



Course: Data Integrity and Authentication

Team Members:

- Yehia Ahmed Tawfiq - 2205126
- Maryam Waheed Zamel - 2205154
- Amina Ahmed Ferra - 2205225
- Mayssoune Hussein Elmasry - 2205251
- Hanin Mohamed Hamoda – 2205232

Project Overview

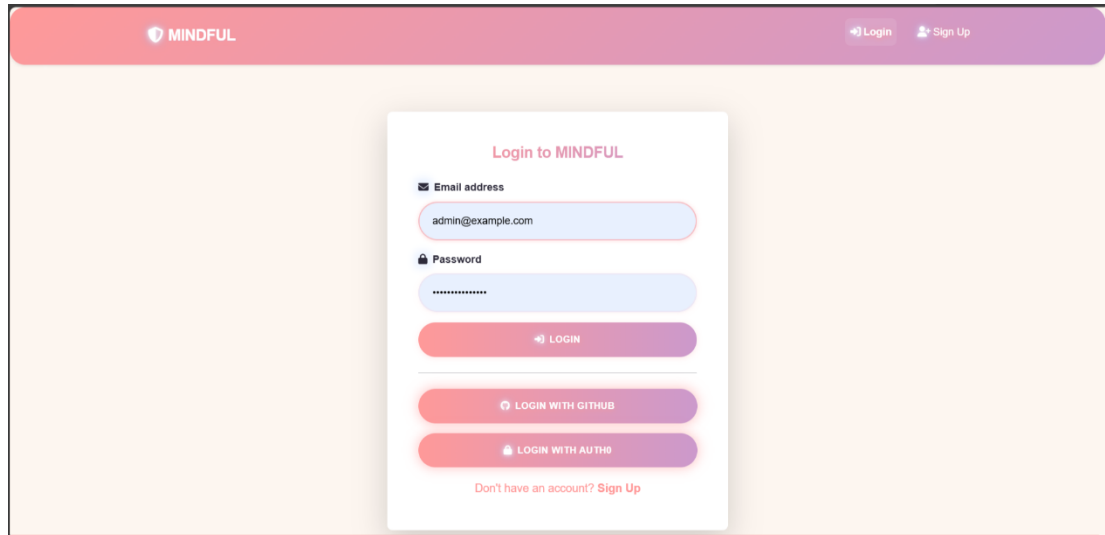
Mindful is a full-stack secure web application designed to manage sensitive health data and wellness records while ensuring data integrity, privacy, and access control. It combines modern authentication mechanisms, secure document handling, and interactive health tracking to simulate a real-world patient support system used in clinics, therapy centres, and corporate wellness programs.

Technologies Used

- **Frontend:** HTML, CSS, Bootstrap
- **Backend:** Python Flask
- **Database:** SQLite + SQLAlchemy
- **Security:** OpenSSL, SHA-256, AES, HMAC, HTTPS
- **Authentication:** OAuth, Okta, 2FA (Google Authenticator)

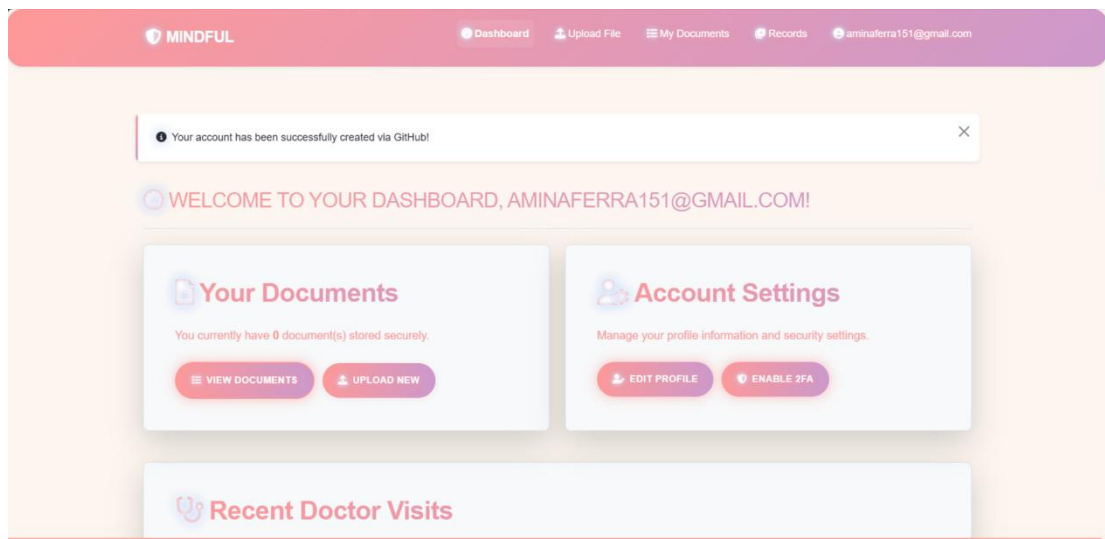
Now, we are going to Show screenshots of each implemented feature with clear explanation of the encryption and authentication flow & A Wireshark capture summary demonstrating secure communication.

1-Login: user/admin can login and the system check if the Credentials are correct from the database & also can login via GitHub or Auth0 Not just manually.



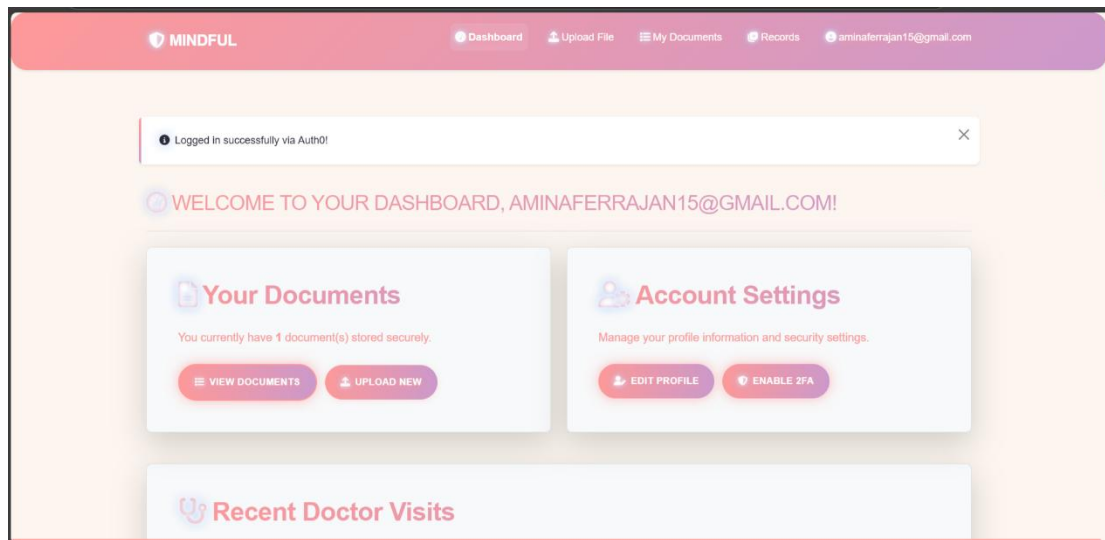
The screenshot shows the login interface for the MINDFUL application. At the top, a pink header bar contains the MINDFUL logo on the left and 'Login' and 'Sign Up' links on the right. The main content area is a light orange gradient. In the center, a white card titled 'Login to MINDFUL' contains the following elements: an 'Email address' field with the text 'admin@example.com', a 'Password' field with masked characters, a red 'LOGIN' button, a red 'LOGIN WITH GITHUB' button, a red 'LOGIN WITH AUTH0' button, and a link 'Don't have an account? Sign Up' at the bottom.

2- OAuth 2.0 Login via GitHub: Enables users to authenticate securely using popular external providers, reducing password management burden.



The screenshot shows the dashboard of the MINDFUL application after a successful login via GitHub. The pink header bar now includes a 'Dashboard' link, 'Upload File', 'My Documents', 'Records', and the user's email 'aminaferra151@gmail.com'. A white notification box at the top states 'Your account has been successfully created via GitHub!'. Below this, a message reads 'WELCOME TO YOUR DASHBOARD, AMINAFERRA151@GMAIL.COM!'. The dashboard features two main sections: 'Your Documents' with a message 'You currently have 0 document(s) stored securely.' and buttons for 'VIEW DOCUMENTS' and 'UPLOAD NEW'; and 'Account Settings' with a message 'Manage your profile information and security settings.' and buttons for 'EDIT PROFILE' and 'ENABLE 2FA'. At the bottom, there is a section titled 'Recent Doctor Visits'.

3- Login via Okta: Same as GitHub, enables users to authenticate securely



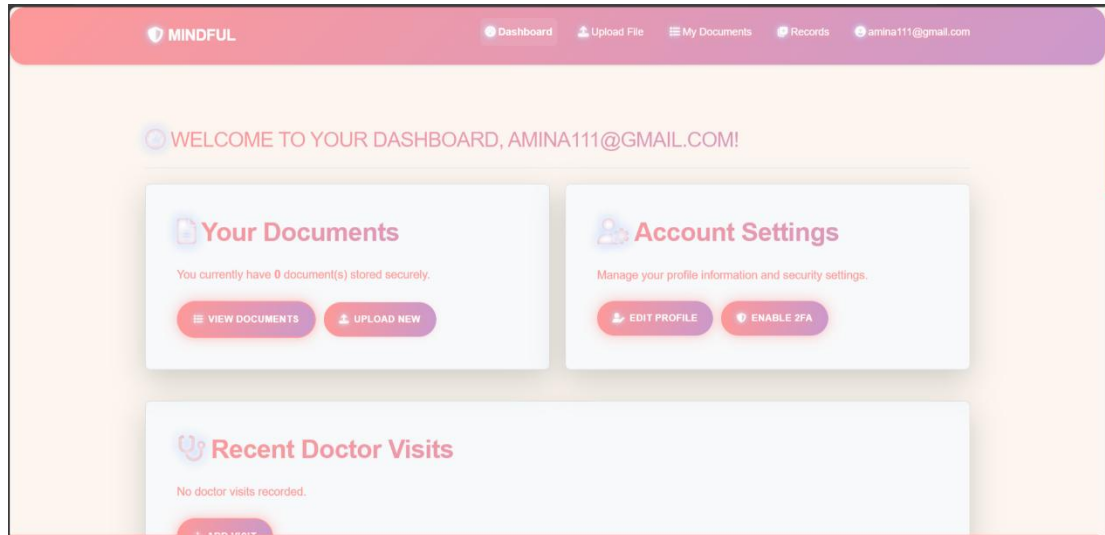
4- Sign up: If the user is new to the Website, he/she must Sign up first to create a new account and there are Policies in creating an account they must follow such as: Email format, Password Policies, Password must match to confirm it.

The screenshot displays the "Create Your MINDFUL Account" sign-up form. The form is titled "Create Your MINDFUL Account" and includes the following fields and instructions:

- Email Address:** A text input field with a placeholder "e.g., user@domain.com". Below it, a note states: "Enter a valid email (e.g., user@domain.com). Disposable emails are not allowed."
- Password:** A text input field with a placeholder "Create a secure password". Below it, a note states: "Password must be at least 12 characters and include: uppercase, lowercase, number, special character."
- Password Requirements:** A list of requirements with red circular icons:
 - At least 12 characters
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one number
 - At least one special character (@#\$%^&*)
- Confirm Password:** A text input field with a placeholder "Re-enter your password". Below it, a note states: "Must match the password above."

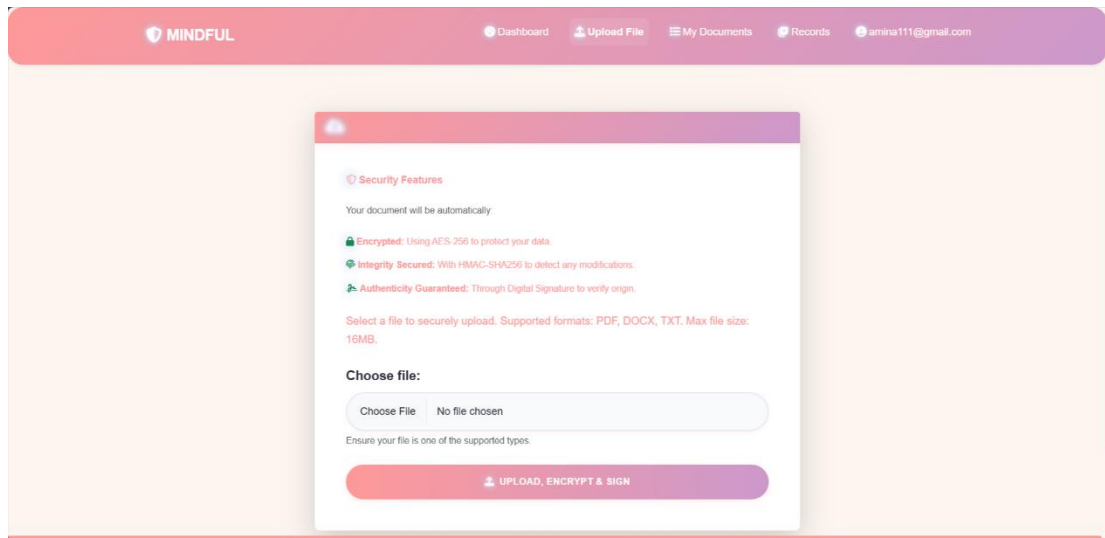
At the bottom of the form, there is a large orange button labeled "SIGN UP".

5- **User Dashboard:** when a new user is logged in, he/she enters this dashboard and can enable 2fa to enforce it each time he/she logs in.

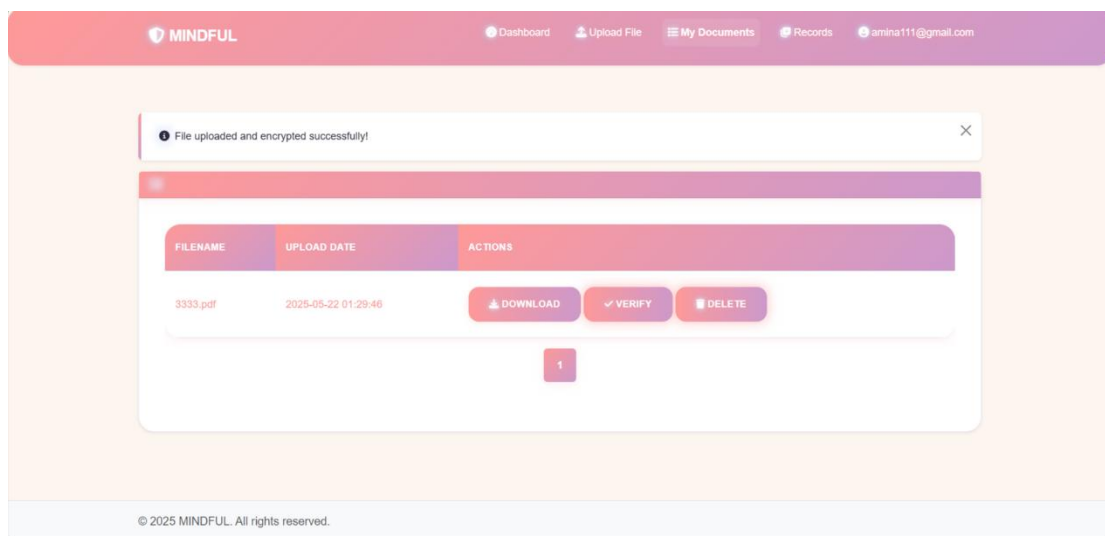


6- **Document Vault:**

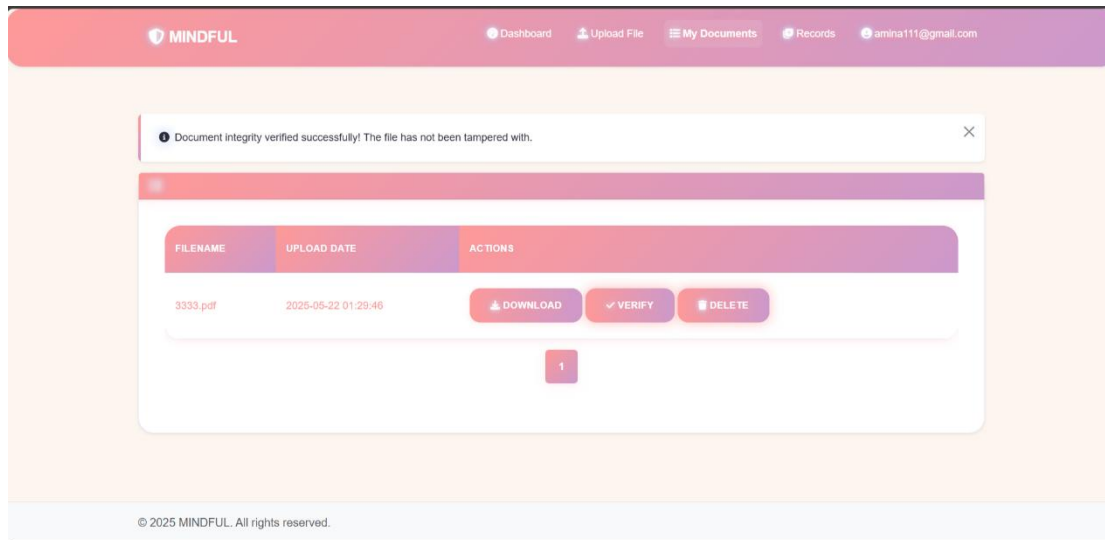
- **Document Upload:** Users can upload PDF, DOCX, and TXT files, which are processed securely.
- **AES Encryption:** All files are encrypted using the Advanced Encryption Standard before storage, ensuring confidentiality.
- **SHA-256 Hashing:** A cryptographic hash is computed for each document to uniquely identify and verify its integrity.
- **HMAC Verification:** the file's integrity is checked to ensure it hasn't been tampered with.
- **Digital Signature:** Uploaded documents are digitally signed, and this signature can be verified later to confirm authenticity.



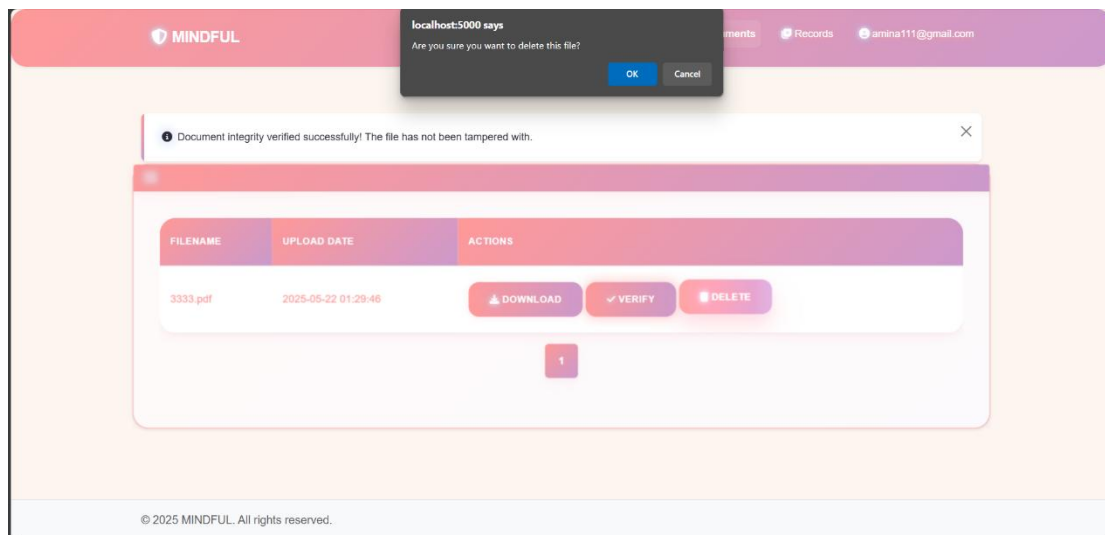
7- **Cont. Documents:** Users can Download their Documents.



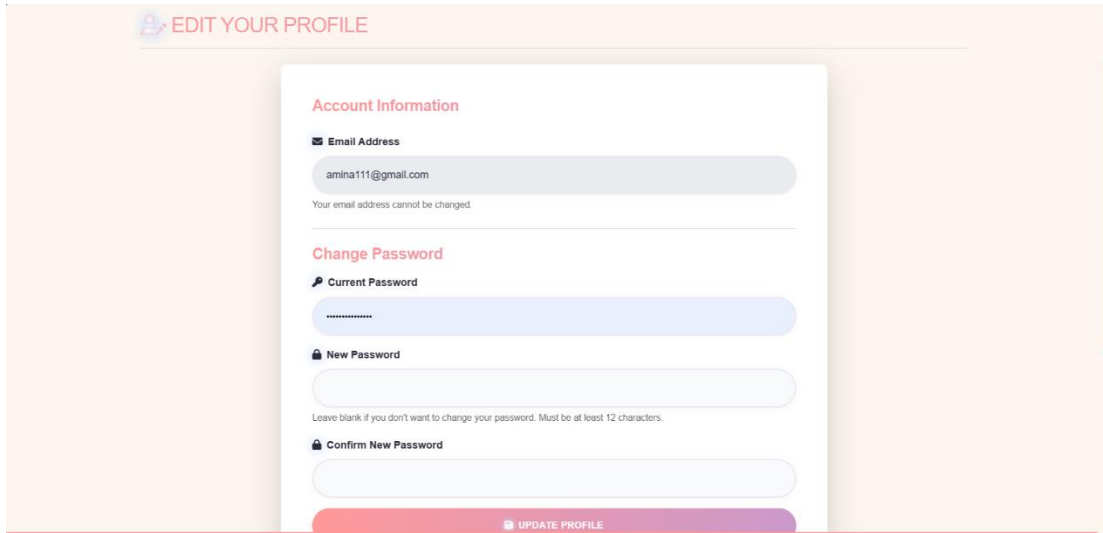
8- Cont. Documents: if the user clicked on verify integrity button, the System checks if the document has been tampered or not then shows a Confirmation message.



9- Cont. Documents: If the user wants to delete a document, the system makes sure that if the user wants to confirm deletion as it cannot be undone.

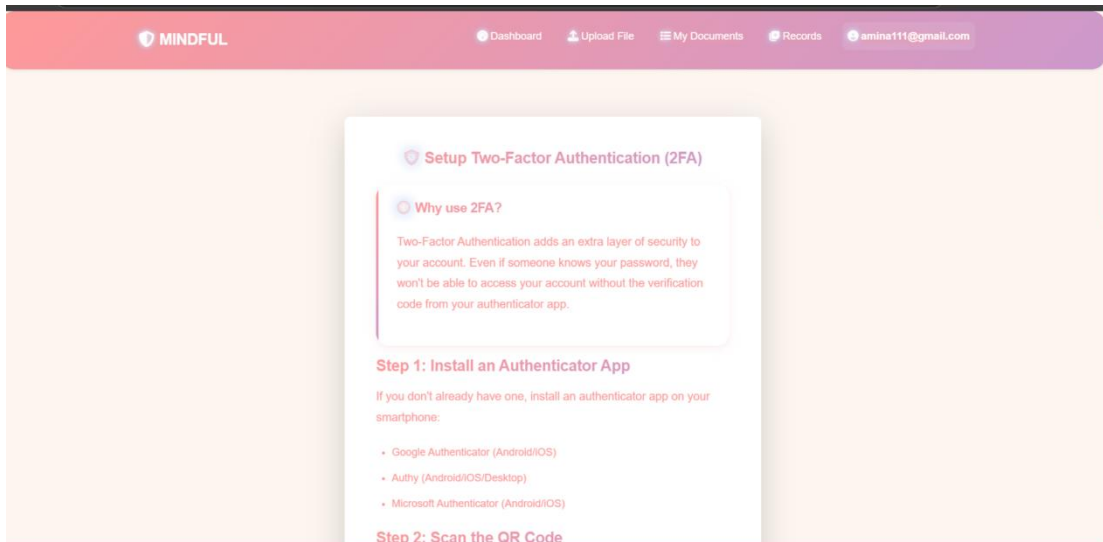


10-Edit Profile: User/Admin can edit their profiles easily as changing the passwords and also there are enforced password policies.



The screenshot shows the 'EDIT YOUR PROFILE' page. It features a white card with a pink header 'Account Information'. Below this, there is a section for 'Email Address' with the value 'amina111@gmail.com' and a note stating 'Your email address cannot be changed.' The next section is 'Change Password', which includes three input fields: 'Current Password' (filled with dots), 'New Password', and 'Confirm New Password'. A note below the 'New Password' field states: 'Leave blank if you don't want to change your password. Must be at least 12 characters.' At the bottom of the card is a pink button labeled 'UPDATE PROFILE'.


11-2FA: If the new user enables 2fa, he/she will scan the QR code via Google Authenticator then enter the valid code (make sure it is not expired) then click verify.



The screenshot shows the 'Setup Two-Factor Authentication (2FA)' page. It features a white card with a pink header 'Setup Two-Factor Authentication (2FA)'. Below this, there is a section titled 'Why use 2FA?' with a description: 'Two-Factor Authentication adds an extra layer of security to your account. Even if someone knows your password, they won't be able to access your account without the verification code from your authenticator app.' The next section is 'Step 1: Install an Authenticator App', which includes a note: 'If you don't already have one, install an authenticator app on your smartphone:' followed by a list of recommended apps: Google Authenticator (Android/iOS), Authy (Android/iOS/Desktop), and Microsoft Authenticator (Android/iOS). The final section is 'Step 2: Scan the QR Code'.

Step 2: Scan the QR Code

Open your authenticator app and scan this QR code:



Can't scan the QR code?

Manually enter this secret key into your authenticator app:

LMIF HU56 73IV ED05 MB6E 2ELO OEZP SFDN

Step 3: Verify Setup

Enter the 6-digit code shown in your authenticator app:

The code changes every 30 seconds. Enter the current code shown in your app.

✕ SKIP FOR NOW ✓ VERIFY AND ENABLE 2FA

12- Cont. 2FA: After enabling, every time the user logs in, the system will ask him/her for a code to verify.

MINDFUL

Login

Sign Up

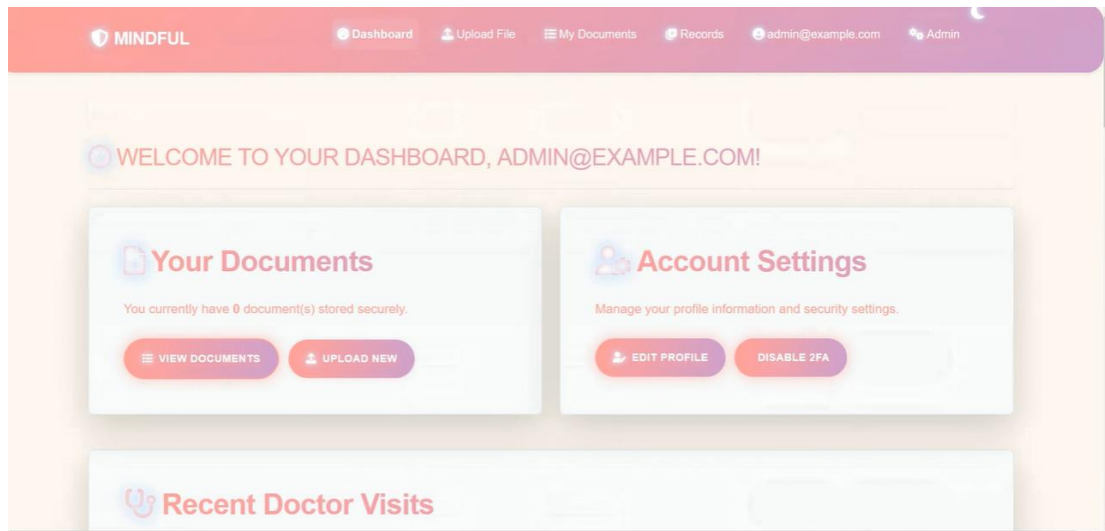
Verify 2FA Code

Enter the 6-digit code from your authenticator app to complete login.

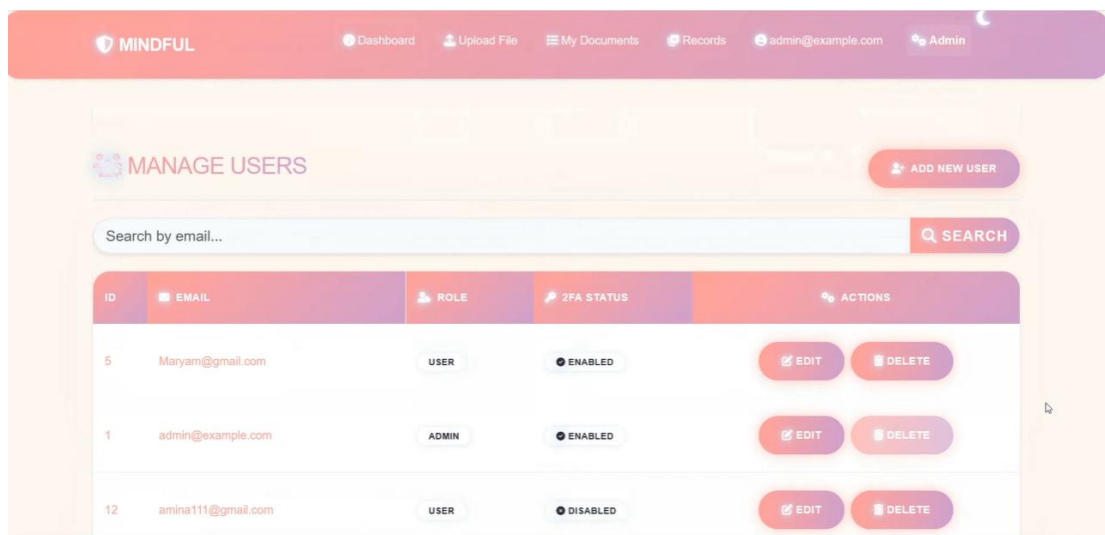
✓ VERIFY CODE

© 2025 MINDFUL. All rights reserved.

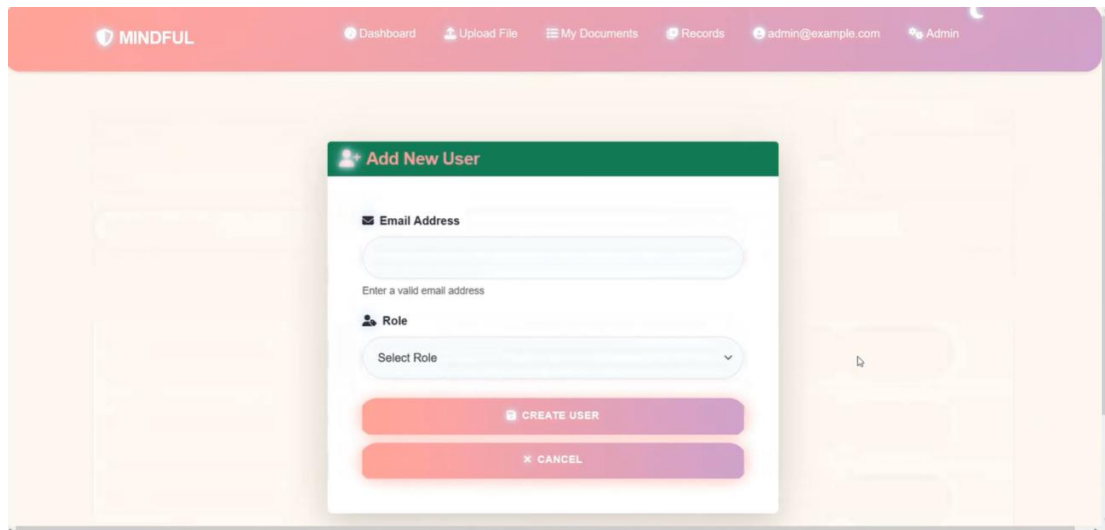
13- Admin Dashboard: the admin can do the same functionalities as the user, but the admin have more control as he has the admin panel that a regular user cannot access.



14- User Management: Here the admin can see all the users on the system, also he can edit/add/delete any user.

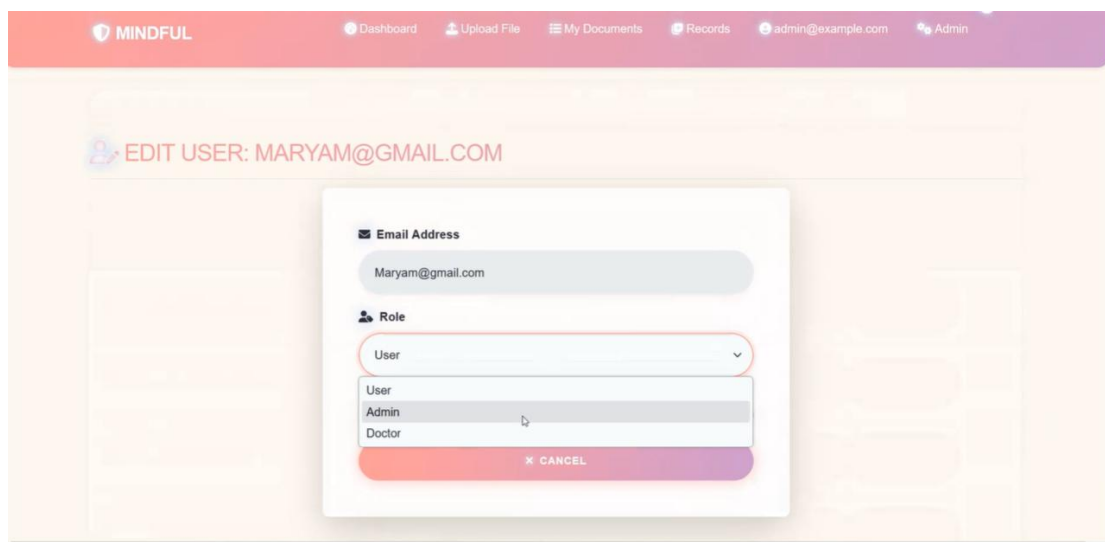


15- Cont. User Management: the admin can add any user and choose his role (all created users via admin is set with a default password that the user can change it later).



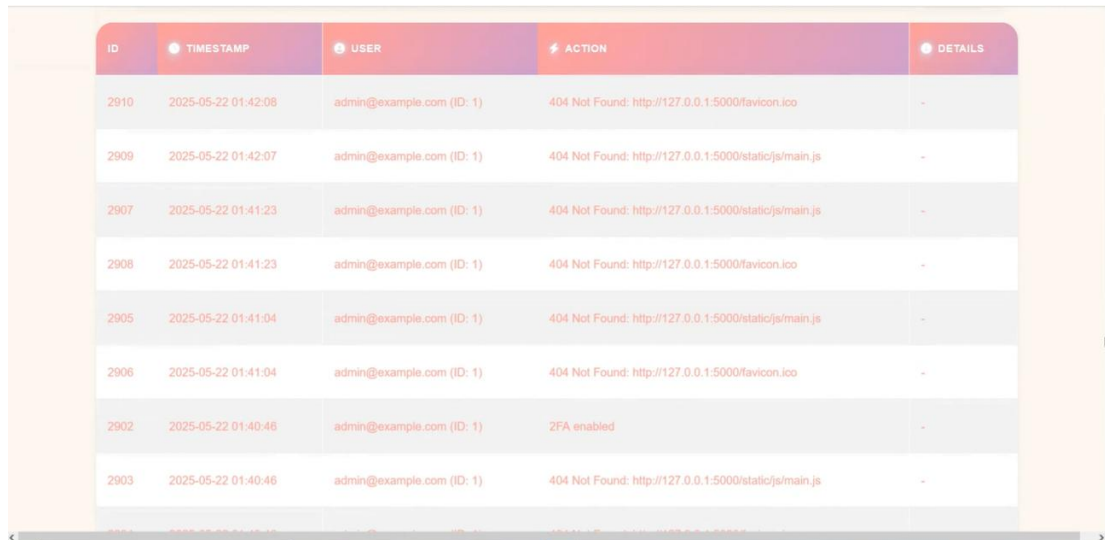
The screenshot shows the 'Add New User' modal in the MINDFUL application. The modal has a green header with a user icon and the title 'Add New User'. It contains two input fields: 'Email Address' with a placeholder 'Enter a valid email address' and 'Role' with a dropdown menu labeled 'Select Role'. At the bottom, there are two buttons: 'CREATE USER' and 'CANCEL'.

16- Cont. User Management: the admin can edit any user by changing his/her role.



The screenshot shows the 'Edit User' modal in the MINDFUL application. The modal has a header with a user icon and the title 'EDIT USER: MARYAM@GMAIL.COM'. It contains two input fields: 'Email Address' with the value 'Maryam@gmail.com' and 'Role' with a dropdown menu showing 'User', 'Admin', and 'Doctor'. At the bottom, there is a 'CANCEL' button.

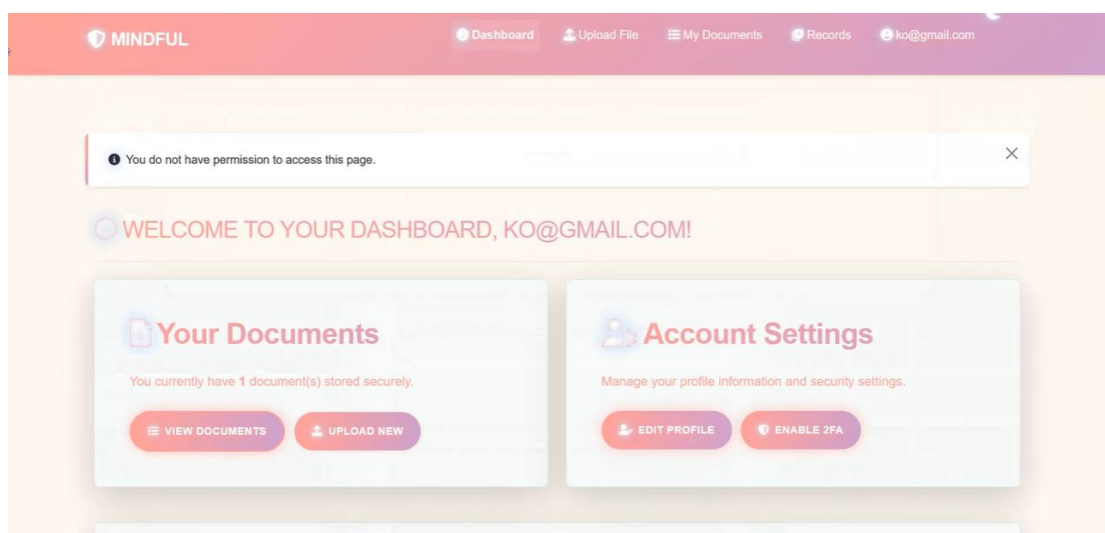
17-Audit logs: here the admin can view all actions that happens on the system (View login history, file uploads, and suspicious actions, session expiration)



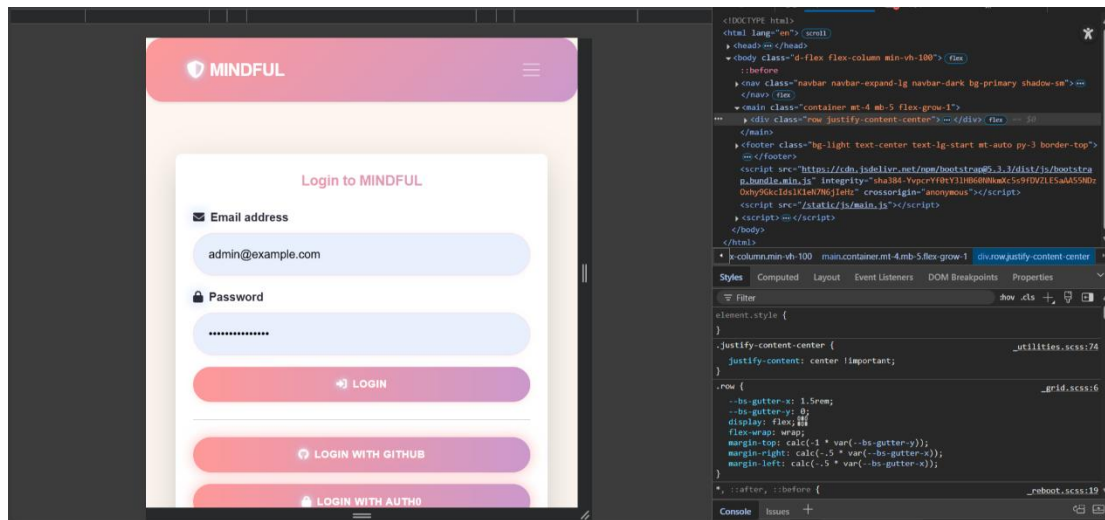
ID	TIMESTAMP	USER	ACTION	DETAILS
2910	2025-05-22 01:42:08	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/favicon.ico	-
2909	2025-05-22 01:42:07	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/static/js/main.js	-
2907	2025-05-22 01:41:23	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/static/js/main.js	-
2908	2025-05-22 01:41:23	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/favicon.ico	-
2905	2025-05-22 01:41:04	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/static/js/main.js	-
2906	2025-05-22 01:41:04	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/favicon.ico	-
2902	2025-05-22 01:40:46	admin@example.com (ID: 1)	2FA enabled	-
2903	2025-05-22 01:40:46	admin@example.com (ID: 1)	404 Not Found: http://127.0.0.1:5000/static/js/main.js	-

18-Secure Admin Endpoints: Access to Admin pages and features is restricted such as http://127.0.0.1:5000/admin/security/audit_logs

If an attacker tries to enter this endpoint it shows him a message that he has no permission to access this route.



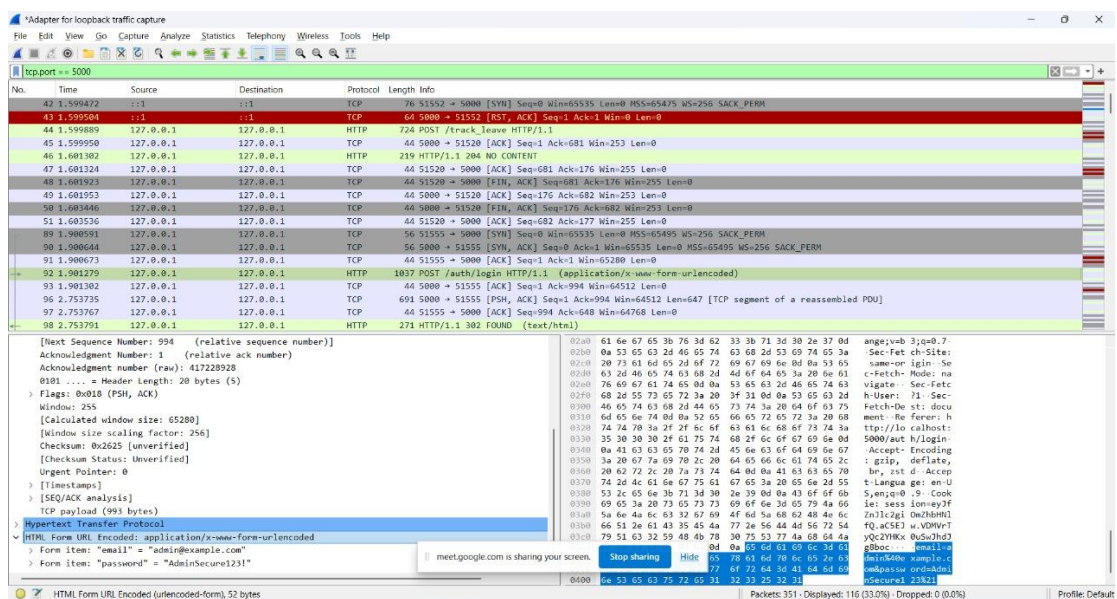
19- UI Requirements: Clean, modern UI using Bootstrap & Responsive (works on desktop and mobile)

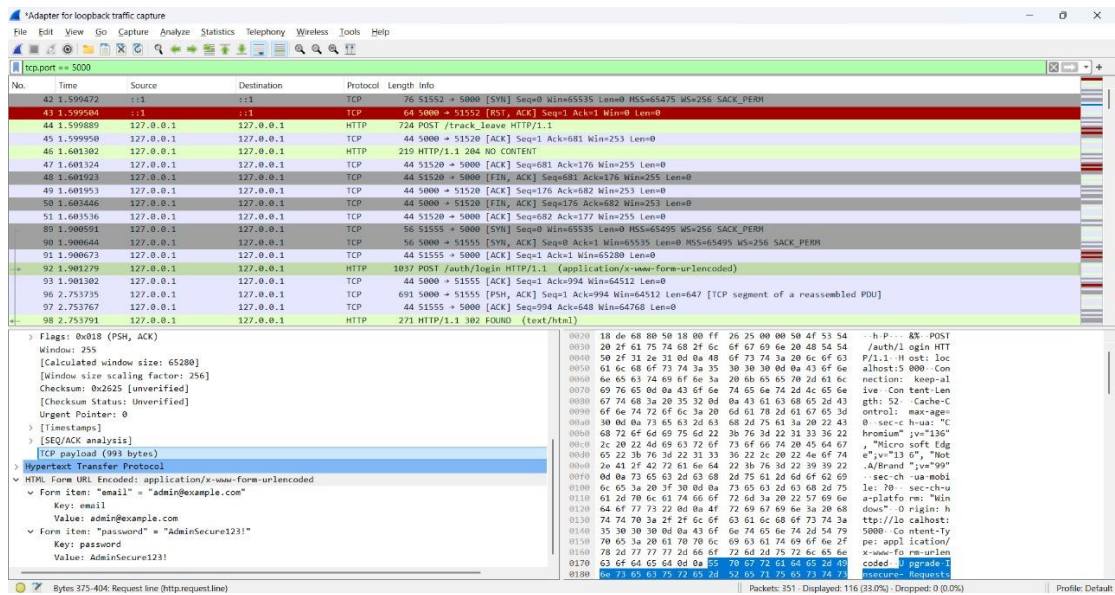


20- we will simulate MITM attacks using Wireshark to demonstrate protection via HTTPS & Shows intercepted vs. protected traffic.

We will run on HTTP first.

Here, as you can see all the credentials are not encrypted anyone can see it so, it can cause man in the middle attack as he can intercept the traffic.





21- HTTPS & Certificate Management: First, Configure local SSL/TLS using OpenSSL Via this command:

(openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout server.key -out server.crt)

Then, Run the app over HTTPS.

As you can see the Credentials is encrypted so, that secures the traffic & protect from MITM.

