BJIT ACADEMY

VAPT VULNERABILITIES

Target: cms.bjitacadey.com
Total vulnerabilities: 08

Submitted by:

Mahmud Iftekhar Asef
ID: 00-30107

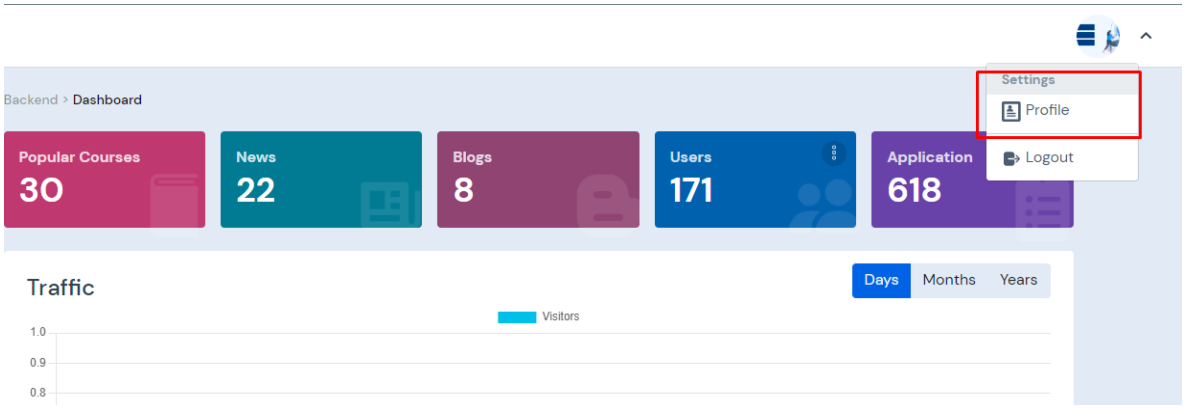
Submitted to:

Sad Murshid Khan Adon
Abdullah Al Nayeem
BJIT group

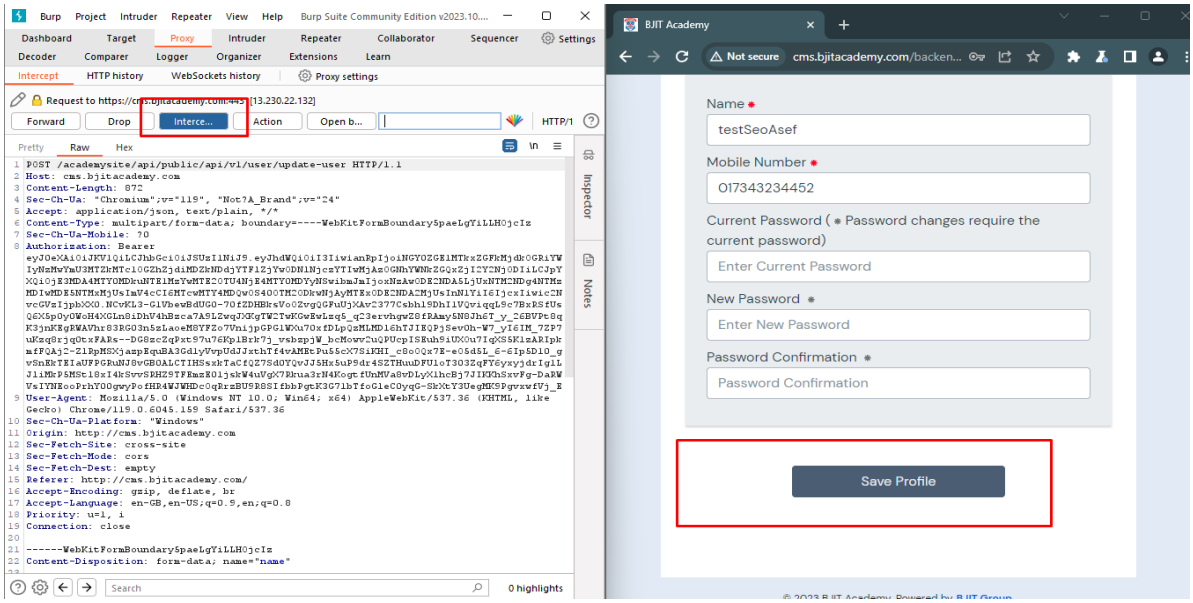
Vulnerability 1

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.bjitacadey.com,
URL/API: POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
POC:

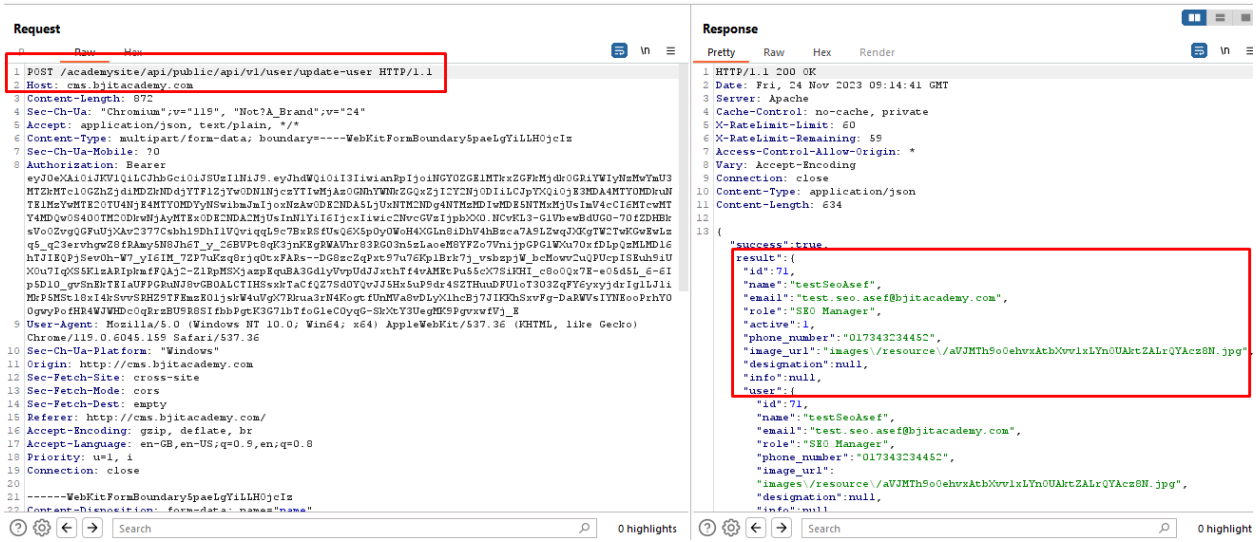
1. First I went to my profile and captured the GET request for personal information update.



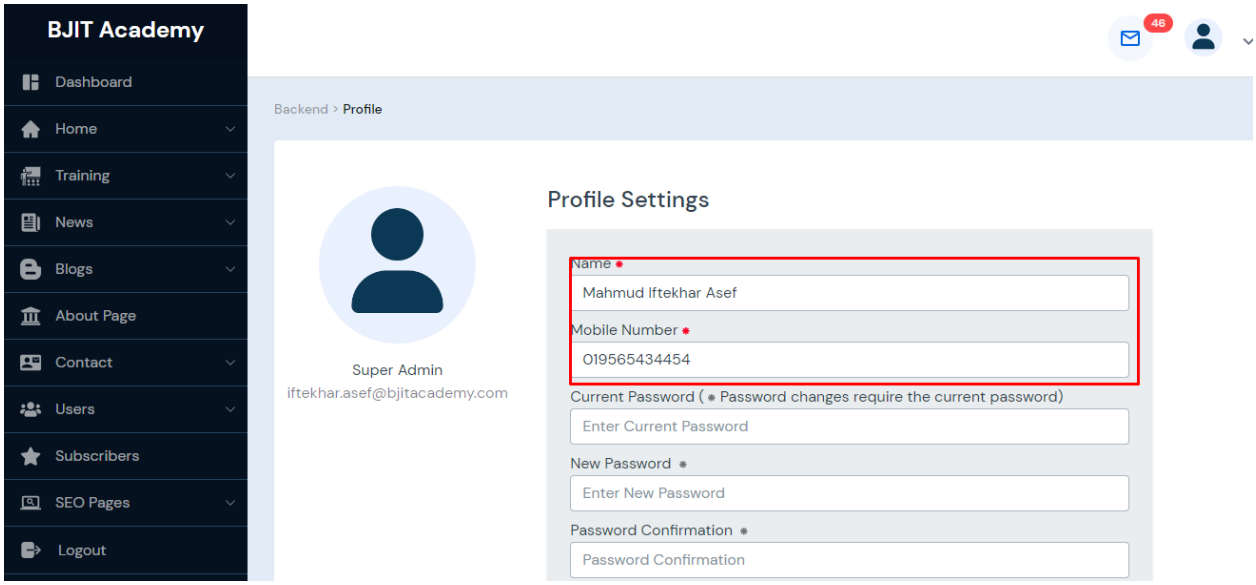
2. Then I clicked the save profile button and captured the request by intercepting it.



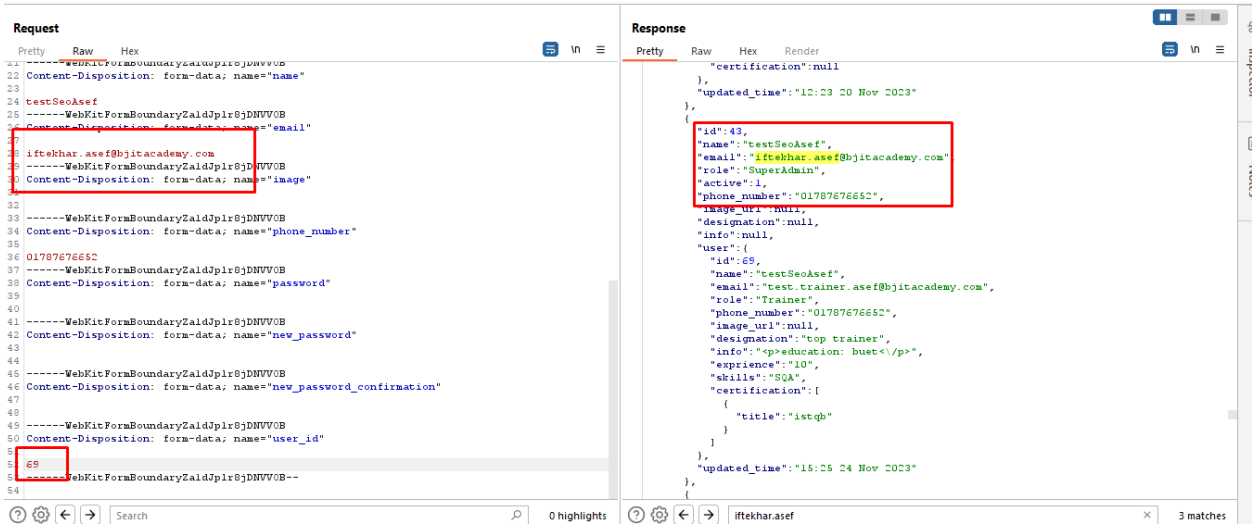
3. Then i sent the request and checked the response.



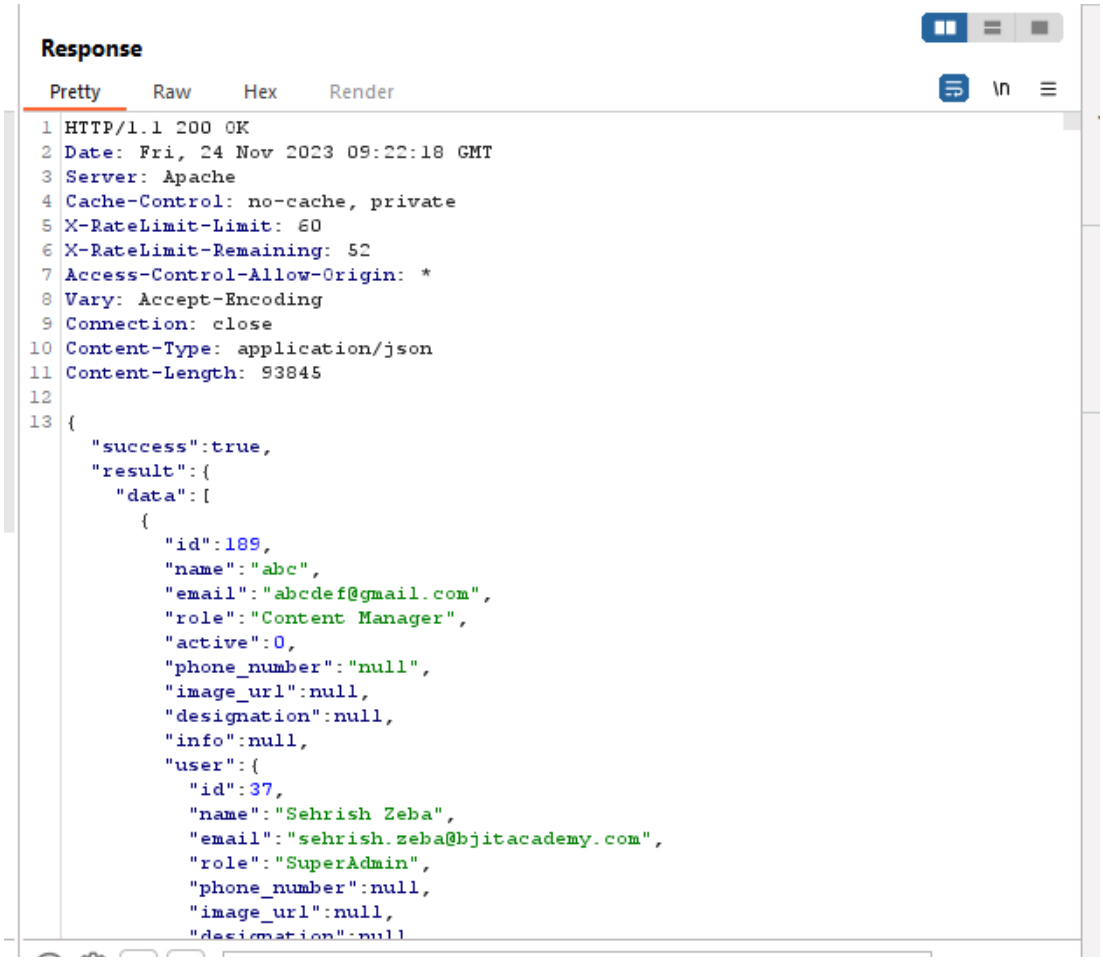
4. Here i also checked the super admin profile to check the user information.



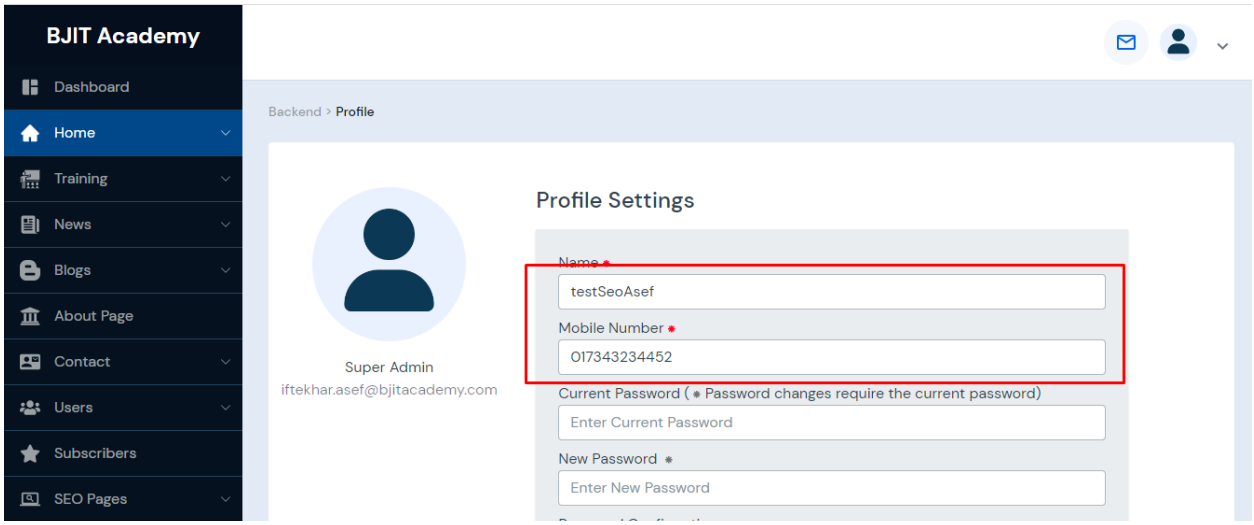
5. Then i changed the email of the user to super admin's email also changed the user id to change the update user by and sent the request and checked the request and got that the super admin's profile is updated with the given value.



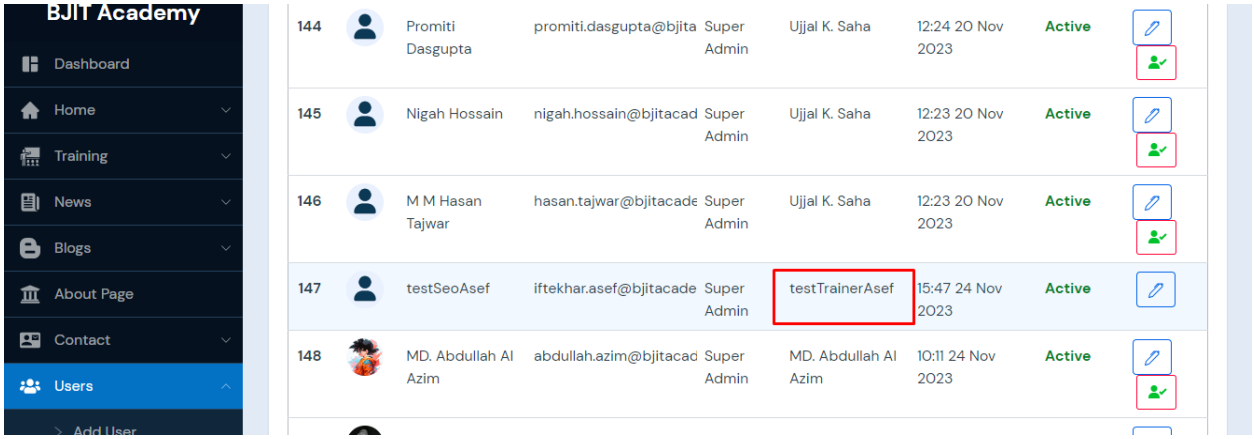
6. Also all the user information is disclosed by that single email change.



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



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.



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.

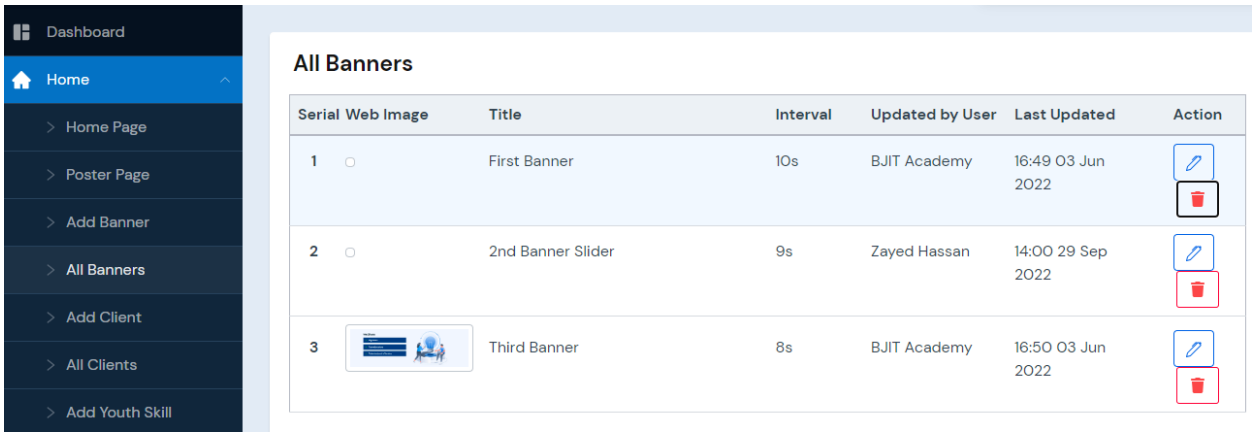
Target: cms.bjitacadey.com

URL/API:

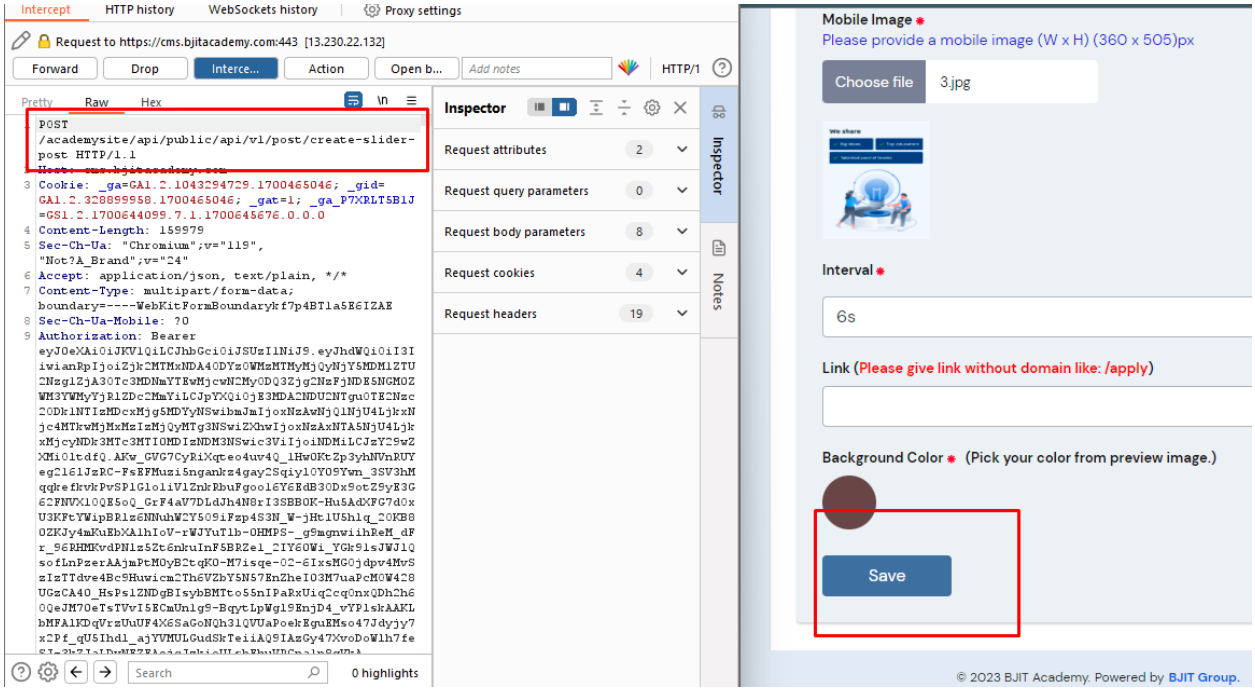
POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1
POST /academysite/api/public/api/v1/post/create-fresh-talent-scope
POST /academysite/api/public/api/v1/testimonial/create-testimonial HTTP/1.1
POST /academysite/api/public/api/v1/location/add-location HTTP/1.1

POC:

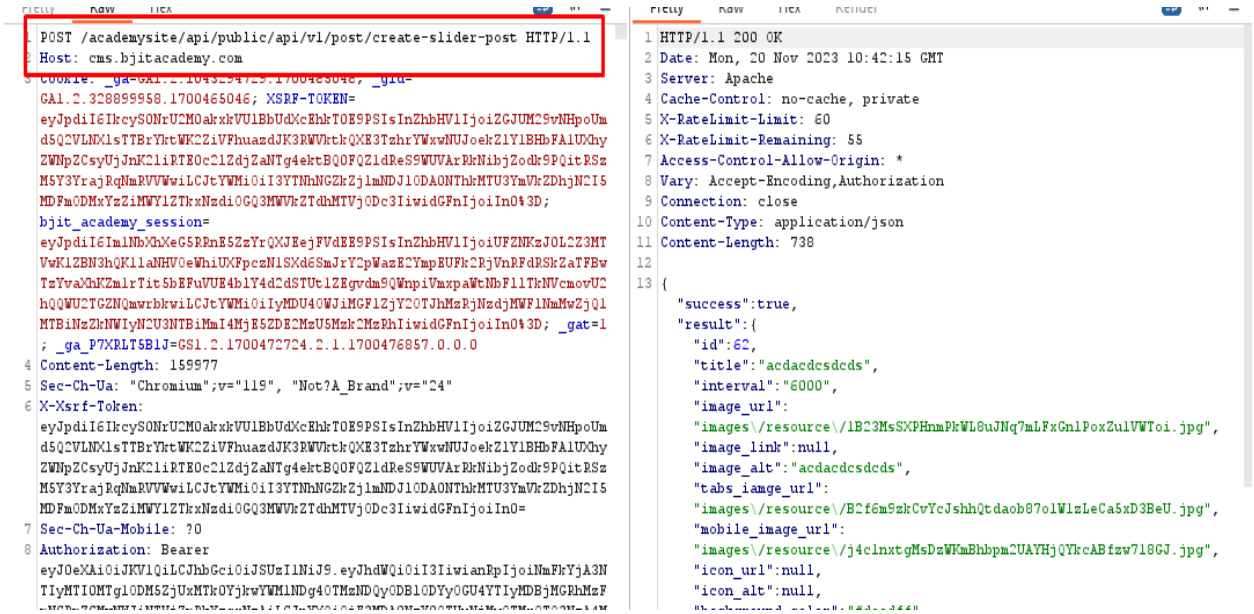
1. Firstly i logged in as super admin user to check all the banners.

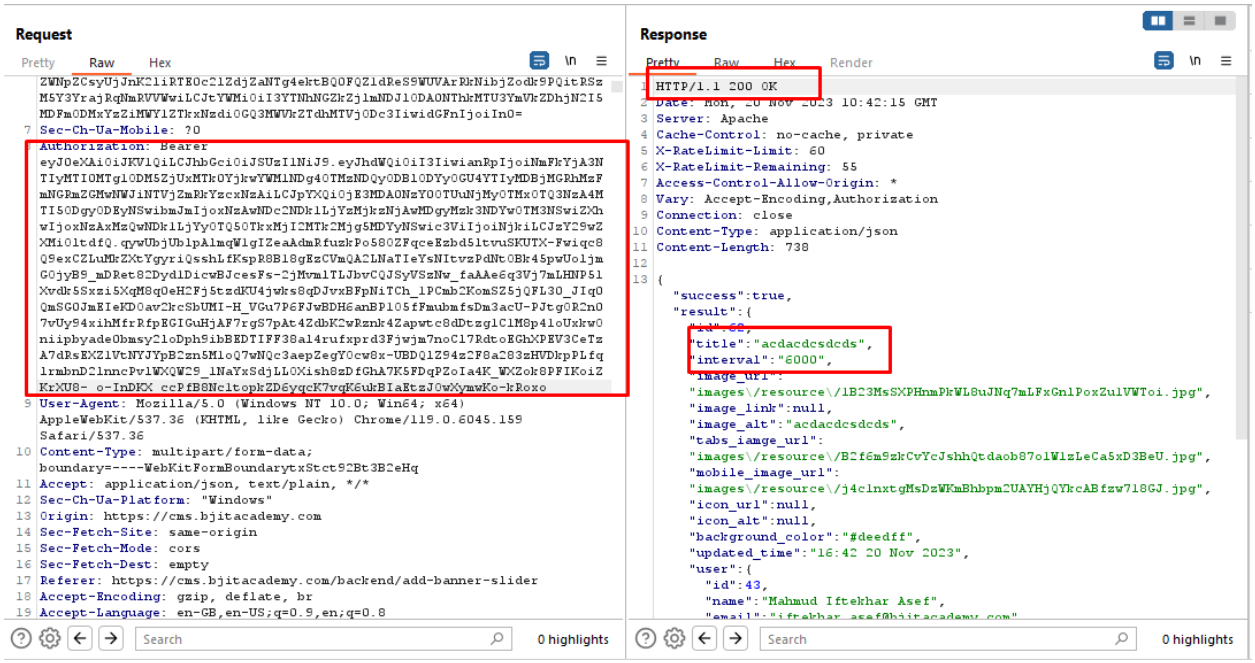


2. Here I captured the add banner request using super admin, clicking the save button and sent it to the repeater.

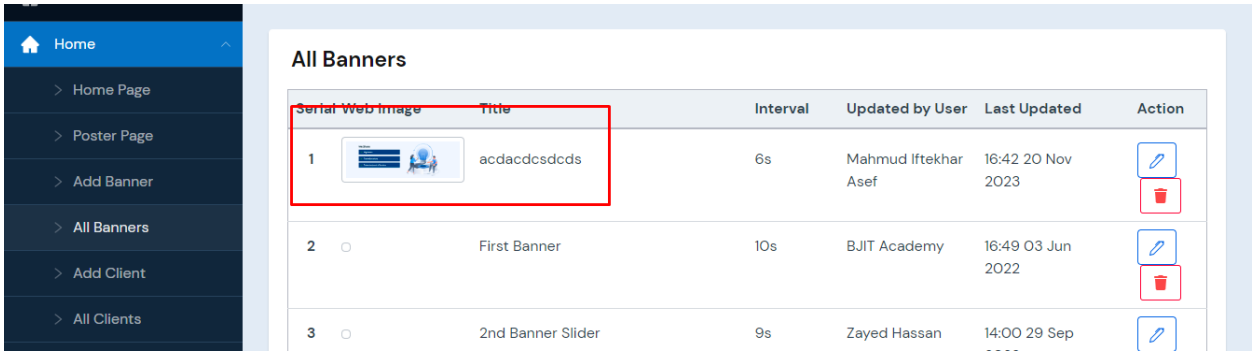


3. After that i got the token of trainer as trainer has the least privilege, and used that for the non privileged request which is adding banner.





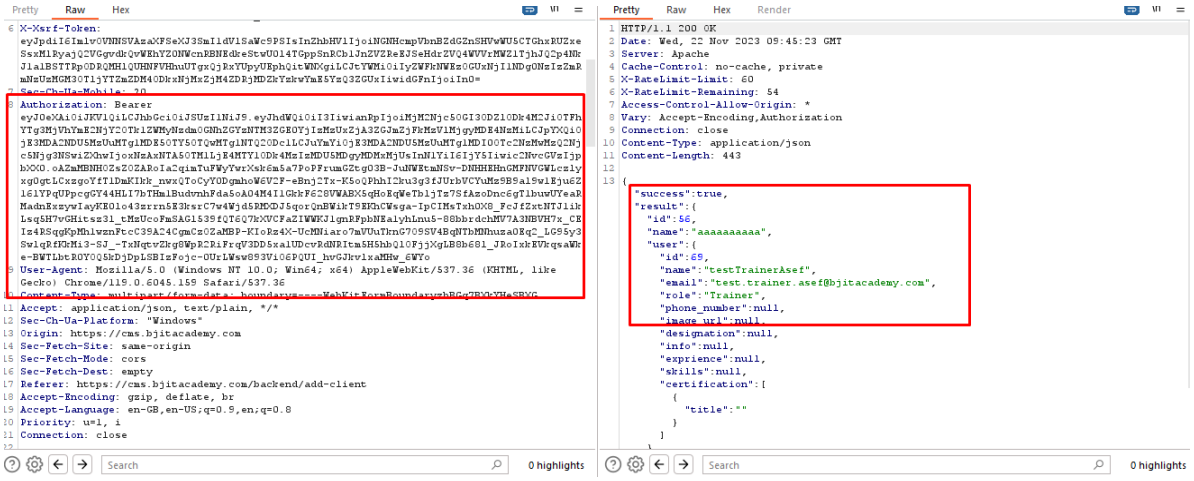
4. After sending the request I got status 200 OK, and from the dashboard the banner is uploaded.



Other URL/API Screenshots:

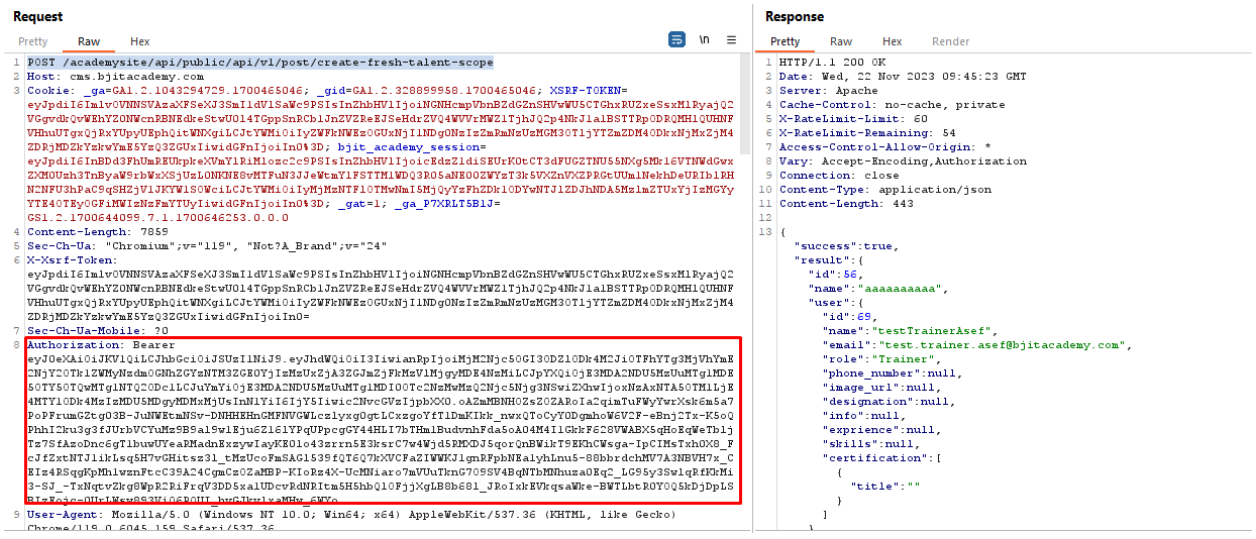
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1

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



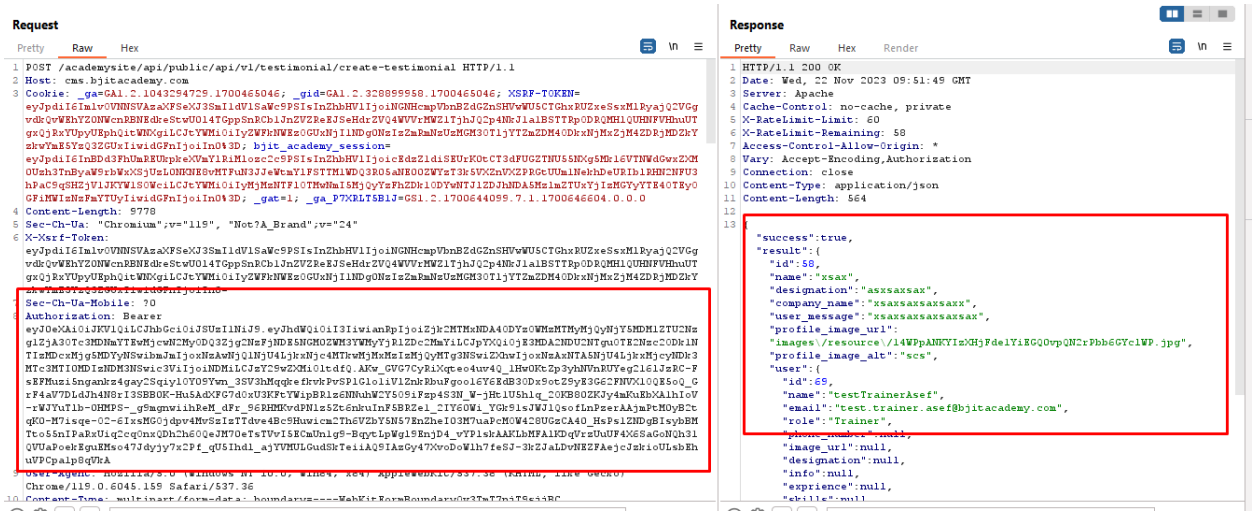
POST /academysite/api/public/api/v1/post/create-fresh-talent-scope

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



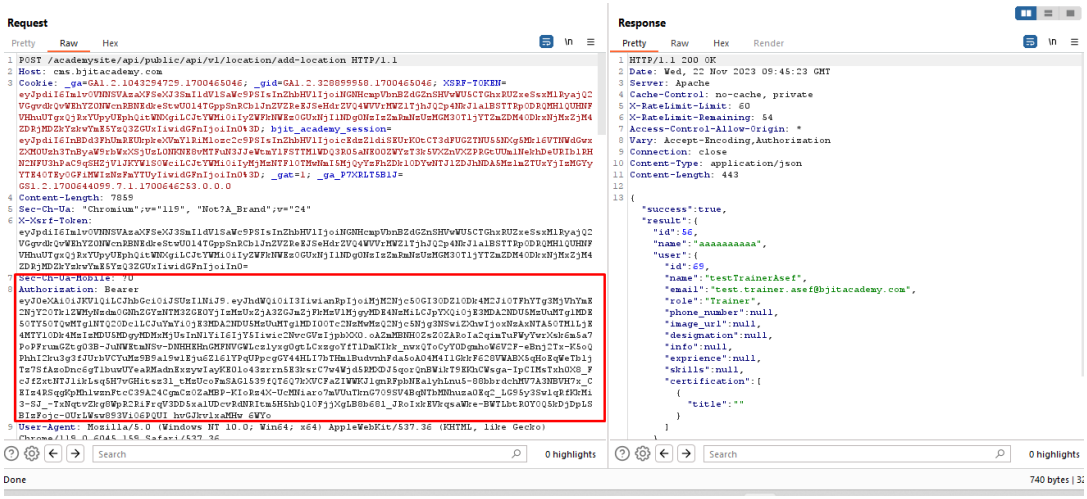
POST /academysite/api/public/api/v1/testimonial/create-testimonial HTTP/1.1

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



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

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

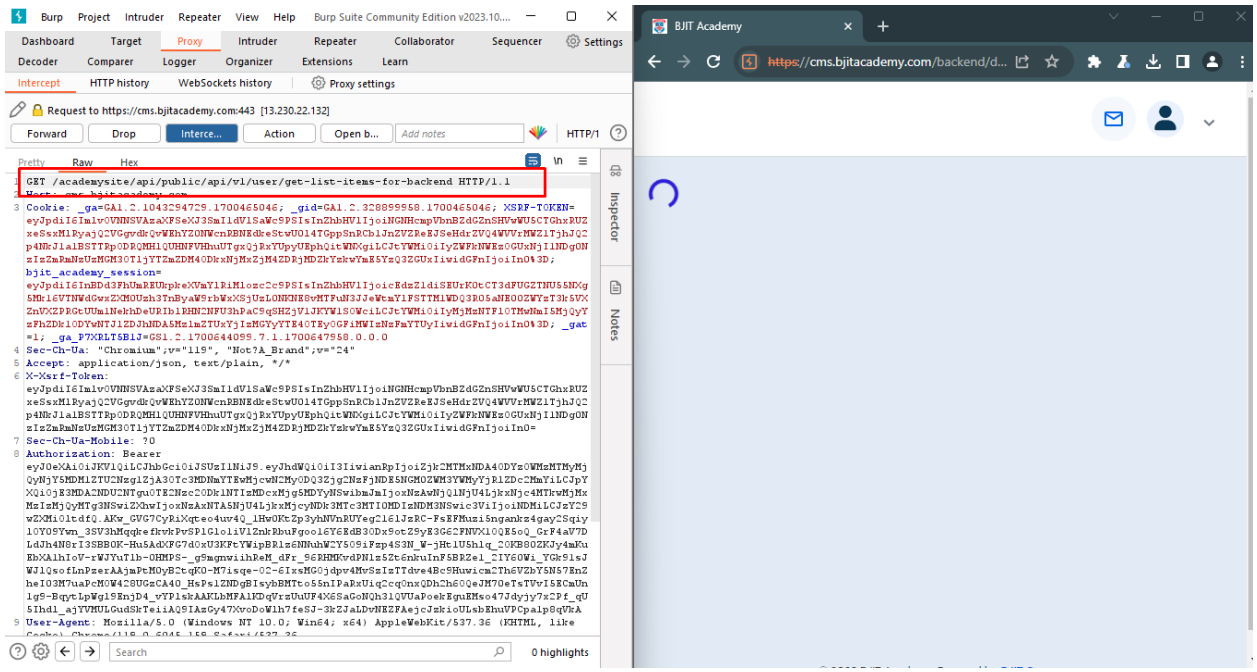


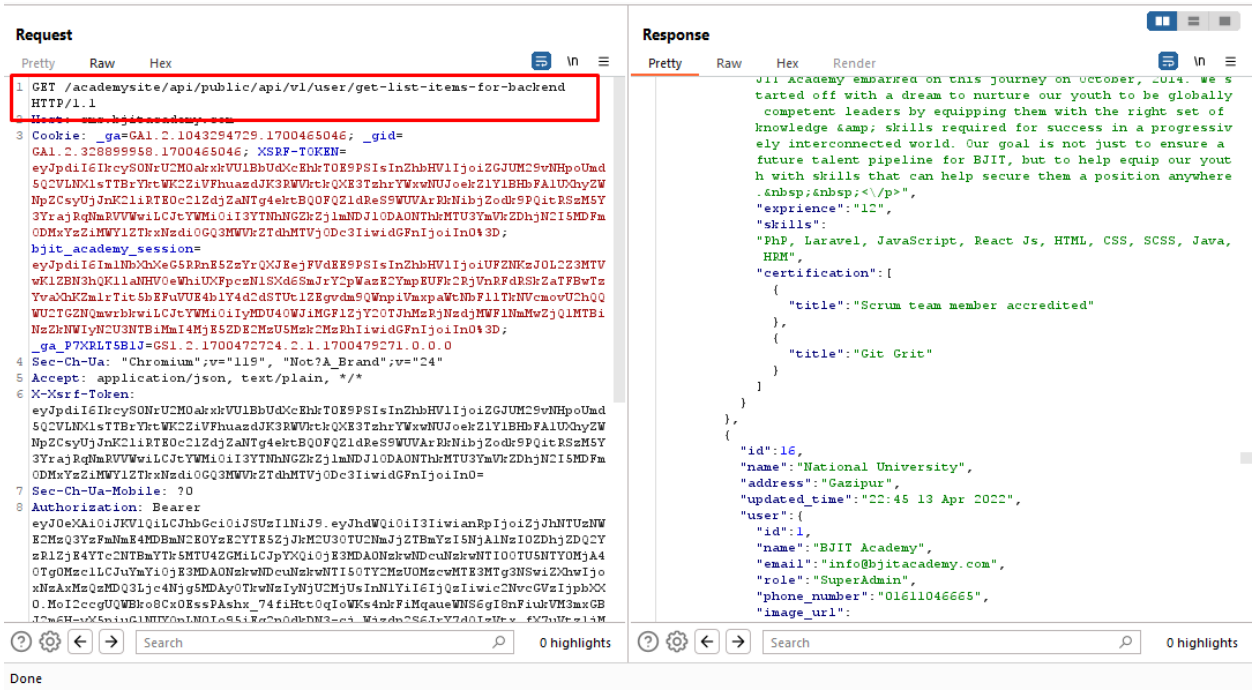
Vulnerability 3

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.bjitacadey.com,
URL/API:
GET /academysite/api/public/api/v1/user/get-list-items-for-backend HTTP/1.
GET /academysite/api/public/api/v1/user/get-all-applications-and-contacts-for-backend HTTP/1.1

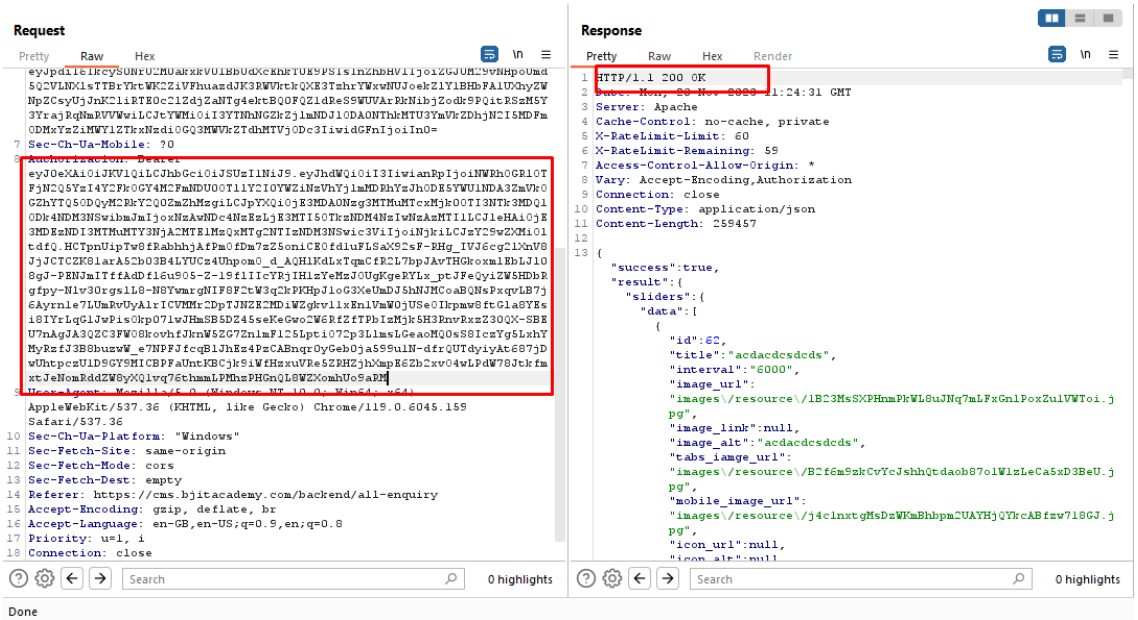
POC:

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



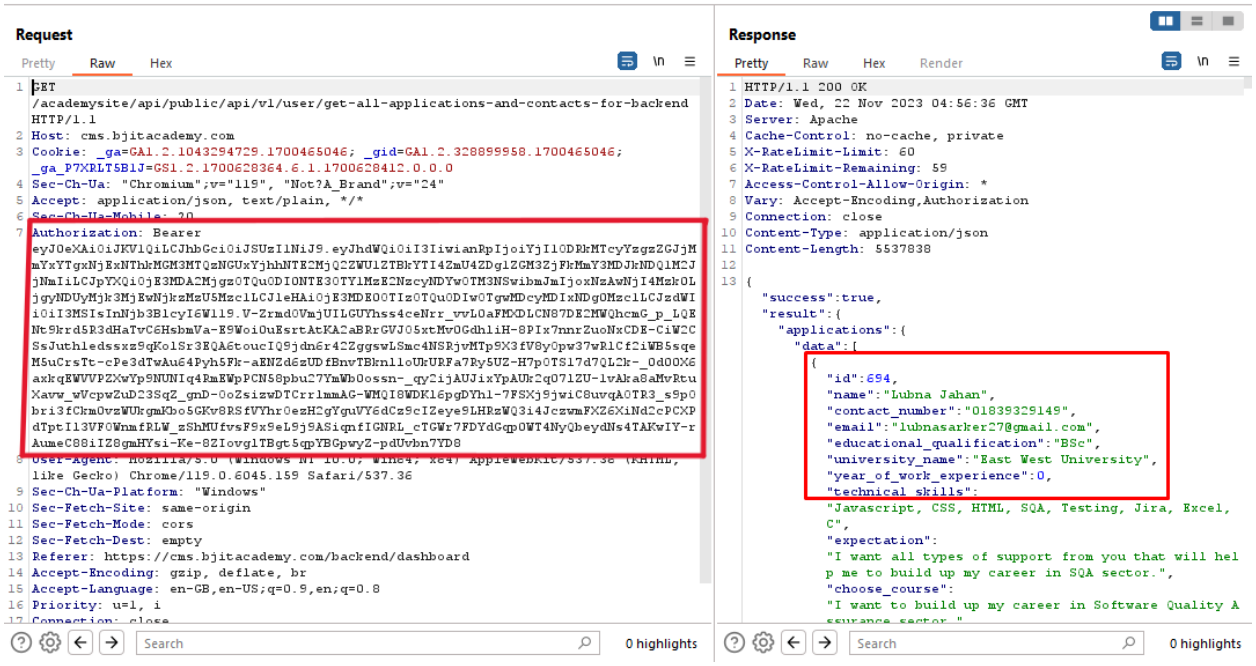


2. Then I changed the token of the super admin to trainer's as trainer shouldn't be allowed to fetch all data, and sent the request which shows the status 200 OK and showing all data.



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

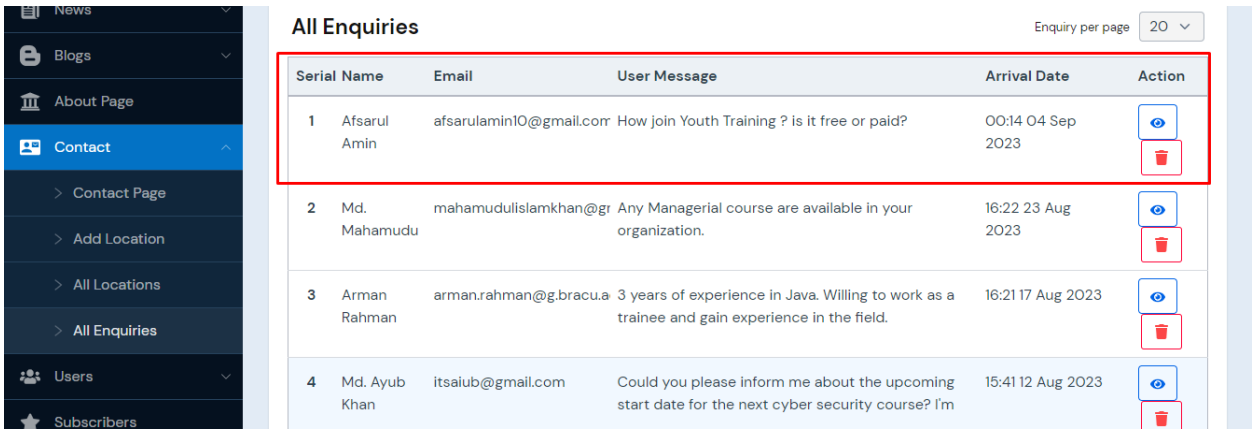
Dashboard>capture request>change token>send request>successful with all information disclosed.



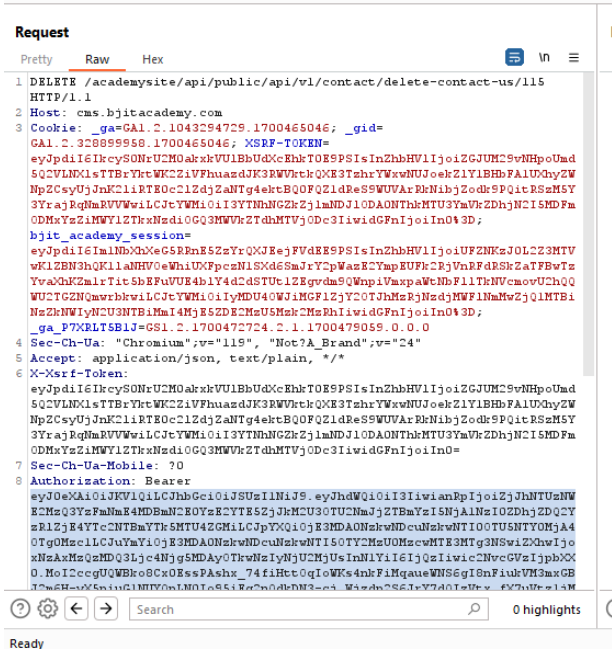
Vulnerability 4

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:

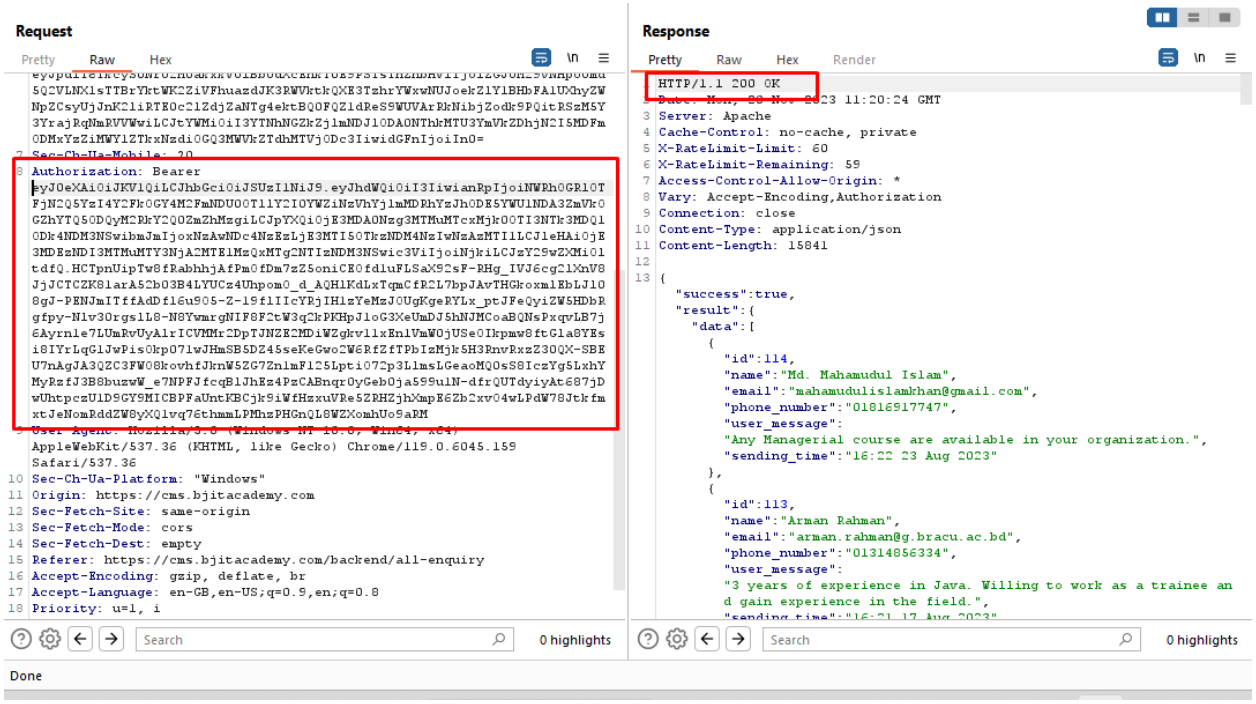
1. First i logged in as admin to see all the contract andBefore deleting the contact, here is the contact i am going to delete.



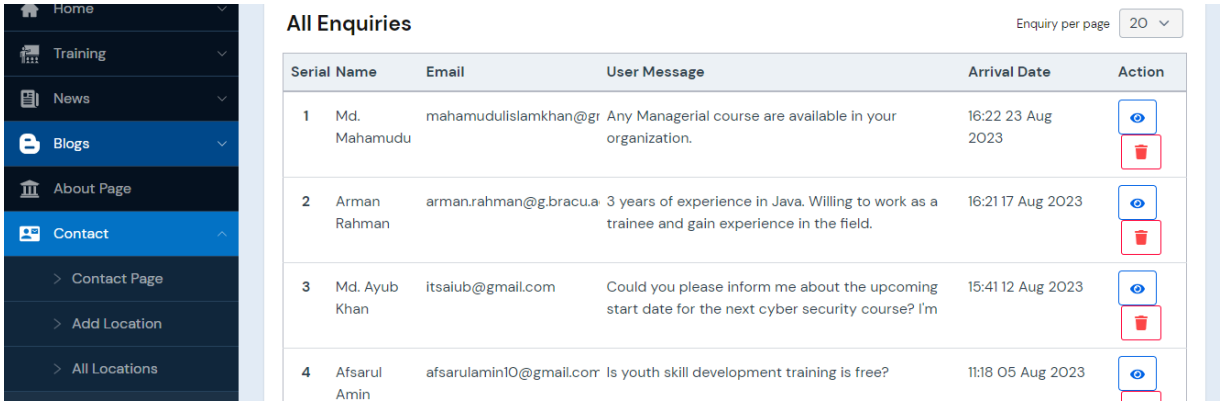
2. I captured the delete contact request by clicking the delete button and sent it to the repeater.



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.



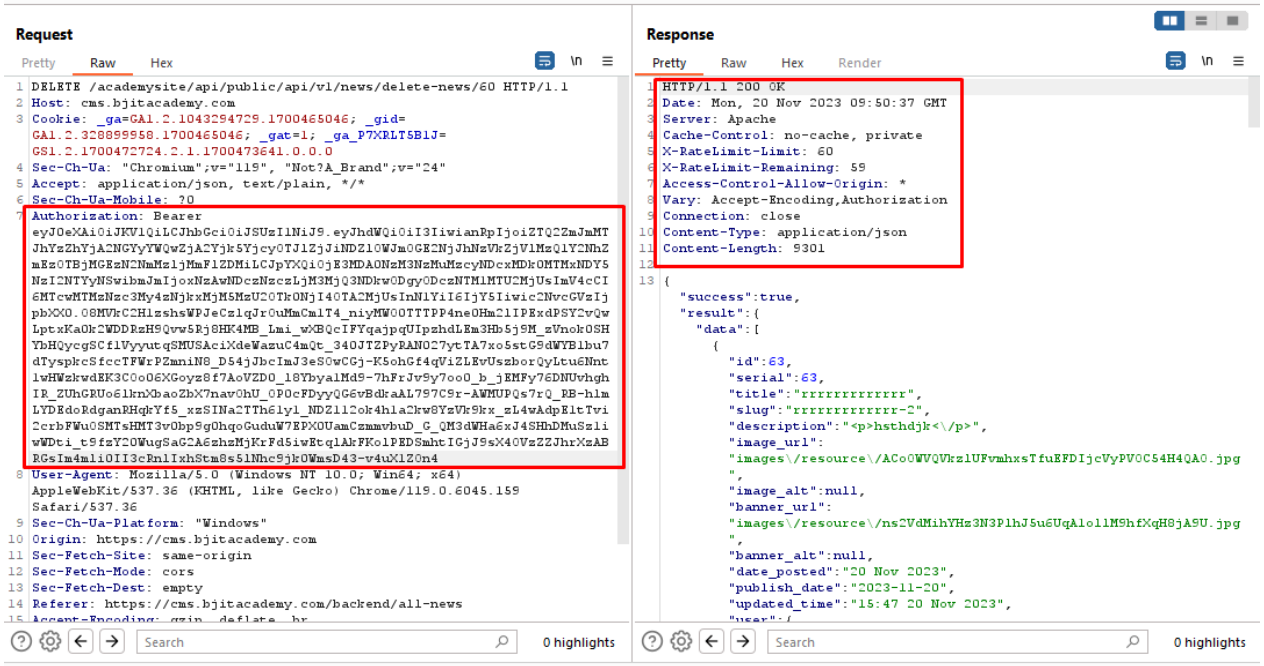
4. After that i checked the front end to ensure the deletion and there is no contact as the deletion was successful.



Other URL/API Screenshots:

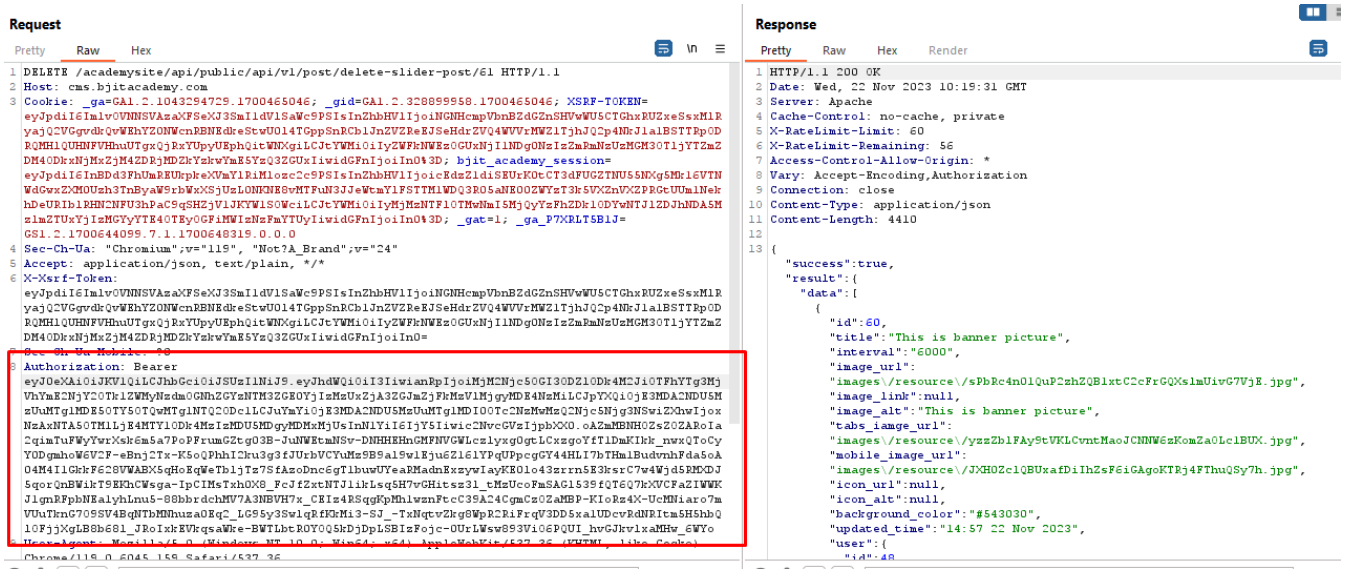
DELETE /academysite/api/public/api/v1/news/delete-news/62 HTTP/1.1

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



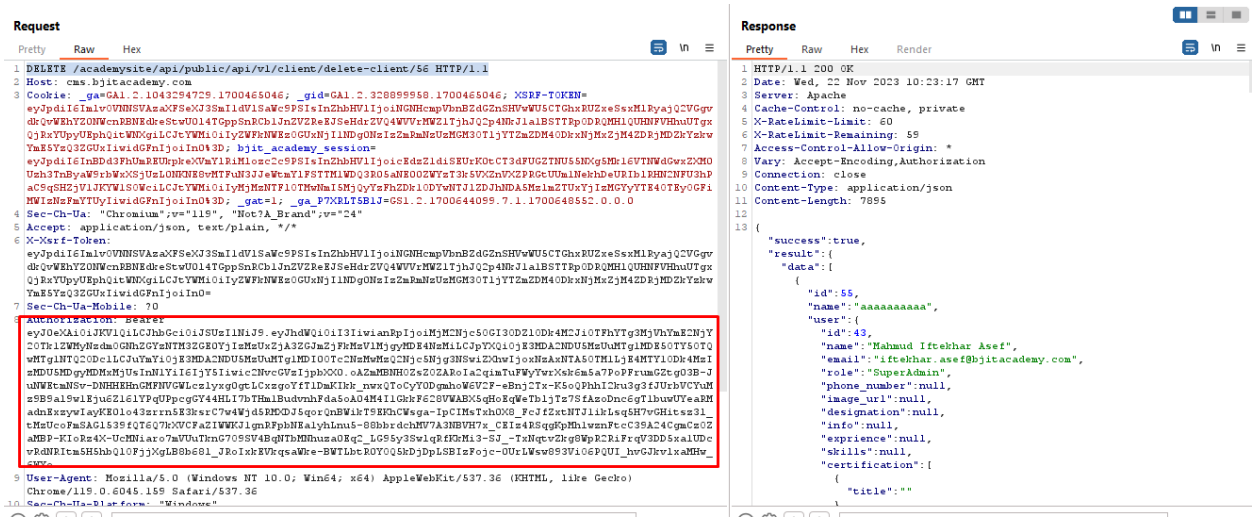
DELETE /academysite/api/public/api/v1/post/delete-slider-post/61 HTTP/1.1

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



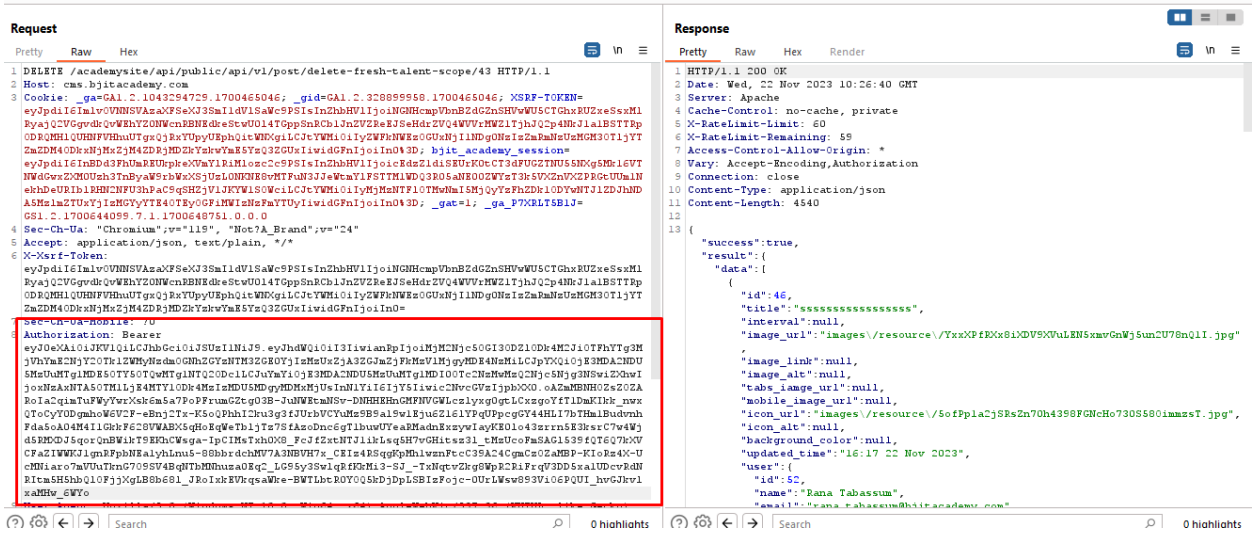
DELETE /academysite/api/public/api/v1/client/delete-client/56 HTTP/1.1

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



DELETE /academysite/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.

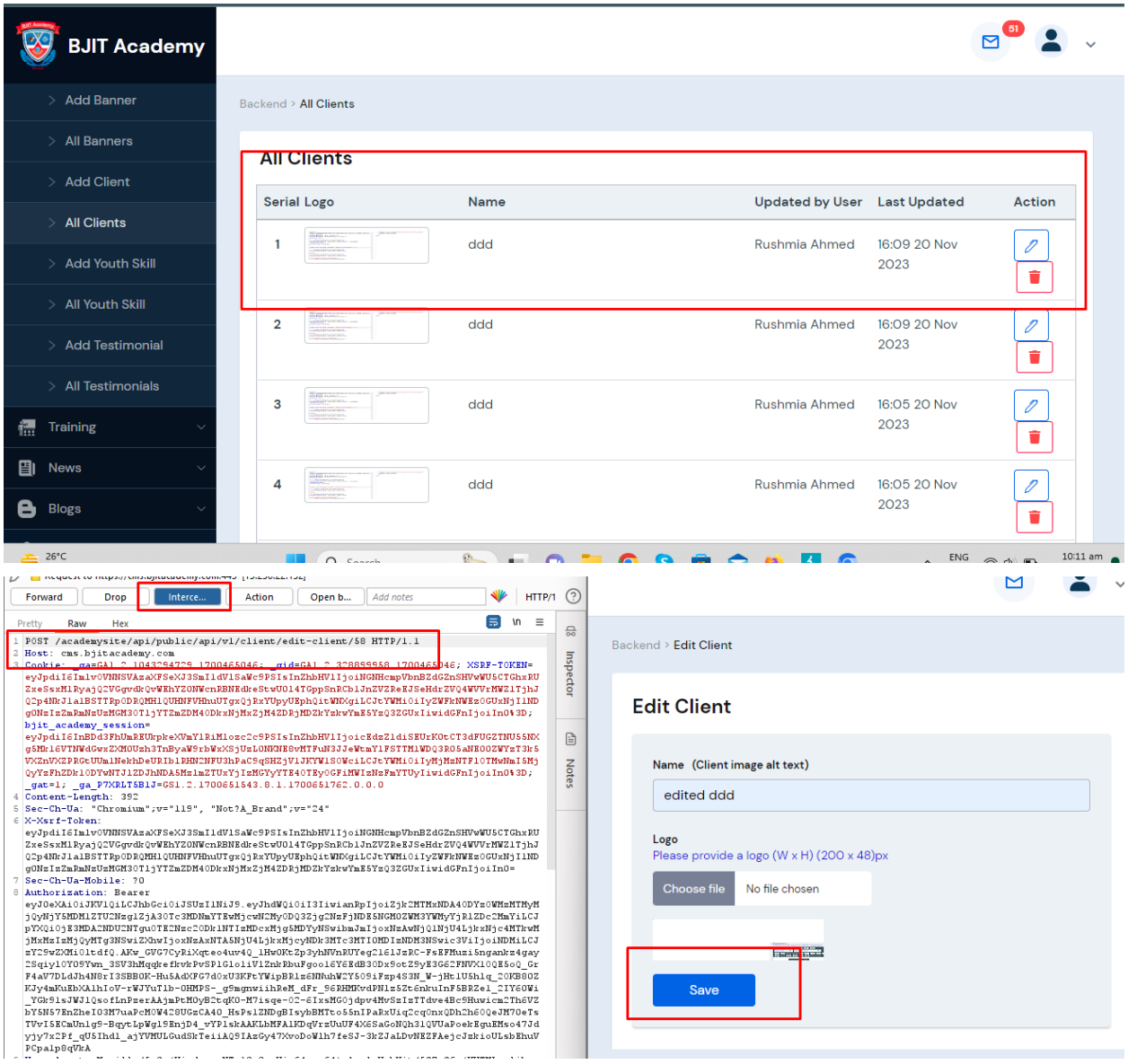
Target:cms.bjitacadey.com

URL/API:

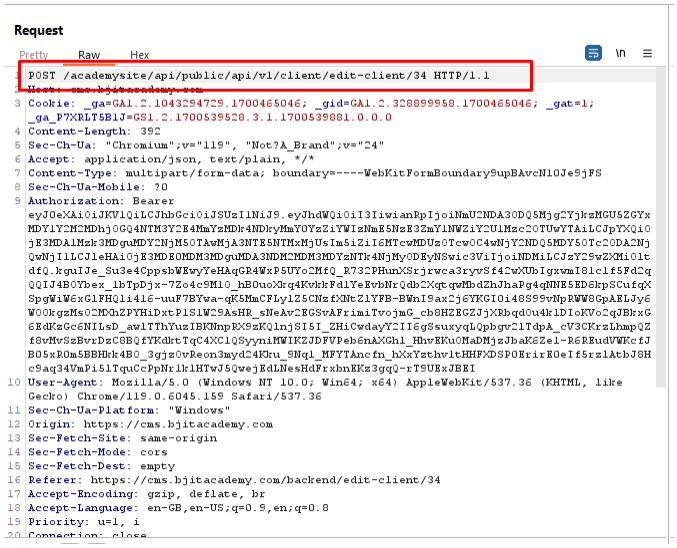
POST /academysite/api/public/api/v1/client/edit-client/34 HTTP/1.1
POST /academysite/api/public/api/v1/post/edit-slider-post/60 HTTP/1.1
POST /academysite/api/public/api/v1/post/edit-fresh-talent-scope/46 HTTP/1.1
POST /academysite/api/public/api/v1/testimonial/edit-testimonial/58 HTTP/1.1
POST /academysite/api/public/api/v1/user/update-user 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

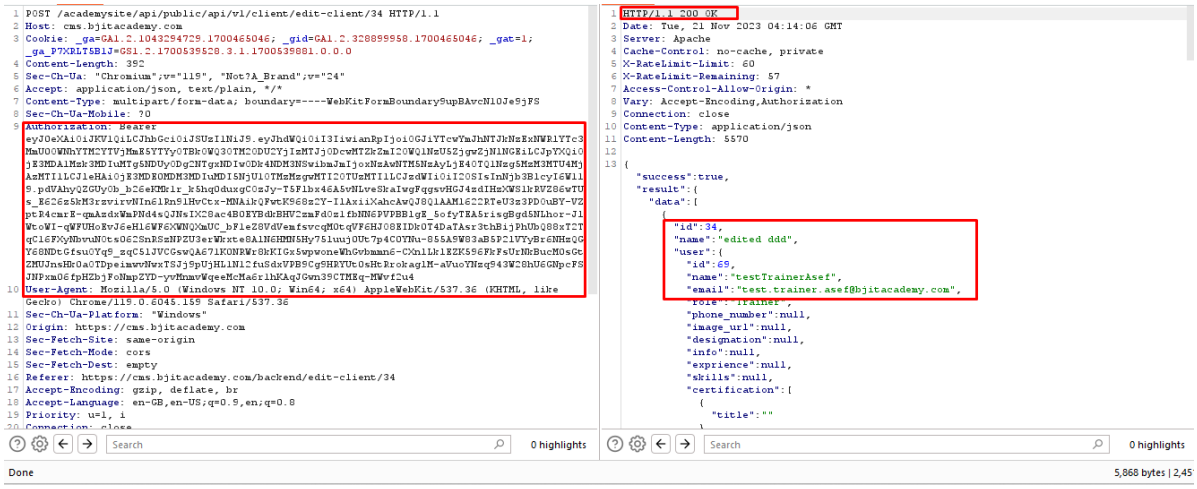
POC:

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

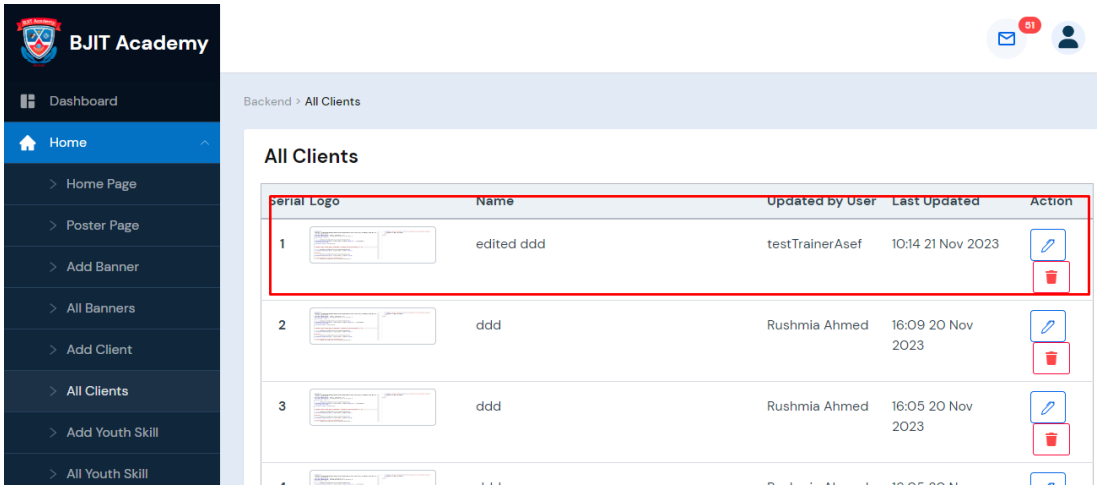


2. After that i sent the request to the repeater and changed the token to trainer's token as it does not have the privilege to any client and sent the request which leads to status 200 OK.



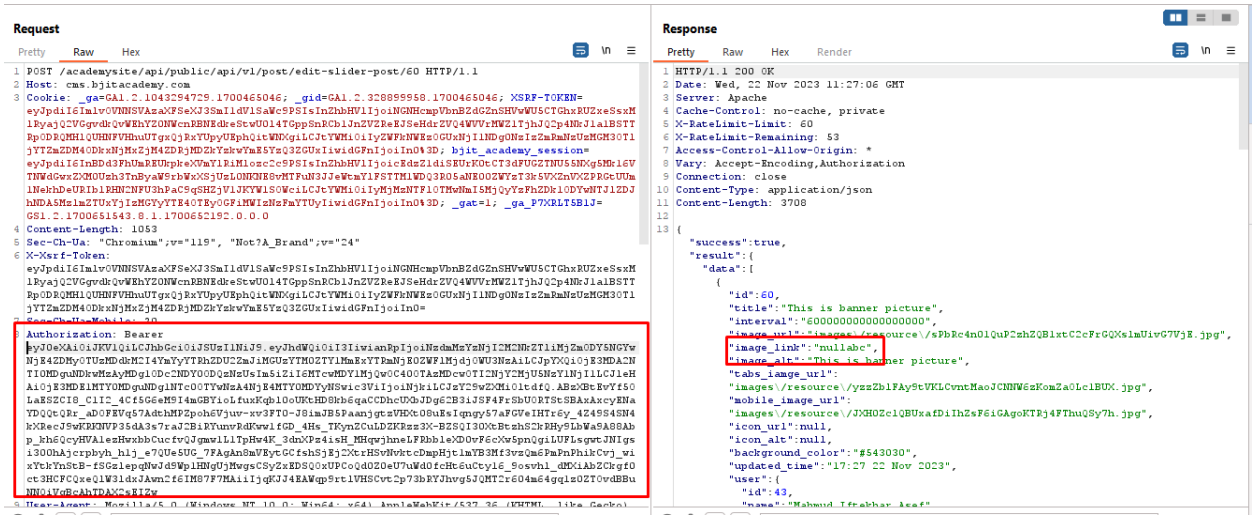


3. After that I checked the front end to ensure the edit and the edit is successful.



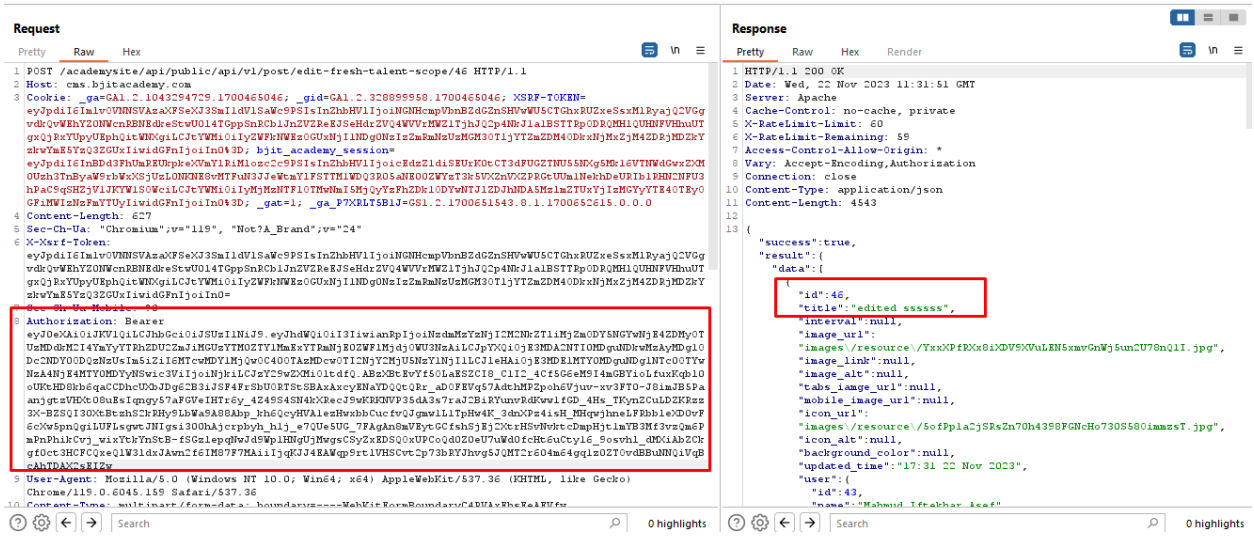
POST /academysite/api/public/api/v1/post/edit-slider-post/60 HTTP/1.1

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



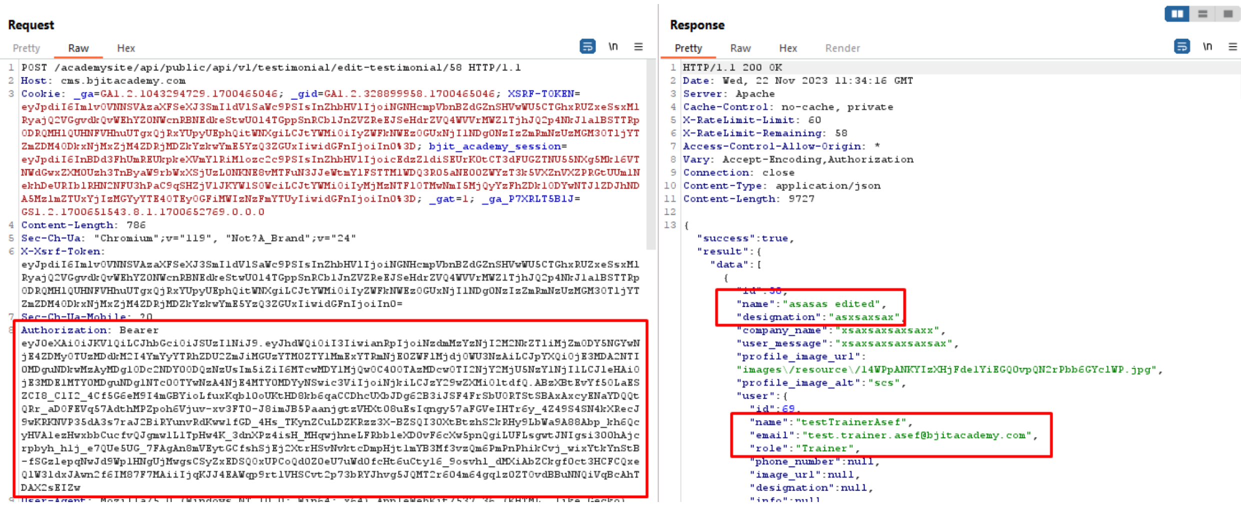
POST /academysite/api/public/api/v1/post/edit-fresh-talent-scope/46 HTTP/1.1

Edit youth skill>capture request>change token>send request>successful edit.



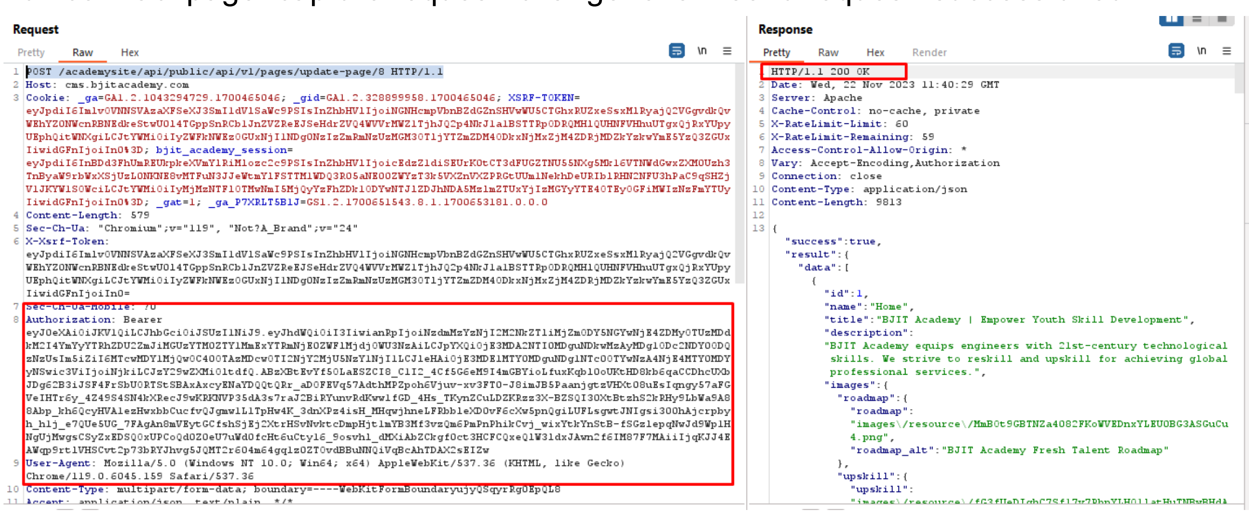
POST /academysite/api/public/api/v1/testimonial/edit-testimonial/58 HTTP/1.1

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



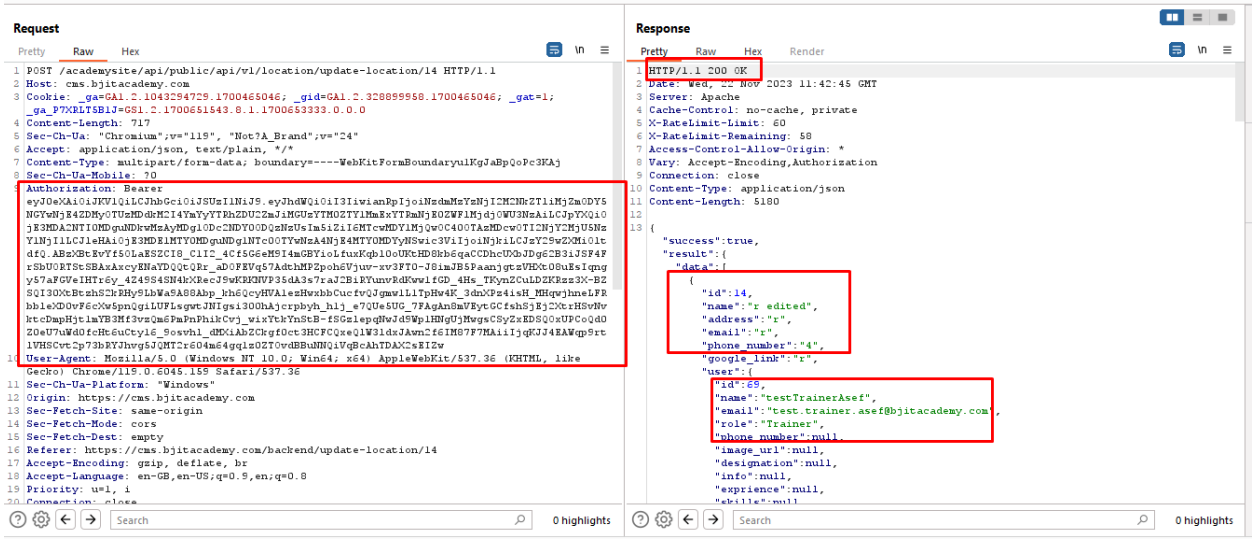
POST /academysite/api/public/api/v1/pages/update-page/8 HTTP/1.1

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



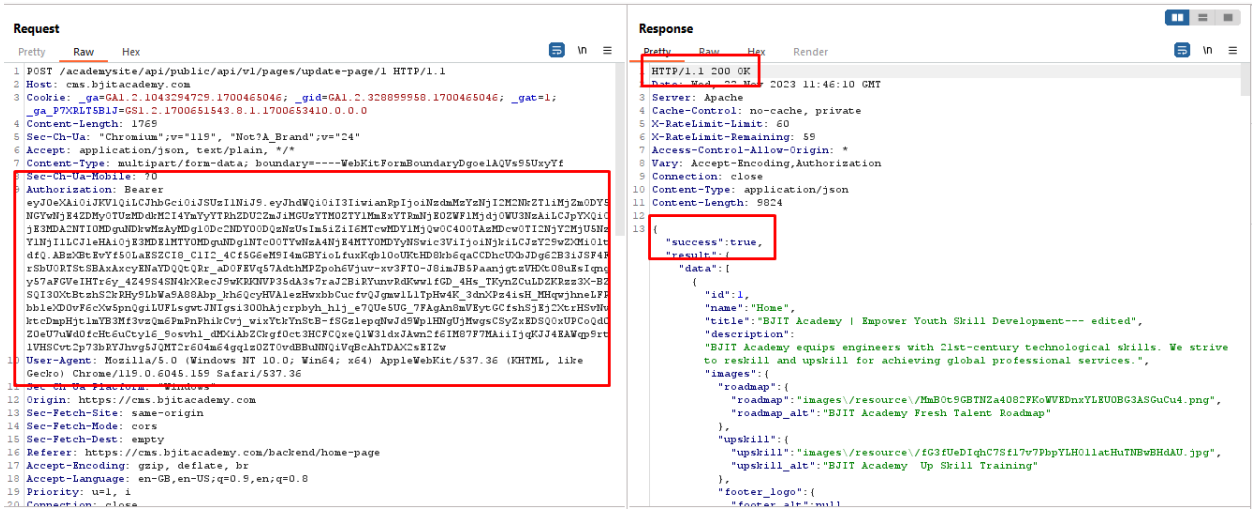
POST /academysite/api/public/api/v1/pages/update-page/14 HTTP/1.1

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.

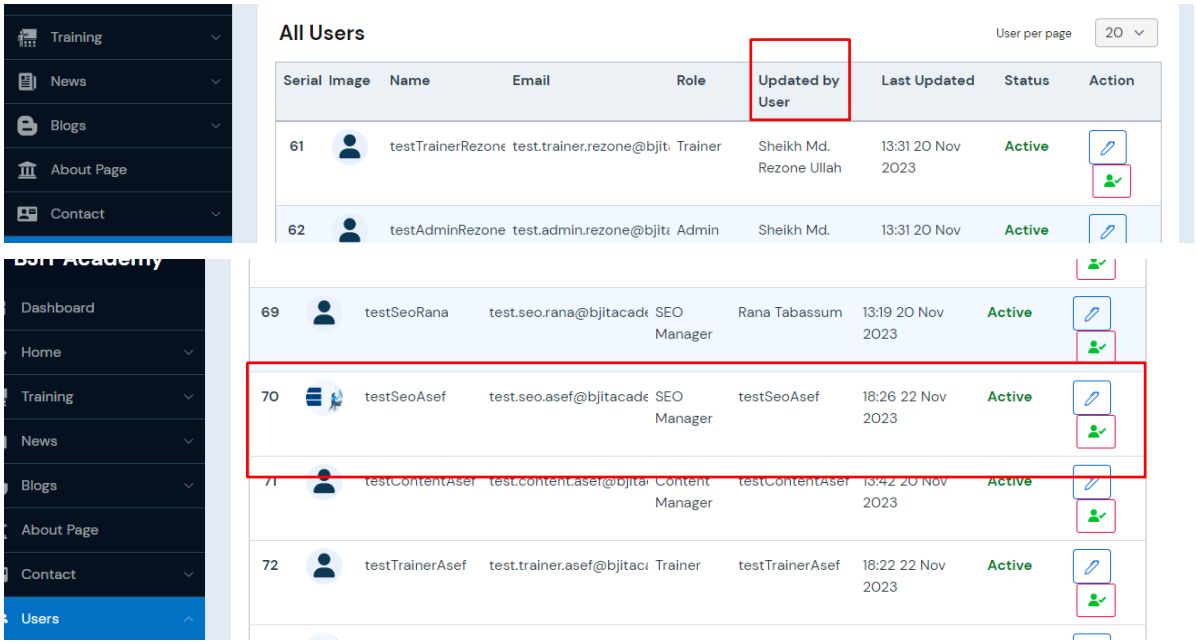
Description: This vulnerability enables unauthorized users to change the "Updated by User" field to different user IDs, disclosing sensitive information and affecting the integrity of user data. The issue highlights a failure in enforcing proper access controls, allowing manipulation of user profiles.

Target: cms.bjitacadey.com

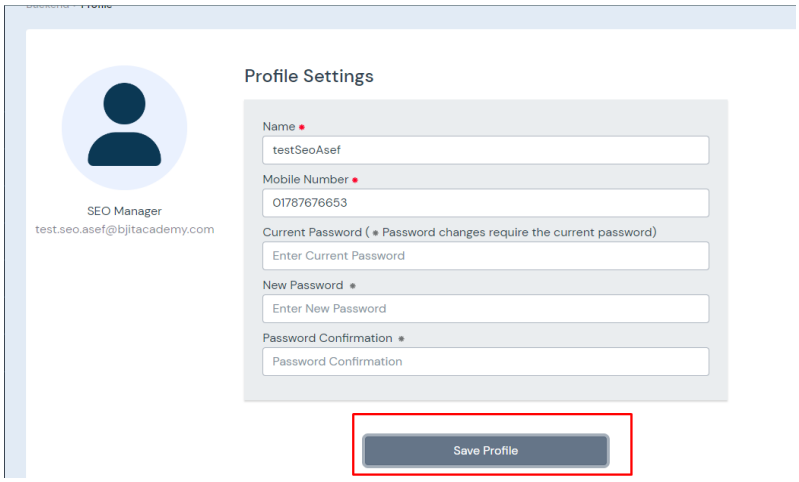
URL/API: POST /academysite/api/public/api/v1/user/update-user HTTP/1.1

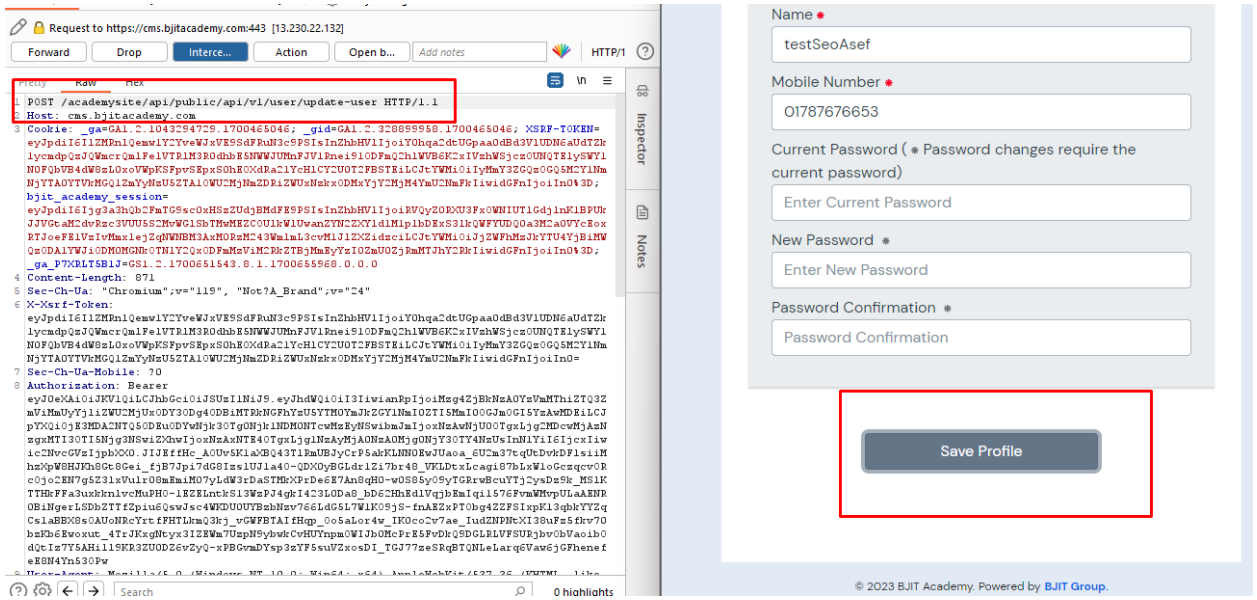
POC:

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

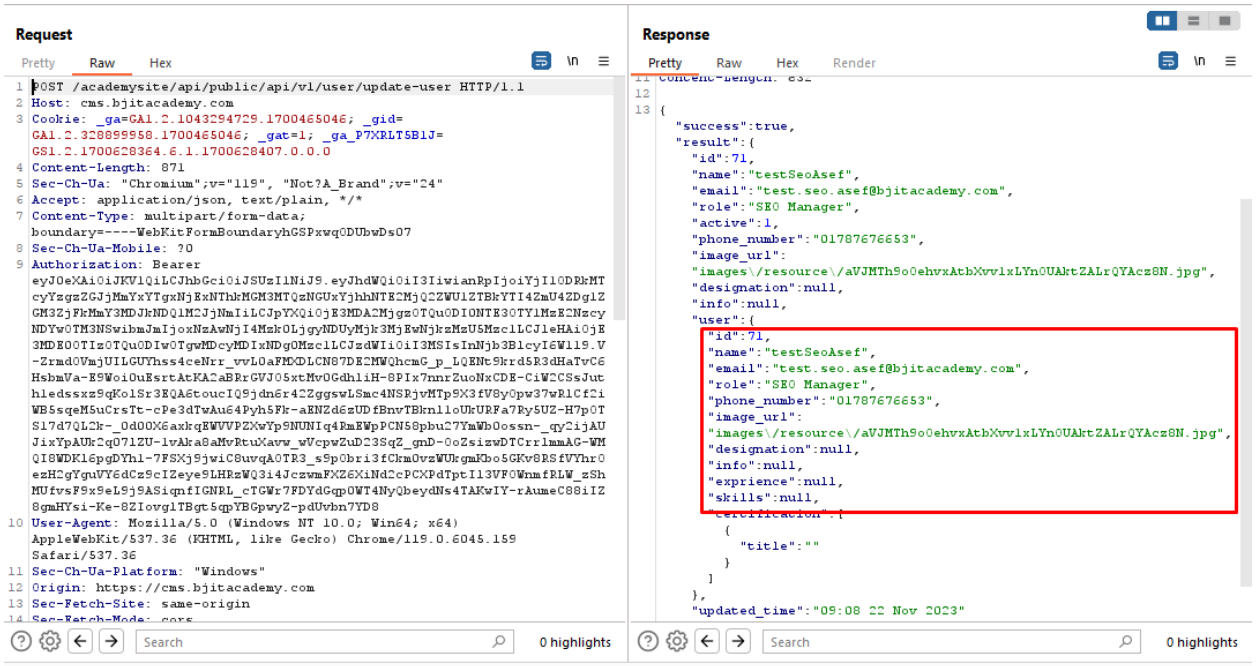


2. Then I went to my update profile setting of the SEO Manager, change phone number and clicked save profile to capture the request.

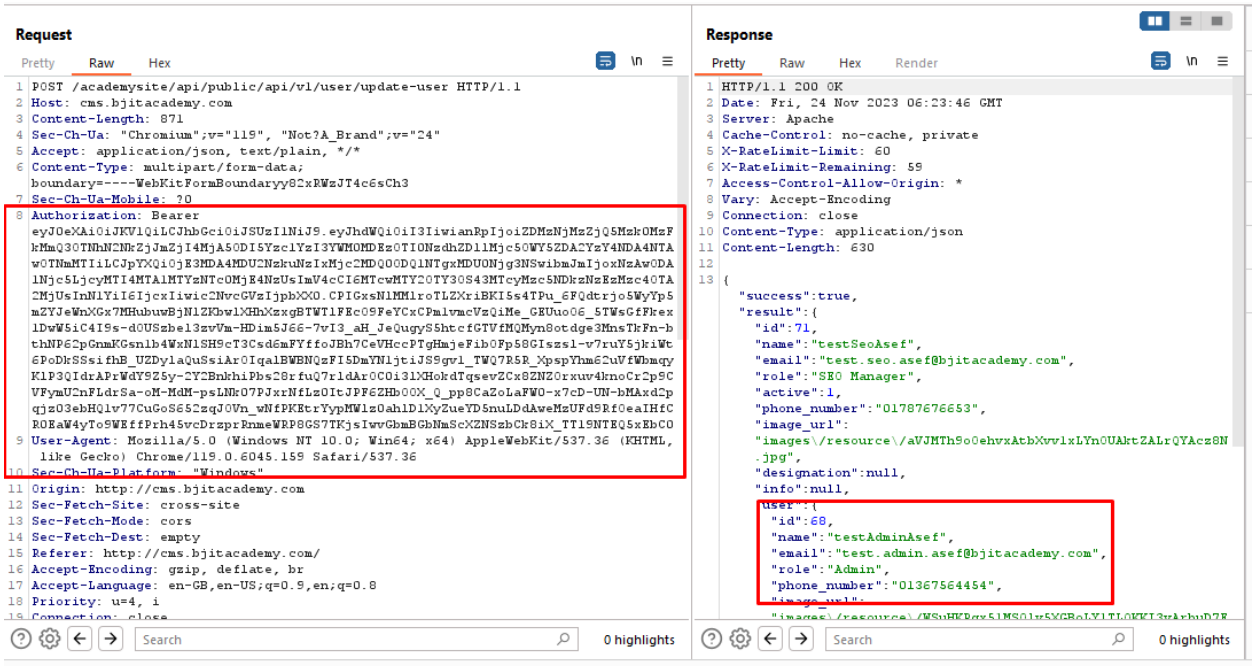


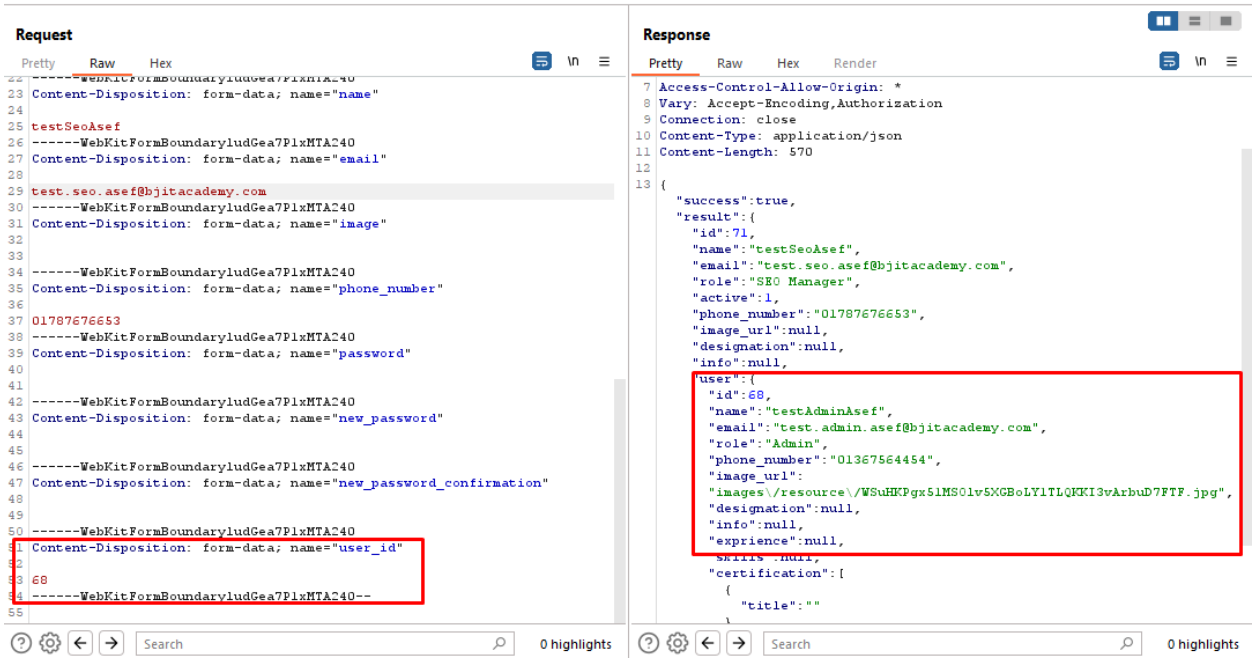


3. Then I sent the request to the repeater and checked the response.

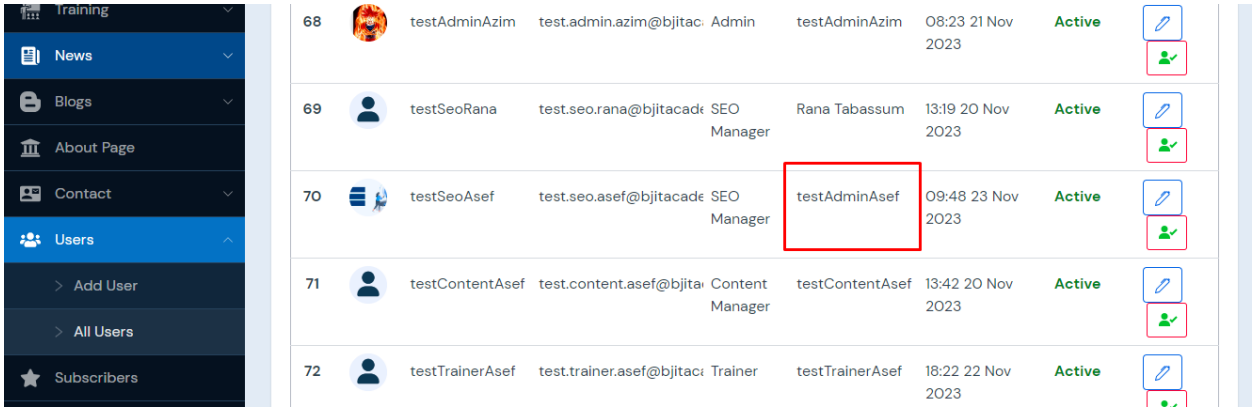


4. After that i changed the token of SEO with trainer's token and also changed the user id to admin's id to check the response and i got the information of admin, which is phone number, image URL which may lead to various attacks also it changes the updated by user name in the all users dashboard ..





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.



Vulnerability 7

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

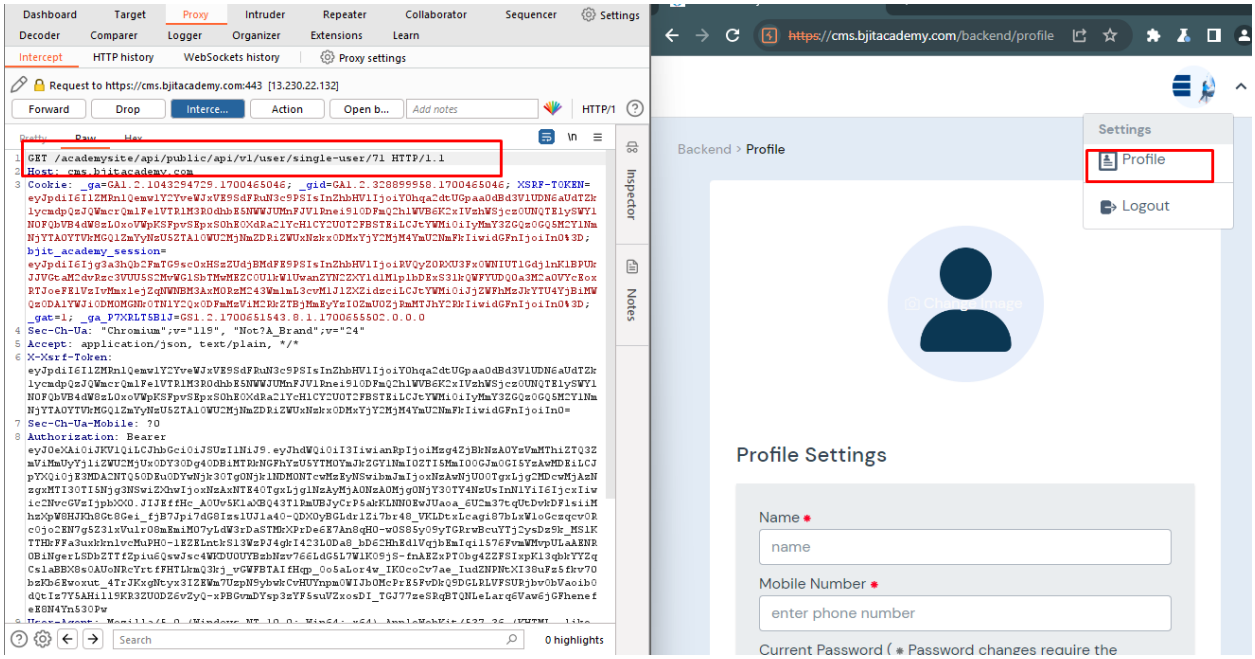
Description: The identified vulnerability allows unauthorized users to disclose sensitive information by manipulating the ID parameter in the API request. By capturing and replicating the GET request initiated by a user to fetch personal information, an attacker can modify the user ID in the parameter.

Target:cms.bjitacadey.com

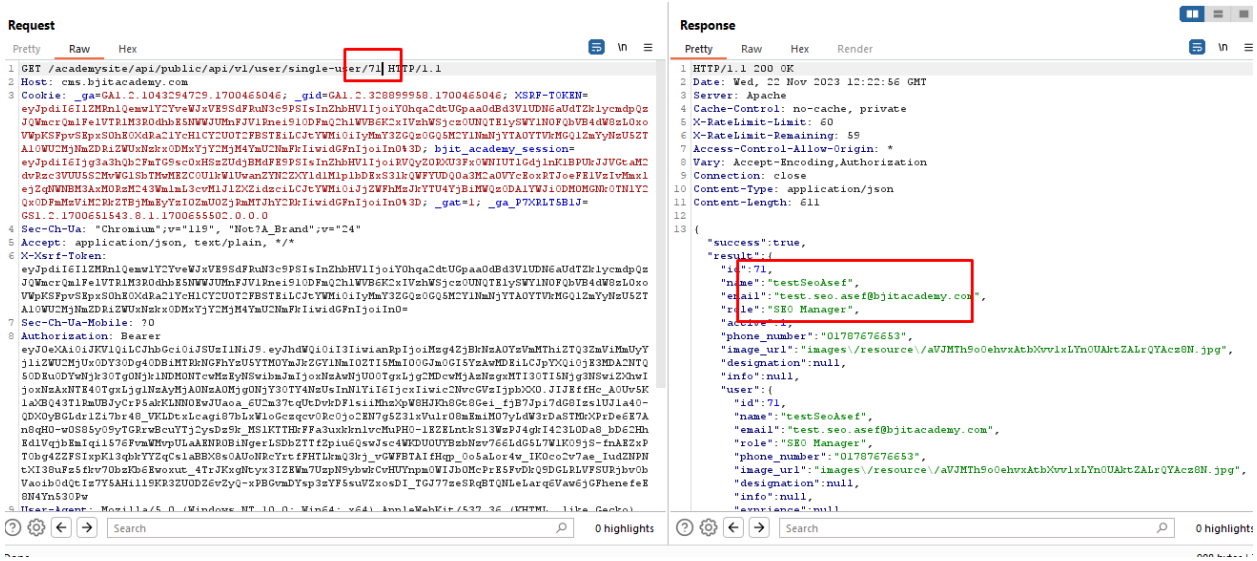
URL/API: GET /academysite/api/public/api/v1/user/single-user/<id> HTTP/1.1

POC:

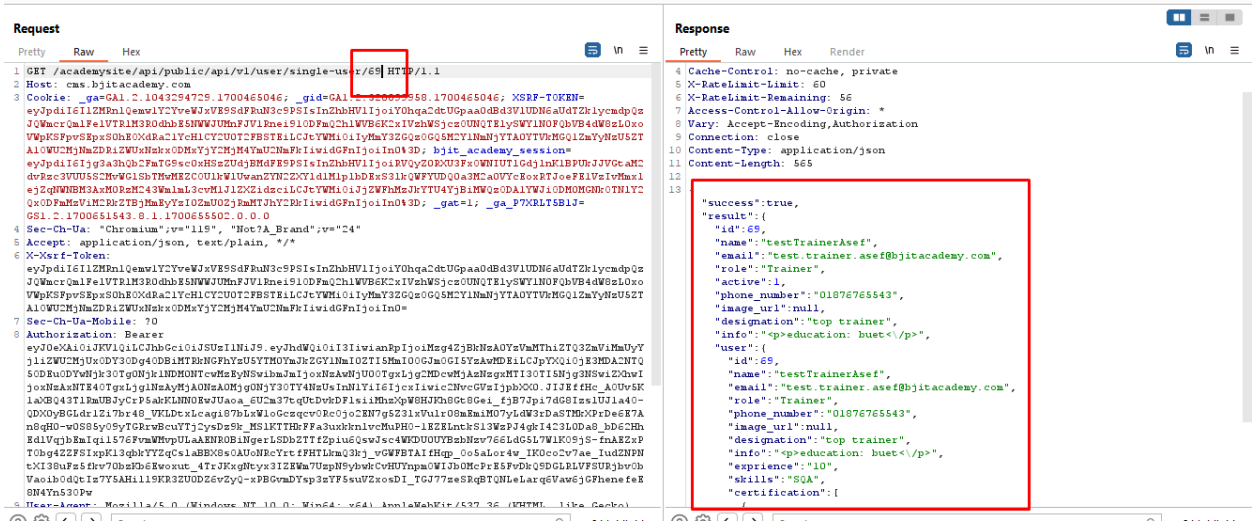
1. First i went to my profile and capture the GET request of the personal information.



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.

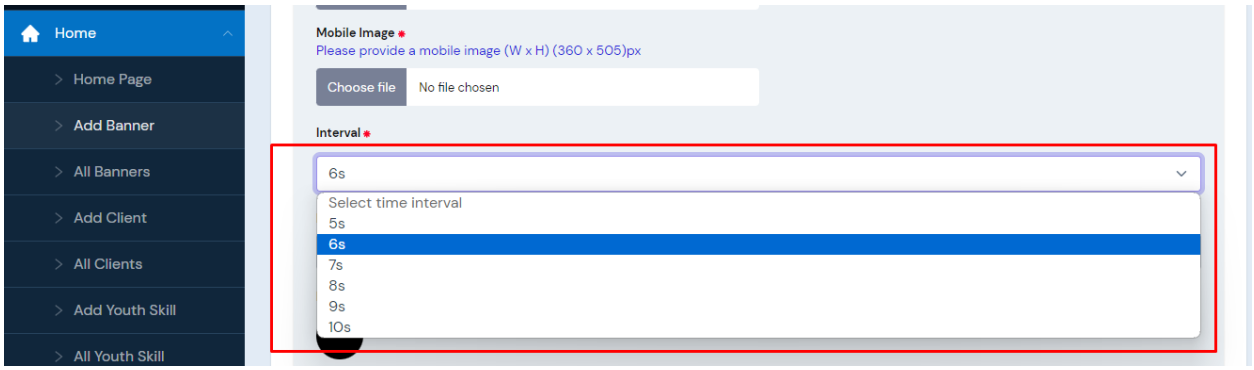
Description: The identified vulnerability allows unauthorized users to manipulate the interval time for creating slider posts also by unauthorized user's token. This manipulation affects the timing of banner intervals on the home page. The issue emphasizes a failure in enforcing proper access controls,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

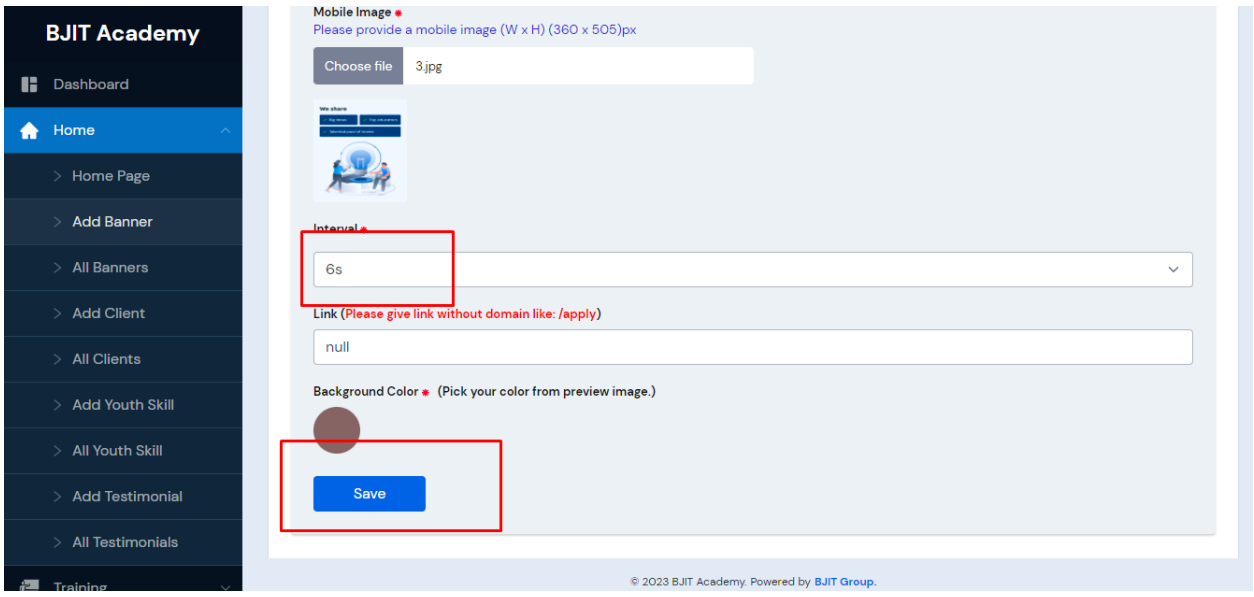
Target:cms.bjitacadey.com

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

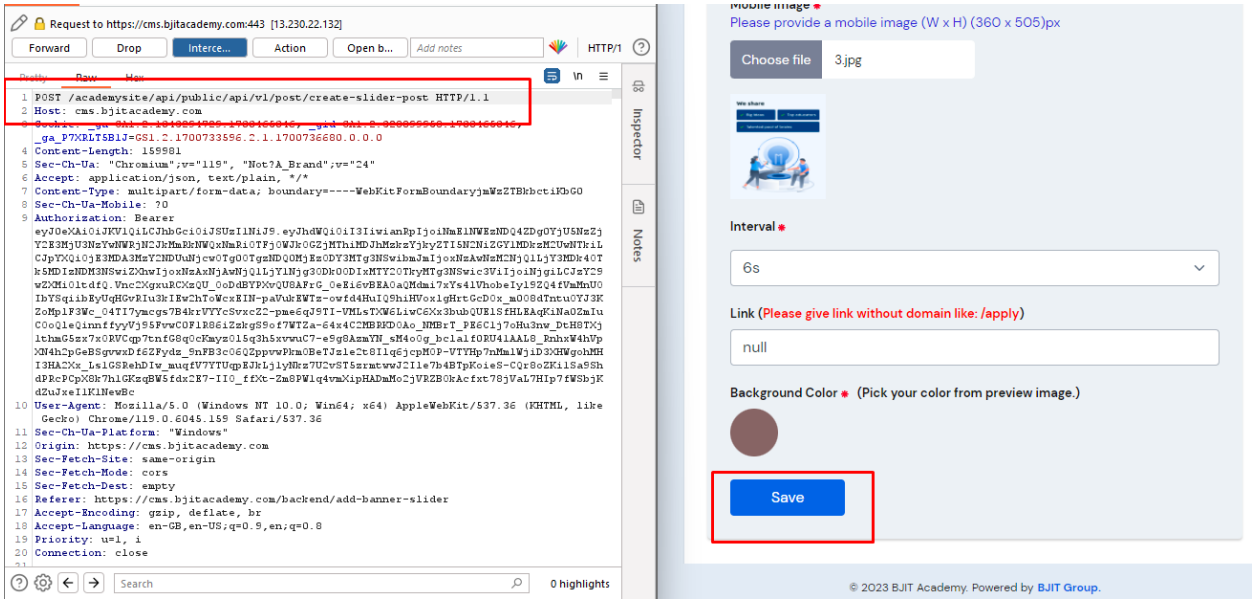
POC:

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.

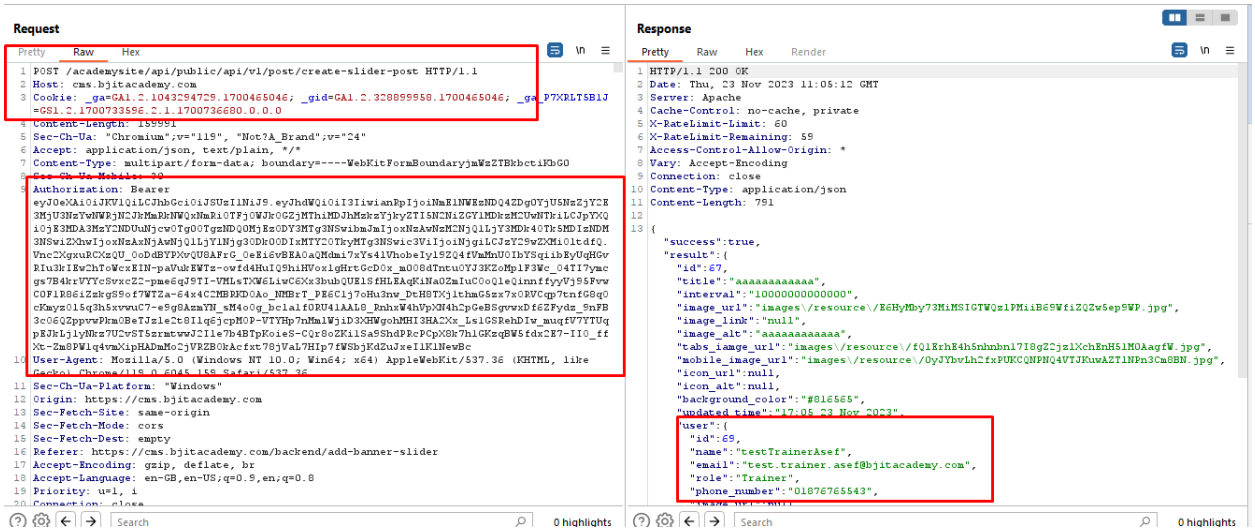


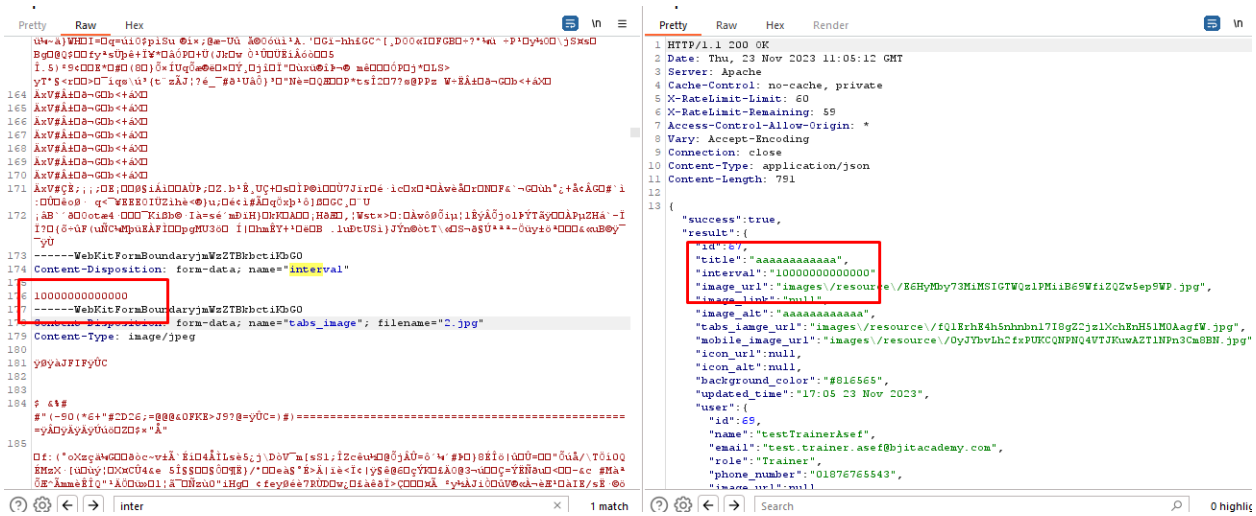


2. After that by clicking the save button i got the request captured and sent it to the repeater



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.





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.