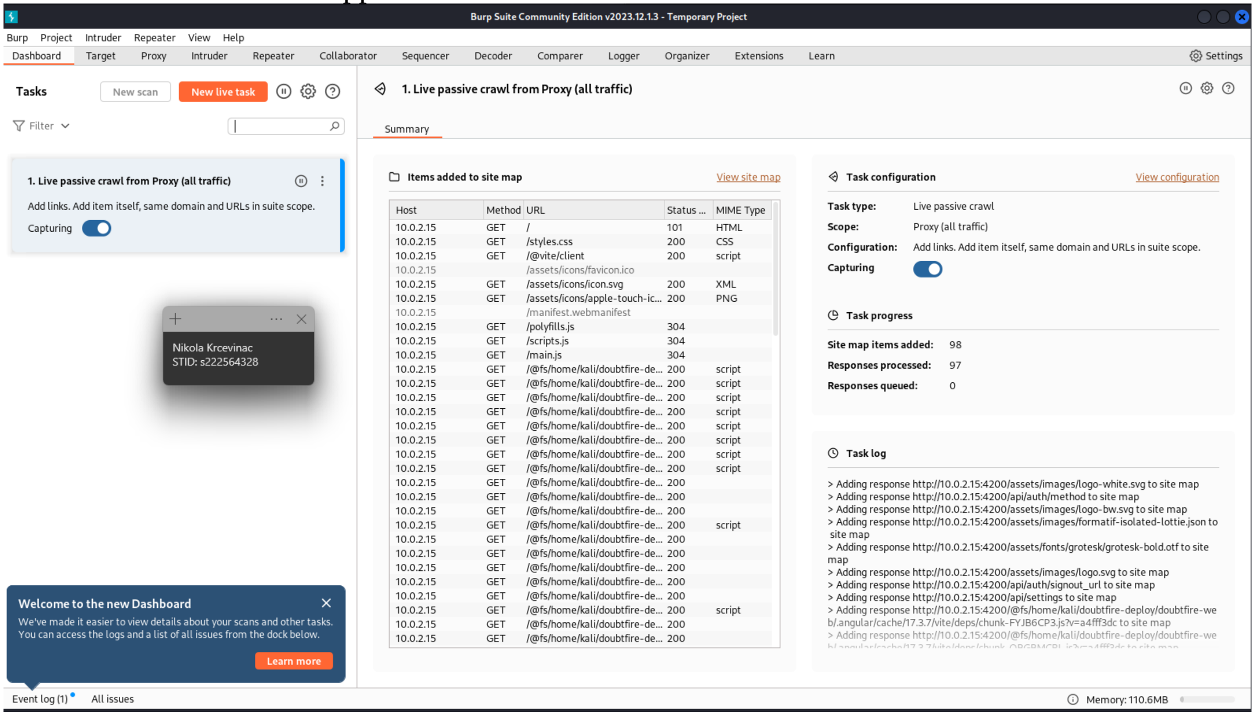
OnTrack Web API:

- Endpoint: GET /api/units/{unit_id}
- Role: Affects *all users* with access to the platform, especially student users gaining unintended access.

Evidence

Step 1: Configure Burp Suite

1. Make sure to install and have burp suite running as Burp Suite set to intercept and map live traffic from the OnTrack application:


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
Settings
Tasks
New scan
New live task
Filter
Summary
Event log (1)
All issues

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Nikola Krcevinac
STID: s222564328

Welcome to the new Dashboard

We've made it easier to view details about your scans and other tasks. You can access the logs and a list of all issues from the dock below.

Learn more

1. Live passive crawl from Proxy (all traffic)

Items added to site map — View site map

Host	Method	URL	Status ...	MIME Type
10.0.2.15	GET	/	101	HTML
10.0.2.15	GET	/styles.css	200	CSS
10.0.2.15	GET	/@vite/client	200	script
10.0.2.15		/assets/icons/favicon.ico		
10.0.2.15	GET	/assets/icons/icon.svg	200	XML
10.0.2.15	GET	/assets/icons/apple-touch-ic...	200	PNG
10.0.2.15		/manifest.webmanifest		
10.0.2.15	GET	/polyfills.js	304	
10.0.2.15	GET	/scripts.js	304	
10.0.2.15	GET	/main.js	304	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	script
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	
10.0.2.15	GET	/@fs/home/kali/doubtfire-de...	200	

Task configuration — View configuration

Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same domain and URLs in suite scope.
Capturing

Task progress

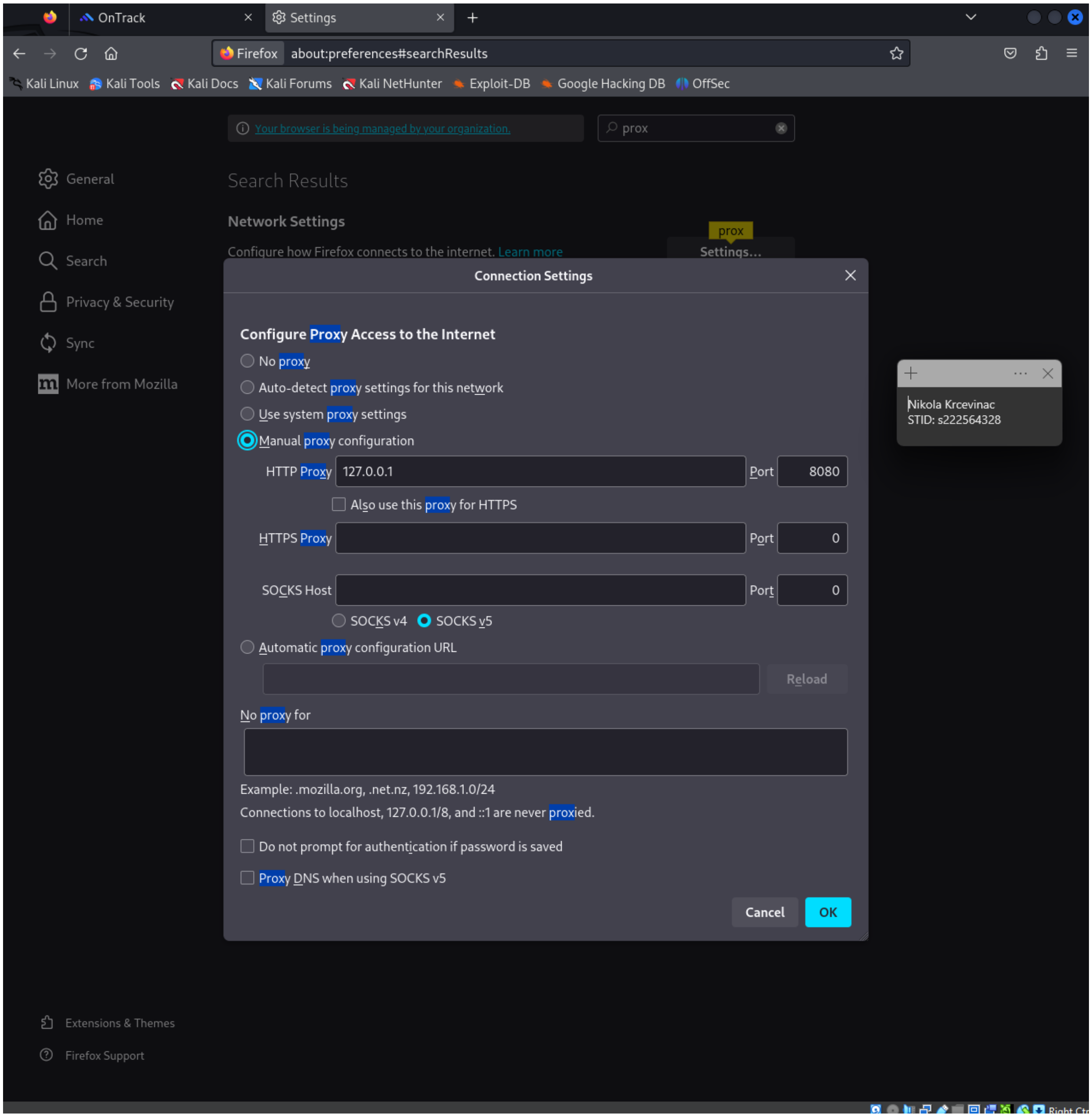
Site map items added: 98
Responses processed: 97
Responses queued: 0

Task log

```
> Adding response http://10.0.2.15:4200/assets/images/logo-white.svg to site map
> Adding response http://10.0.2.15:4200/api/auth/method to site map
> Adding response http://10.0.2.15:4200/assets/images/logo-bw.svg to site map
> Adding response http://10.0.2.15:4200/assets/images/formatif-isolated-lottie.json to
 site map
> Adding response http://10.0.2.15:4200/assets/fonts/grotesk/grotesk-bold.otf to site
map
> Adding response http://10.0.2.15:4200/assets/images/logo.svg to site map
> Adding response http://10.0.2.15:4200/api/auth/signout_url to site map
> Adding response http://10.0.2.15:4200/api/settings to site map
> Adding response http://10.0.2.15:4200/@fs/home/kali/doubtfire-deploy/doubtfire-we
b/.angular/cache/17.3.7/vite/deps/chunk-FYJB6CP3.js?v=a4fff3dc to site map
> Adding response http://10.0.2.15:4200/@fs/home/kali/doubtfire-deploy/doubtfire-we
b/.angular/cache/17.3.7/vite/deps/chunk-OBGBMCBL.js?v=a4fff3dc to site map
```

Memory: 110.6MB

2. In Firefox got to settings preferences and search “proxy”, then click the Network Settings button to them input the same information as shown in the below image:



Nikola Krcevinac
STID: s222564328

Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

□ Also use this proxy for HTTPS

HTTPS Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

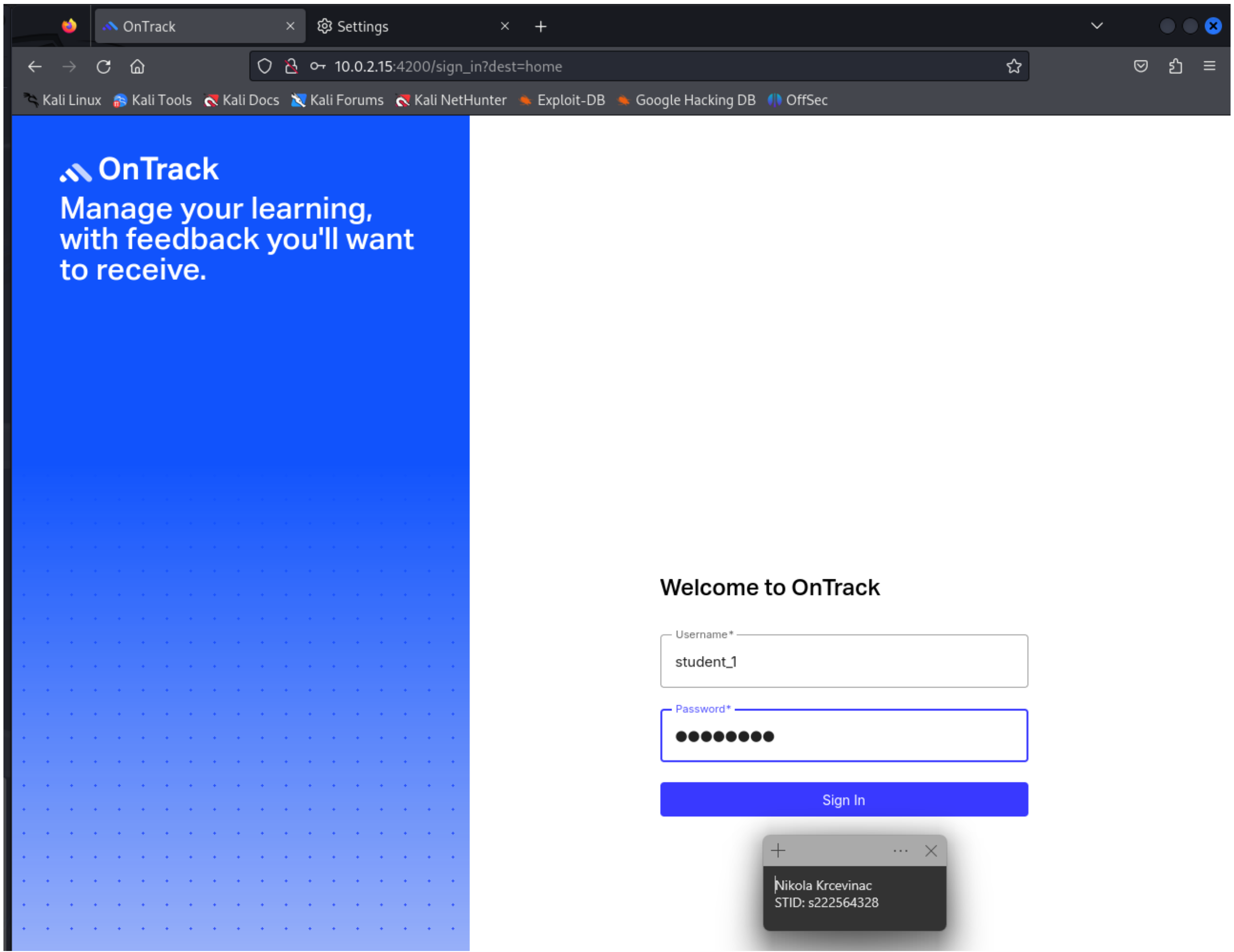
□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

Cancel OK

Step 2: Login as Student User

1. Used the student_1 login details and signed in as seen below:



OnTrack

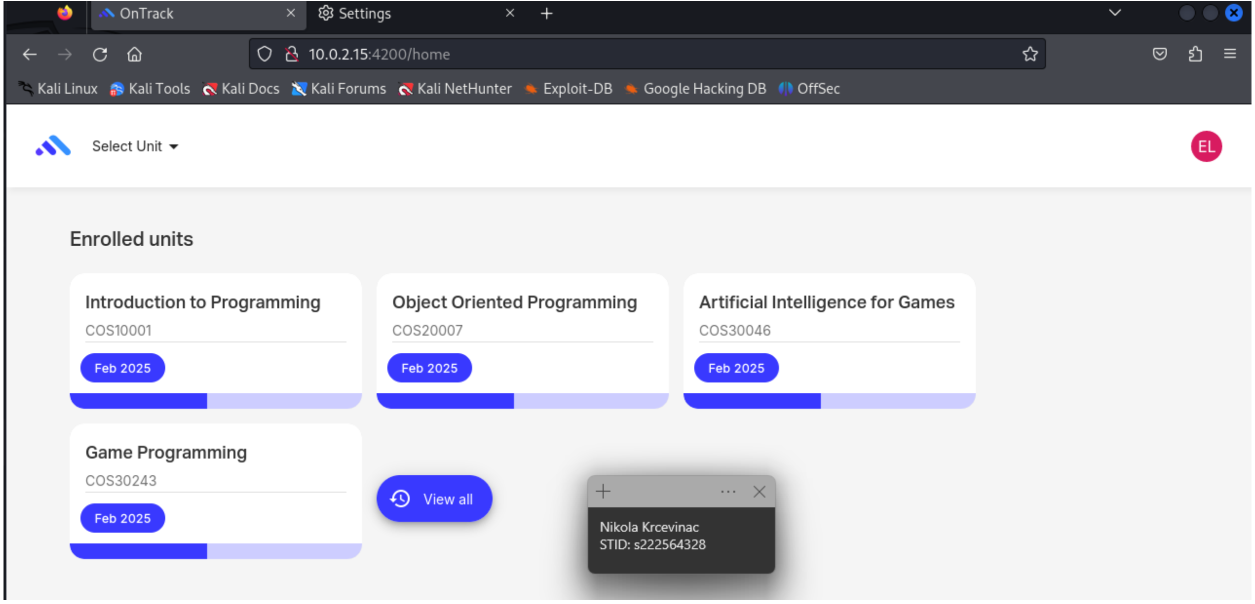
Manage your learning, with feedback you'll want to receive.

Welcome to OnTrack

Username*: student_1

Password*: ●●●●●●●●

Nikola Krcevinac
STID: s222564328



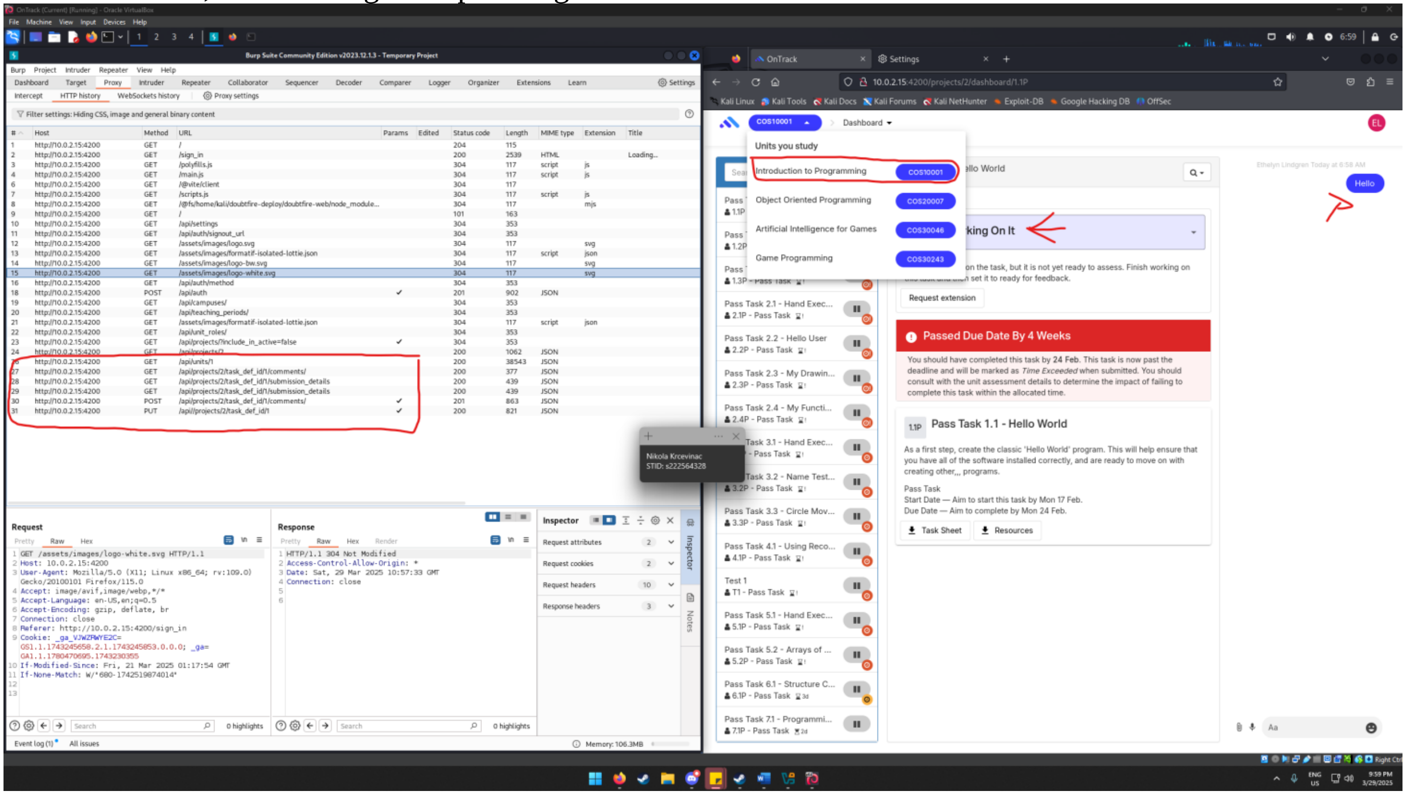
Enrolled units

Introduction to Programming COS10001 Feb 2025	Object Oriented Programming COS20007 Feb 2025	Artificial Intelligence for Games COS30046 Feb 2025
Game Programming COS30243 Feb 2025		

Nikola Krcevinac
STID: s222564328

Step 3: Intercepts API Call to Unit Endpoint

1. Below on the left I clicked on Proxy -> HTTP History and then on the right started clicking random buttons, commenting and uploading to create HTTP traffic as seen below:



Burp Suite Community Edition v2023.12.1.3 - Temporary Project

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
1	http://10.0.2.15:4200	GET	/			204	115			
2	http://10.0.2.15:4200	GET	/sign_in			200	2539	HTML		Loading...
3	http://10.0.2.15:4200	GET	/polyfills.js			304	117	script	js	
4	http://10.0.2.15:4200	GET	/main.js			304	117	script	js	
6	http://10.0.2.15:4200	GET	/@vite/client			304	117			
7	http://10.0.2.15:4200	GET	/scripts.js			304	117	script	js	
8	http://10.0.2.15:4200	GET	/@fs/home/kali/doubtfire-deploy/doubtfire-web/node_module...			304	117		mjs	
9	http://10.0.2.15:4200	GET	/			101	163			
10	http://10.0.2.15:4200	GET	/api/settings			304	353			
11	http://10.0.2.15:4200	GET	/api/auth/signout_url			304	353			
12	http://10.0.2.15:4200	GET	/assets/images/logo.svg			304	117		svg	
13	http://10.0.2.15:4200	GET	/assets/images/formatif-isolated-lottie.json			304	117	script	json	
14	http://10.0.2.15:4200	GET	/assets/images/logo-bw.svg			304	117		svg	
15	http://10.0.2.15:4200	GET	/assets/images/logo-white.svg			304	117		svg	
16	http://10.0.2.15:4200	GET	/api/auth/method			304	353			
18	http://10.0.2.15:4200	POST	/api/auth	✓		201	902	JSON		
19	http://10.0.2.15:4200	GET	/api/campuses/			304	353			
20	http://10.0.2.15:4200	GET	/api/teaching_periods/			304	353			
21	http://10.0.2.15:4200	GET	/assets/images/formatif-isolated-lottie.json			304	117	script	json	
22	http://10.0.2.15:4200	GET	/api/unit_roles/			304	353			
23	http://10.0.2.15:4200	GET	/api/projects/?include_in_active=false	✓		304	353			
24	http://10.0.2.15:4200	GET	/api/projects/2			200	1062	JSON		
26	http://10.0.2.15:4200	GET	/api/units/1			200	38543	JSON		
27	http://10.0.2.15:4200	GET	/api/projects/2/task_def_id/1/comments/			200	377	JSON		
28	http://10.0.2.15:4200	GET	/api/projects/2/task_def_id/1/submission_details			200	439	JSON		
29	http://10.0.2.15:4200	GET	/api/projects/2/task_def_id/1/submission_details			200	439	JSON		
30	http://10.0.2.15:4200	POST	/api/projects/2/task_def_id/1/comments/	✓		201	863	JSON		
31	http://10.0.2.15:4200	PUT	/api//projects/2/task_def_id/1	✓		200	821	JSON		

Nikola Krcevinac
STID: s222564328

Request

```
GET /assets/images/logo-white.svg HTTP/1.1
Host: 10.0.2.15:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.0.2.15:4200/sign_in
Cookie: _ga_VJWZRWYE2C=
GS1.1.1743245658.2.1.1743245853.0.0.0; _ga=
GA1.1.1780470695.1743230355
If-Modified-Since: Fri, 21 Mar 2025 01:17:54 GMT
If-None-Match: W/"680-1742519874014"
```

Response

```
HTTP/1.1 304 Not Modified
Access-Control-Allow-Origin: *
Date: Sat, 29 Mar 2025 10:57:33 GMT
Connection: close
```

10.0.2.15:4200/projects/2/dashboard/1.1P

Units you study

Introduction to Programming	COS10001
Object Oriented Programming	COS20007
Artificial Intelligence for Games	COS30046
Game Programming	COS30243

Pass Task 2.1 - Hand Exec...
2.1P - Pass Task

Pass Task 2.2 - Hello User
2.2P - Pass Task

Pass Task 2.3 - My Drawin...
2.3P - Pass Task

Pass Task 2.4 - My Functi...
2.4P - Pass Task

Pass Task 3.1 - Hand Exec...
3.1P - Pass Task

Pass Task 3.2 - Name Test...
3.2P - Pass Task

Pass Task 3.3 - Circle Mov...
3.3P - Pass Task

Pass Task 4.1 - Using Reco...
4.1P - Pass Task

Test 1
T1 - Pass Task

Pass Task 5.1 - Hand Exec...
5.1P - Pass Task

Pass Task 5.2 - Arrays of ...
5.2P - Pass Task

Pass Task 6.1 - Structure C...
6.1P - Pass Task

Pass Task 7.1 - Programmi...
7.1P - Pass Task

...king On It

...on the task, but it is not yet ready to assess. Finish working on this task and then set it to ready for feedback.

Request extension

Passed Due Date By 4 Weeks

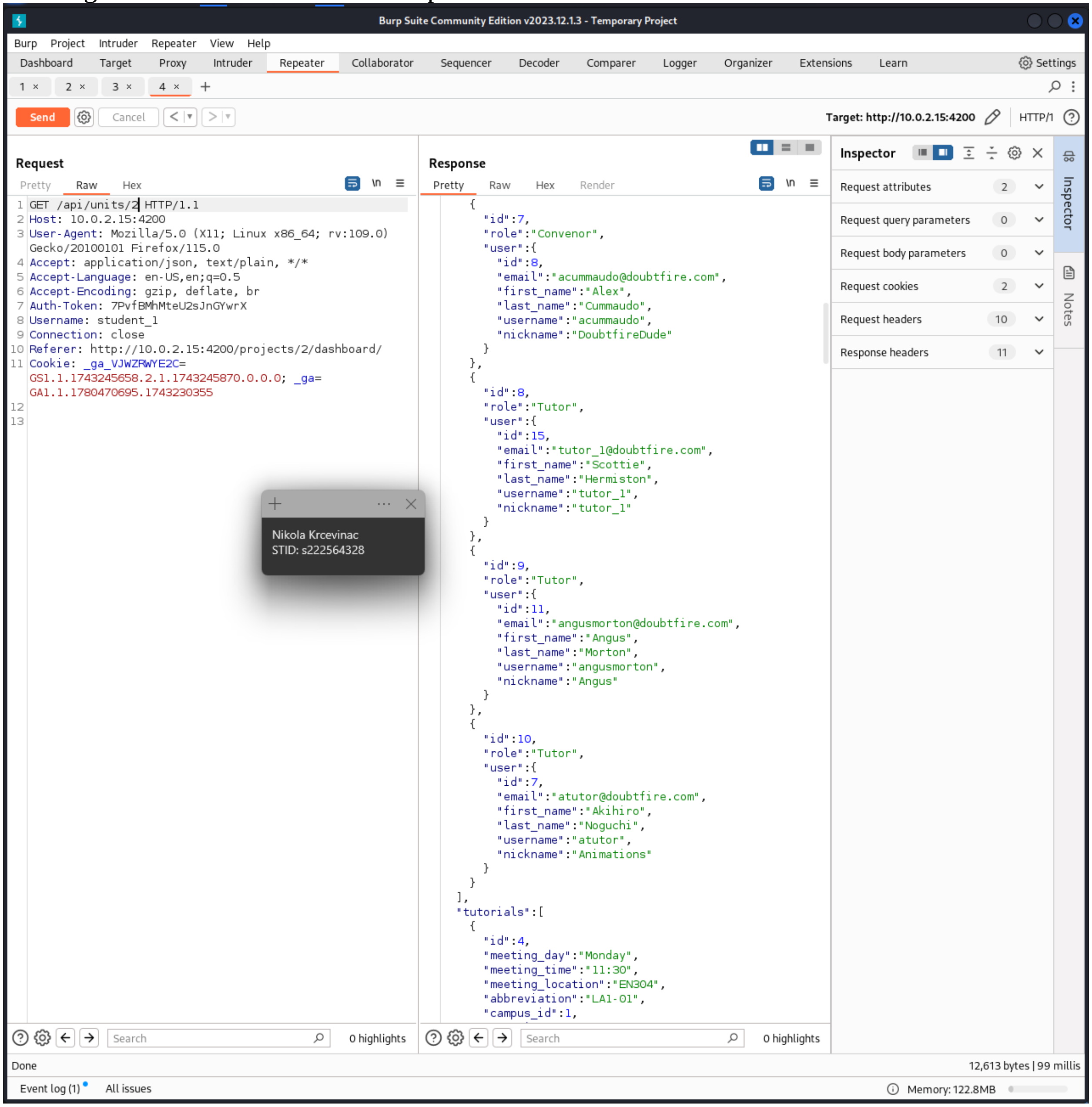
You should have completed this task by **24 Feb**. This task is now past the deadline and will be marked as *Time Exceeded* when submitted. You should consult with the unit assessment details to determine the impact of failing to complete this task within the allocated time.

1.1P Pass Task 1.1 - Hello World

As a first step, create the classic 'Hello World' program. This will help ensure that you have all of the software installed correctly, and are ready to move on with creating other,,, programs.

Pass Task
Start Date — Aim to start this task by Mon 17 Feb.
Due Date — Aim to complete by Mon 24 Feb.

2. After that I right clicked the “GET /api/units/1” and sent to Repeater in Burp. Below you can see two images where you can cleary seen the names of the Convenor and Tutor visibly, thus showing unauthorized staff data in response:

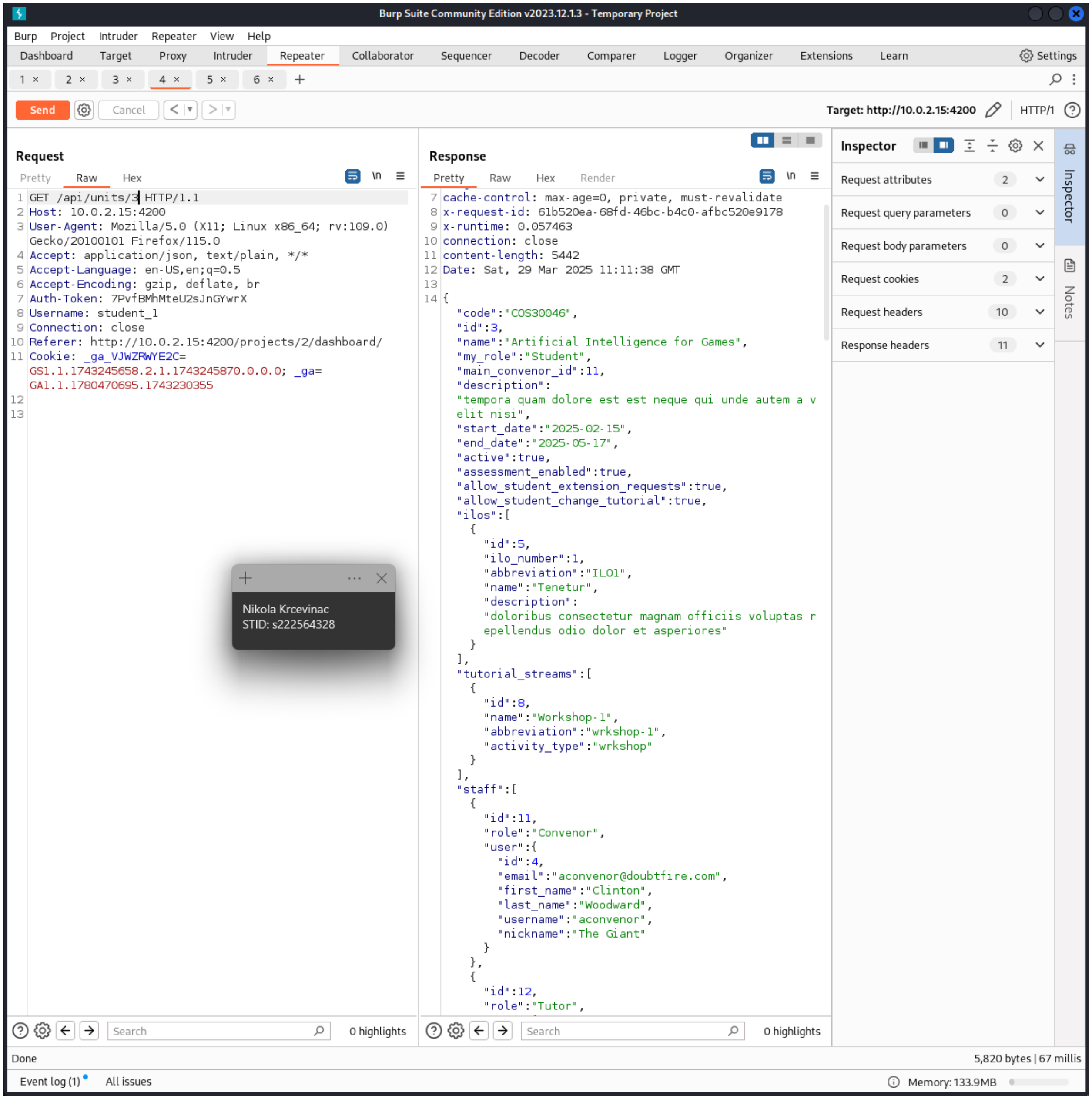

Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × 3 × 4 ×
Send
Cancel
Target: http://10.0.2.15:4200
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 10
Response headers 11
Notes
Search
0 highlights
Search
0 highlights
Done
12,613 bytes | 99 millis
Event log (1)
All issues
Memory: 122.8MB

Nikola Krcevinac
STID: s222564328

```
GET /api/units/2 HTTP/1.1
Host: 10.0.2.15:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: 7PvfBMhMteU2sJnGYwrX
Username: student_1
Connection: close
Referer: http://10.0.2.15:4200/projects/2/dashboard/
Cookie: _ga_VJWZRWYE2C=
GS1.1.1743245658.2.1.1743245870.0.0.0; _ga=
GA1.1.1780470695.1743230355


```

```
    {
      "id":7,
      "role":"Convenor",
      "user":{
        "id":8,
        "email":"acummaudo@doubtfire.com",
        "first_name":"Alex",
        "last_name":"Cummaudo",
        "username":"acummaudo",
        "nickname":"DoubtfireDude"
      }
    },
    {
      "id":8,
      "role":"Tutor",
      "user":{
        "id":15,
        "email":"tutor_1@doubtfire.com",
        "first_name":"Scottie",
        "last_name":"Hermiston",
        "username":"tutor_1",
        "nickname":"tutor_1"
      }
    },
    {
      "id":9,
      "role":"Tutor",
      "user":{
        "id":11,
        "email":"angusmorton@doubtfire.com",
        "first_name":"Angus",
        "last_name":"Morton",
        "username":"angusmorton",
        "nickname":"Angus"
      }
    },
    {
      "id":10,
      "role":"Tutor",
      "user":{
        "id":7,
        "email":"atutor@doubtfire.com",
        "first_name":"Akihiro",
        "last_name":"Noguchi",
        "username":"atutor",
        "nickname":"Animations"
      }
    }
  ],
  "tutorials":[
    {
      "id":4,
      "meeting_day":"Monday",
      "meeting_time":"11:30",
      "meeting_location":"EN304",
      "abbreviation":"LA1-01",
      "campus_id":1,
```


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
Settings
1 × 2 × 3 × 4 × 5 × 6 × +
Send
Cancel
Target: http://10.0.2.15:4200
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Search
0 highlights
Event log (1)
All issues
Memory: 133.9MB

Request

```
GET /api/units/3 HTTP/1.1
Host: 10.0.2.15:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: 7PvfBMhMteU2sJnGYwrX
Username: student_1
Connection: close
Referer: http://10.0.2.15:4200/projects/2/dashboard/
Cookie: _ga_VJWZRWYE2C=
GS1.1.1743245658.2.1.1743245870.0.0.0; _ga=
GA1.1.1780470695.1743230355
```

Nikola Krcevinac
STID: s222564328

Response

```
cache-control: max-age=0, private, must-revalidate
x-request-id: 61b520ea-68fd-46bc-b4c0-afbc520e9178
x-runtime: 0.057463
connection: close
content-length: 5442
Date: Sat, 29 Mar 2025 11:11:38 GMT

{
  "code":"COS30046",
  "id":3,
  "name":"Artificial Intelligence for Games",
  "my_role":"Student",
  "main_convenor_id":11,
  "description":
  "tempora quam dolore est est neque qui unde autem a v
  elit nisi",
  "start_date":"2025-02-15",
  "end_date":"2025-05-17",
  "active":true,
  "assessment_enabled":true,
  "allow_student_extension_requests":true,
  "allow_student_change_tutorial":true,
  "ilos":[
    {
      "id":5,
      "ilo_number":1,
      "abbreviation":"ILO1",
      "name":"Tenetur",
      "description":
      "doloribus consectetur magnam officiis voluptas r
      epellendus odio dolor et asperiores"
    }
  ],
  "tutorial_streams":[
    {
      "id":8,
      "name":"Workshop-1",
      "abbreviation":"wrkshop-1",
      "activity_type":"wrkshop"
    }
  ],
  "staff":[
    {
      "id":11,
      "role":"Convenor",
      "user":{
        "id":4,
        "email":"aconvenor@doubtfire.com",
        "first_name":"Clinton",
        "last_name":"Woodward",
        "username":"aconvenor",
        "nickname":"The Giant"
      }
    },
    {
      "id":12,
      "role":"Tutor",
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	10
Response headers	11

Done

5,820 bytes | 67 millis

Remediation Advice

The application fails to implement proper access controls for sensitive data in its API endpoints.

Mitigations:

- Implement role-based access control (RBAC) on API endpoints to restrict data based on user privileges.
- Ensure sensitive user information (such as staff emails, names, and roles) is only accessible to authorized users (e.g., Admins or the staff themselves).
- Sanitize API responses and avoid over-sharing data that is not required by the frontend for the user's role.
- Conduct regular access control reviews and enforce the least privilege access principles.

References

- OWASP: Insecure Direct Object References (IDOR)
- OWASP Top 10 – Broken Access Control
- Burp Suite Documentation

Contact Details

Name/Teams: Nicholas Krcevinac
Email: s222564328@deakin.edu.au

Pentest Leader Feedback.

Nice work!