Finding Name: Publicly Accessible API Documentation via Swagger

Name	Team	Role	Project	Quality Assurance	Is this a re-tested Finding?
Filipe Oliveira	OnTrack	Pen-Tester	AppAttack	Wahidullah Hashimi	No

Was this Finding Successful?
Yes

Finding Description

The swagger-generated Api documentation is publicly accessible via the unauthenticated endpoint: http://172.18.0.1:4200/api/swagger_doc.json this exposes the entire backend Api structure, including sensitive internal routes like PUT /api/users/{id}and GET /api/users
By utilizing this documentation, an attacker can discover hidden API routes not exposed through the front end of the website. Although the app prevents unauthorized role change and other protected actions, the ability to submit those requests without proper feedback shows weakaccess controls and poor feedback handling.

Risk Rating

Impact: Major
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

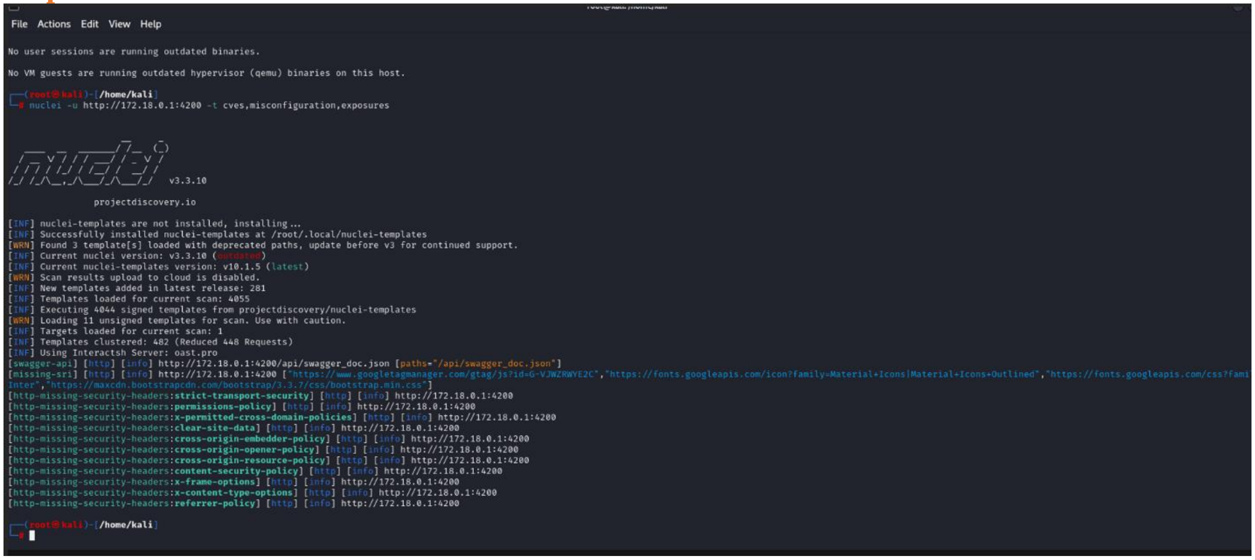
If an attacker gains access to a user’s authentication token, they can fully impersonate the victim without needing a password. This could lead to exposure of academic records, assignment submissions and may allow unauthorised access to admin modifications. If this occurred on a live, production grade system over an open or shared network, it could result in unauthorised access to student information, data privacy violations and erosion of trust in the system’s security.

Affected Assets

- GET /api/swagger_doc.json
- All endpoints defined in swagger

Evidence

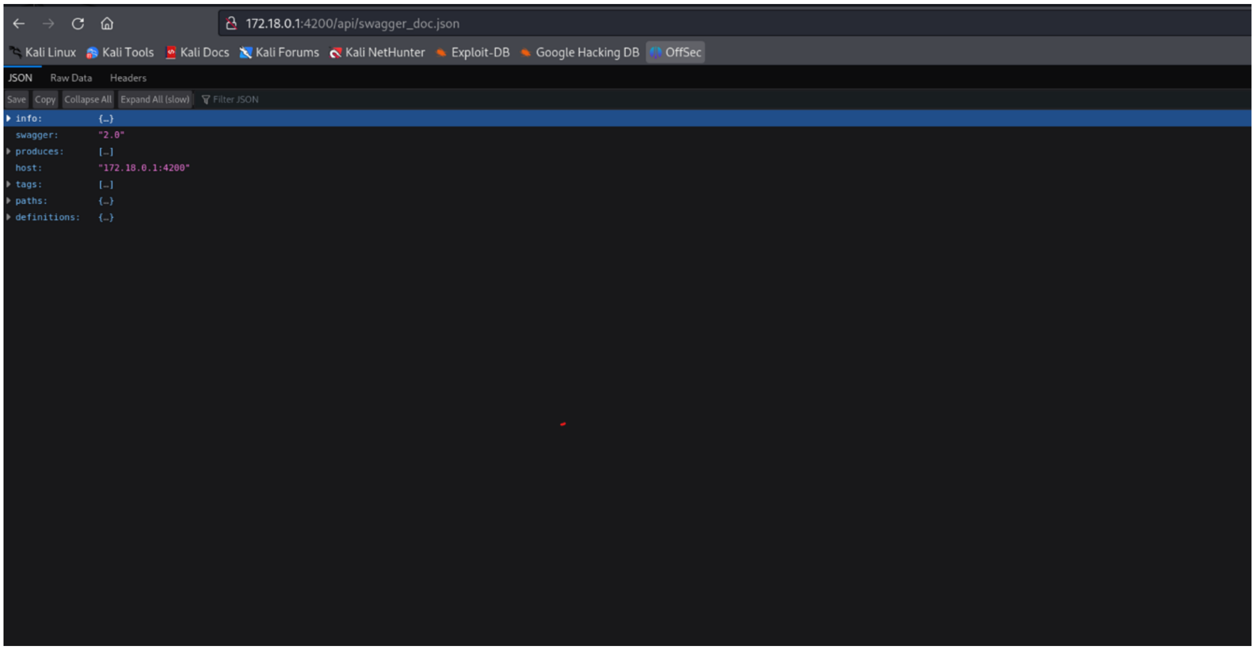
Step 1: download and run Nuclei



```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(root㉿kali)-[/home/kali]
└─# nuclei -u http://172.18.0.1:4200 -t cves,misconfiguration,exposures


                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.10

                projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully installed nuclei-templates at /root/.local/nuclei-templates
[WRN] Found 3 template[s] loaded with deprecated paths, update before v3 for continued support.
[INF] Current nuclei version: v3.3.10 (outdated)
[INF] Current nuclei-templates version: v10.1.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 281
[INF] Templates loaded for current scan: 4055
[INF] Executing 4044 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 11 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 482 (Reduced 448 Requests)
[INF] Using Interactsh Server: oast.pro
[swagger-api] [http] [info] http://172.18.0.1:4200/api/swagger_doc.json [paths="/api/swagger_doc.json"]
[missing-sri] [http] [info] http://172.18.0.1:4200 ["https://www.googletagmanager.com/gtag/js?id=G-VJWZRWYE2C","https://fonts.googleapis.com/icon?family=Material+Icons|Material+Icons+Outlined","https://fonts.googleapis.com/css?fami
Inter","https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css"]
[http-missing-security-headers:strict-transport-security] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:permissions-policy] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:clear-site-data] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:content-security-policy] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:x-frame-options] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:x-content-type-options] [http] [info] http://172.18.0.1:4200
[http-missing-security-headers:referrer-policy] [http] [info] http://172.18.0.1:4200

┌──(root㉿kali)-[/home/kali]
└─# 
```

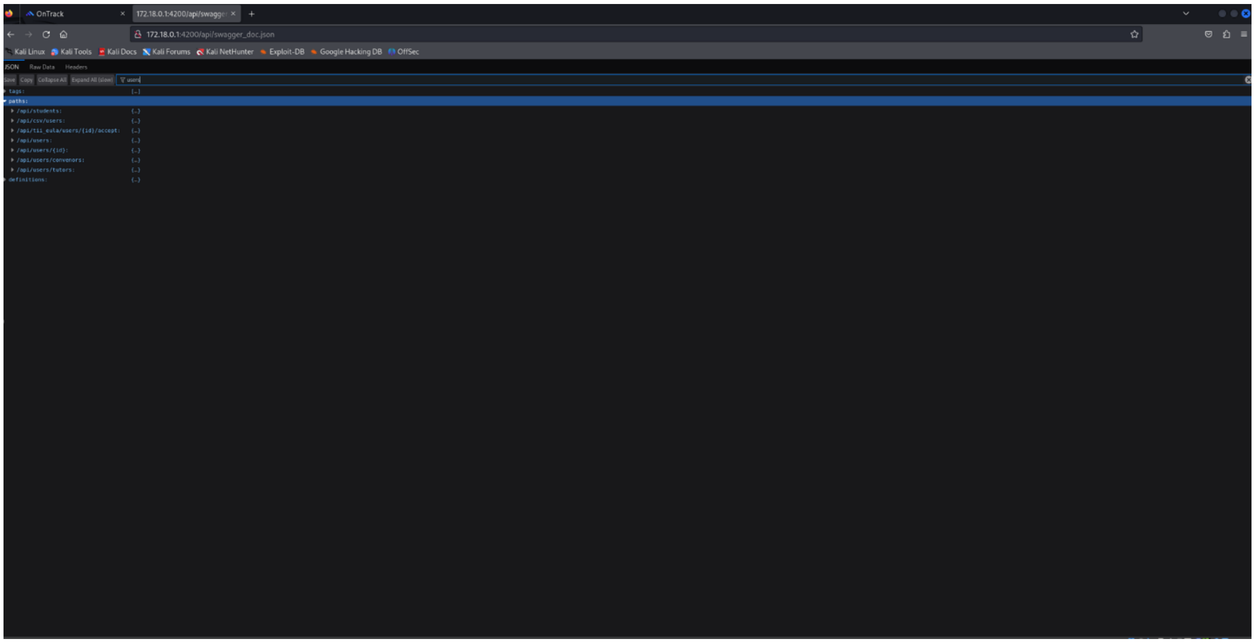
In this above screenshot we can see one of the vulnerabilities is a public API along with its URL to access it

Step 2: Copy and paste the URL in browser

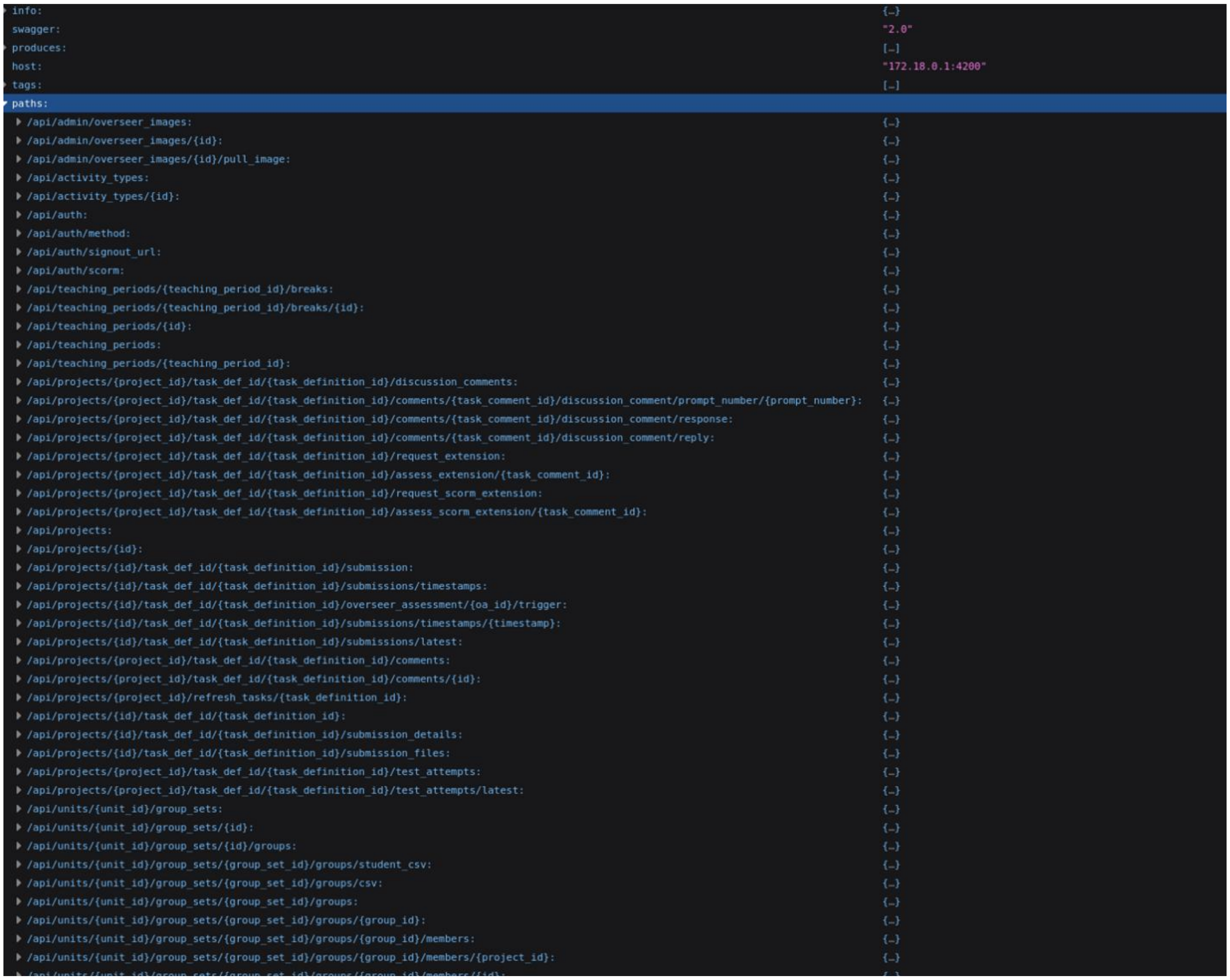


```
▸ info:          {…}
  swagger:       "2.0"
▸ produces:      […]
  host:          "172.18.0.1:4200"
▸ tags:          […]
▸ paths:         {…}
▸ definitions:   {…}
```

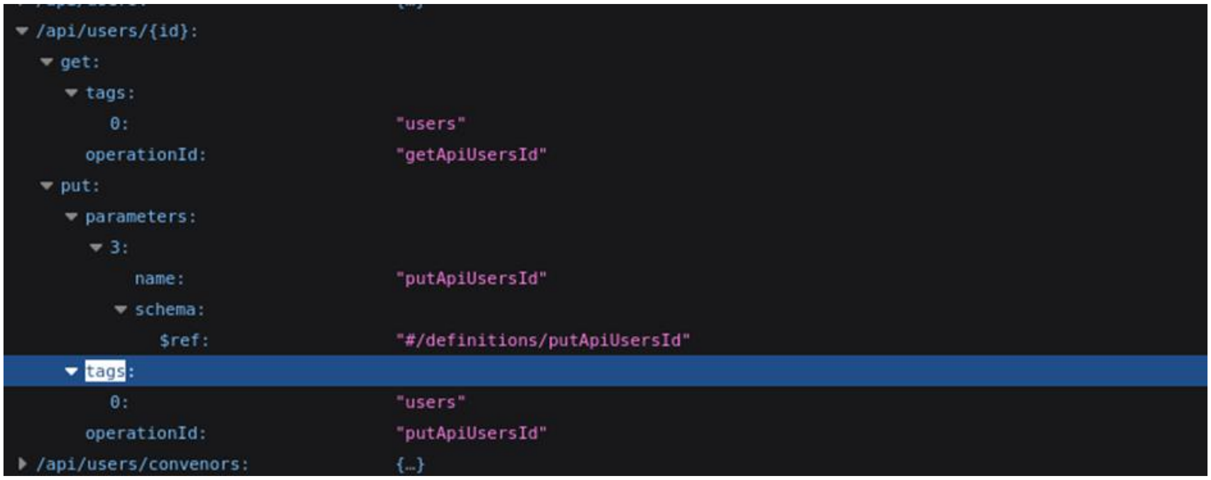
we now have access to the API and can go through it to reveal end points like /api/users



```
▸ tags:                                  […]
▾ paths:
  ▸ /api/students:                       {…}
  ▸ /api/csv/users:                      {…}
  ▸ /api/tii_eula/users/{id}/accept:     {…}
  ▸ /api/users:                          {…}
  ▸ /api/users/{id}:                     {…}
  ▸ /api/users/convenors:                {…}
  ▸ /api/users/tutors:                   {…}
▸ definitions:                           {…}
```

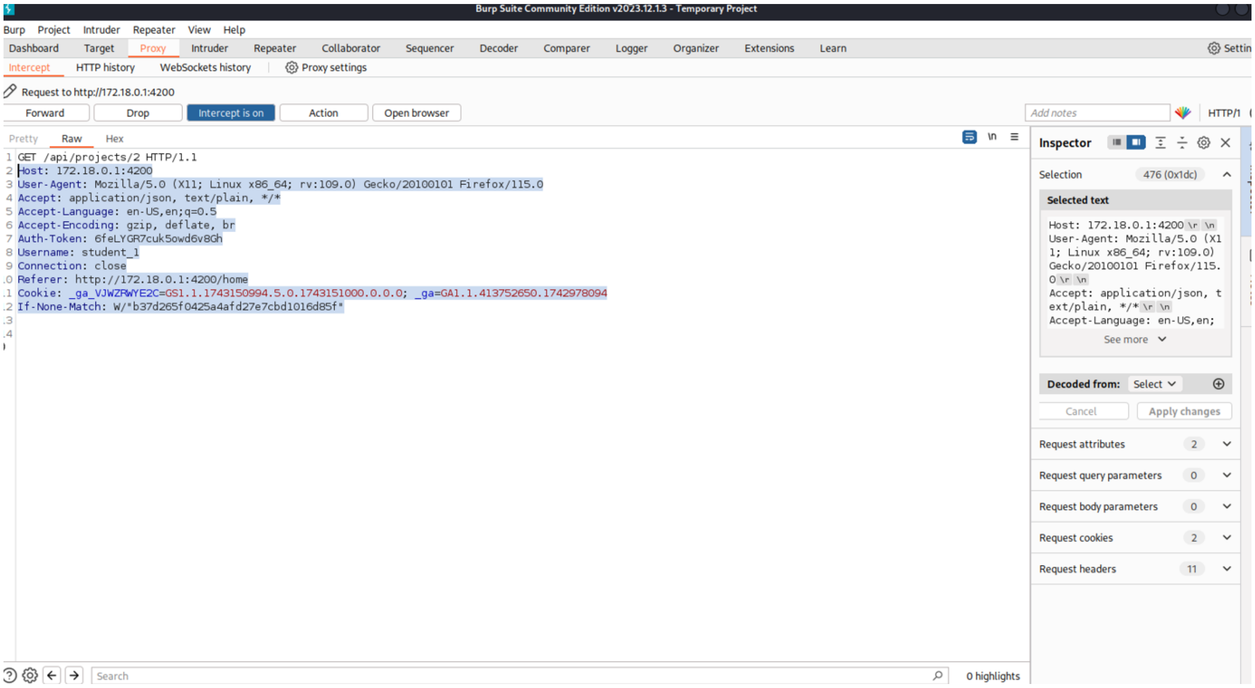


```
info:                                                                                                      {…}
swagger:                                                                                                   "2.0"
produces:                                                                                                  […]
host:                                                                                                      "172.18.0.1:4200"
tags:                                                                                                      […]
paths:
  /api/admin/overseer_images:                                                                              {…}
  /api/admin/overseer_images/{id}:                                                                         {…}
  /api/admin/overseer_images/{id}/pull_image:                                                              {…}
  /api/activity_types:                                                                                     {…}
  /api/activity_types/{id}:                                                                                {…}
  /api/auth:                                                                                               {…}
  /api/auth/method:                                                                                        {…}
  /api/auth/signout_url:                                                                                   {…}
  /api/auth/scorm:                                                                                         {…}
  /api/teaching_periods/{teaching_period_id}/breaks:                                                       {…}
  /api/teaching_periods/{teaching_period_id}/breaks/{id}:                                                  {…}
  /api/teaching_periods/{id}:                                                                              {…}
  /api/teaching_periods:                                                                                   {…}
  /api/teaching_periods/{teaching_period_id}:                                                              {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/discussion_comments:                         {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/comments/{task_comment_id}/discussion_comment/prompt_number/{prompt_number}: {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/comments/{task_comment_id}/discussion_comment/response: {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/comments/{task_comment_id}/discussion_comment/reply: {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/request_extension:                           {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/assess_extension/{task_comment_id}:          {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/request_scorm_extension:                     {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/assess_scorm_extension/{task_comment_id}:    {…}
  /api/projects:                                                                                           {…}
  /api/projects/{id}:                                                                                      {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/submission:                                          {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/submissions/timestamps:                              {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/overseer_assessment/{oa_id}/trigger:                 {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/submissions/timestamps/{timestamp}:                  {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/submissions/latest:                                  {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/comments:                                    {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/comments/{id}:                               {…}
  /api/projects/{project_id}/refresh_tasks/{task_definition_id}:                                           {…}
  /api/projects/{id}/task_def_id/{task_definition_id}:                                                     {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/submission_details:                                  {…}
  /api/projects/{id}/task_def_id/{task_definition_id}/submission_files:                                    {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/test_attempts:                               {…}
  /api/projects/{project_id}/task_def_id/{task_definition_id}/test_attempts/latest:                        {…}
  /api/units/{unit_id}/group_sets:                                                                         {…}
  /api/units/{unit_id}/group_sets/{id}:                                                                    {…}
  /api/units/{unit_id}/group_sets/{id}/groups:                                                             {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups/student_csv:                                       {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups/csv:                                               {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups:                                                   {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups/{group_id}:                                        {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups/{group_id}/members:                                {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups/{group_id}/members/{project_id}:                   {…}
  /api/units/{unit_id}/group_sets/{group_set_id}/groups/{group_id}/members/{id}:                           {…}
```



```
/api/users/{id}:
  get:
    tags:
      0:                        "users"
    operationId:                "getApiUsersId"
  put:
    parameters:
      3:
        name:                   "putApiUsersId"
        schema:
          $ref:                 "#/definitions/putApiUsersId"
    tags:
      0:                        "users"
    operationId:                "putApiUsersId"
/api/users/convenors:           {…}
```

Step 3: Open and setup burp suite



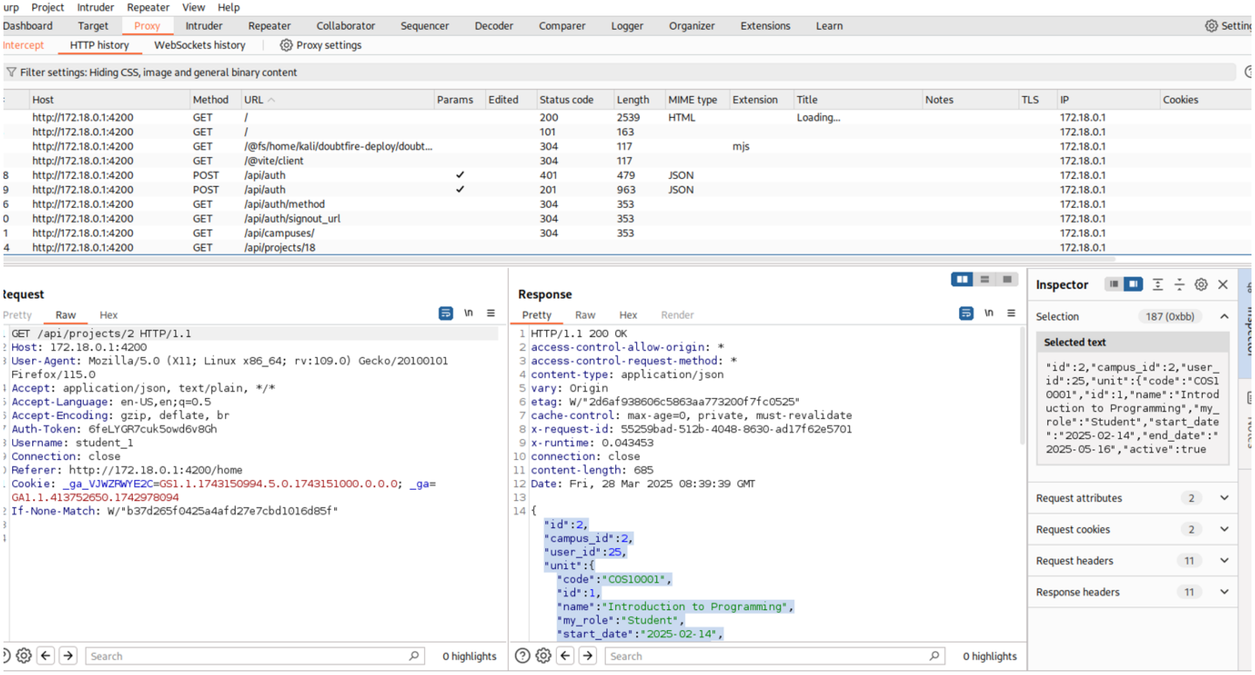
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settin
Intercept HTTP history WebSockets history Proxy settings
Request to http://172.18.0.1:4200
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Selection 476 (0x1dc)
Selected text
See more
Decoded from: Select
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 11
Search
0 highlights

```
GET /api/projects/2 HTTP/1.1
Host: 172.18.0.1:4200
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: 6feLYGR7cuk5owd6v8Gh
Username: student_1
Connection: close
Referer: http://172.18.0.1:4200/home
Cookie: _ga_VJWZRWYE2C=GS1.1.1743150994.5.0.1743151000.0.0.0; _ga=GA1.1.413752650.1742978094
If-None-Match: W/"b37d265f0425a4afd27e7cbd1016d85f"
```

```
Host: 172.18.0.1:4200 \r \n
User-Agent: Mozilla/5.0 (X1
1; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.
0 \r \n
Accept: application/json, t
ext/plain, */* \r \n
Accept-Language: en-US,en;
```

So we login as a student as normal and keep sending the requests through while still intercepting the packets. We take note of our authentication token and cookies.

Step 4: Check user ID



urp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settin
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 187 (0xbb)
Selected text
Request attributes 2
Request cookies 2
Request headers 11
Response headers 11
Search
0 highlights

	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
	http://172.18.0.1:4200	GET	/			200	2539	HTML		Loading...			172.18.0.1	
	http://172.18.0.1:4200	GET	/			101	163						172.18.0.1	
	http://172.18.0.1:4200	GET	/@fs/home/kali/doubtfire-deploy/doubt...			304	117		mjs				172.18.0.1	
	http://172.18.0.1:4200	GET	/@vite/client			304	117						172.18.0.1	
8	http://172.18.0.1:4200	POST	/api/auth	✓		401	479	JSON					172.18.0.1	
9	http://172.18.0.1:4200	POST	/api/auth	✓		201	963	JSON					172.18.0.1	
6	http://172.18.0.1:4200	GET	/api/auth/method			304	353						172.18.0.1	
0	http://172.18.0.1:4200	GET	/api/auth/signout_url			304	353						172.18.0.1	
1	http://172.18.0.1:4200	GET	/api/campuses/			304	353						172.18.0.1	
4	http://172.18.0.1:4200	GET	/api/projects/18										172.18.0.1	

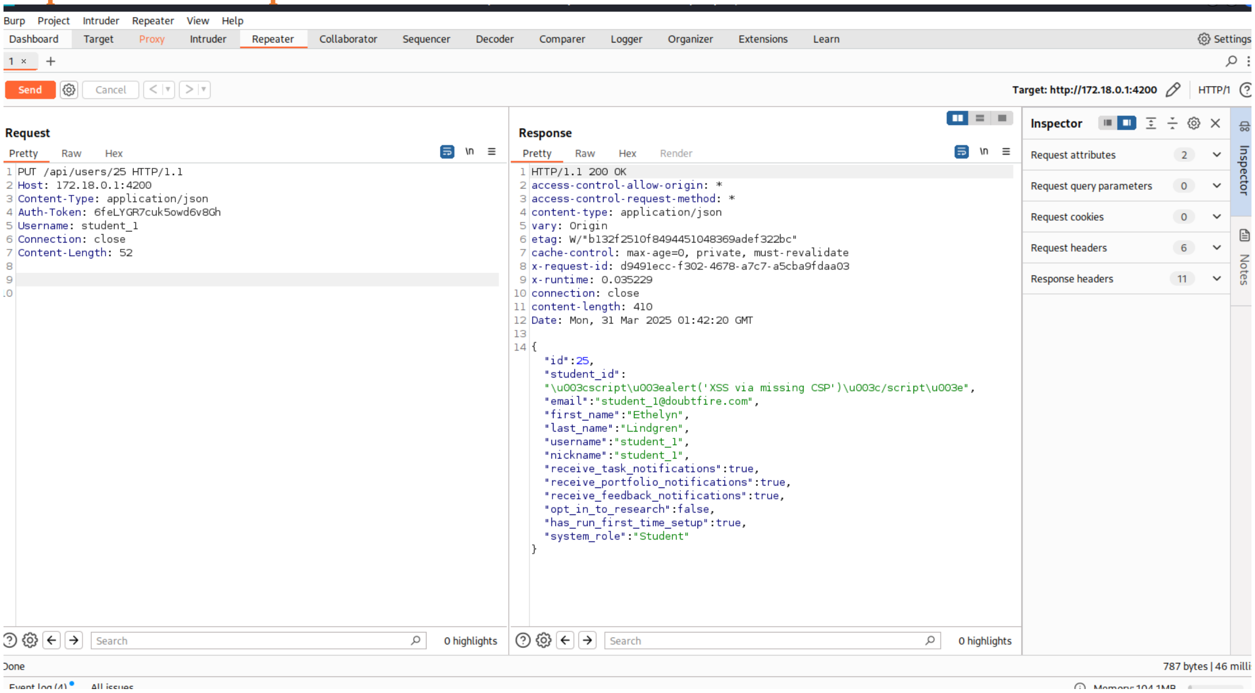
```
GET /api/projects/2 HTTP/1.1
Host: 172.18.0.1:4200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Auth-Token: 6feLYGR7cuk5owd6v8Gh
Username: student_1
Connection: close
Referer: http://172.18.0.1:4200/home
Cookie: _ga_VJWZRWYE2C=GS1.1.1743150994.5.0.1743151000.0.0.0; _ga=
GA1.1.413752650.1742978094
If-None-Match: W/"b37d265f0425a4afd27e7cbd1016d85f"
```

```
HTTP/1.1 200 OK
access-control-allow-origin: *
access-control-request-method: *
content-type: application/json
vary: Origin
etag: W/"2d6af938606c5863aa773200f7fc0525"
cache-control: max-age=0, private, must-revalidate
x-request-id: 55259bad-512b-4048-8630-ad17f62e5701
x-runtime: 0.043453
connection: close
content-length: 685
Date: Fri, 28 Mar 2025 08:39:39 GMT

{
  "id":2,
  "campus_id":2,
  "user_id":25,
  "unit":{
    "code":"COS10001",
    "id":1,
    "name":"Introduction to Programming",
    "my_role":"Student",
    "start_date":"2025-02-14",
```

```
"id":2,"campus_id":2,"user_
id":25,"unit":{"code":"COS1
0001","id":1,"name":"Introd
uction to Programming","my_
role":"Student","start_date
":"2025-02-14","end_date":"
2025-05-16","active":true
```

Next go to http history and sift through packets that have /api . This shows me all the fields associated with my user and can correctly note that my user is 25.

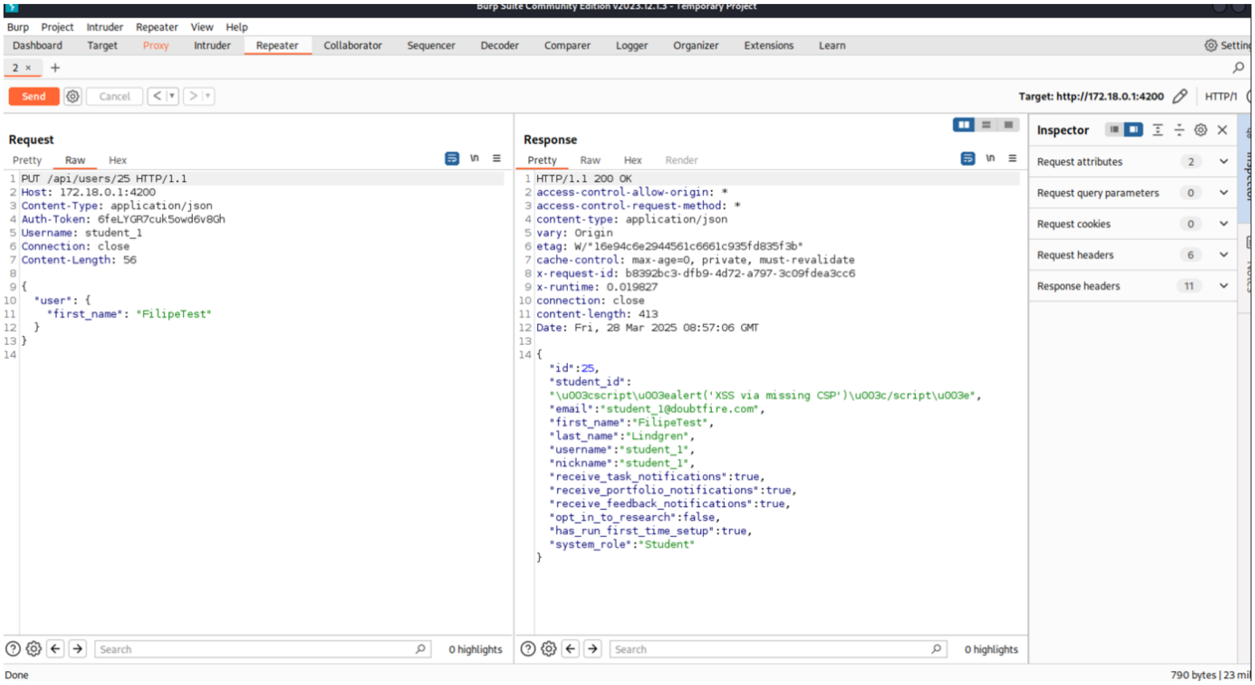
Step 5: Go to the repeater tab



```
PUT /api/users/25 HTTP/1.1
Host: 172.18.0.1:4200
Content-Type: application/json
Auth-Token: 6feLYGR7cuk5owd6v8Gh
Username: student_1
Connection: close
Content-Length: 52
```

```
HTTP/1.1 200 OK
access-control-allow-origin: *
access-control-request-method: *
content-type: application/json
vary: Origin
etag: W/"b132f2510f8494451048369adef322bc"
cache-control: max-age=0, private, must-revalidate
x-request-id: d9491ecc-f302-4678-a7c7-a5cba9fdaa03
x-runtime: 0.035229
connection: close
content-length: 410
Date: Mon, 31 Mar 2025 01:42:20 GMT

{
  "id":25,
  "student_id":
  "\u003cscript\u003ealert('XSS via missing CSP')\u003c/script\u003e",
  "email":"student_1@doubtfire.com",
  "first_name":"Ethelyn",
  "last_name":"Lindgren",
  "username":"student_1",
  "nickname":"student_1",
  "receive_task_notifications":true,
  "receive_portfolio_notifications":true,
  "receive_feedback_notifications":true,
  "opt_in_to_research":false,
  "has_run_first_time_setup":true,
  "system_role":"Student"
}
```

As seen above this now shows the information of student one as a whole. Because we know how the backend API is setup, we can push requests and changes to this information.


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
2 ×
Send
Cancel
Target: http://172.18.0.1:4200
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request cookies 0
Request headers 6
Response headers 11
Search
0 highlights
Done
790 bytes | 23 mil

```
PUT /api/users/25 HTTP/1.1
Host: 172.18.0.1:4200
Content-Type: application/json
Auth-Token: 6feLYGR7cuk5owd6v8Gh
Username: student_1
Connection: close
Content-Length: 56

{
  "user": {
    "first_name": "FilipeTest"
  }
}
```

```
HTTP/1.1 200 OK
access-control-allow-origin: *
access-control-request-method: *
content-type: application/json
vary: Origin
etag: W/"16e94c6e2944561c6661c935fd835f3b"
cache-control: max-age=0, private, must-revalidate
x-request-id: b8392bc3-dfb9-4d72-a797-3c09fdea3cc6
x-runtime: 0.019827
connection: close
content-length: 413
Date: Fri, 28 Mar 2025 08:57:06 GMT

{
  "id":25,
  "student_id":
  "\u003cscript\u003ealert('XSS via missing CSP')\u003c/script\u003e",
  "email":"student_1@doubtfire.com",
  "first_name":"FilipeTest",
  "last_name":"Lindgren",
  "username":"student_1",
  "nickname":"student_1",
  "receive_task_notifications":true,
  "receive_portfolio_notifications":true,
  "receive_feedback_notifications":true,
  "opt_in_to_research":false,
  "has_run_first_time_setup":true,
  "system_role":"Student"
}
```

On the left is the packet that I tested and pushed onto the system, on the right is the confirmation of the server information. (I tried to do system role too, however that seemed to be properly authenticated before making changes, so I could not change that.)

Remediation Advice

- Restrict access to API documentation endpoints like swagger_doc.json
- Require authentication and authorisation before exposing backend routes and parameters
- Implement strict validation on all sensitive user attributes(role_id)
- Ensure proper response code (403 Forbidden) for unauthorised updates.

References

OWASP Session Management Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Wireshark Official Website (Download & Docs) https://www.wireshark.org/

Burp Suite Repeater Documentation

https://portswigger.net/burp/documentation/desktop/tools/repeater

Okta Developer Blog – Why You Should Always Use HTTPS

https://developer.okta.com/blog/2019/08/22/why-you-should-always-use-https

OWASP Cheat Sheet Series Main Page (Optional for extra references)
https://cheatsheetseries.owasp.org/

Contact Details

Filipe Oliveira s222478779@deakin.edu.au

Pentest Leader Feedback.

Overall, great work! The finding is well-documented with clear steps to follow. However, please ensure consistency in font size and style, as there were some inconsistencies in your report. I have corrected them for you. Additionally, there were a few minor grammatical issues, such as the use of a lowercase “i” in the middle of a sentence and some missing commas, but these have been corrected for you as well.