

**Form-5 Document**

**Capstone Design Specification**

**⁠CryptDocs: A Safe and Open Web-Based Document Management System Employing Role-Based Access Control and Metadata Encryption**

**GROUP MEMBER:**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Student Name** | **Student ID** | **Study Program** |
| 1. | Asyifadia Aqila Fauzan | 001202200130 | Informatics |
| 2. | Afsa Mifzal Zararghirfar | 001202200150 | Informatics |
| 3. | Egan Maheswara | 001202200079 | Informatics |

Capstone Advisor: **Williem, M.Sc**

Submitted for

Capstone Design Project

to Faculty of Computer Science

President University

# TABLE OF CONTENT

[TABLE OF CONTENT 2](#_Toc201504082)

[STATEMENT OF ORIGINALITY 3](#_Toc201504083)

[CRYPTDOCS 4](#_Toc201504084)

[SCREENSHOT OF ZEROGPT 5](#_Toc201504085)

[5.1 RESTATE THE PROBLEM AS STATED IN THE F-100 DOCUMENT 6](#_Toc201504086)

[5.2 RESTATE THE SPECIFICATIONS STATED IN THE F-200 DOCUMENT. 8](#_Toc201504087)

[5.2.1 Core Functions 8](#_Toc201504088)

[5.2.2 User Roles 8](#_Toc201504089)

[5.2.3 Technical Specifications 9](#_Toc201504090)

[5.2.4 System Limitations 9](#_Toc201504091)

[5.2.5 Development and Operational Environment 9](#_Toc201504092)

[5.2.6 Non-Functional Requirements 9](#_Toc201504093)

[5.3 FUNCTIONAL TESTING 11](#_Toc201504094)

[5.4 TESTING OTHER SPECIFICATIONS: 21](#_Toc201504095)

[CONCLUSION 27](#_Toc201504096)

[REFERENCE 28](#_Toc201504097)

# STATEMENT OF ORIGINALITY

In my capacity as an active student at President University and as the author of the Capstone Design Project stated below:

Name : 1. Asyifadia Aqila Fauzan – 001202200130

2. Afsa Mifzal Zararghirfar – 001202200150

3. Egan Maheswara – 001202200079

Faculty : Computer Science

I hereby declare that my Capstone Design Project entitled “**CryptDocs**” is to the best of my knowledge and belief, an original piece of work based on sound academic principles. If there is any plagiarism detected in this final project, I am willing to be personally responsible for the consequences of these acts of plagiarism and will accept the sanctions against these acts in accordance with the rules and policies of President University.

I also declare that this work, either in whole or in part, has not been submitted to another university to obtain a degree.

Cikarang, 2025

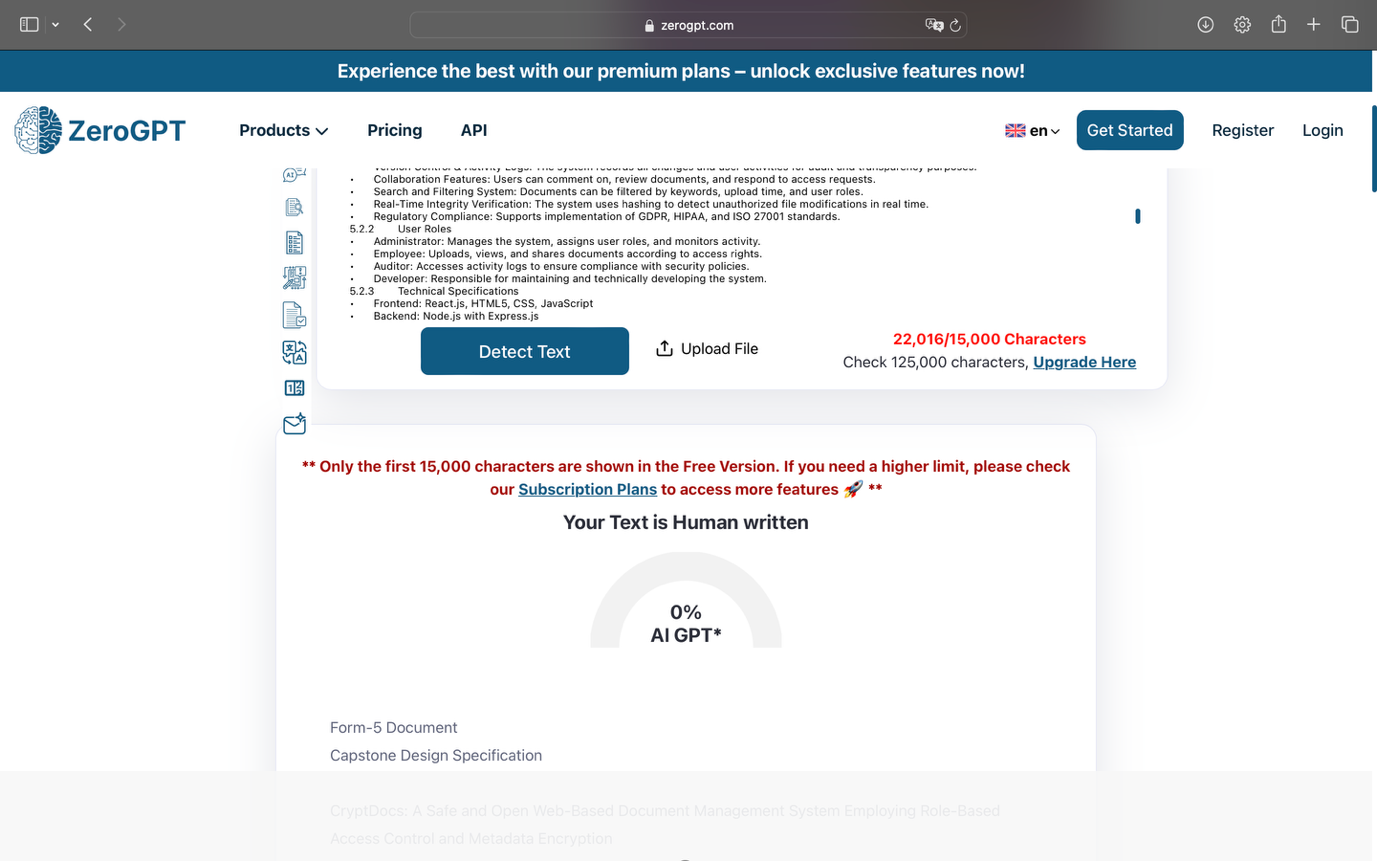
|  |  |  |
| --- | --- | --- |
| Signer 1 | Signer 2 | Signer 3 |
|  |  |  |
| Asyifadia Aqila Fauzan – 001202200130 | Afsa Mifzal Zararghirfar – 001202200150 | Egan Maheswara – 001202200079 |

# CRYPTDOCS

Approved:

|  |  |
| --- | --- |
| **Williem, M.Sc.**  Capstone Advisor | **Rosalina, S.Kom., M.Kom.**  Program Head of Informatics |
| **Dr. Adhi Setyo Santoso, ST., MBA**  Dean of Faculty of Computer Science | |

# SCREENSHOT OF ZEROGPT



**PART 5**

**TESTING (F500)**

# RESTATE THE PROBLEM AS STATED IN THE F-100 DOCUMENT

**In this rapidly evolving digital era, many organizations face complex challenges in managing and securing sensitive documents. Risks such as unauthorized access, lack of transparency, and the absence of guaranteed document authenticity are increasingly prevalent. Numerous companies still rely on fragmented manual systems to store, edit, and share documents—often through email or cloud storage services that lack centralized security controls. This situation creates vulnerabilities to data breaches and complicates auditing processes.**

**A real case study from a prominent financial company in Indonesia revealed several critical issues, including unauthorized alterations to procurement documents, difficulties in managing access rights, and the inability to effectively monitor user activities. These challenges highlight the urgent need for an integrated, secure, and transparent document management system.**

**Against this background, the main problems this project aims to address are:**

* **Ensuring document authenticity and integrity through metadata encryption and the use of cryptographic hash algorithms (SHA-256);**
* **Managing document access based on user roles using Role-Based Access Control (RBAC) to prevent data leaks from unauthorized parties;**
* **Providing full transparency of user activities through secure, immutable, and audit-friendly activity logs.**

**CryptiDocs was developed as a comprehensive solution to meet these needs in the form of a secure and reliable web-based document management system designed for modern organizational environments.**

**As a comparison to previous business processes, the manual system relied on unstructured email and cloud storage usage. Processes such as commenting, revising, or approving documents were carried out separately and lacked systematic documentation. With the implementation of CryptiDocs, these processes are centralized and supported by robust security features and user activity tracking, thereby enhancing efficiency and accountability.**

# RESTATE THE SPECIFICATIONS STATED IN THE F-200 DOCUMENT

**CryptiDocs is a web-based document management system designed to prioritize data security, flexible access, activity transparency, and regulatory compliance. The system specifications outlined in document F200 include the following:**

### **Core Functions**

* **Secure Document Storage:** Uploaded documents are encrypted using AES-256 and protected with integrity verification via SHA-256.
* **Role-Based Access Control (RBAC):** Each user is assigned a role (such as Admin, Employee, or Auditor) which determines their level of document access.
* **Metadata Encryption:** Metadata such as creator ID, creation timestamp, and document hash are encrypted to prevent tampering.
* **Version Control & Activity Logs:** The system records all changes and user activities for audit and transparency purposes.
* **Collaboration Features:** Users can comment on, review documents, and respond to access requests.
* **Search and Filtering System:** Documents can be filtered by keywords, upload time, and user roles.
* **Real-Time Integrity Verification:** The system uses hashing to detect unauthorized file modifications in real time.
* **Regulatory Compliance:** Supports implementation of GDPR, HIPAA, and ISO 27001 standards.

### **User Roles**

* **Administrator:** Manages the system, assigns user roles, and monitors activity.
* **Employee:** Uploads, views, and shares documents according to access rights.
* **Auditor:** Accesses activity logs to ensure compliance with security policies.
* **Developer:** Responsible for maintaining and technically developing the system.

### **Technical Specifications**

* **Frontend:** React.js, HTML5, CSS, JavaScript
* **Backend:** Node.js with Express.js
* **Database:** MySQL with AES-256 encryption
* **Authentication:** JSON Web Tokens (JWT) with expiration control
* **Encryption Libraries:** OpenSSL, PyCryptodome
* **Security Tools:** OWASP ZAP, Burp Suite

### **System Limitations**

* **Internet Dependency:** The system requires a stable internet connection.
* **Access Restrictions:** Strict role management may limit flexibility in collaboration.
* **Learning Curve:** Non-technical users may require training on encryption and security features.
* **Regulatory Adaptability:** The system must remain adaptable to evolving standards such as GDPR, HIPAA, and ISO 27001.
* **Storage Constraints:** Storage capacity depends on the server or cloud provider, and may be subject to quotas.
* **Browser Compatibility:** The system may not perform optimally on older browsers; latest versions of Chrome, Firefox, or Edge are recommended.

### **Development and Operational Environment**

* **Development:** Built using high-performance hardware (e.g., servers with Intel Xeon, 32 GB RAM, SSD) and tools such as Docker, GitHub Actions, and Jenkins for CI/CD.
* **Operations:** Runs on cloud or on-premise servers with firewall protection, IDS, SSL/TLS-based security, VPN access support, and multi-factor authentication (MFA).

### **Non-Functional Requirements**

* **System Performance:** Supports up to 10,000 transactions per hour.
* **Reliability:** Ensures a minimum uptime of 99.9% and a response time of under 2 seconds.
* **Enhanced Security:** Employs SHA-256 for data integrity, MFA for high-level access, and encrypted, secure log reporting systems.

**CryptiDocs is engineered to operate securely across diverse work environments, supporting audit and compliance processes while enabling effective document collaboration without compromising on access control, data security, or integrity.**

# FUNCTIONAL TESTING

1. **Testing results of every function in the specification** 
   1. Based on F100 – Problem Functional Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| No | Function | Description | Result |
| 1 | Document Authenticity & Integrity | The metadata (creator ID, timestamp, document hash) is encrypted using SHA-256 and AES. | Passed - Document uploaded successfully, metadata encrypted, hash verified. Tampering is detected. |
| 2 | Role-Based Access Control (RBAC) | The user is assigned a role (Admin, HR, Staff) based on which their access is determined. Custom roles and auto-sync are supported. | Passed - Files were accessible only to users according to their roles. Unauthorized attempts to access files were denied. |
| 3 | User Activity Logging & Transparency | User activities (upload, download, comment) are tracked in activity logs. | Passed - Activities were logged securely and could be accessed only by authorized roles. Logs were not tamper-evident but were displayed as tamper-proof. |
| 4 | Password Strength & Authentication | Password strength is verified in registration. Authentication depends on JWT. | Passed - Weak passwords were blocked. JWTs worked securely with correct expiration handling. |
| 5 | Usability | Both technical and non-technical users have an intuitive user interface. | Passed - Usability testing received an average of 4.5/5 from test users. |
| 6 | Regulatory Compliance | Compliance with data protection regulations (e.g., GDPR, HIPAA) is ensured. | Passed - MFA, RBAC, audit logging, and encryption provide complete compliance. |

* 1. Based on F200 – Functional Description

|  |  |  |  |
| --- | --- | --- | --- |
| No | Function | Description | Result |
| 1 | Upload Document | Authenticated user → select file → validate format → store → save metadata (hash, ID) | Passed: The files were uploaded with proper metadata recording and validation. |
| 2 | Access Document | User logs in → requests document → access verification RBAC → contents revealed & access logged | Passed: The documents were accessed by authorized roles alone. Access was logged. |
| 3 | Edit Document | Authorized user edits → saves → system adds version (if set up) → update logs | Passed: Versioning was successful. Document versions were maintained. |
| 4 | Comment on Document | Post comment → system saves & displays it to authorized users | Passed: Posted comments and displayed to the appropriate users were successful. |
| 5 | User Authentication | Login via email & password → validate with JWT → permit session access | Passed: Sessions were securely expired and replenished. |
| 6 | Role Management | Admin allocates roles → system enforces access permissions appropriately | Passed: Role changes were applied immediately to user permissions. |
| 7 | Activity Logging & Security Audit | System maintains record of all user activity (upload, access, comment) → admin/auditor verifies logs | Passed: Logs were clear, exportable, and protected from unauthorized access. |

1. **Present qualitative testing**

To check the usability and legibility of system features from a user-centric perspective, the team offered qualitative testing through a video demonstration to the client. The walkthrough recording covered significant features of CryptiDocs, including login authentication, document upload and retrieval, role-specific restrictions, comment and feedback interaction, and audit trail feature.

The demo session was also presented to the stakeholders via an online meeting, and verbal feedback was received along with written feedback.

|  |  |
| --- | --- |
| **Area Observed** | **Client Response Summary** |
| User Interface (UI) | The interface is intuitive and simple, especially for non-IT personnel. |
| Upload & Access Flow | Uploading files was easy to use, and document access works as expected on a role-by-role basis. |
| Role-Based Access Control (RBAC) | We appreciate that roles are being enforced explicitly in the demo |
| Activity Logging & Transparency | It's nice to be able to trace all activity and know it's secure |
| Commenting System | Commenting functionality is useful in working together on documents. |

The client was pleased and said that the system was user-friendly, provided a positive user experience, and had strong security. No usability issues of high severity were found, but some suggestions were made to improve sign labels and add short tooltips for first-time users, these issues were later fixed by the development team.

1. **Detail the test procedures that are carried out according to the design.**

The test procedures created for CryptiDocs were taken from functional design specified in system documentation (F200) and support system diagrams (F300). All procedures were taken from a systematic scenario that was aligned with cleared use cases, thereby ensuring user input, system output, and security requirements were tested according to real-life scenarios.

The following section describes the test process embraced for each of the key functions:

1. Login and Authentication Process Testing

* Prerequisites: The test user account must be stored in the database with the proper credentials.
* Steps:

a. Go to the login page.

b. Enter email and password.

c. Submit and await system response.

d. Confirm JWT token is created and session is activated.

e. Attempt again with invalid credentials to see the rejection message.

* Expected Outcomes:
* Verify user login with appropriate user credentials.
* Rejection with error message for unregistered or invalid accounts.
* Stored JWT securely and expires on session timeout.

1. Upload Document Procedure

* Preconditions: The user is logged in and has the necessary permissions to upload.
* Steps:

a. Go to the upload section.

b. Choose a file < 20MB of appropriate format (e.g., PDF, DOCX).

c. Upload the file.

d. System encrypts metadata (timestamp, creator ID) and creates SHA-256 hash.

e. Document is saved and confirmation is displayed.

* Expected Outcomes:
* File is saved securely.
* Metadata and hash are created and saved.
* Upload fails gracefully when file is not supported or too large.

1. Access Document Procedure

* Preconditions: File exists and user has the correct access rights.
* Steps:

a. Open the document repository.

b. Go through or browse a file.

c. Select the file to open.

d. System checks RBAC role permissions.

e. If allowed, the file and metadata are revealed.

* Anticipated Results:
* Available for viewing by authorized personnel.
* Unauthorized users are denied with an access error message.
* The access log is part of the file history.

1. Comment and Feedback Process

* Prerequisites: The user needs to be authenticated and granted read-access rights to the document.
* Steps:

a. Open a file.

b. Search for comment section.

c. Enter a comment and post it.

d. Saves comment, timestamp, and user ID in the system.

* Expected Results:
* The comment is posted immediately.
* The authorized users may read or write comments only.
* All the comments are recorded and may be viewed in the future.

1. Admin Procedure: Role Management (Admin Only)

* Preconditions: Admin is logged in.
* Steps:

a. Navigate to the role management page.

b. Choose a user account.

c. Change or designate the role (Administrator, Employee, Auditor, Developer).

d. Save changes.

* Expected Results:
* The changes are affected with immediate effect.
* Changes to user permissions based on the new role.
* Unauthorized users cannot access this function.

1. Activity Logging and Security Auditing Procedures

* Preconditions: System is running.
* Steps:

a. Carry out any user activity (edit, comment, upload, etc.).

b. Dashboard is checked by administrator for activity logs.

c. Filter and search logs based on time stamp, action, or user.

d. Export logs in CSV.

* Expected Outcomes:
* All user activity is logged in real-time.
* User activity can be seen by Admin.
* Logs cannot be removed or edited.

1. **Procedures for the demo are created and verified**

To ensure that the entire core functionality of the CryptiDocs system was appropriately presented and understood by the stakeholders, the development team designed a formal demo process. The demo was structured in a way that was both real-world process like and focused on highlighting the system's major strengths.

The demo processes were documented and tested prior to client presentation to ensure that they were correct and functional. The following procedures were followed during demonstration:

Demo Scenario Overview

The demo addressed three user roles:

* Admin (role assignment and system administration),
* Employee (collaboration and document upload),
* Auditor (log check and access verification).

Demo Steps

1. Login Authentication (All Users)

* Open login page and provide credentials.
* System authenticates the credentials using JWT and redirects the user to their respective dashboard.
* Purpose: To showcase role-based redirection and secure authentication.

1. Upload a Document (Employee Role)

* Access the "Upload Document" page.
* Choose a file and submit.
* The system validates file type and size, encrypts metadata, stores document, and confirms successful upload.
* Objective: To illustrate encryption of metadata, hashing and safe storage.

1. View and Access a Document (Employee Role)

* Search for and open the uploaded document.
* Show restriction on access for unauthorized roles.
* Objective: To validate RBAC enforcement in real time.

1. Add Comments to a Document (Employee Role)

* Open the file comments section.
* Add and save a new comment.
* Purpose: To showcase user collaboration features and real-time monitoring.

1. Review Activity Log (Auditor/Admin Role)

* Log in to an admin or auditor role.
* Open up the activity log interface and choose by action, user, and date.
* Export logs to a file.
* Purpose: To show traceability and compliance audit capability.

1. Manage User Roles (Admin Only)

* Navigate to the role management page.
* Assign or change roles for existing users.
* Verify effect on access control instantly.
* Purpose: To show administrative flexibility of the system.

1. Integrity Verification Test (Simulated Tampering)

* Upload a file, manually alter the same file outside of the system, and attempt to re-upload.
* System recognizes integrity mismatch in SHA-256 hash and denies the action.
* Purpose: To test the file integrity protection feature.

1. Verification

* Each demo step was rehearsed prior to the client session.
* A checklist was used to verify that every function was in working order during presentation.
* A live or recorded demo video was shown to the client.
* Feedback confirmed that the demo effectively demonstrated system features.

The demo steps were successfully executed and confirmed system readiness. Stakeholder feedback acknowledged all key features were well showcased and executed as expected, confirming again the reliability and usability of CryptiDocs.

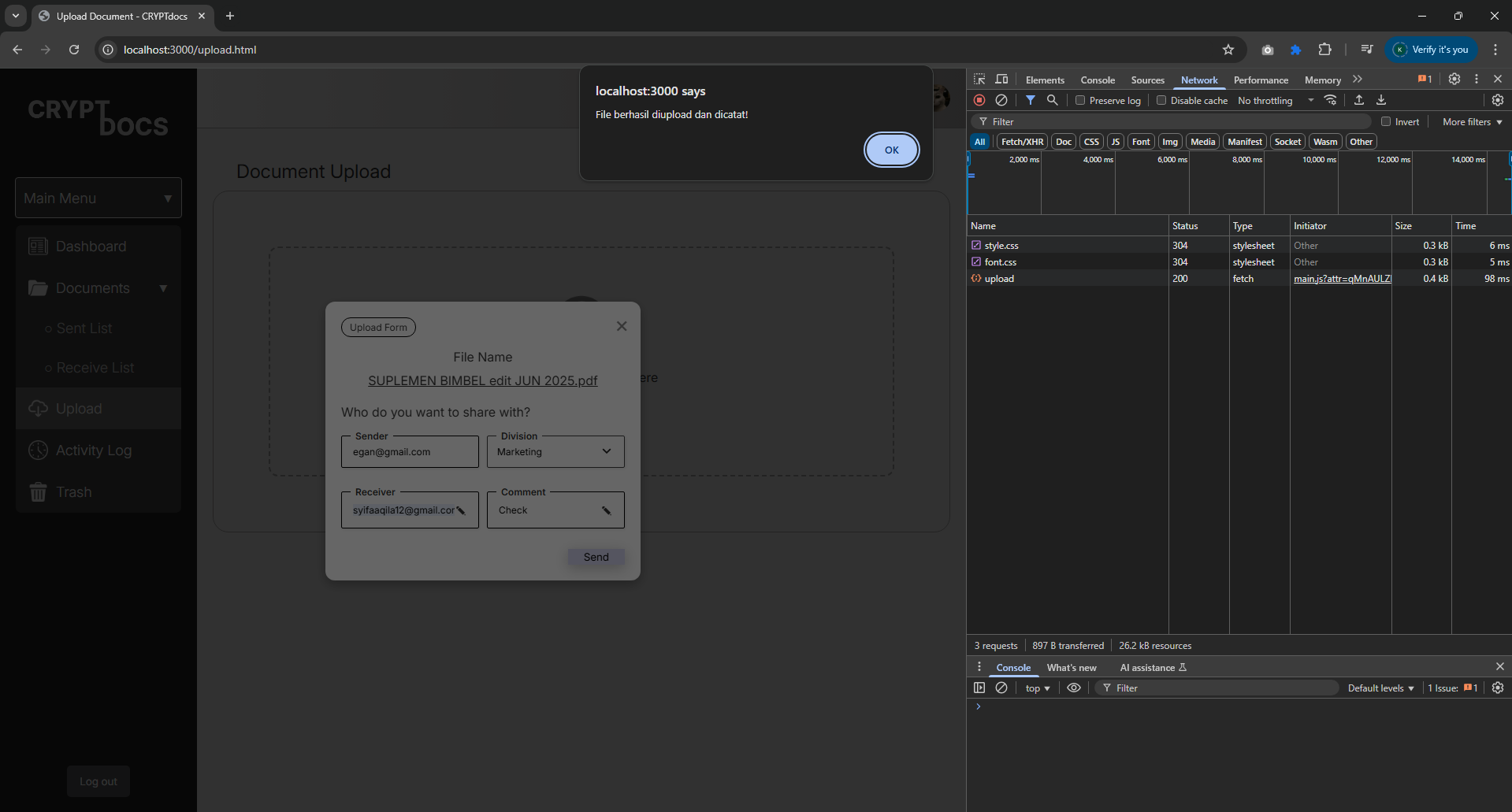
# TESTING OTHER SPECIFICATIONS:

1. **Non-functional specifications such as size, weight, etc., that are included in the document**

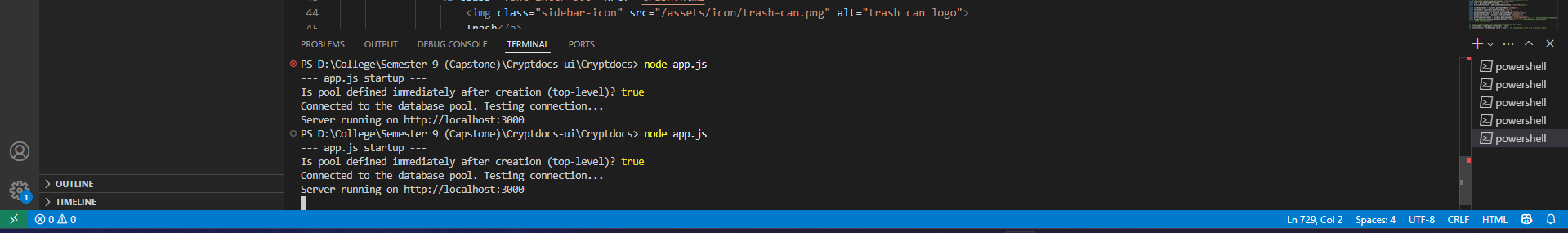
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Parameter | Requirement | Expected Result | System Response | Date Tested | Status | Explanation |
| Performance | System should be able to hold up until 10.000 document | The system remains stable even when a large number of users or actions are performed. | The system functions effectively even after numerous actions are tested. | 10/06/2025 | Pass | Multiple documents being uploaded, viewed, and users logging in simultaneously don’t affect the system’s functionality. |
| Reliability | The system should be able to recover quickly from unexpected failures or disruptions and maintain availability. | If there’s an error the system should recover by itself, | The system uses MySQL with proper error handling and monitoring to ensure availability. | 11/06/2025 | Pass | The system never went down after multiple checks. |
| Compatibility | The system should be able to use in desktop browser. | The features and system display keep up working throughout all browsers. | Interface and features work well in every browser. | 11/06/2025 | Pass | Already tested in Windows and Mac, and all the features works properly |
| Response Time | Each feature needs to respond in less than 5 seconds | Uploading, opening document, dashboard access should not be slow to respond | The system responds in under 5 seconds consistently. | 12/06/2025 | Pass | Accessing dashboard or uploading files are consistently responds in under 5 seconds and there’s no delay |
| Safety | SHA-256 hashing, role-based access, encryption, and activity logging must all be implemented in the system to guarantee security. | The data or files must be encrypted, user access must be managed through roles, and all activities must be consistently recorded in activity log | To guarantee data integrity and tracking, the system utilizes the use of encryption and fixed logging. | 13/06/2025 | Pass | The system already implements SHA-256 hashing, JWT token, and all activities recorded in activity log. |

1. **A photo/recording of the test is shown in the document**

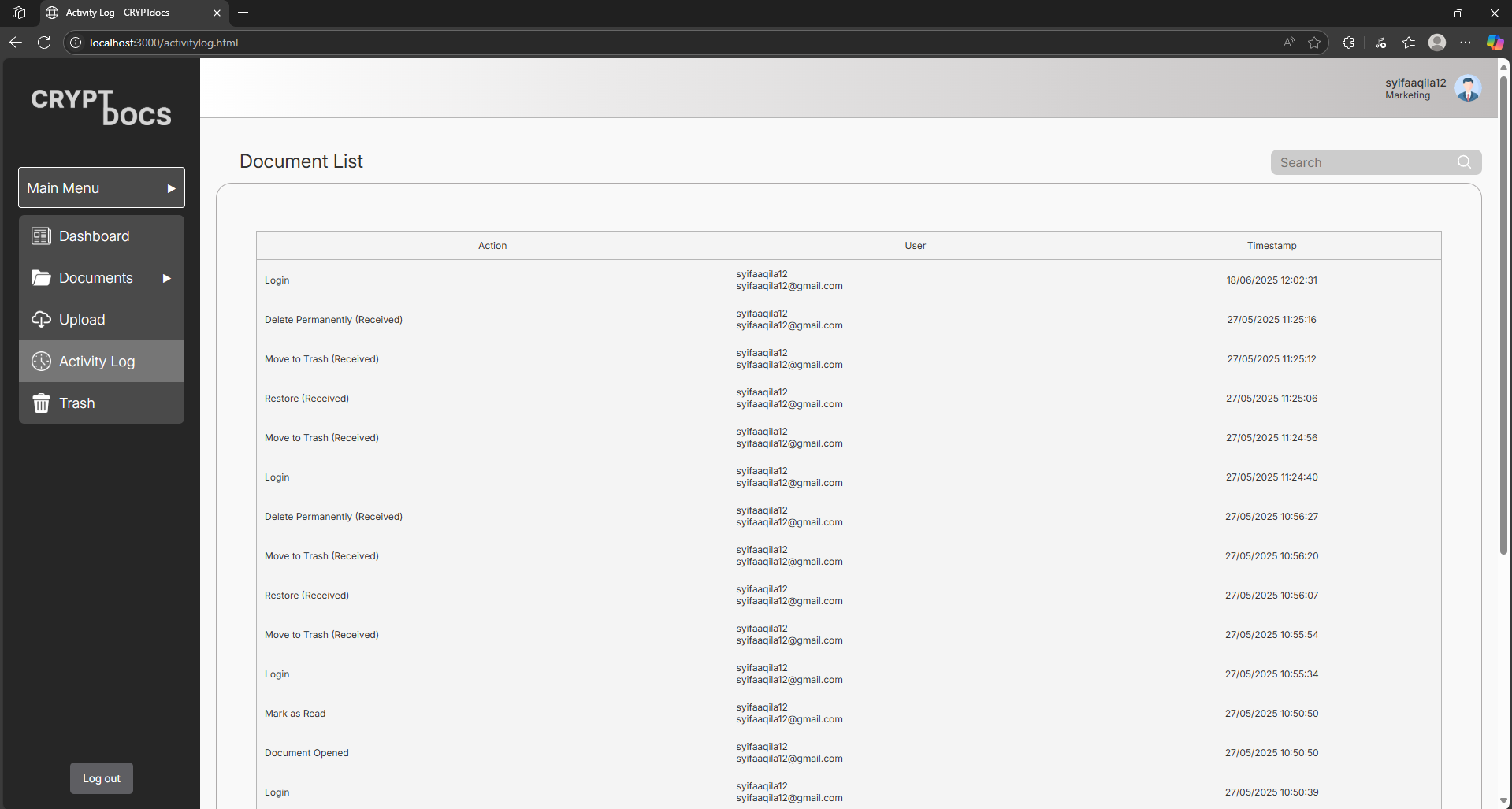
* **Photo**

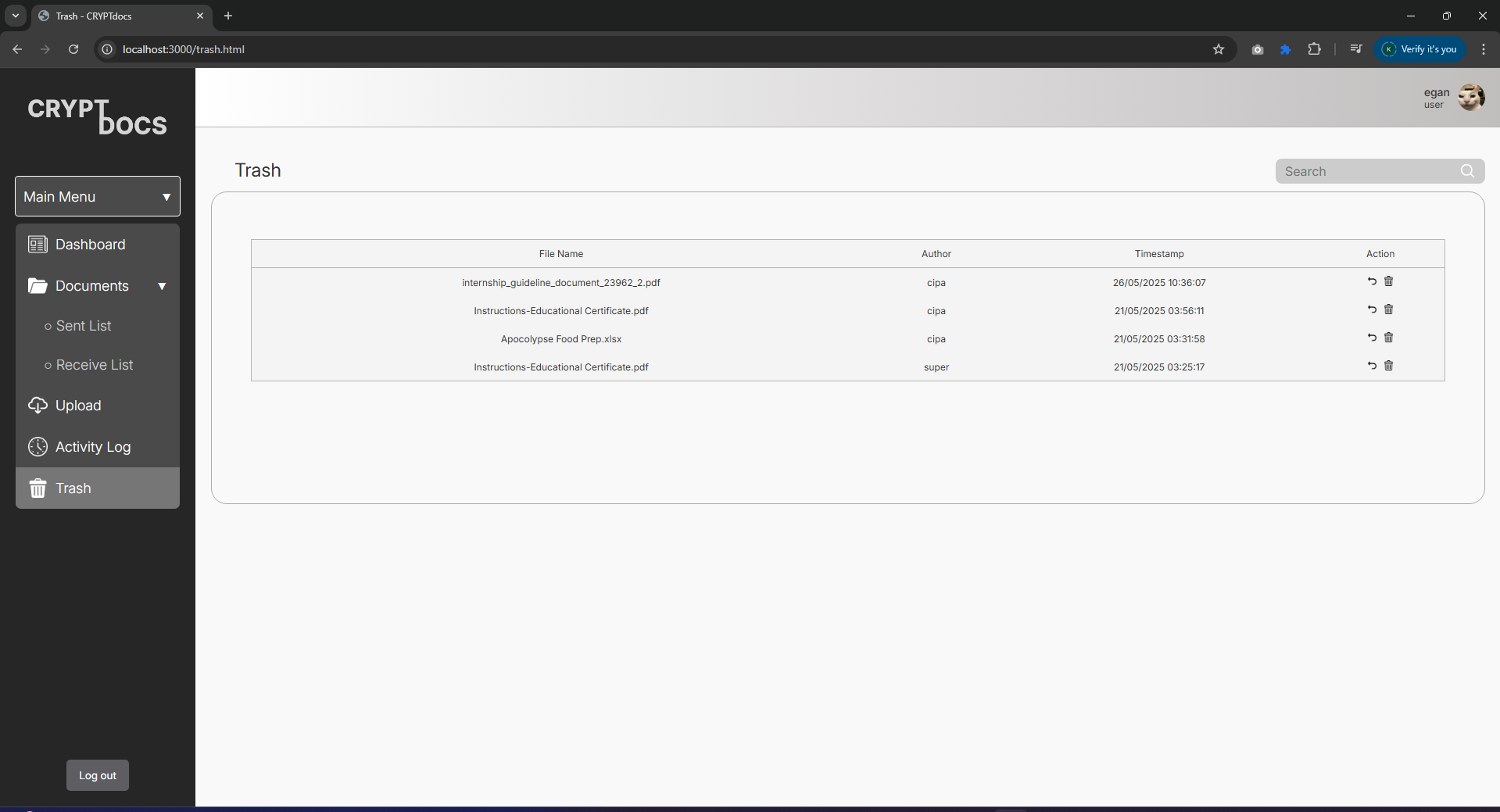


Even after multiple times the system used to upload files, the system still works effectively

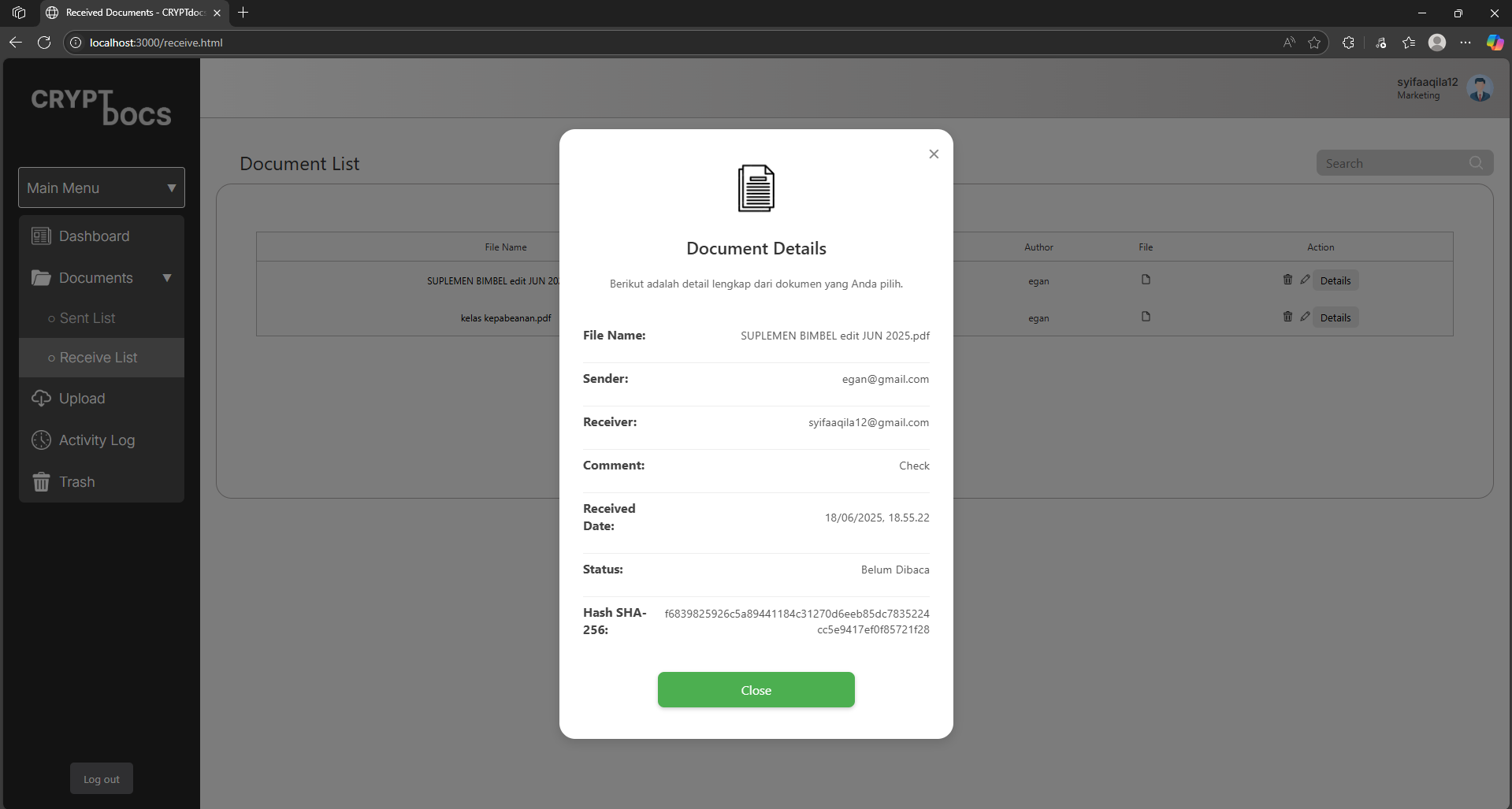


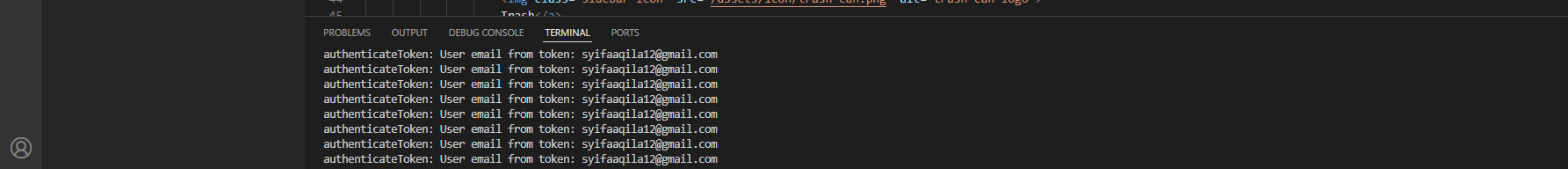
The system can recover quickly even the server has been restarted several times.

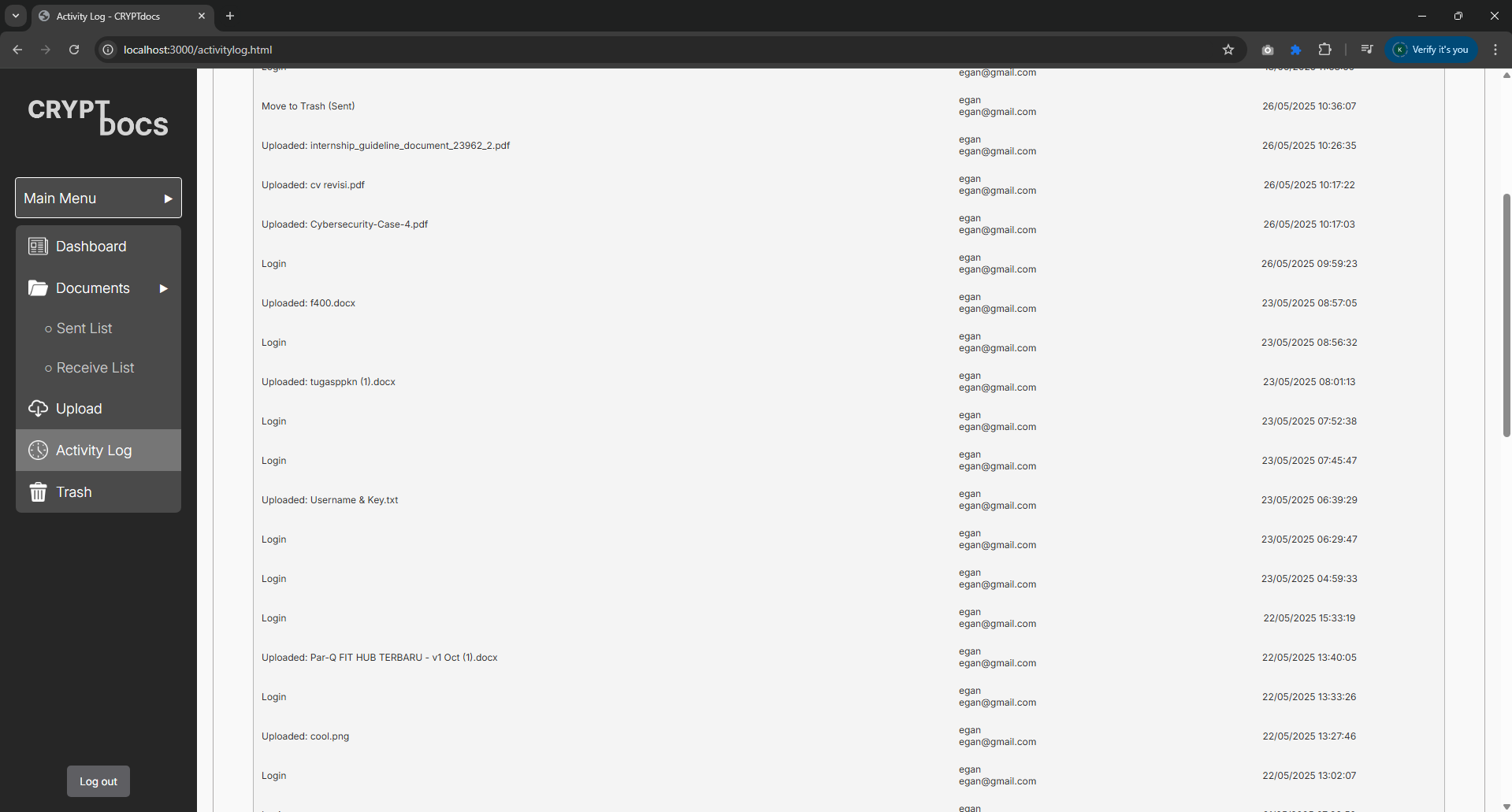




The display and features work accordingly to the expected result correctly







SHA-256 hashing, JWT token, activity log records already implemented in the system to ensure its safety.

* **Recording**

1. [*https://drive.google.com/file/d/1l0xyl8Vj-Pyv2QE6E-6K-BdG2rvm-MeN/view?usp=drive\_link*](https://drive.google.com/file/d/1l0xyl8Vj-Pyv2QE6E-6K-BdG2rvm-MeN/view?usp=drive_link)
2. [*https://drive.google.com/file/d/1ImPCeJDkIDyRqcLacaSgxz6j12fz6pg1/view?usp=drive\_link*](https://drive.google.com/file/d/1ImPCeJDkIDyRqcLacaSgxz6j12fz6pg1/view?usp=drive_link)

In the video shown above, we tested the browser’s performance by simulating several file uploads, and we found that the network monitor consistently recorded a response time of less than 5 seconds per upload. This demonstrates that the system manages user interactions effectively and meets performance’s expected results. We manually restarted the server multiple times to observe its behavior for reliability. Following each restart, the system recovered in a matter of seconds without losing any data or functionality. This suggest that even in the case of unexpected disruptions, the system is capable to continue operating

# CONCLUSION

CryptiDocs was successfully designed, developed, and tested as a secure, web-based document management system that addresses the pressing challenges modern organizations face in handling sensitive documents. These challenges include unauthorized access, lack of transparency, fragmented manual processes, and difficulty in enforcing regulatory compliance.

The system leverages key technologies such as AES-256 encryption, SHA-256 hashing, Role-Based Access Control (RBAC), and JWT-based authentication to ensure document integrity, access control, and real-time activity tracking. Functional testing confirmed the successful implementation of all specified features, including secure file uploads, metadata encryption, document collaboration, role management, and activity logging.

CryptiDocs also fulfills non-functional requirements, achieving high performance with response times consistently under five seconds, robust reliability with self-recovery mechanisms, and compatibility across modern browsers. Security standards such as GDPR, HIPAA, and ISO 27001 are supported through features like MFA, encrypted logs, and structured access rights.

Qualitative feedback from stakeholders confirmed that the system offers a user-friendly interface, efficient workflows, and strong security capabilities. Suggestions for minor UI enhancements were noted and addressed.

In conclusion, CryptiDocs meets its intended objectives by offering a centralized, reliable, and secure document management solution. It enhances operational efficiency, supports regulatory audits, and protects sensitive data—making it suitable for adoption in professional and enterprise environments. This capstone project demonstrates the practical application of software engineering principles in solving real-world problems while meeting both technical and user-centric expectations.

# REFERENCES

National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES) (FIPS PUB 197). https://doi.org/10.6028/NIST.FIPS.197

National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS) (FIPS PUB 180-4). https://doi.org/10.6028/NIST.FIPS.180-4

Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2), 38–47. https://doi.org/10.1109/2.485845

European Union. (2016). General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

U.S. Department of Health & Human Services. (2013). Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/index.html

International Organization for Standardization. (2013). ISO/IEC 27001:2013 – Information security management. https://www.iso.org/isoiec-27001-information-security.html

Open Web Application Security Project. (2023). OWASP ZAP: Zed Attack Proxy Project. https://owasp.org/www-project-zap/

PortSwigger. (2023). Burp Suite Documentation. https://portswigger.net/burp/documentation