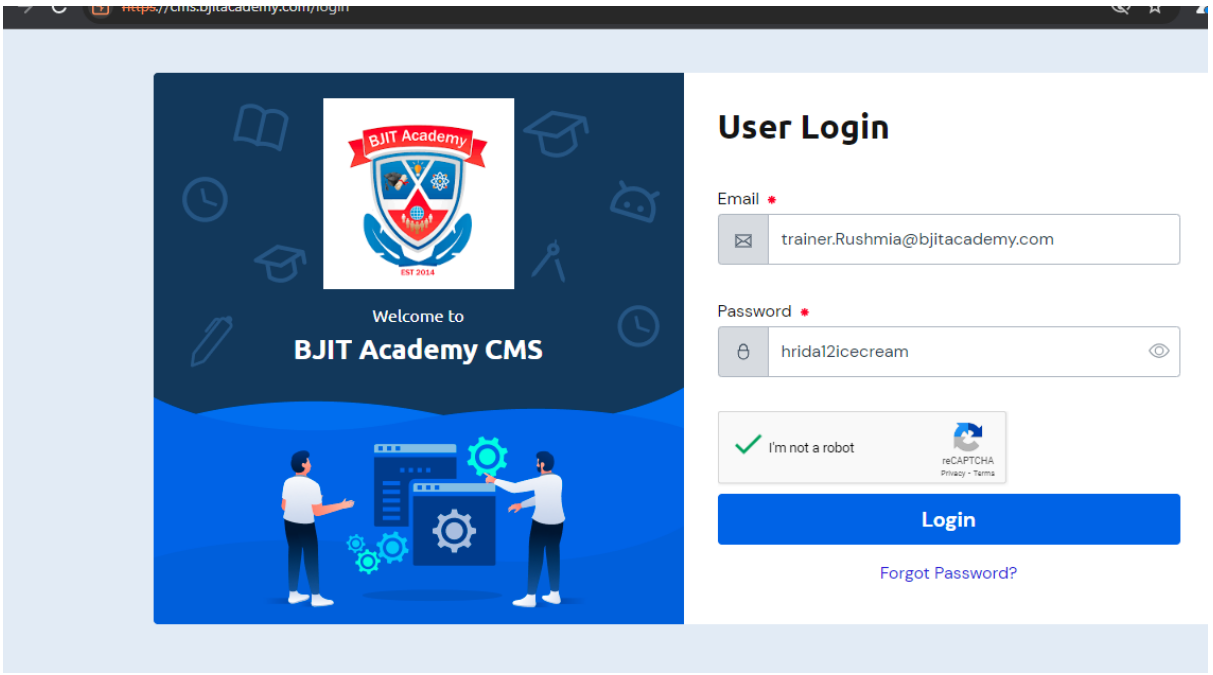
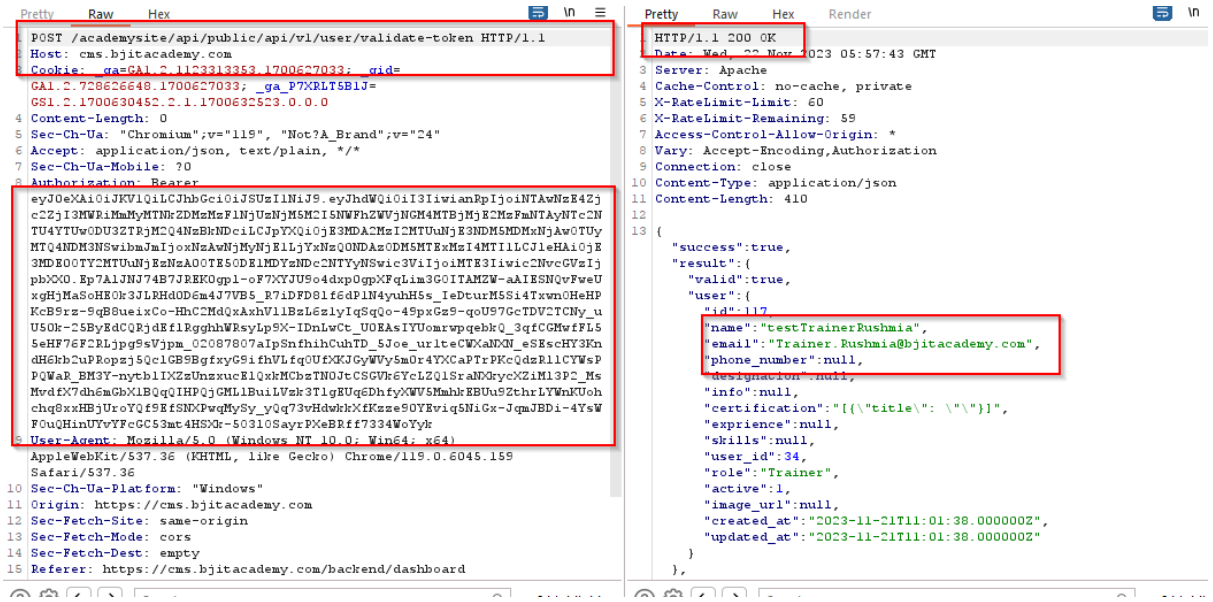
Name: Rushmia Ahmed
ID:30098
Course: Vulnerability Assessment & Penetration Testing
Submitted To: Sad Murshid khan Adon and Abdullah Al Nayeem.

Access Control:

Vulnerability-1:

Title:Users(**Admin,Trainer,SEO-Manager,Content-Manager**) have the permission **creating-news** using **Bearer token** , but only super admins should do so.
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/news/create-news HTTP/1.1
Proof of Concept:
Step-1:Install burpsuit from browser
Go to Proxy tab
Now Go to Open browser
Bowse https://cms.bjitacademy.com/login
Login as Trainer

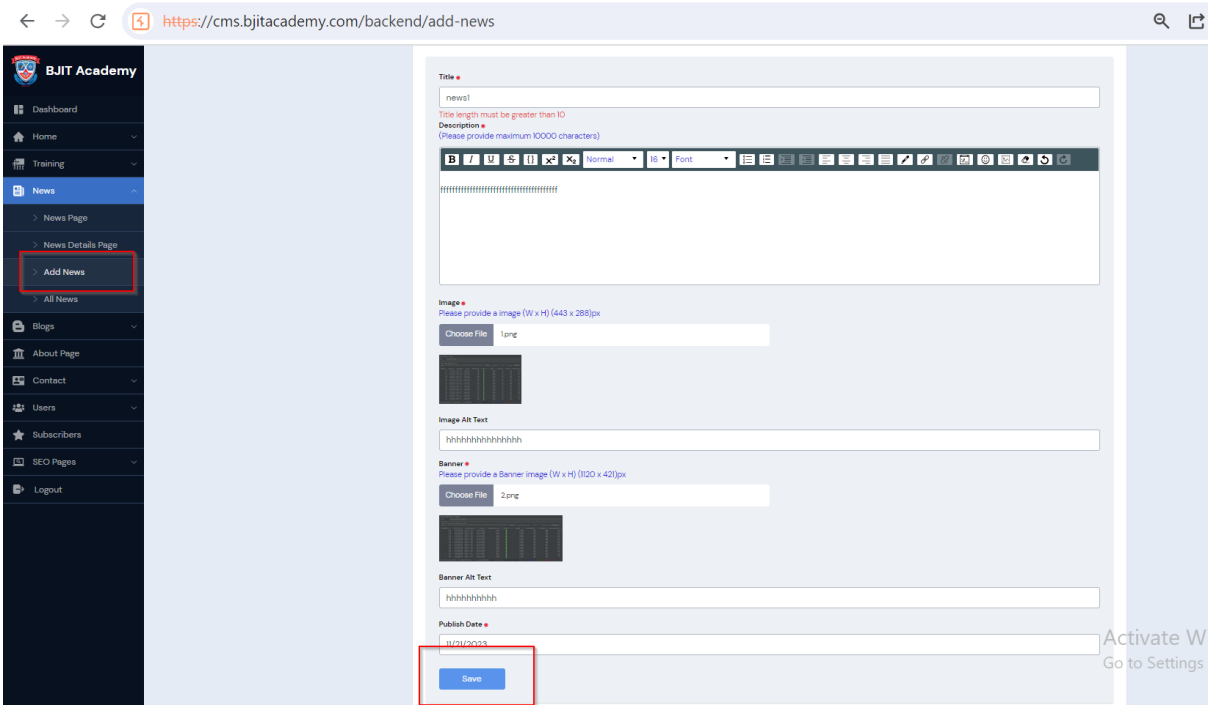




Step-2:

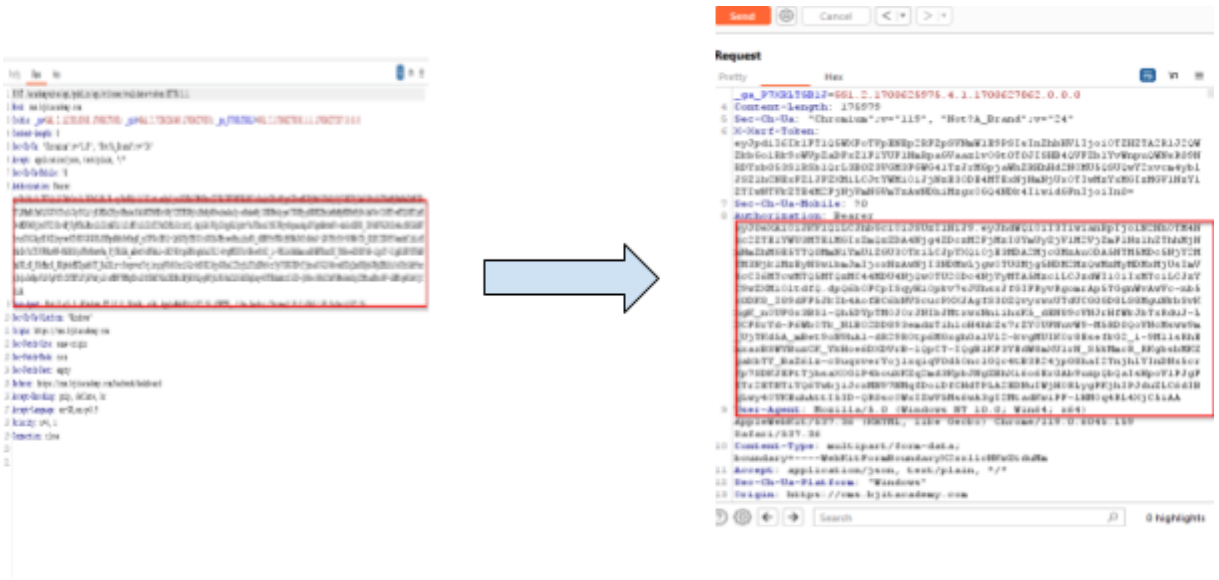
- Ensure that the "Intercept is on" button is activated
- Capture the request
- Send the request to repeater
- Collect token and id

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



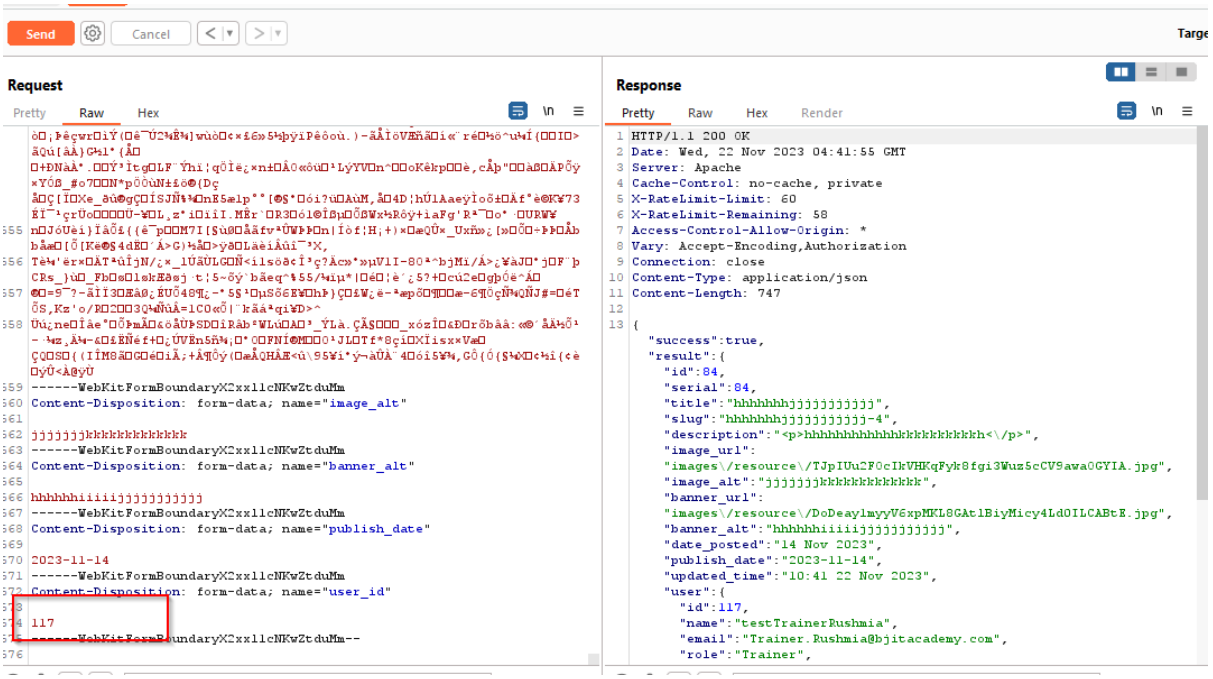
Step-5:

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



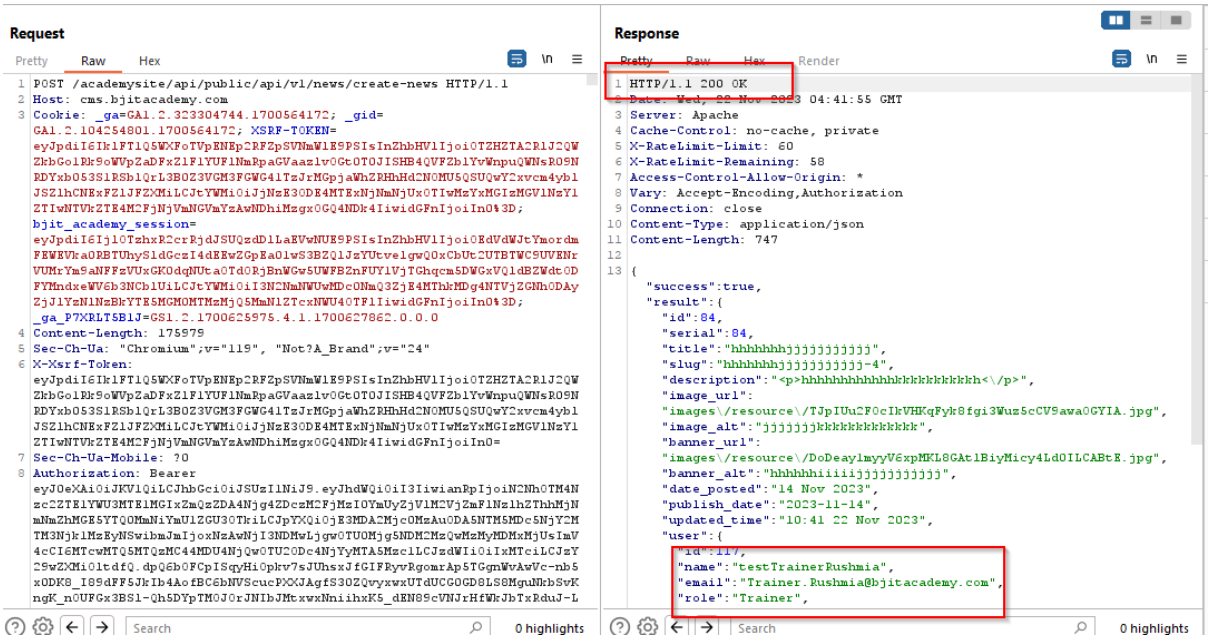
Step-6:

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



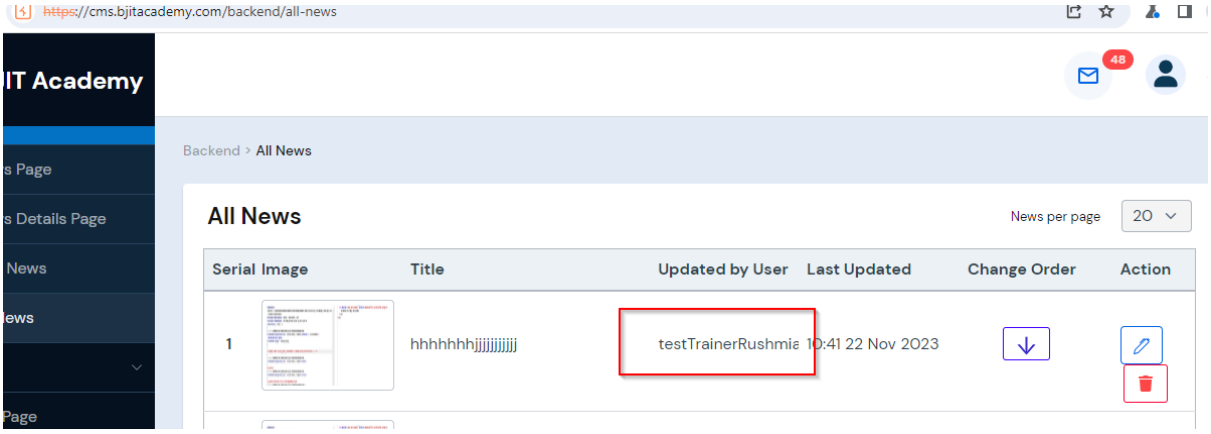
Step-7:

.Replace the superadmin role POST in the HTTP/1.1 /academysite/api/public/api/v1/news/create-news URL with a copy of the trainer role from the trainers url in the response.



Step-8:

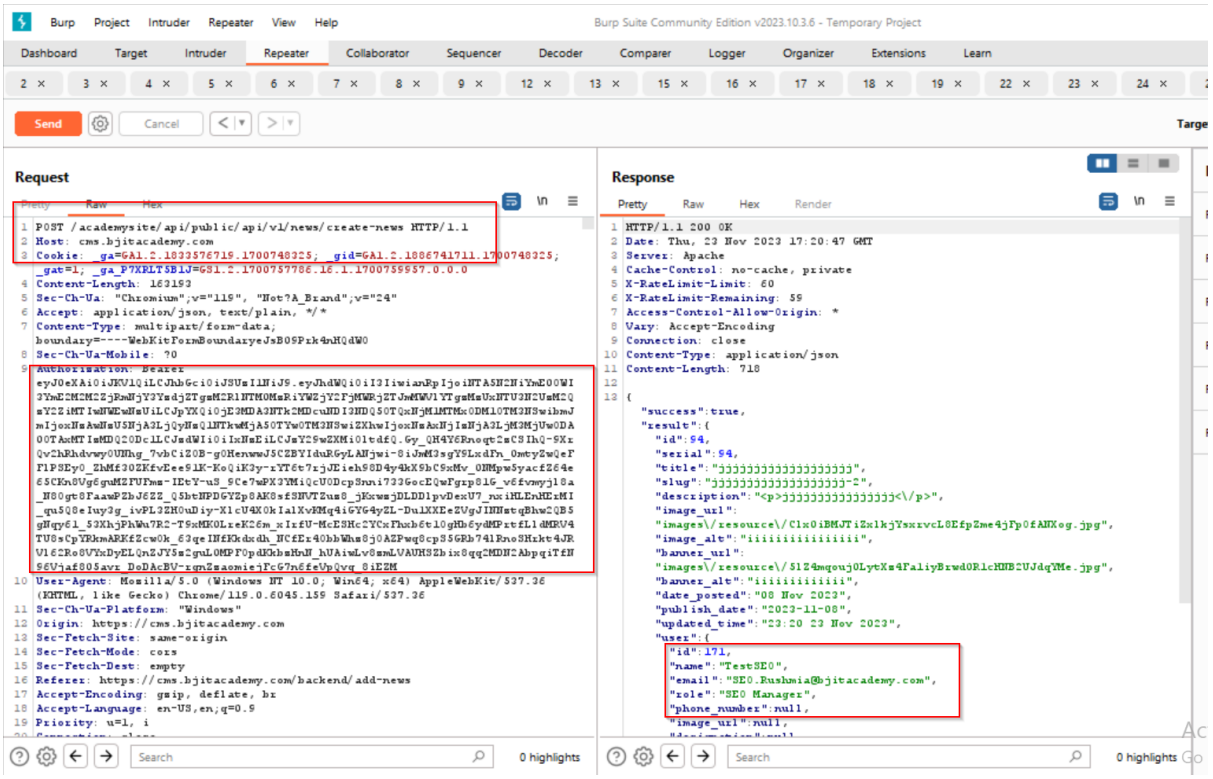
After Giving a trainer token and role in the HTTP/1.1 /academysite/api/public/api/v1/news/create-news URL provides a status code of 200.

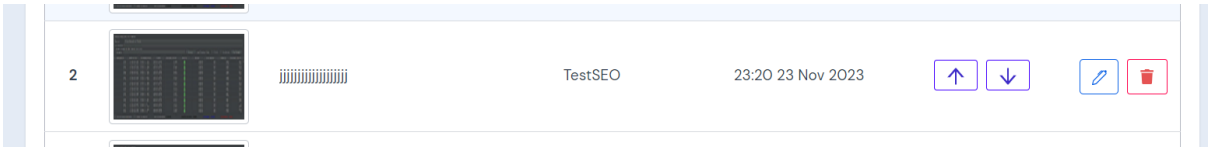


Conclusion: Thus, a trainer has the ability to create news, something that should only be done by a superadmin.

Similar to SEO

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

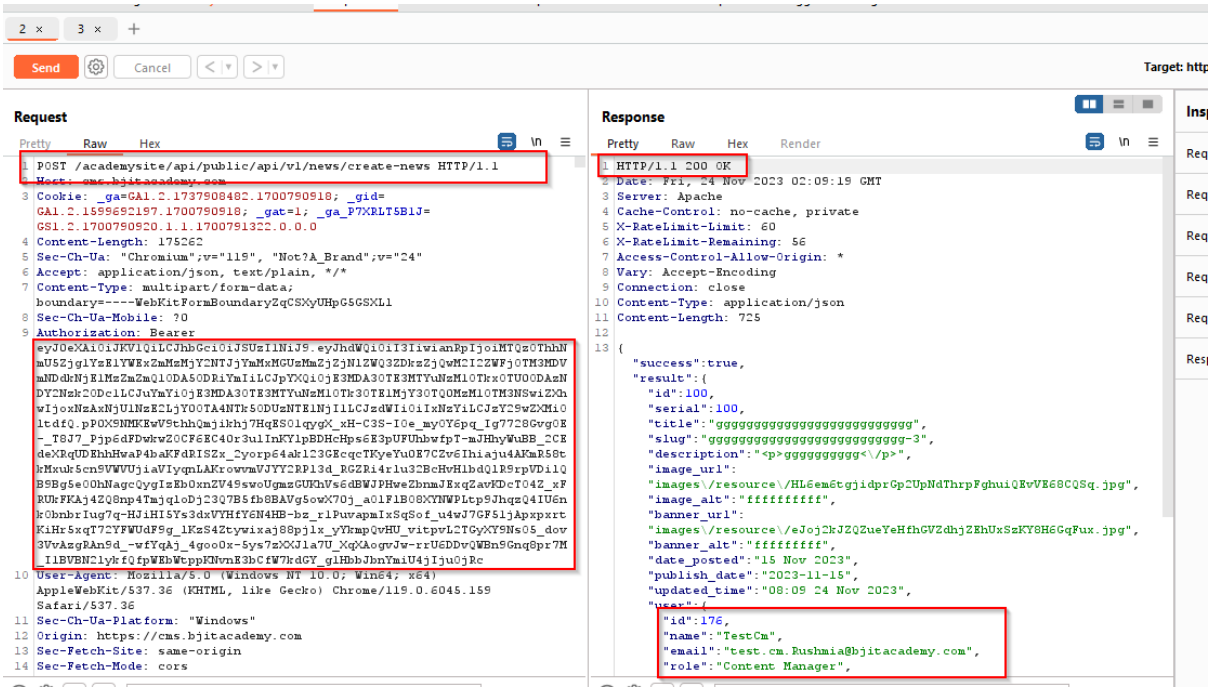


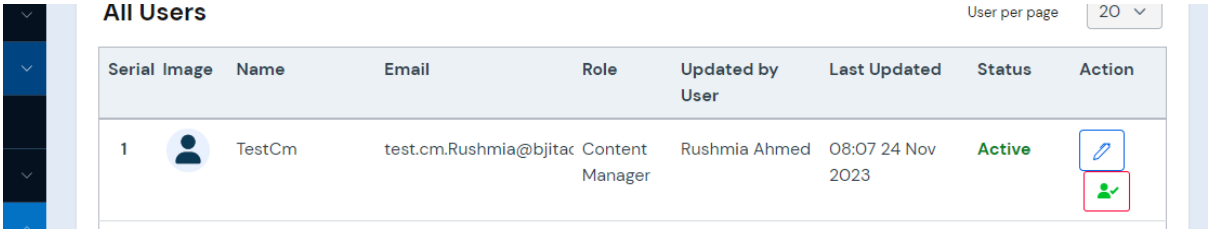


Similar to Content-Manager

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

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





Total Affected URL:

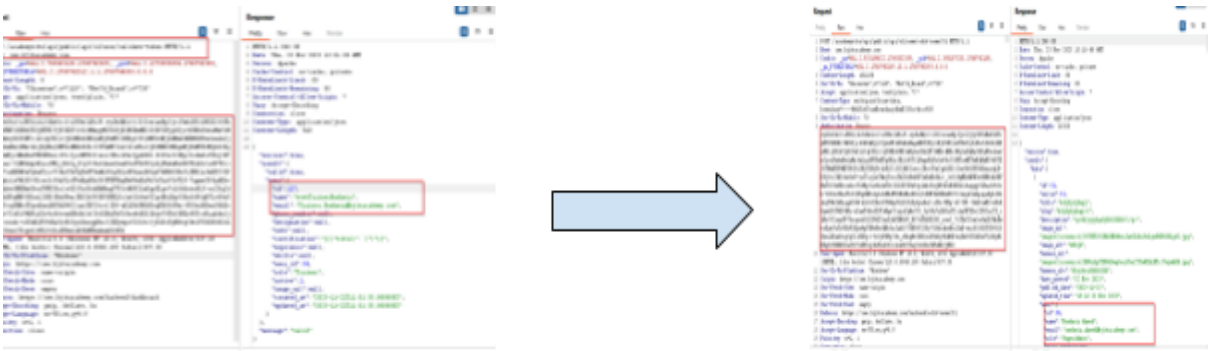
Vulnerability-2:

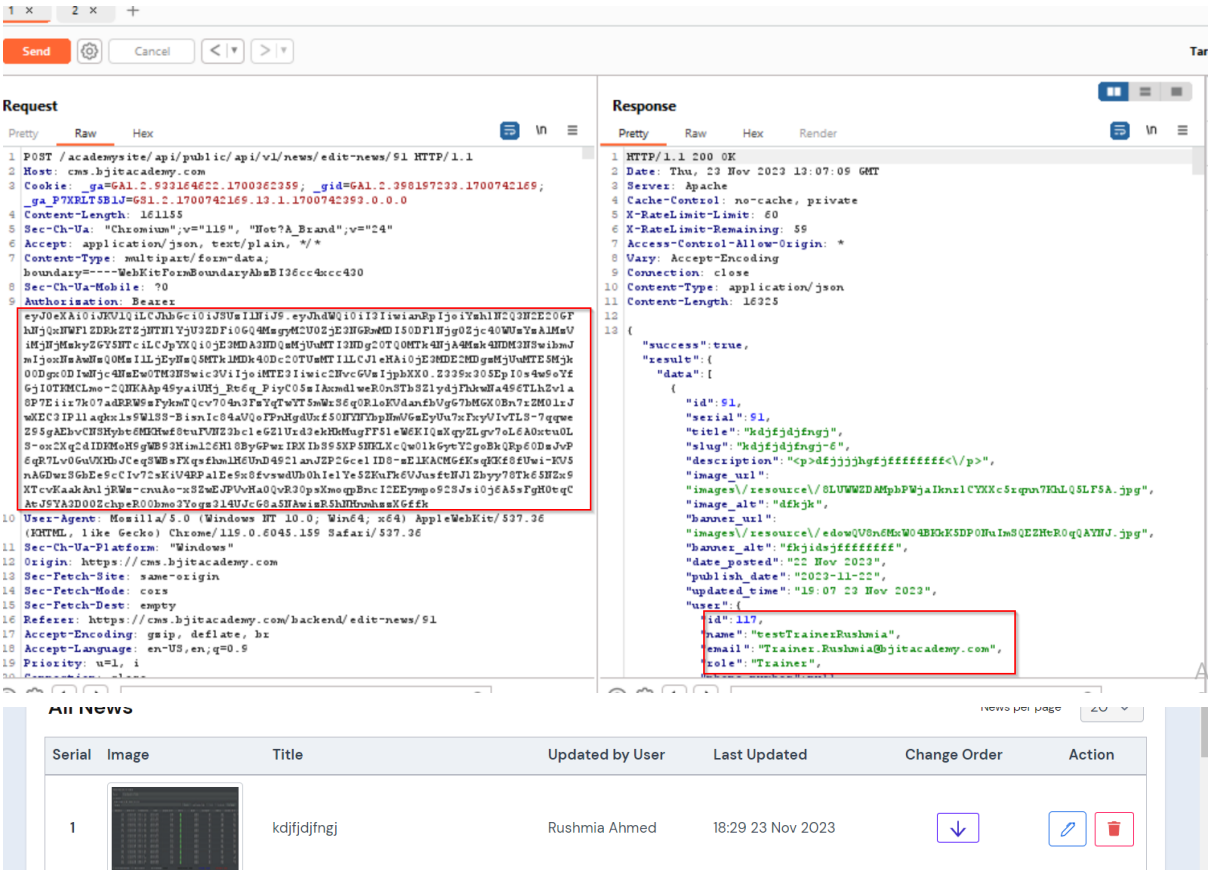
Edit News:

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

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

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



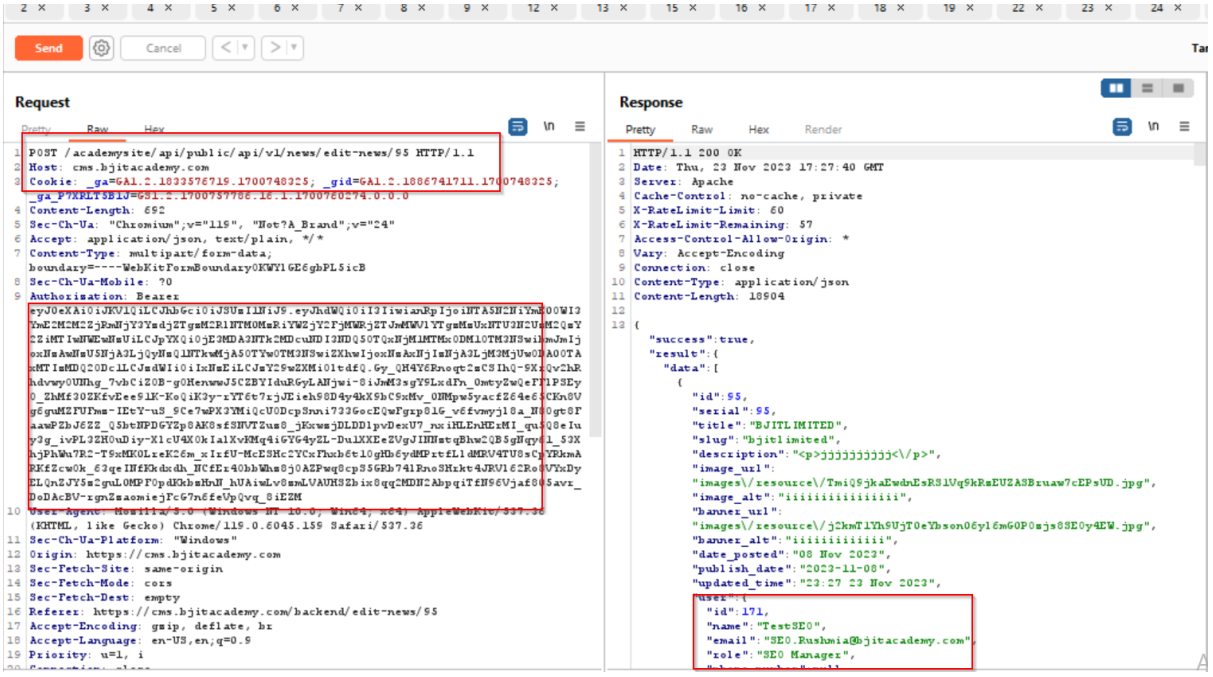


After Giving a trainer token and role in the HTTP/1.1 /academysite/api/public/api/v1/news/edit-news URL provides a status code of 200.

Similar to SEO

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

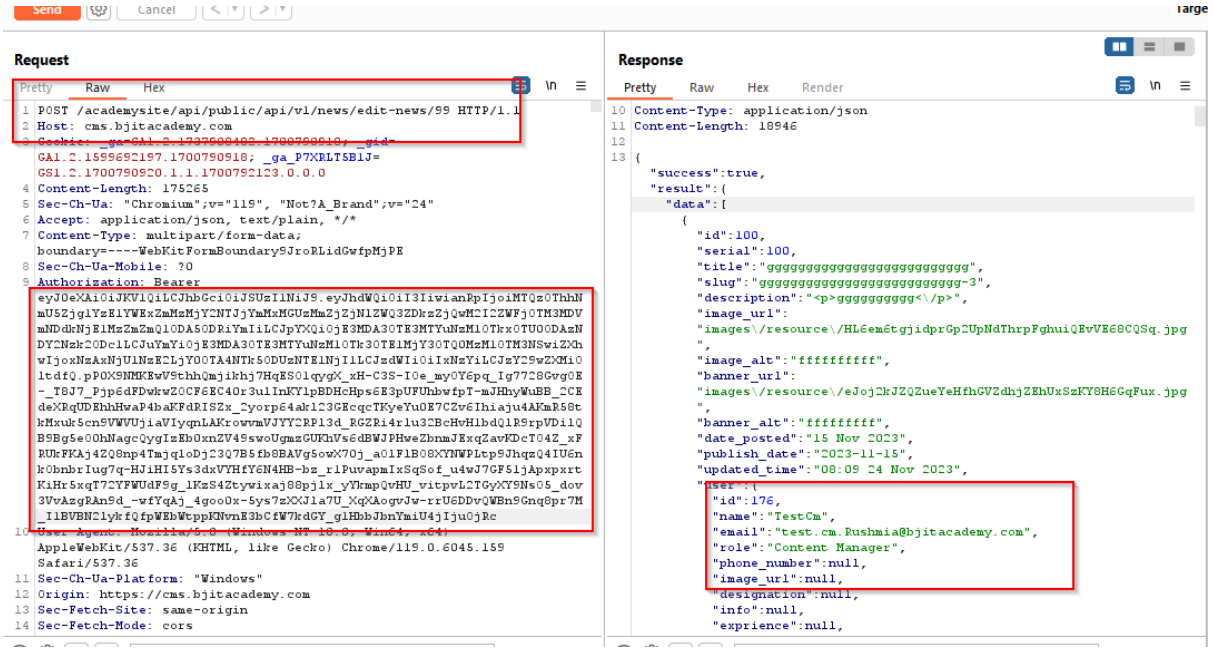
API:POST /academysite/api/public/api/v1/news/edit-news/95 HTTP/1.1



Similar to Content-Manager

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

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



Total Affected URL:

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

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

Vulnerability-3:

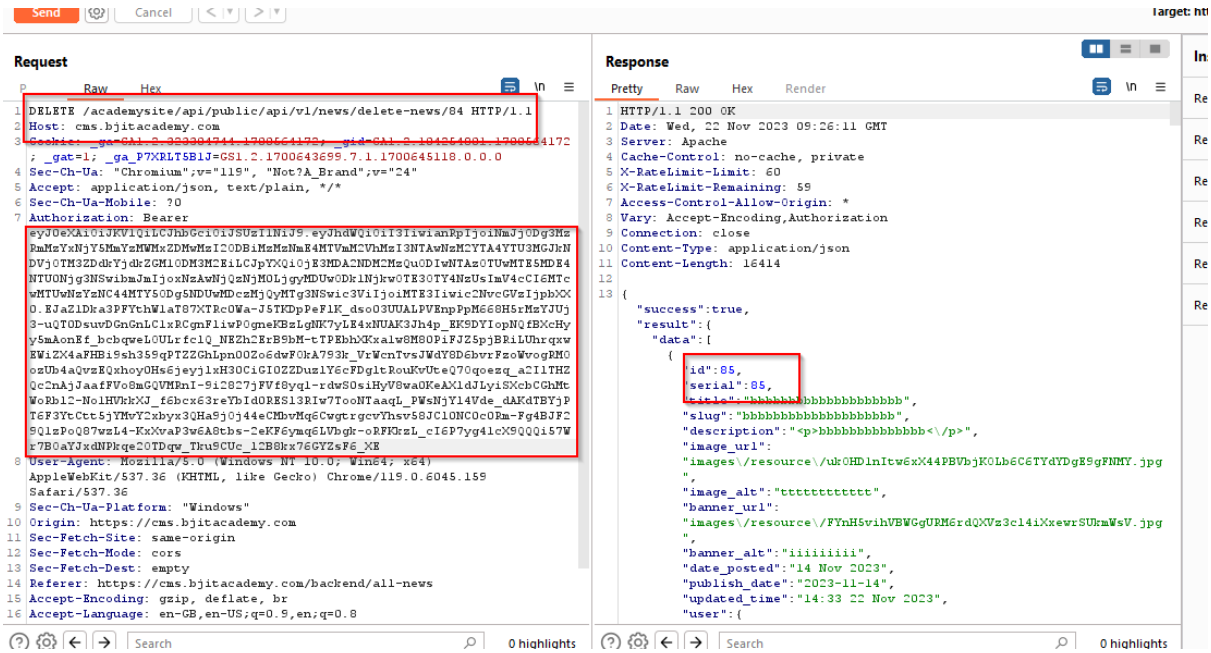
Delete News:

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

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

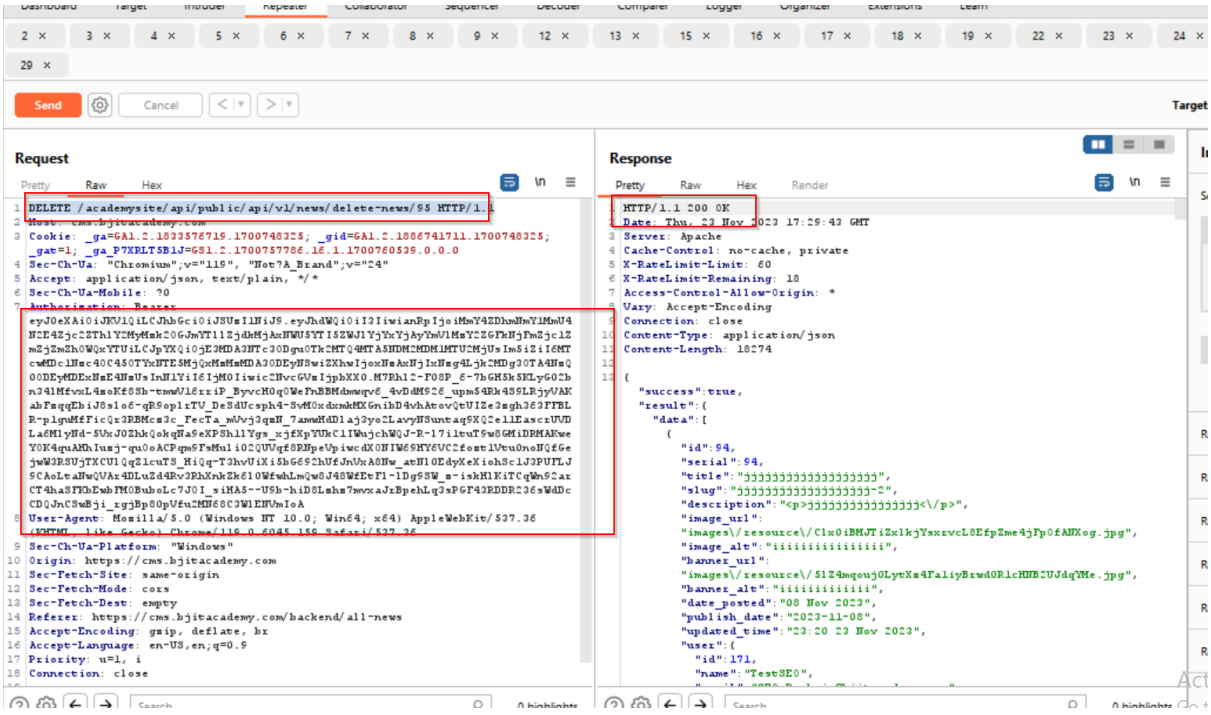
API:POST /academysite/api/public/api/v1/news/delete-news/91 HTTP/1.1

Logged in as Trainer:

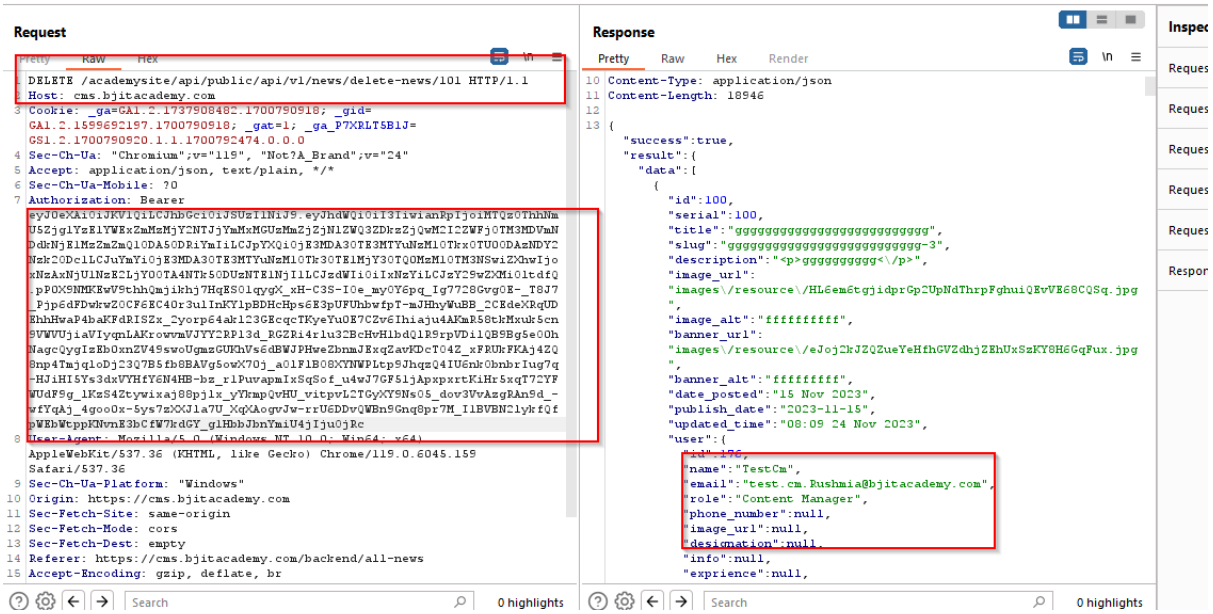


Copy the trainer token now, and replace it with the superadmin's token in the /academysite/api/public/api/v1/news/delete-news/84 HTTP/1.1.
After Giving a trainer token and role in the/academysite/api/public/api/v1/news/delete-news/84 HTTP/1.1. URL provides a status code of 200.

Similar to SEO
Target:https://cms.bjitacademy.com/login
API:DELETE /academysite/api/public/api/v1/news/delete-news/95 HTTP/1.1

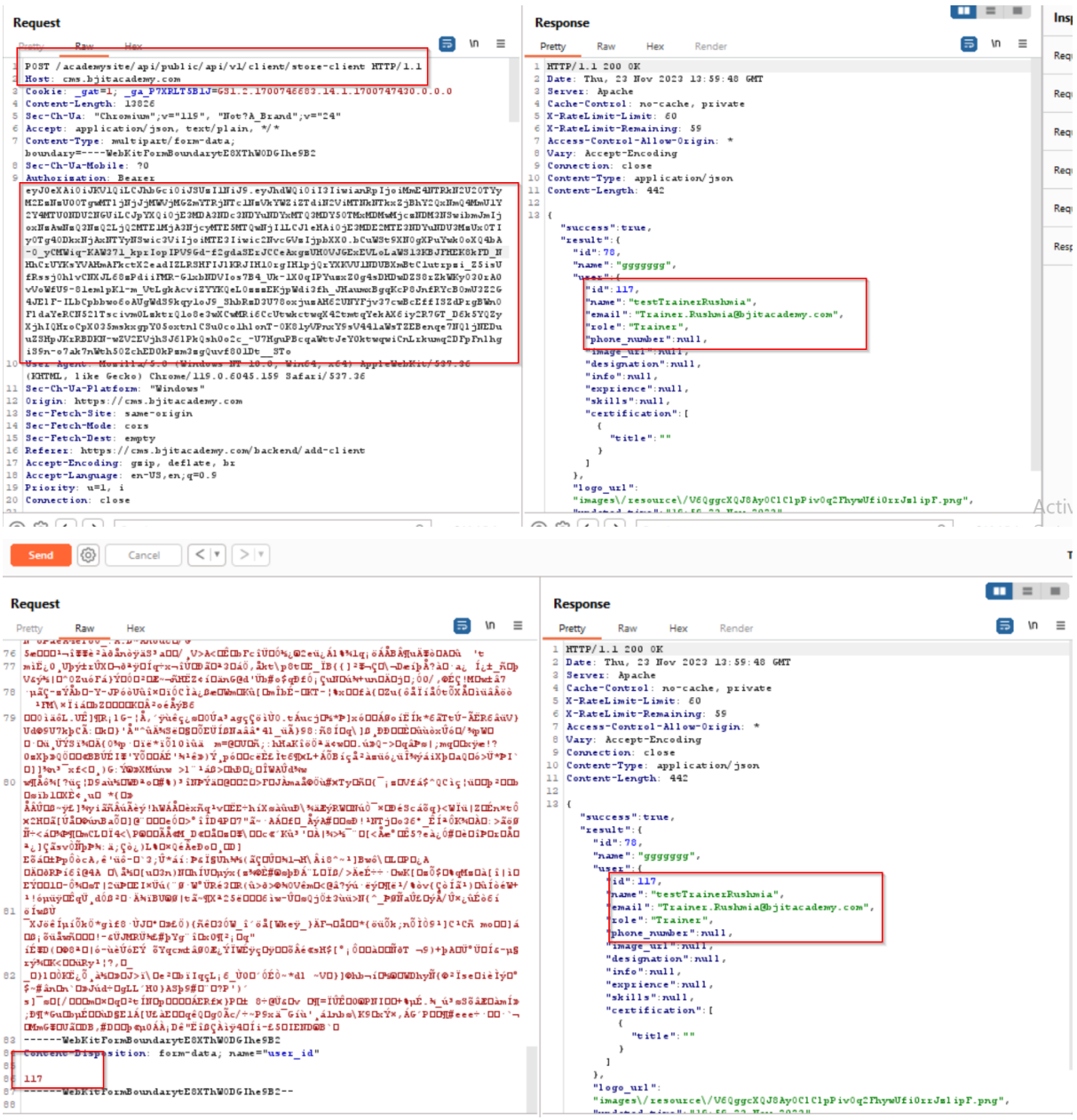


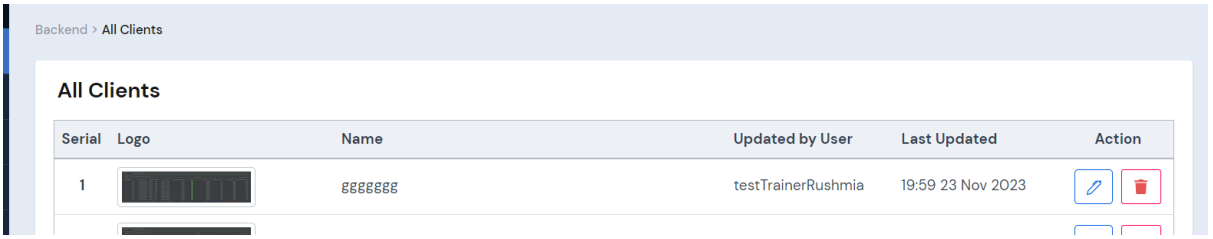
Similar to Content Manager
Target:https://cms.bjitacademy.com/login
API:DELETE /academysite/api/public/api/v1/news/delete-news/95 HTTP/1.1



Add Client:

Logged in as Trainer
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/client/store-client HTTP/1.1



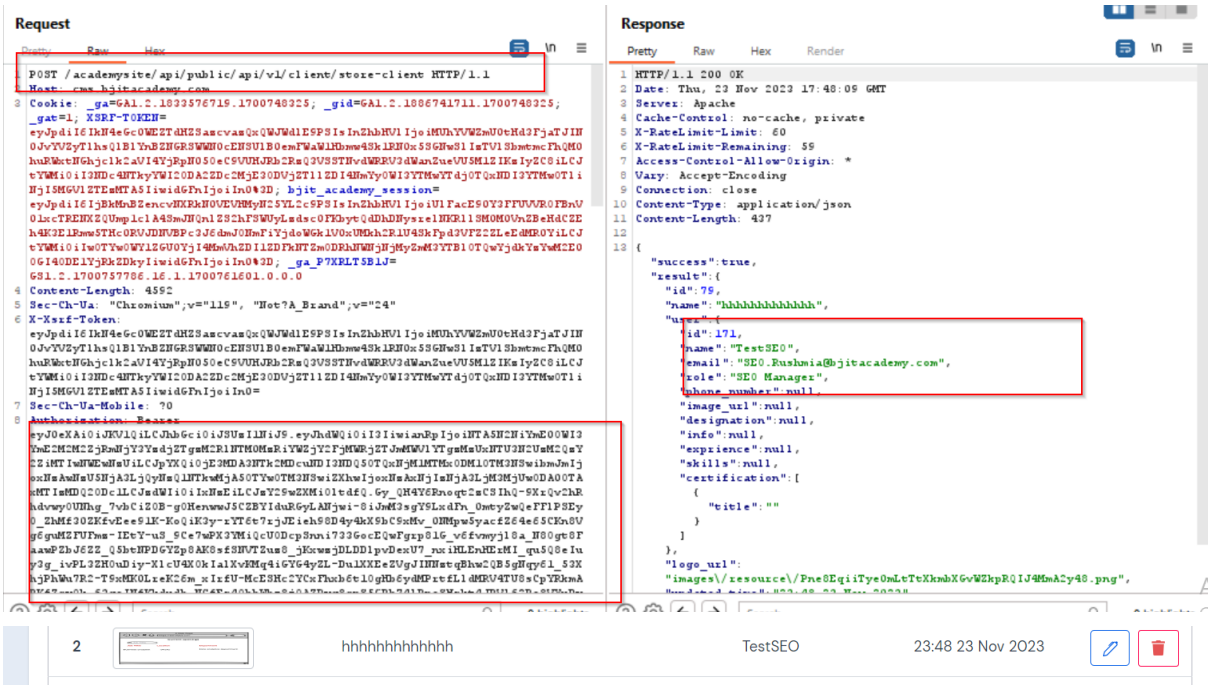


Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.
After Giving a trainer token and role in POST /academysite/api/public/api/v1/client/store-client HTTP/1.1. URL provides a status code of 200.

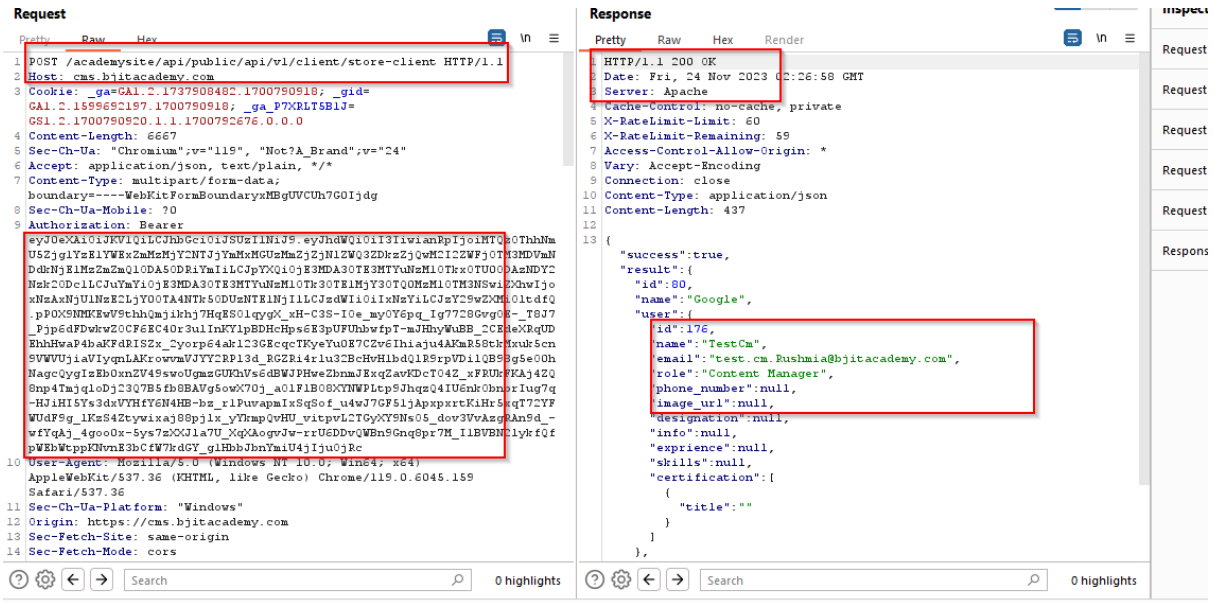
Similar to SEO

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

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



Similar to Content Manager

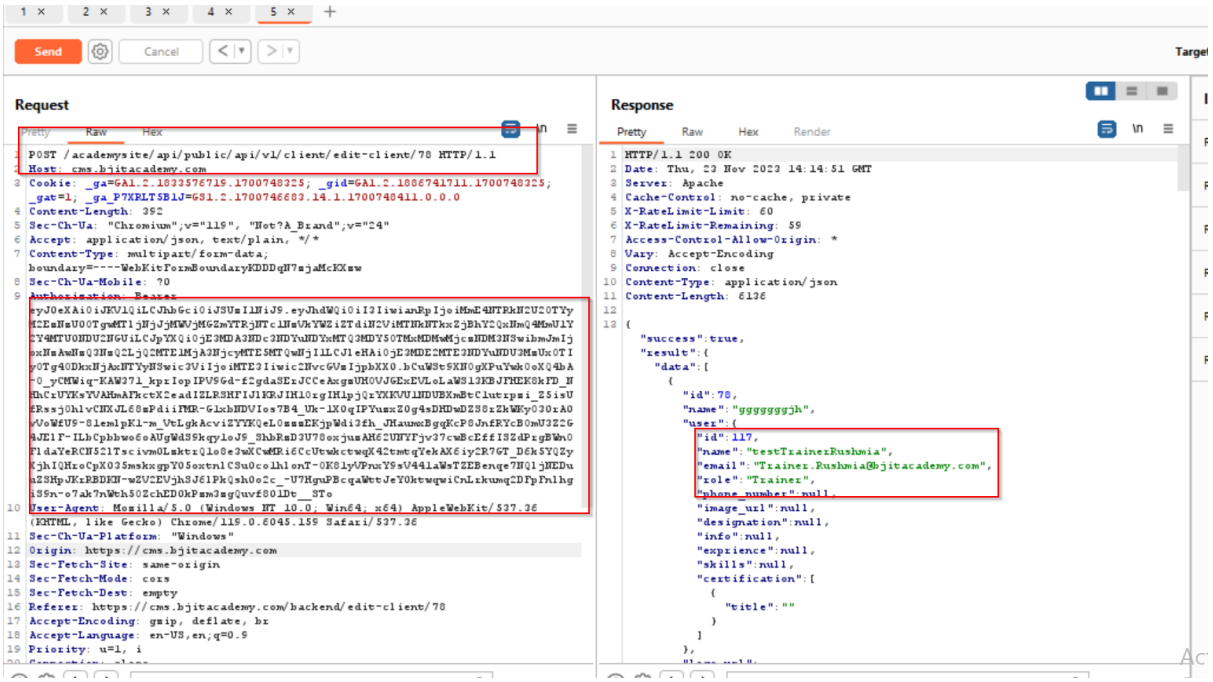


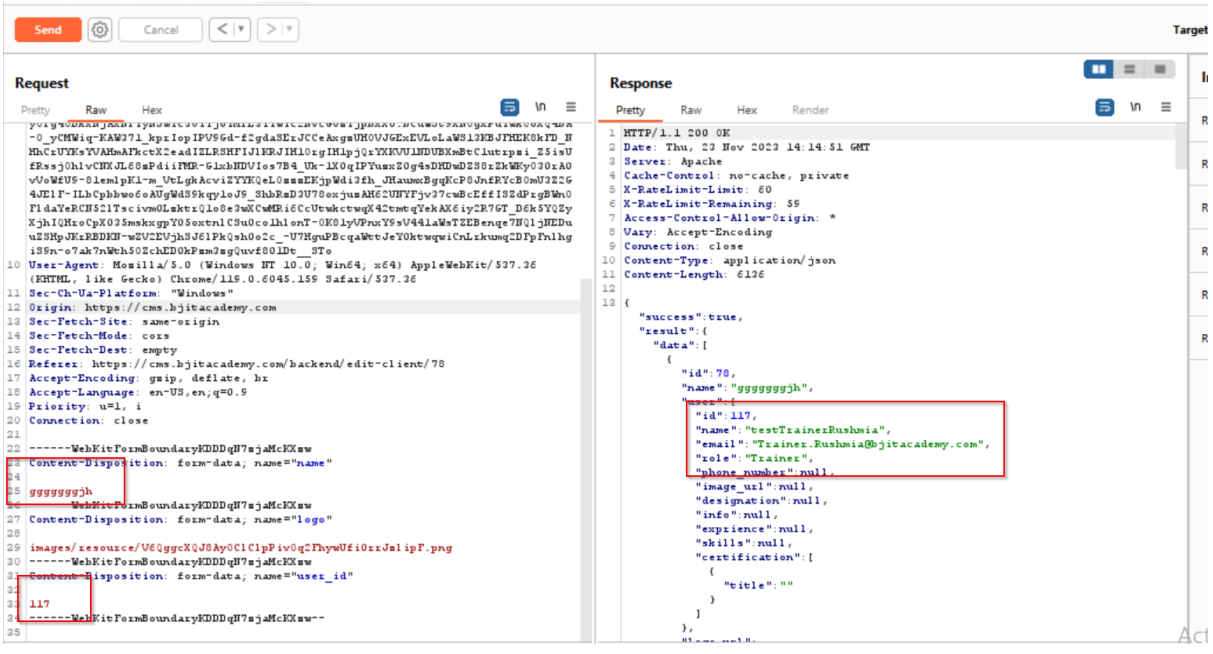
Edit Client:

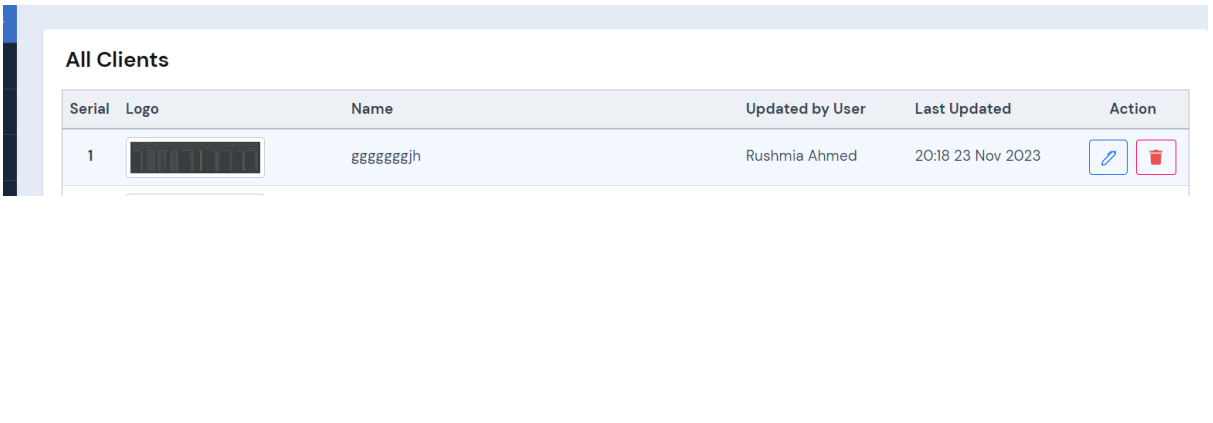
Logged in as trainer

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

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

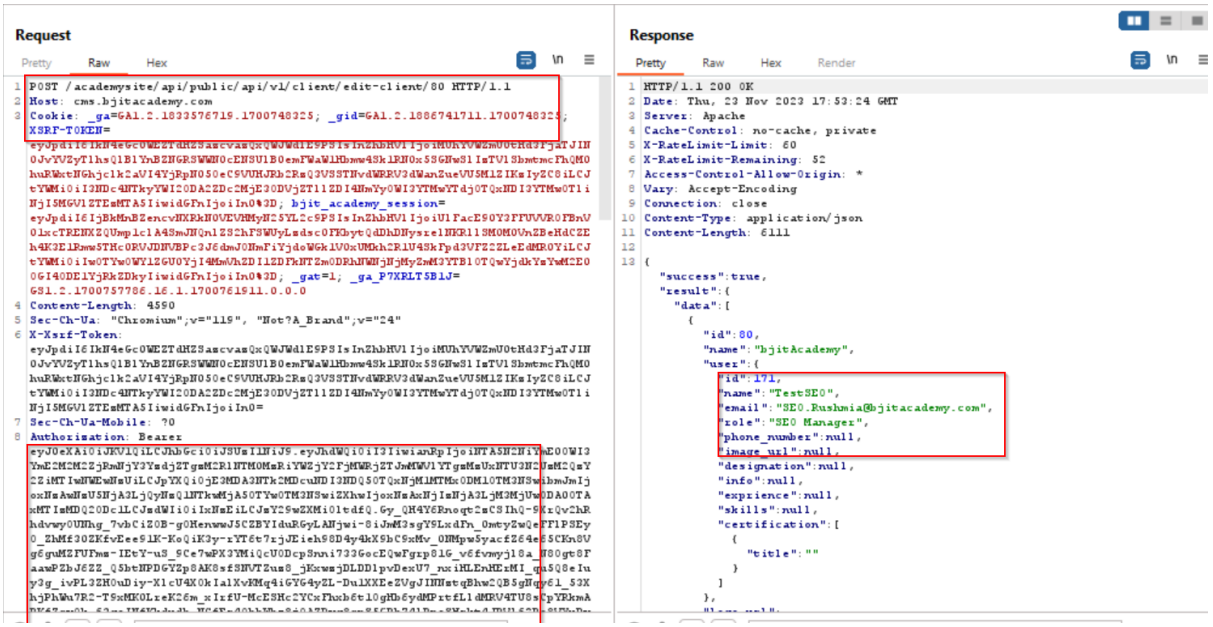

Send
Cancel
Request
Response
Pretty
Raw
Hex
Render
POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1
Host: cms.bjitacademy.com
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 14:14:51 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 6136
"success":true,
"result":{
"data":[
"id":78,
"name":"ggggggggjh",
"user":{
"id":117,
"name":"testTrainerRushmia",
"email":"Trainer.Rushmia@bjitacademy.com",
"role":"Trainer",
"phone_number":null,
"image_url":null,
"designation":null,
"info":null,
"exprience":null,
"skills":null,
"certification":[
"title":""


Send
Cancel
Request
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2023 14:14:51 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: 6136
"success":true,
"result":{
"data":[
"id":78,
"name":"ggggggggjh",
"user":{
"id":117,
"name":"testTrainerRushmia",
"email":"Trainer.Rushmia@bjitacademy.com",
"role":"Trainer",
"phone_number":null,
"image_url":null,
"designation":null,
"info":null,
"exprience":null,
"skills":null,
"certification":[
"title":""

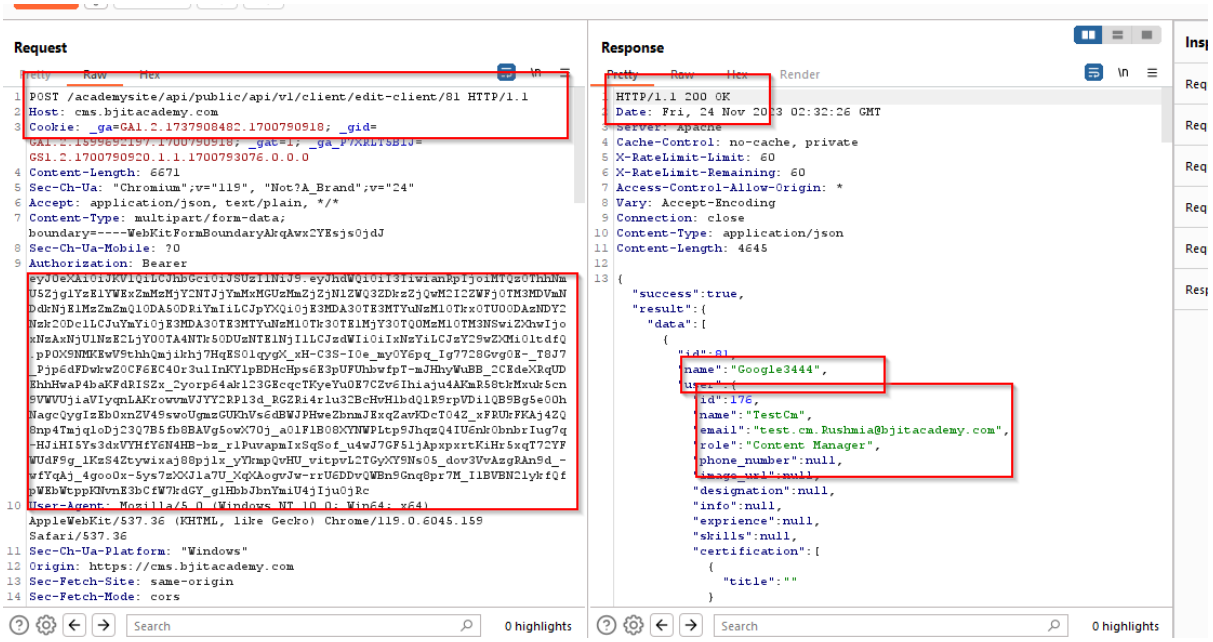

All Clients
Serial
Logo
Name
Updated by User
Last Updated
Action
1
ggggggggjh
Rushmia Ahmed
20:18 23 Nov 2023

Copy the trainer token now, and replace it with the superadmin's token in the POST POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1
After Giving a trainer token and role in POST POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1. URL provides a status code of 200.

Similar to SEO
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1

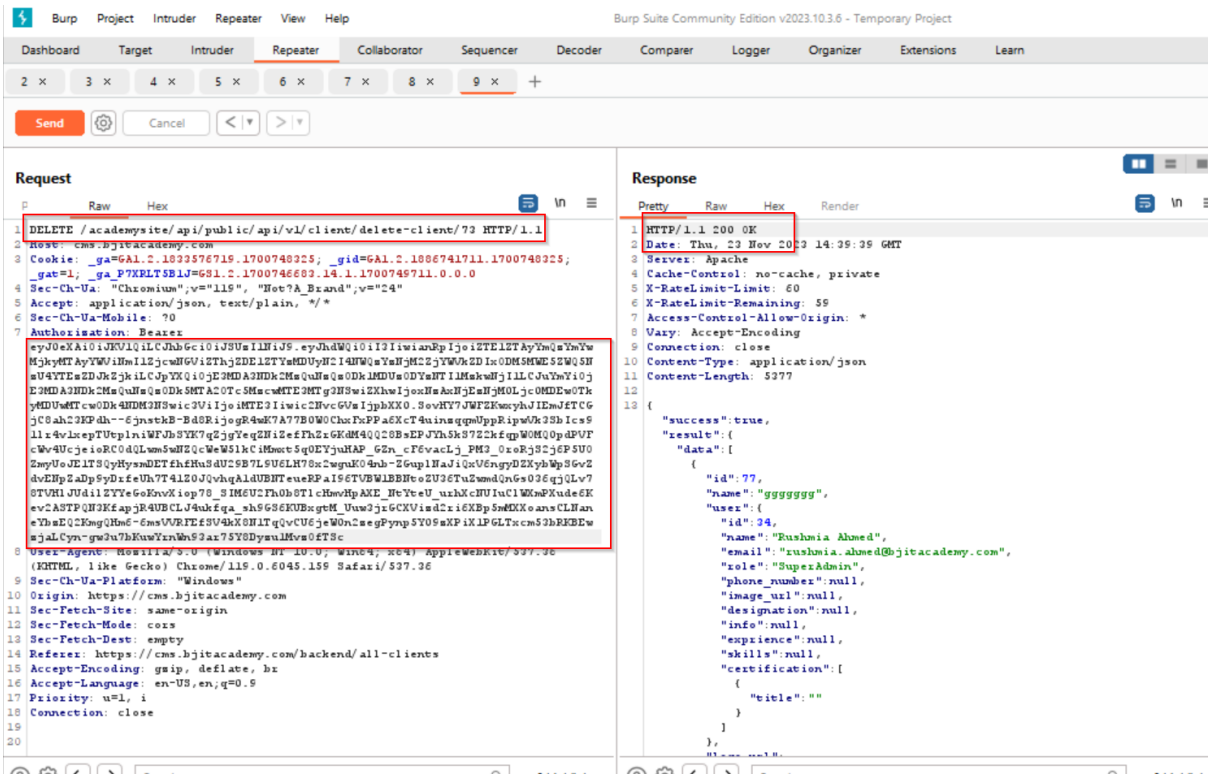


Similar to Content-Manager
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/client/edit-client/78 HTTP/1.1



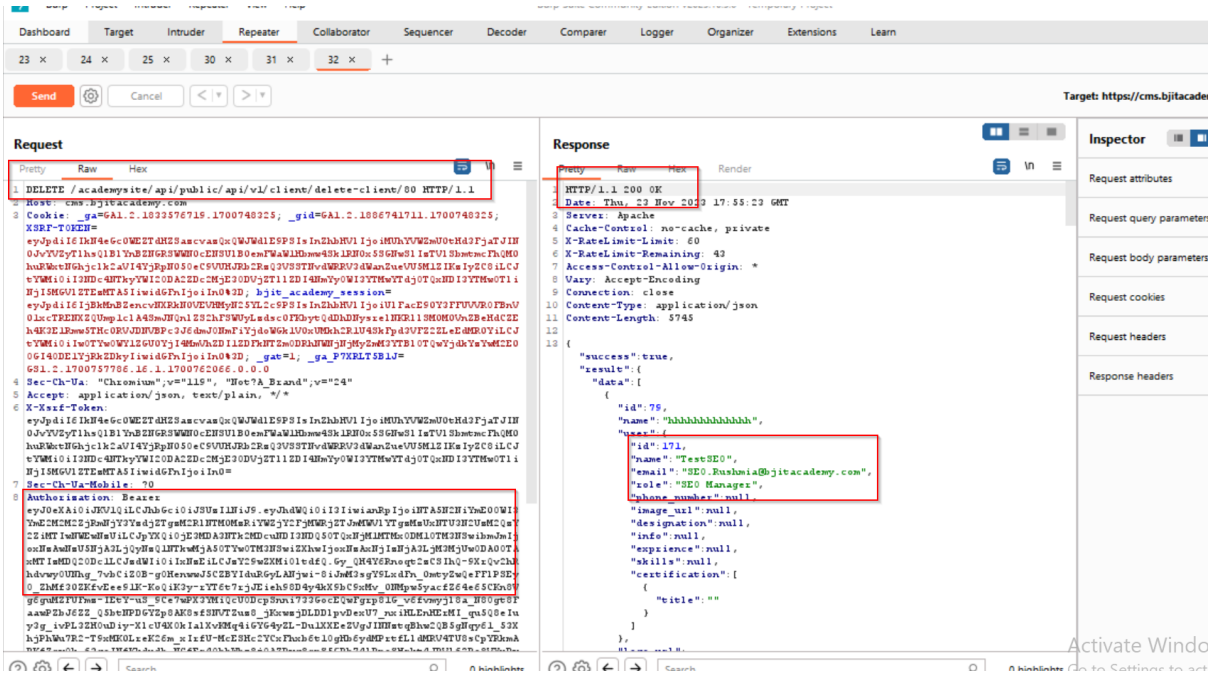
Delete Client:

Logged in as Trainer
Target:https://cms.bjitacademy.com/login
API:DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1



Copy the trainer token now, and replace it with the superadmin's token in the DELETE DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1 HTTP/1.1
After Giving a trainer token and role in DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1. URL provides a status code of 200.

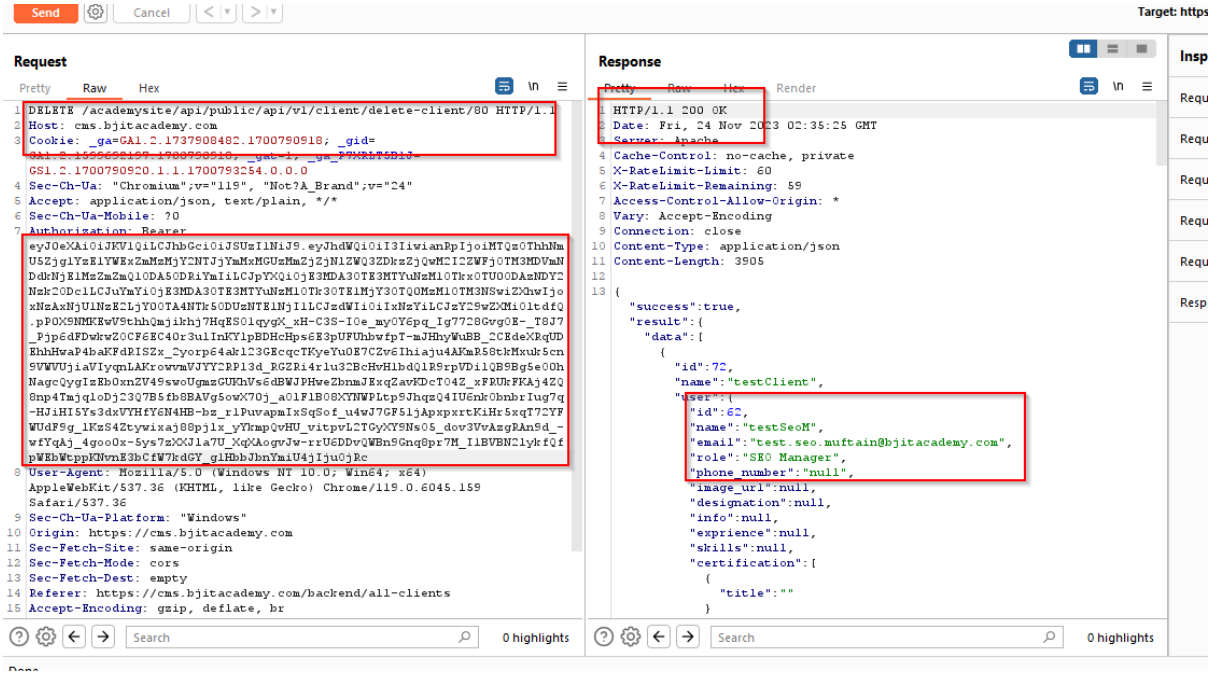
Similar to SEO
Target:https://cms.bjitacademy.com/login
API:DELETE /academysite/api/public/api/v1/client/delete-client/73 HTTP/1.1



Similar to Content-Manager

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

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

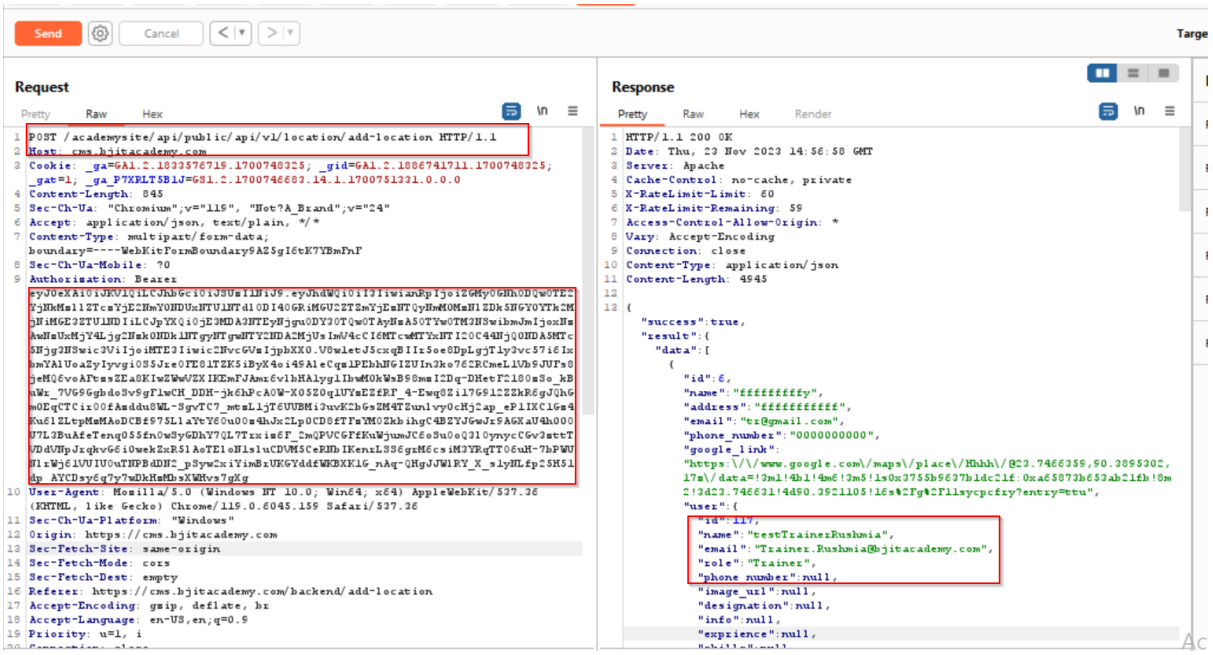


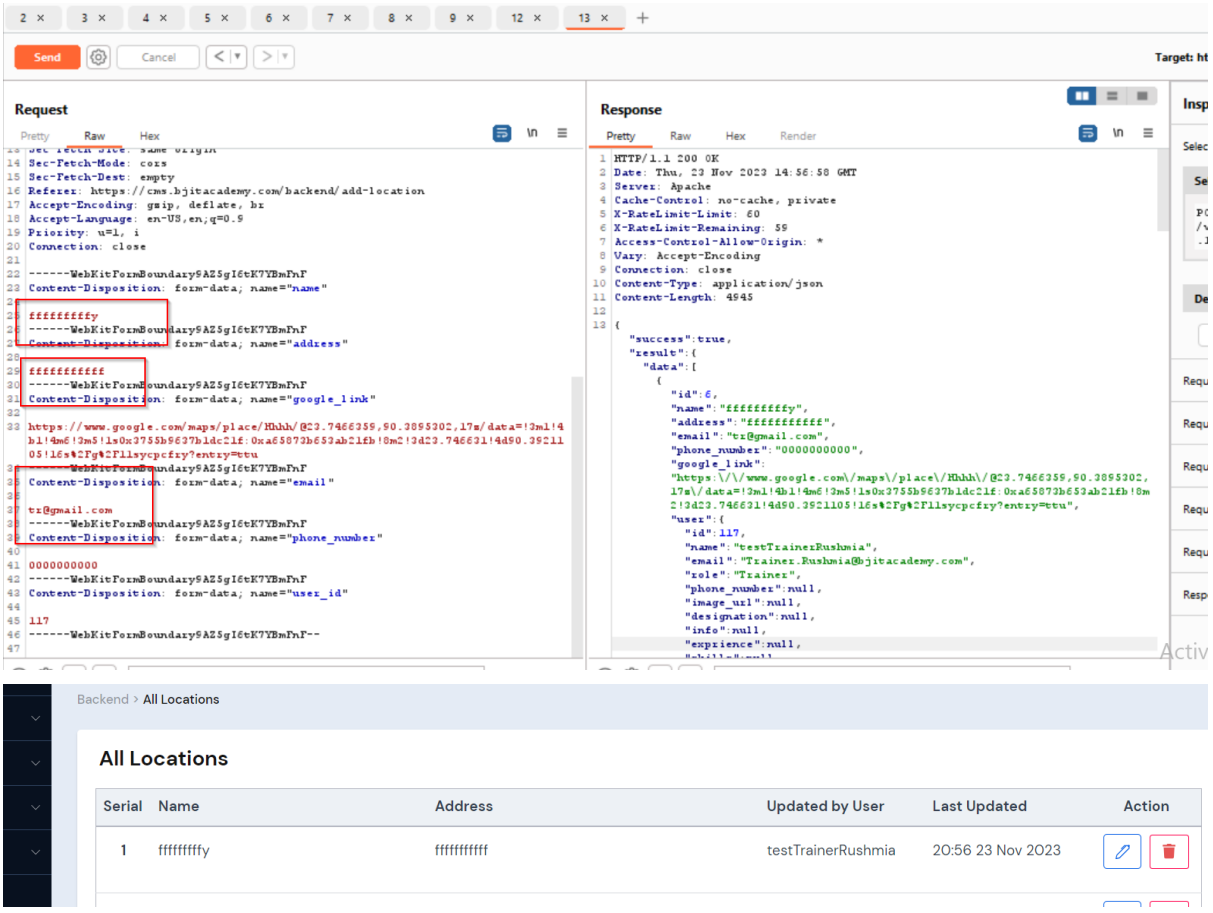
Add Location:

Logged in As Trainer

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

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



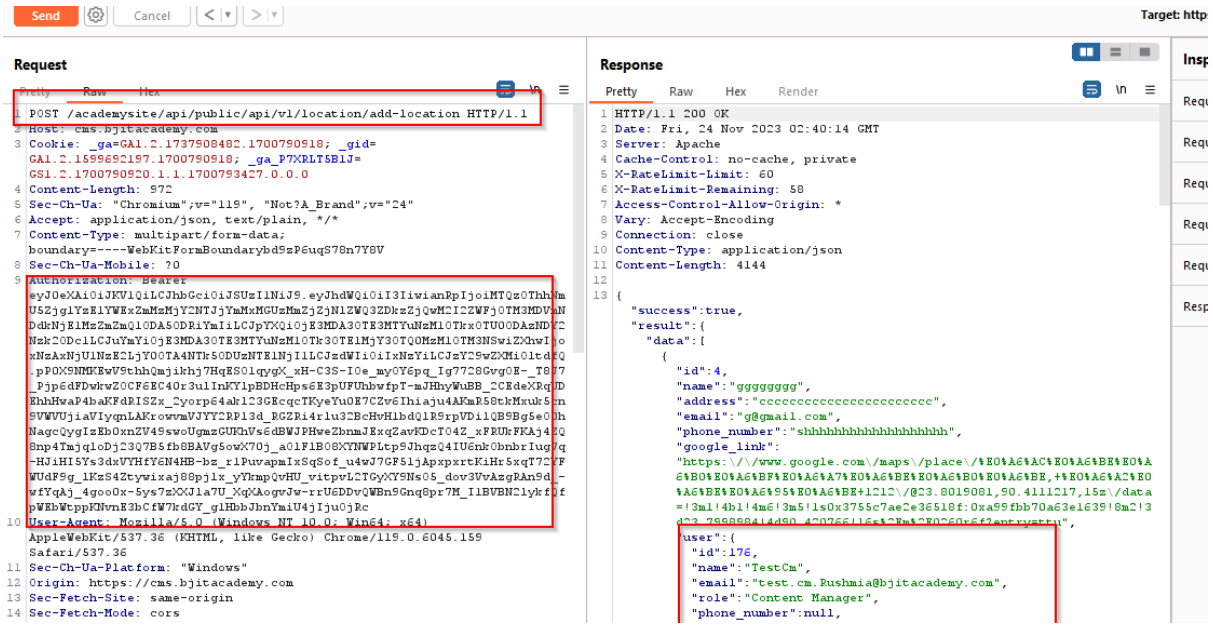


Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/location/add-location HTTP/1.1 HTTP/1.1 HTTP/1.1 After Giving a trainer token and role in POST /academysite/api/public/api/v1/location/add-location HTTP/1.11. URL provides a status code of 200.

Similar to Content Manager

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

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

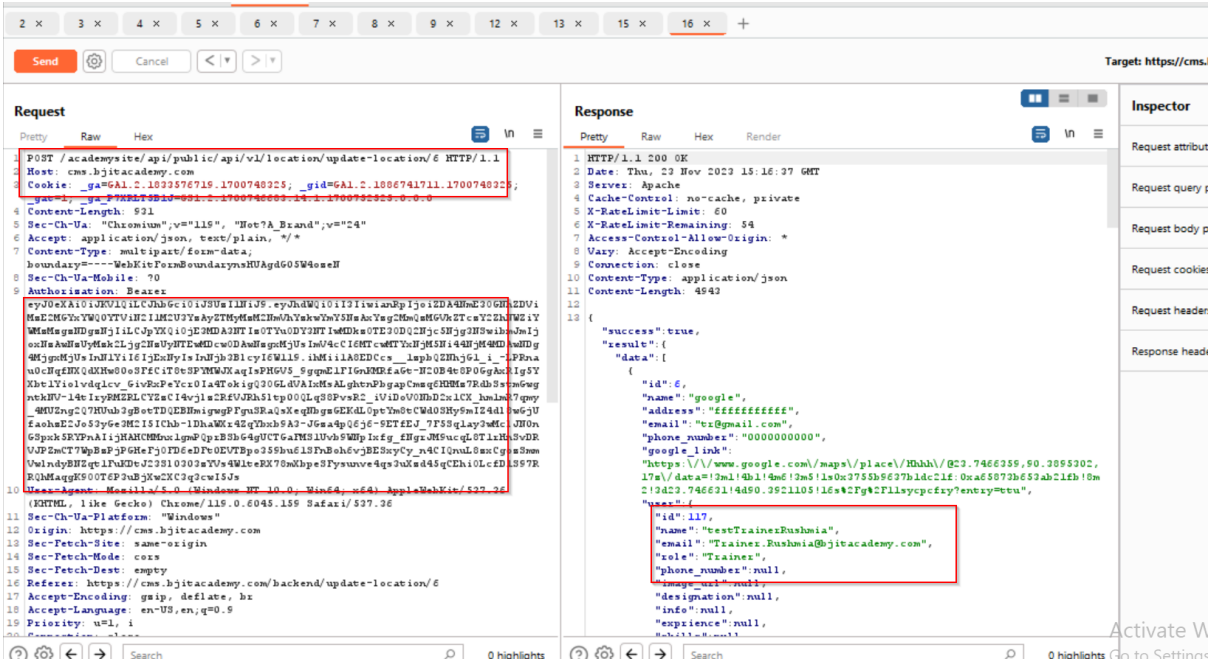


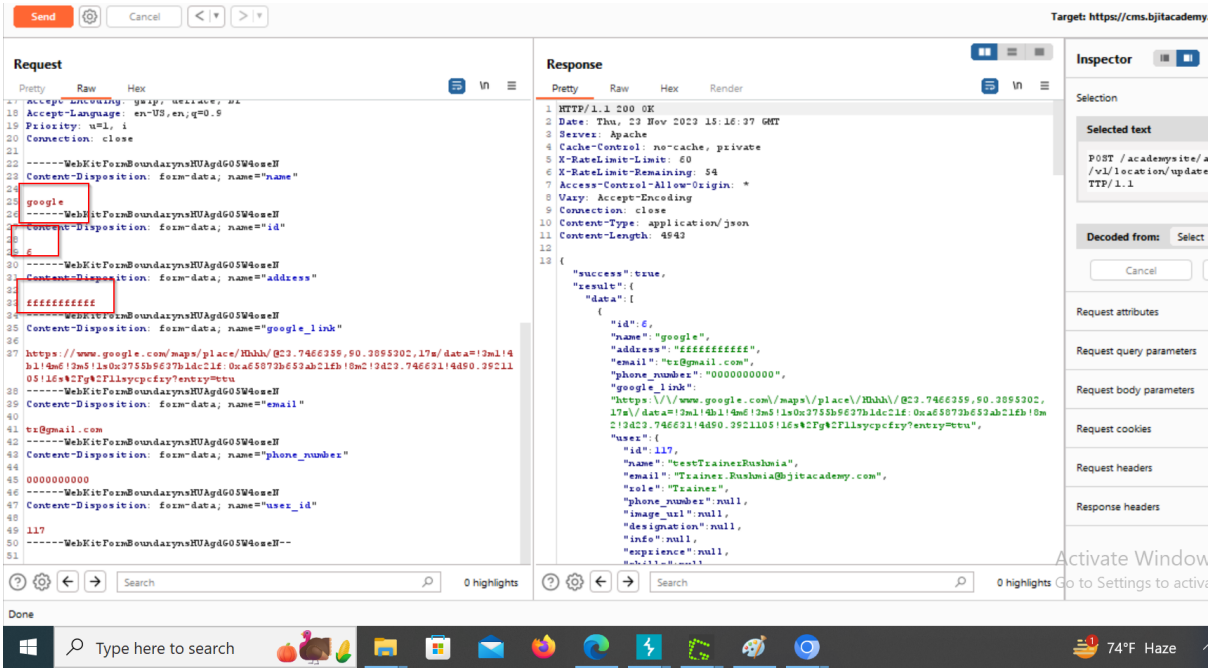
Edit Location:

Logged in as Trainer

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

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



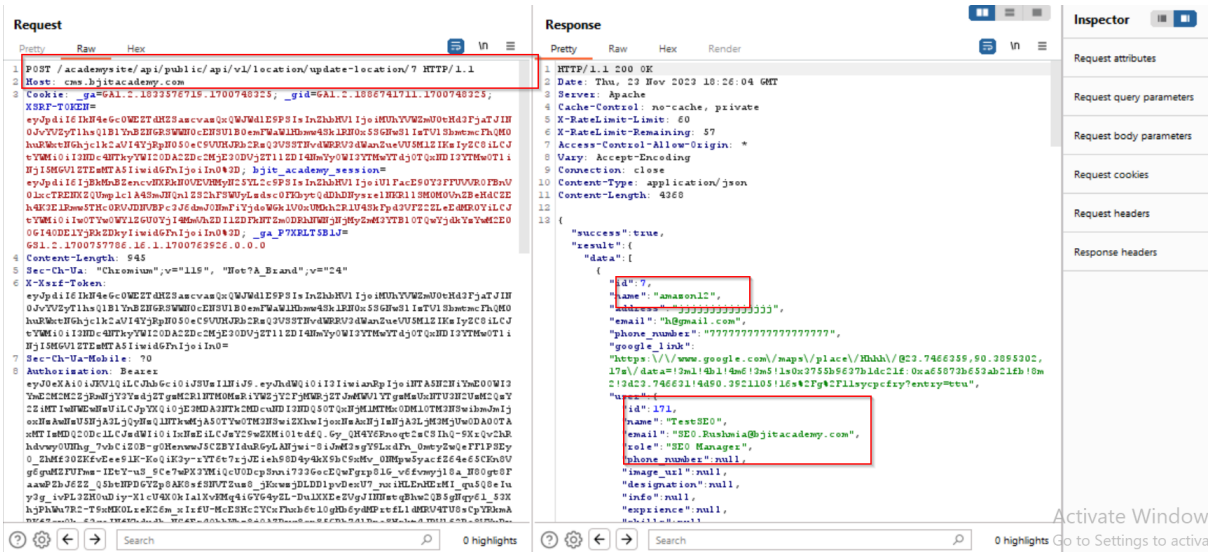


Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1
After Giving a trainer token and role inPOST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1 provides a status code of 200.

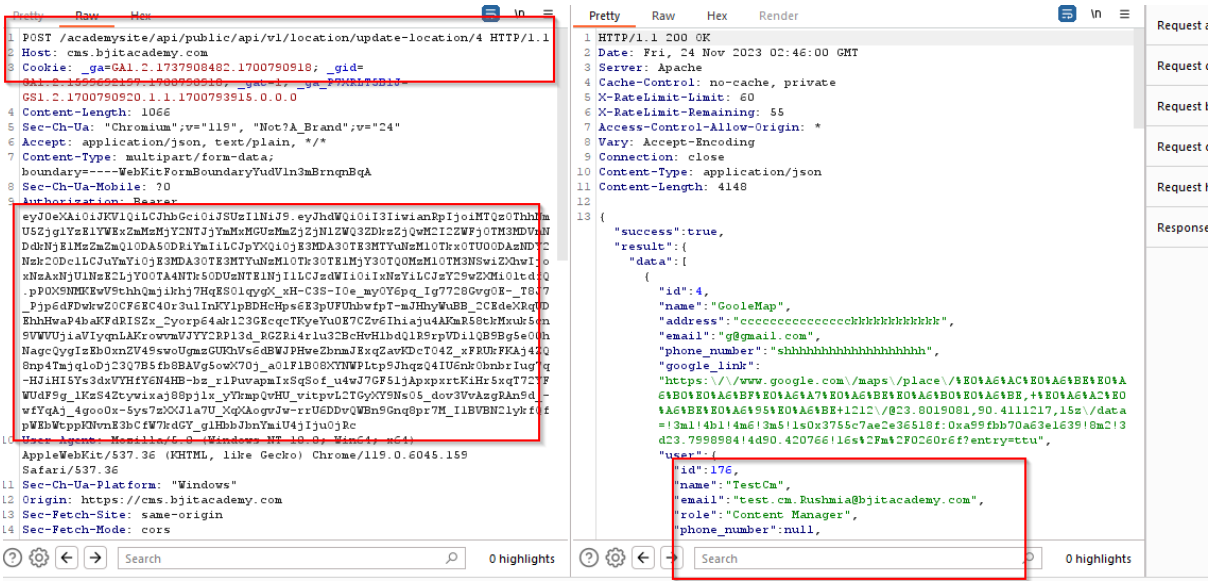
Similar to SEO

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

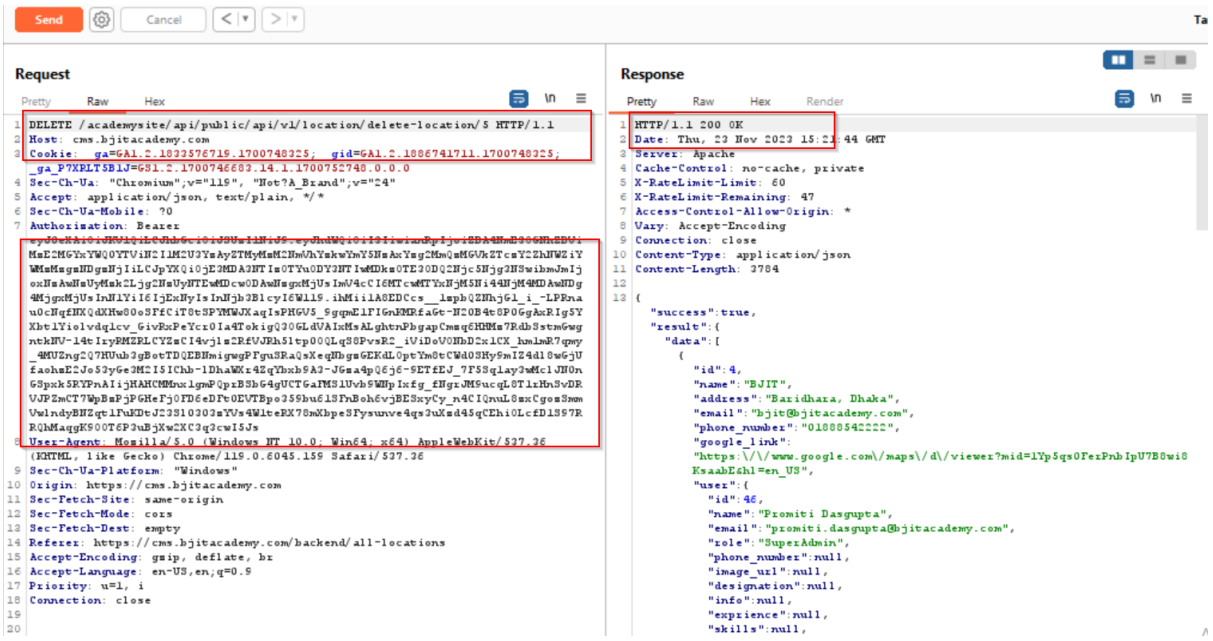
API:POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1



Similar to Content-Manager
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/location/update-location/6 HTTP/1.1



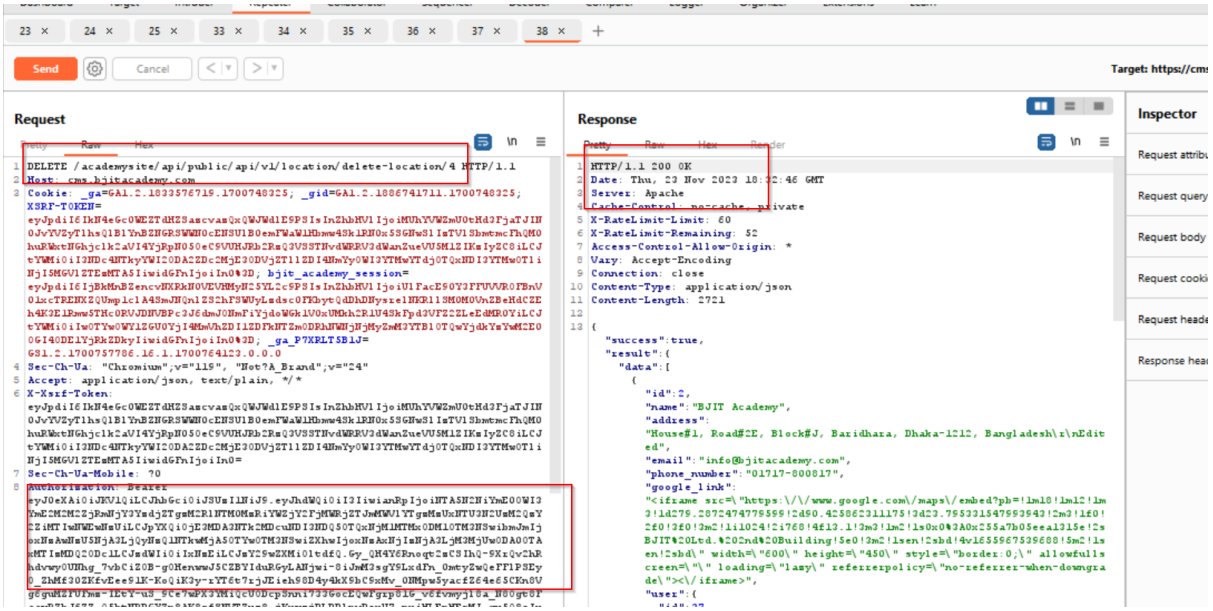
Delete Location:
Logged in as Trainer
Target:https://cms.bjitacademy.com/login
API:DELETE /academysite/api/public/api/v1/location/delete-location/5 HTTP/1.1



Similar to SEO

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

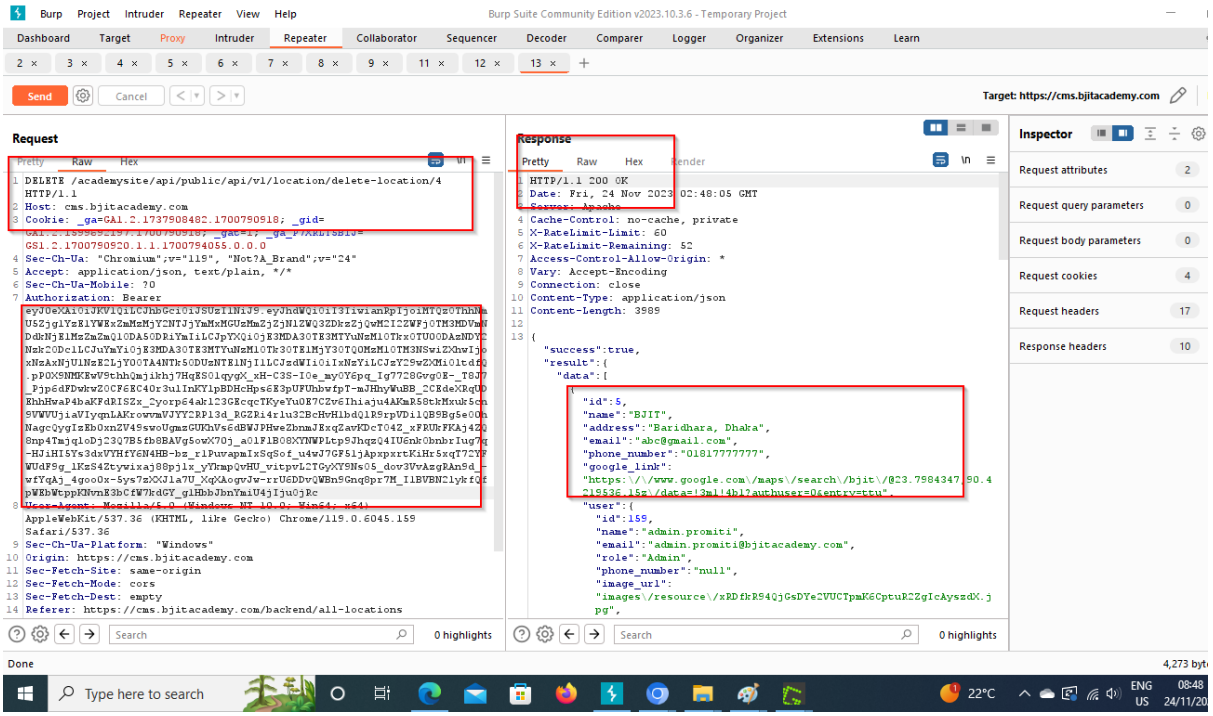
API:DELETE /academysite/api/public/api/v1/location/delete-location/5 HTTP/1.1



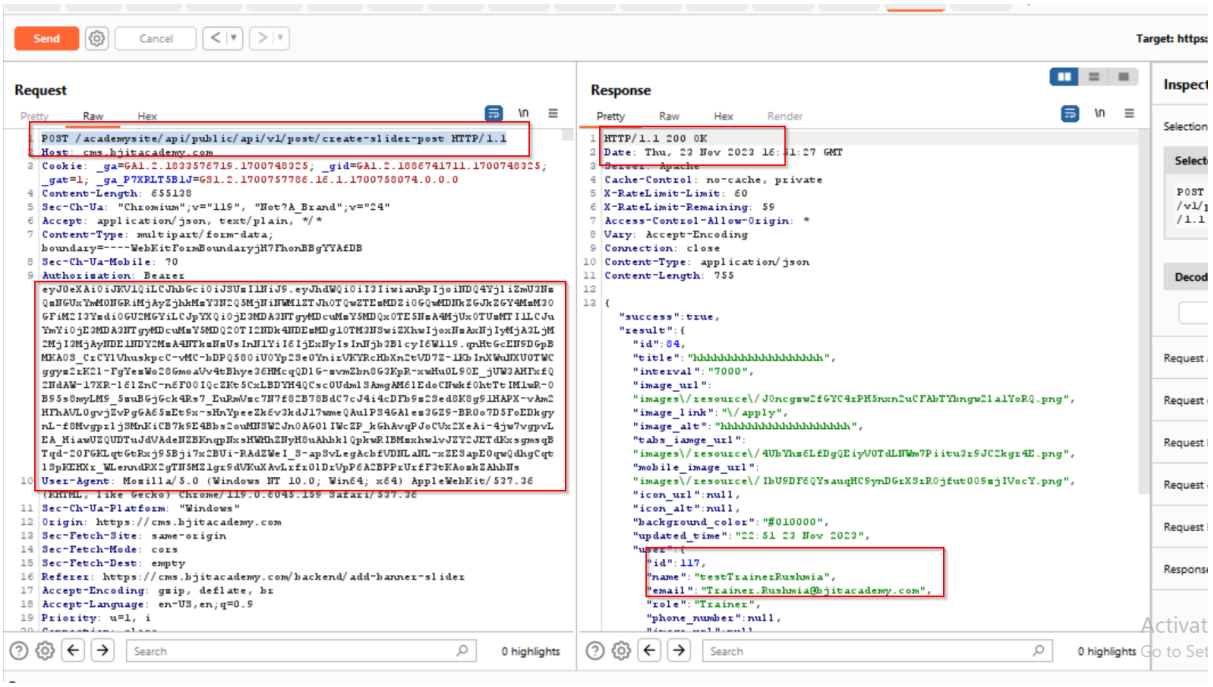
Similar to Content-Manager

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

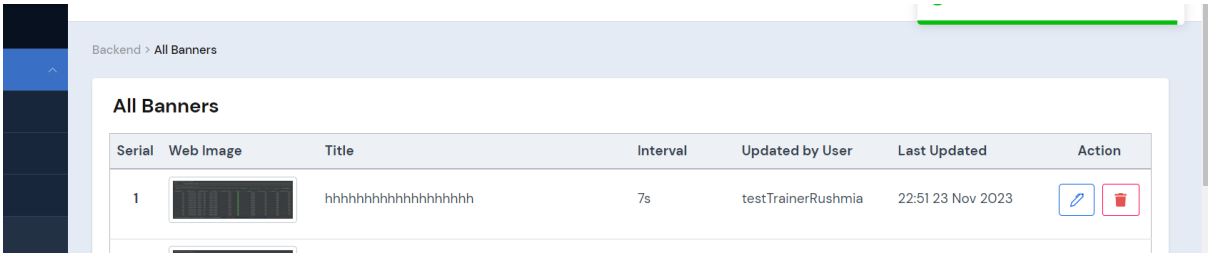
API:DELETE /academysite/api/public/api/v1/location/delete-location/5 HTTP/1.1



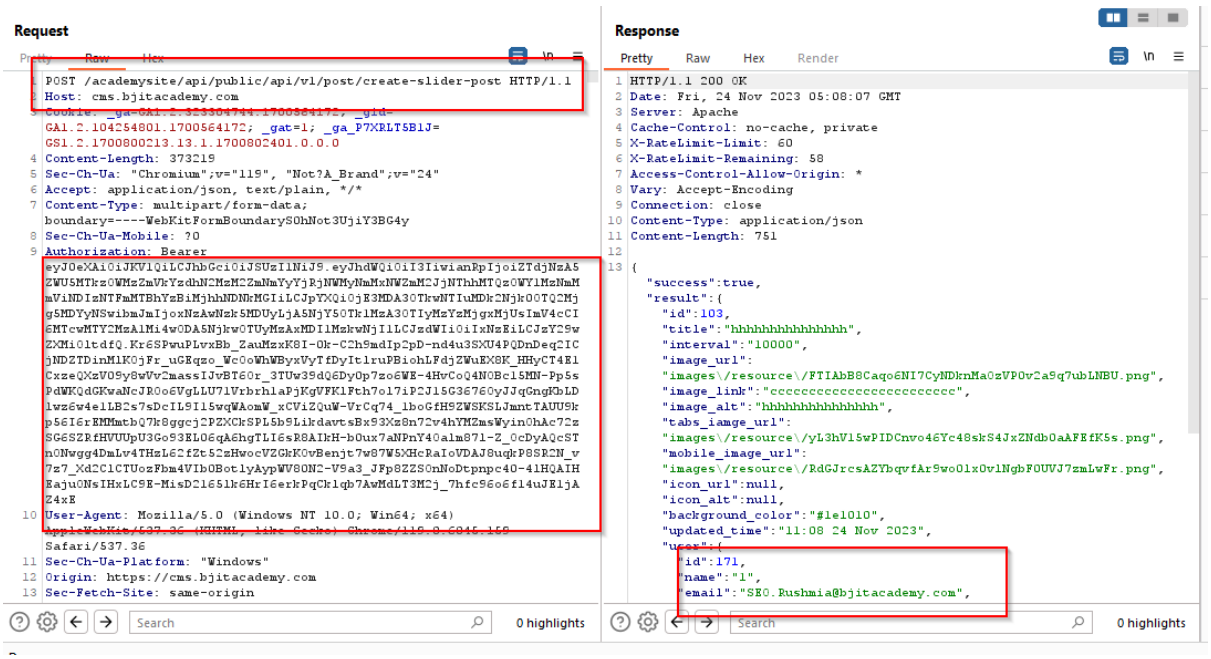
Add Slider:
Logged in as Trainer
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1



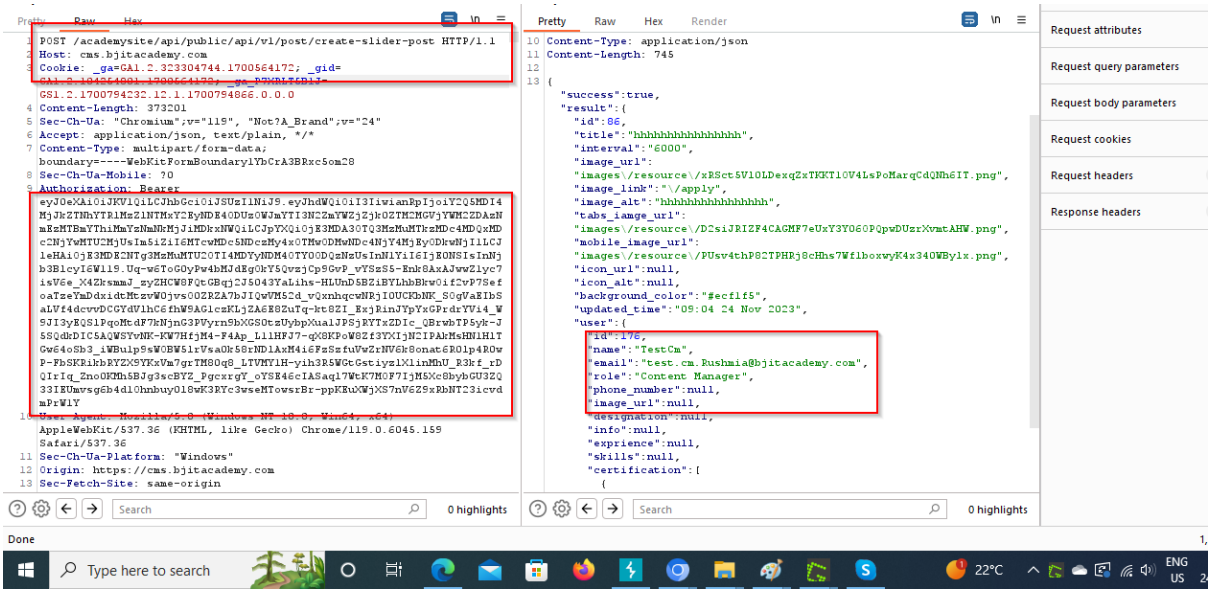
Copy the trainer token now, and replace it with the superadmin's token in the POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1
After Giving a trainer token and role in POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1 provides a status code of 200.



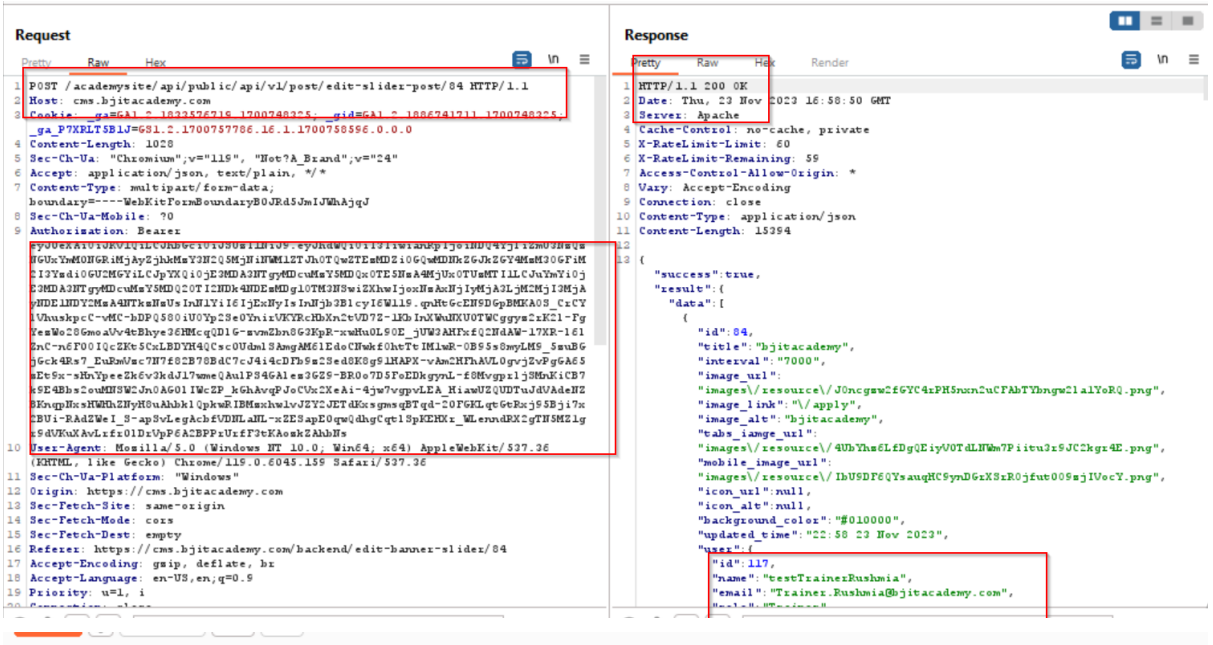
Similar to SEO
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1

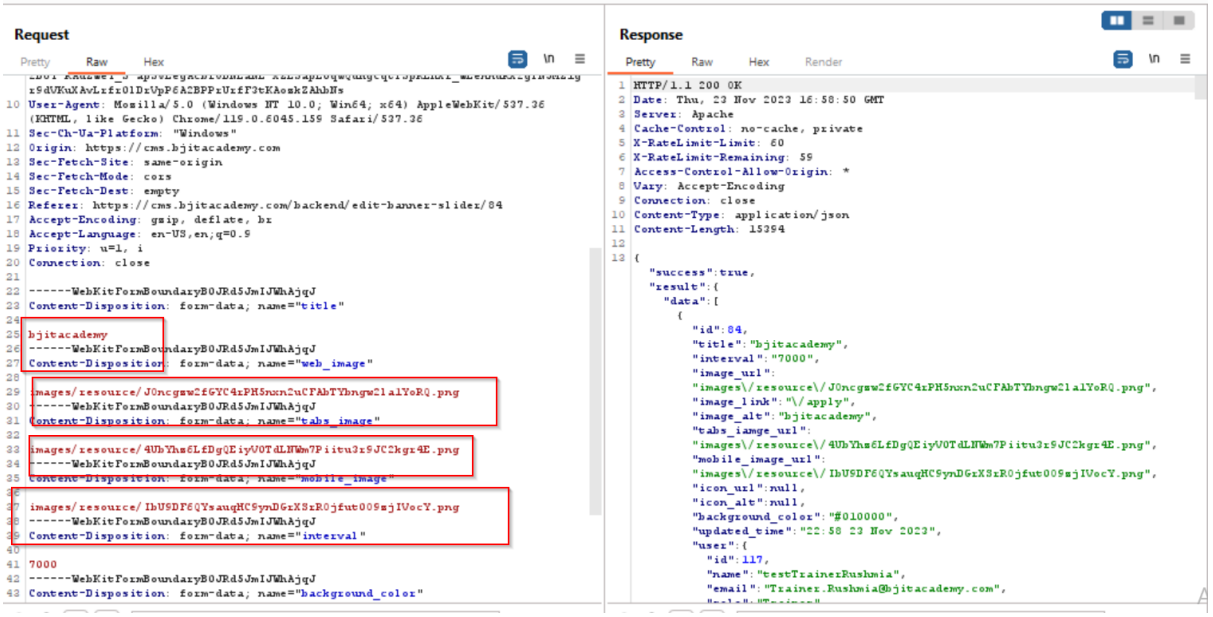


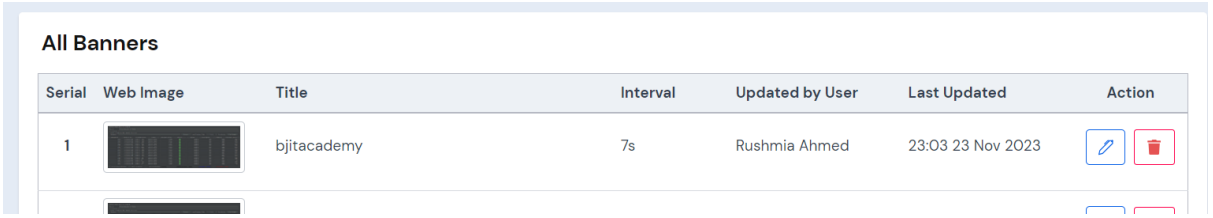
Similar to Content Manager
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1



Edit Slider:
Logged in as Trainer
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1

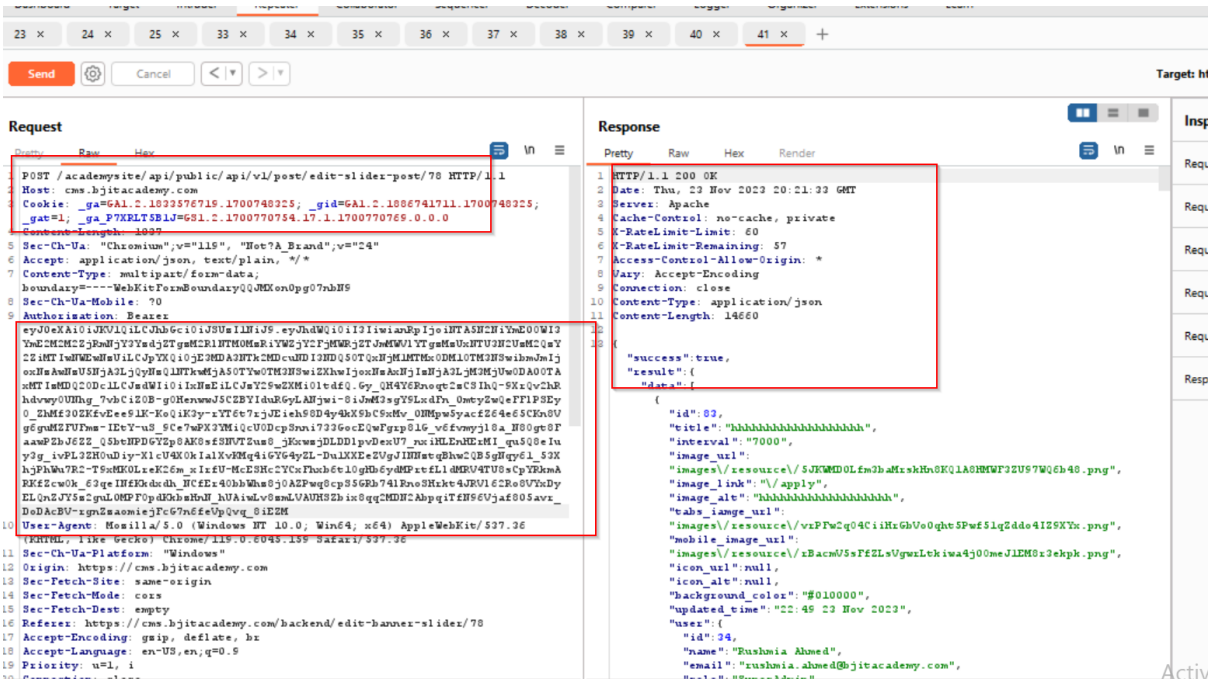






Copy the trainer token now, and replace it with the superadmin's token in thePOST /academysite/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1
After Giving a trainer token and role in POST /academysite/api/public/api/v1/post/create-slider-post HTTP/1.1 provides a status code of 200.

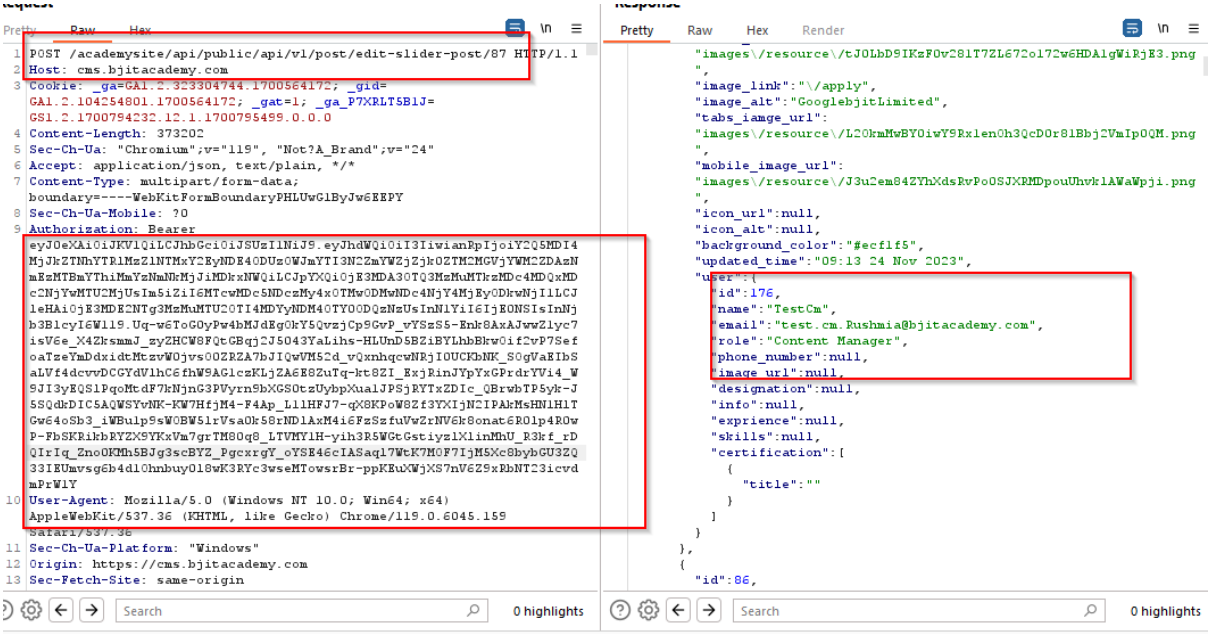
Similar to SEO
Target:https://cms.bjitacademy.com/login
API:POST /academysite/api/public/api/v1/post/edit-slider-post/84 HTTP/1.1



Similar to Content-Manager

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

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

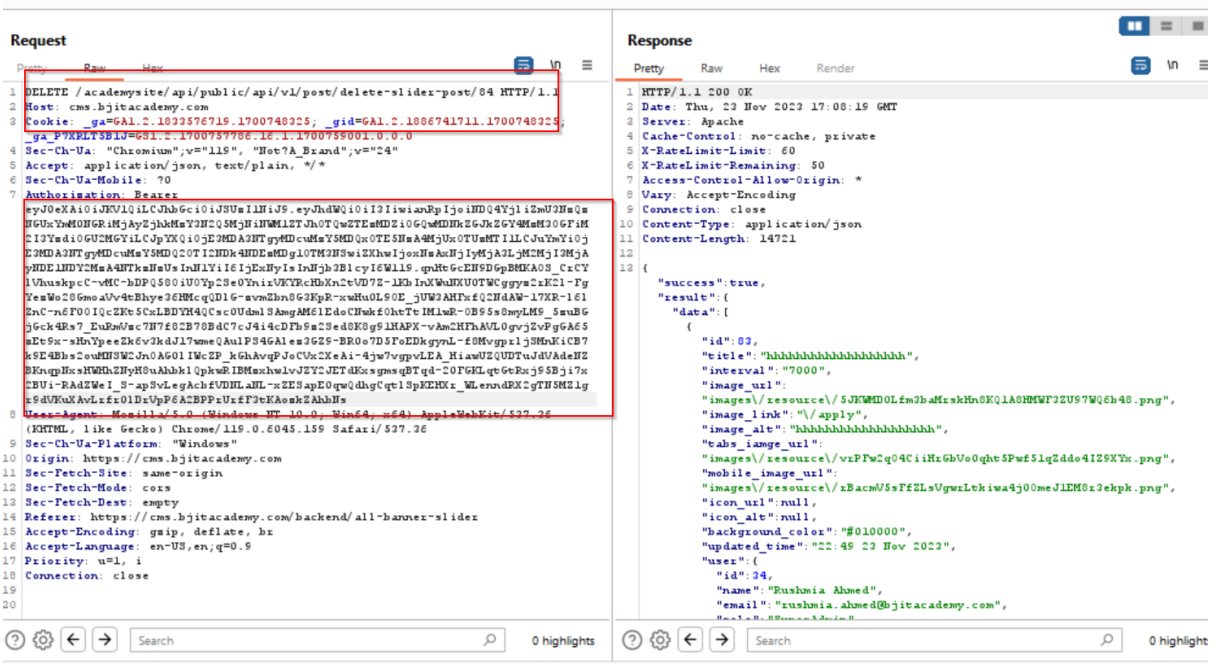


Delete Slider:

Logged in as Trainer

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

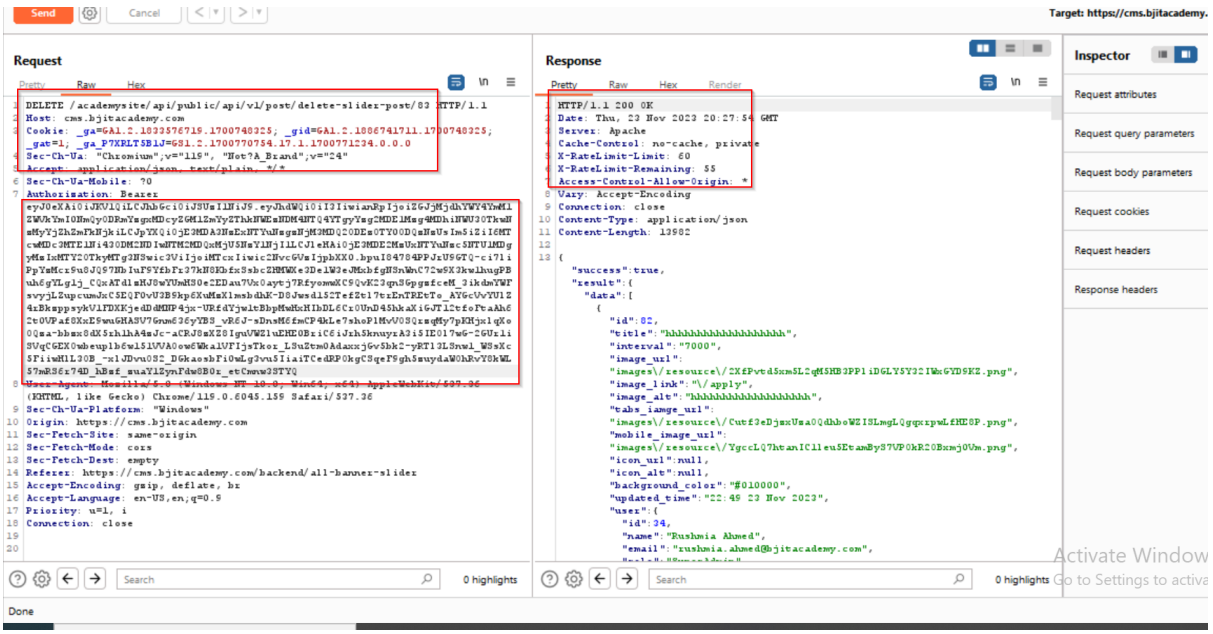
API:DELETE /academysite/api/public/api/v1/post/delete-slider-post/84 HTTP/1.1



Similar to SEO

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

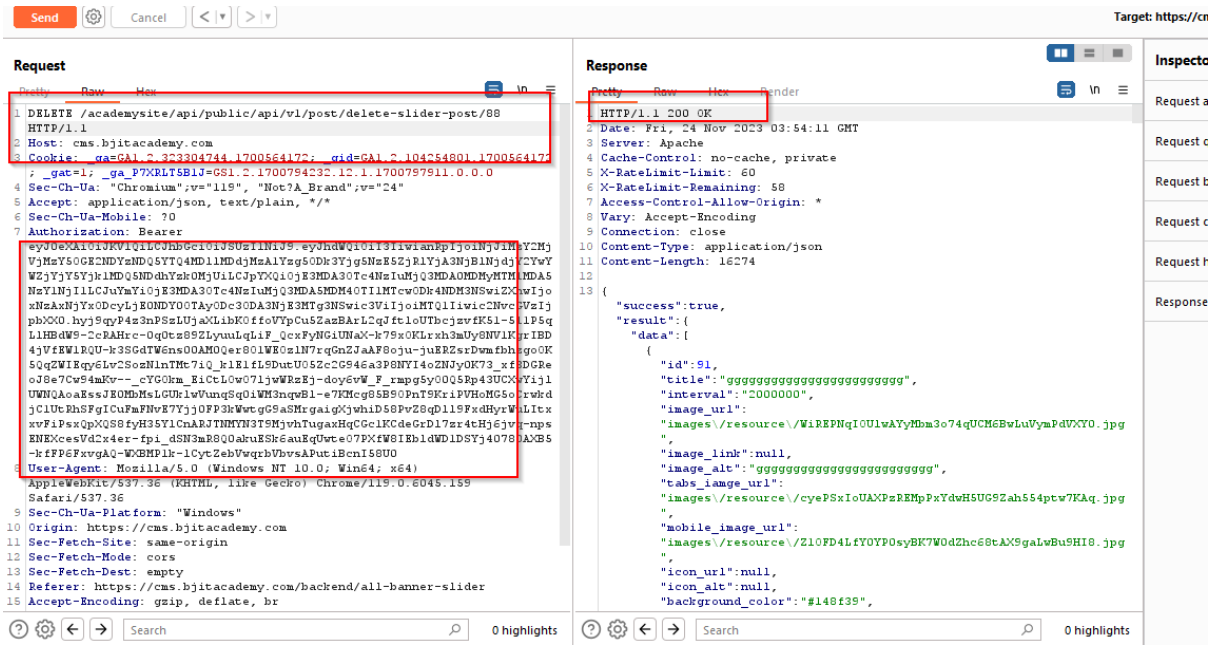
API:DELETE /academysite/api/public/api/v1/post/delete-slider-post/84 HTTP/1.1



Similar to Content-Manager:

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

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



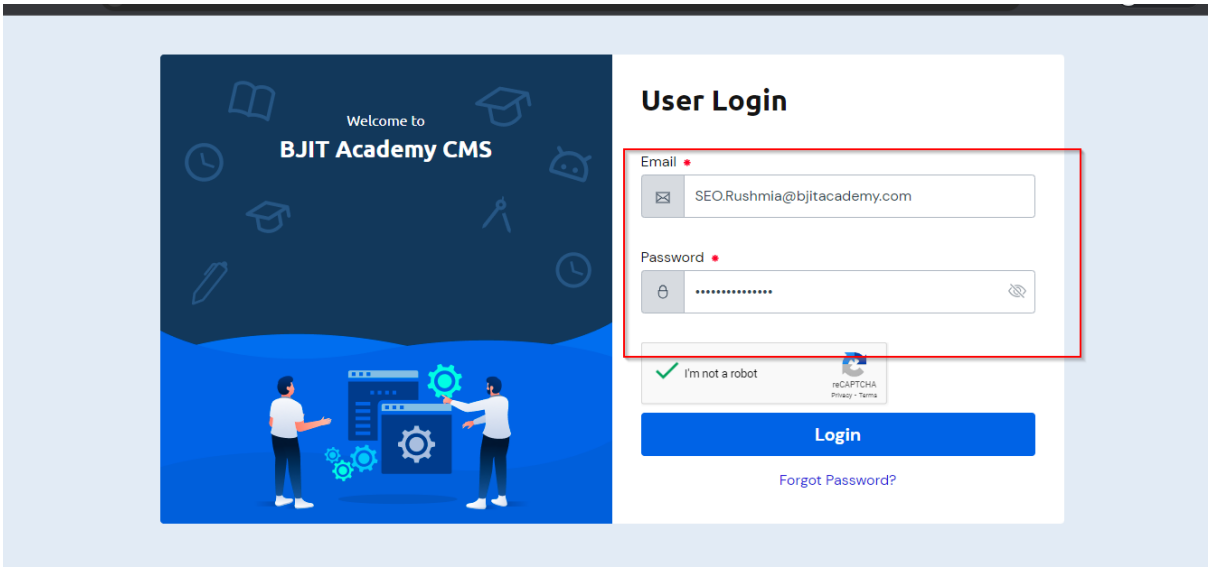
privilege acceleration:

Vulnerability-4:

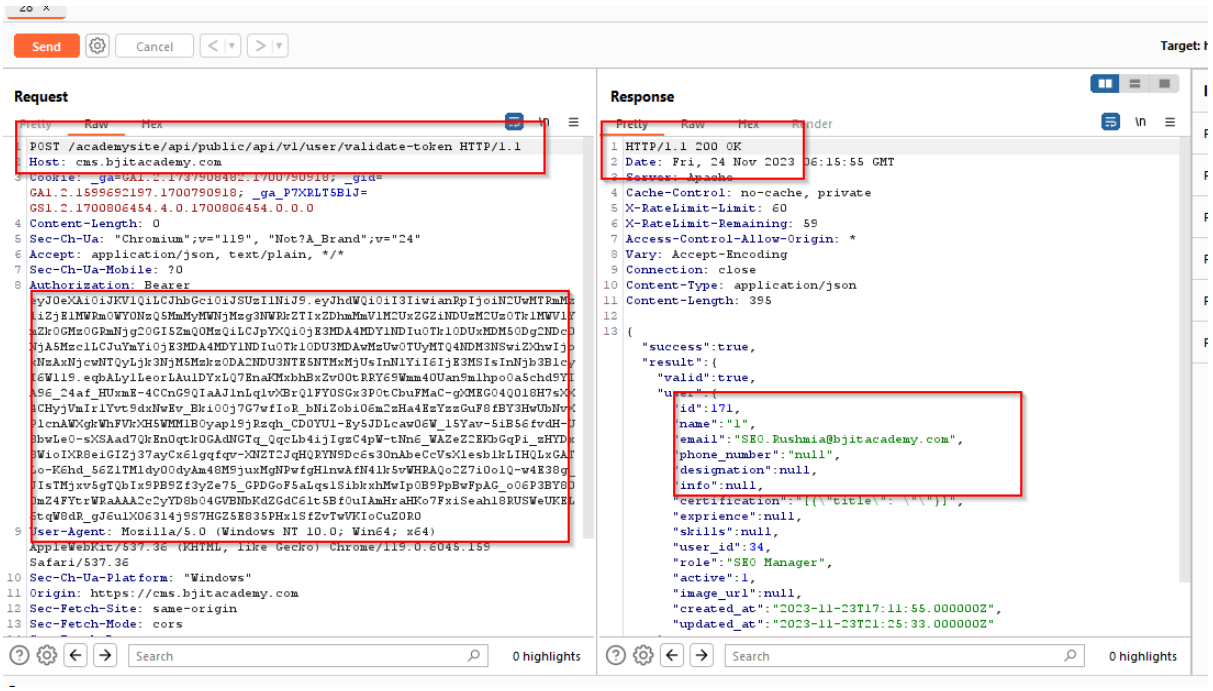
Title:Users(**Trainer,Admin,SEO,Content-Manager**) have the permission **changing role** using **user-id** , but only super admins should do so

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

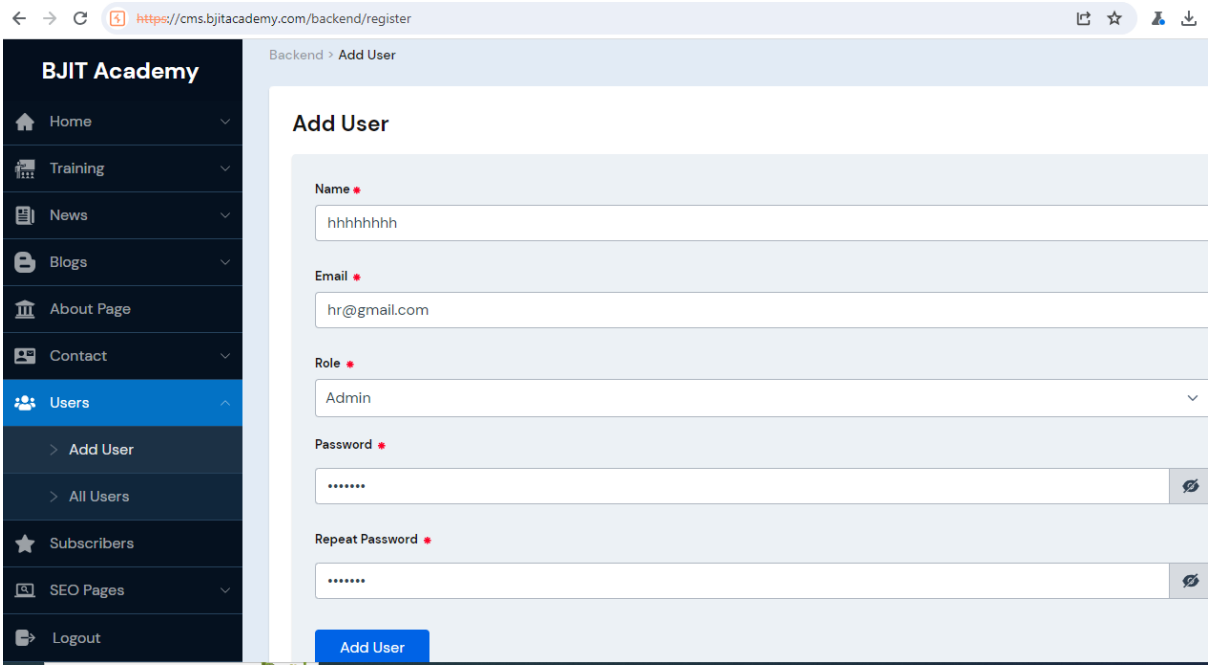
API:POST /academysite/api/public/api/v1/user/update-user-by-super-admin HTTP/1.1



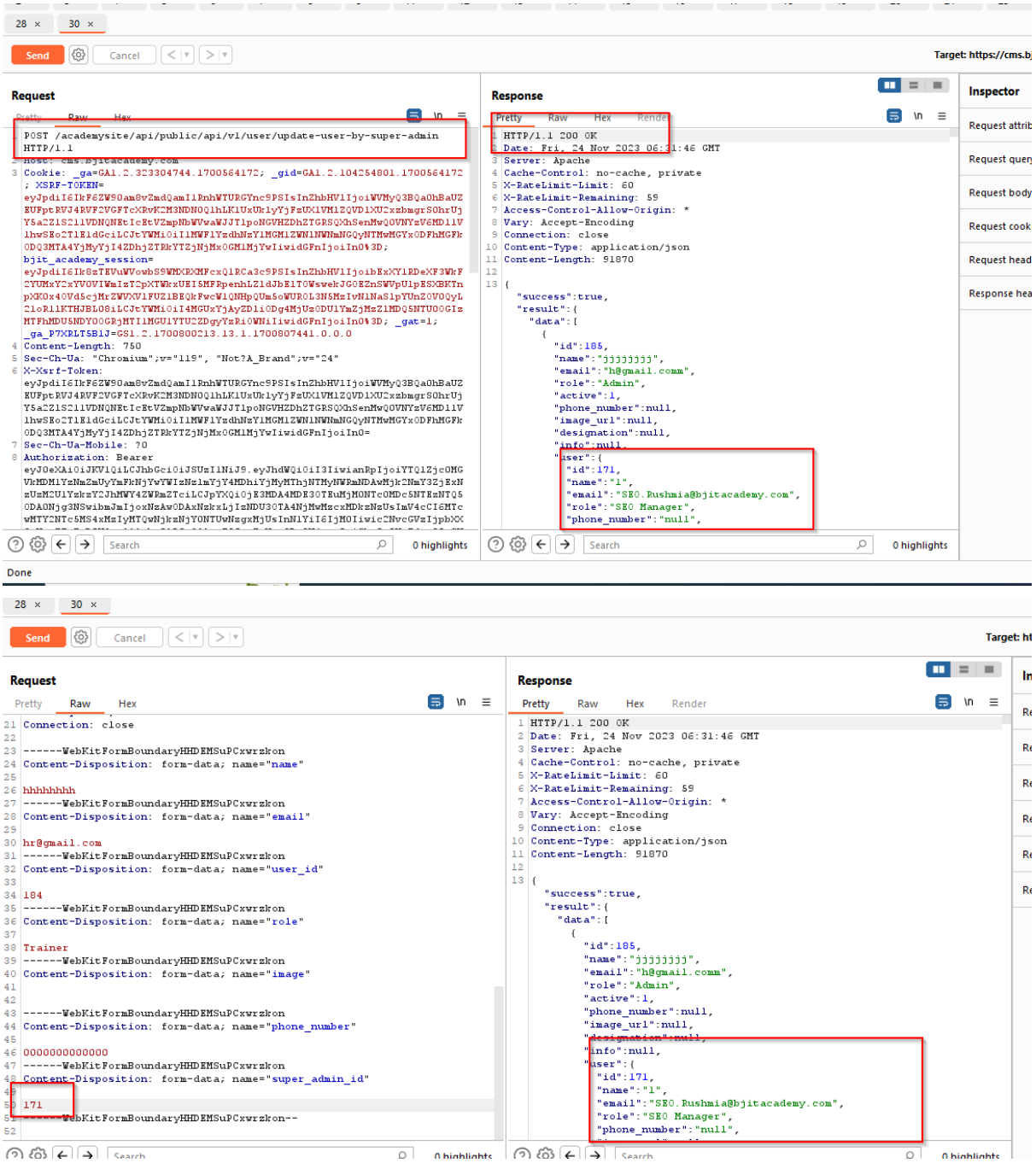
Step-1:Logged in as SEO



Step-2:Capture the request by intercept on in the burpsuite
Send the request to repeater
Collect user-id



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



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

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