Reverse Engineering Laboratory Information Management Systems (LIMS) for Enhanced Security

Laasya Vajjala, Surya Pramod Vadapalli

10/26/2024

A Capstone Project Proposal
Master of Science in Computer Science
Washington State University

Vision and Project Goals

Laboratory Information Management Systems (LIMS) are integral to research environments, managing crucial data and workflows. However, these systems are vulnerable to cyberattacks that could compromise sensitive research data. This project aims to **reverse-engineer a LIMS platform**, identify security vulnerabilities, and implement robust measures such as **multi-factor authentication (MFA)**, **encrypted data storage**, and **secure database access** to safeguard against unauthorized access and data manipulation.

The goals of this project are to:

- Reverse-engineer a LIMS platform to identify vulnerabilities.
- Implement security measures like MFA, encrypted storage, and secure database access.
- Validate the effectiveness of these solutions through security testing.

Positioning of the Project

Security in LIMS platforms has often been overlooked in favor of functionality, despite the significant risks posed by inadequate security protocols. Common vulnerabilities include weak authentication mechanisms and insecure database access. Previous research has focused on the functionality of LIMS platforms, but this project will expand that work by emphasizing the importance of securing these systems.

Through reverse engineering, the project will uncover vulnerabilities and propose security solutions that could be applicable across various LIMS platforms, contributing to the broader field of **cybersecurity in scientific data management**.

Scope and Requirements

The scope of the project includes the following key steps:

- **Step 1**: Research and selection of a LIMS platform.
- **Step 2**: Reverse engineering of the selected LIMS platform to analyze its architecture and identify security gaps.
- **Step 3**: Implementation of security measures such as MFA, encryption, and secure database protocols.
- **Step 4**: Validation of security measures through testing and simulated attacks.

Functional Requirements:

- Implement MFA for better authentication.
- Encrypt sensitive research data both at rest and in transit.
- Secure database access to prevent unauthorized data retrieval.

Process

The project will be executed using an agile development process, with regular updates to the project group. Each sprint will last one week, during which specific milestones will be achieved and presented for feedback.

Project Plan

The following is the planned schedule to finish all the milestones:

Week	**Milestone**	**Person Responsible**
Week 1	Research and selection of LIMS platform	Laasya Vajjala
Week 1	Research on common vulnerabilities in LIMS	Surya Pramod Vadapalli
Week 2	Reverse engineering of the LIMS platform	Laasya Vajjala
Week 2	Vulnerability identification	Surya Pramod Vadapalli
Week 3	Implement multi-factor authentication (MFA)	Laasya Vajjala
Week 3	Secure database access and encryption	Surya Pramod Vadapalli
Week 4	Testing and penetration simulations	Laasya Vajjala
Week 4	Documentation and final report	Surya Pramod Vadapalli

Evaluation Criteria

The success of this project will be measured by:

- Identifying vulnerabilities within the LIMS platform.
- Successfully implementing security solutions (MFA, encryption, secure database access).
- Demonstrating the effectiveness of these solutions through tests that simulate common cyberattacks.

Current Progress

Currently, the team has researched potential LIMS platforms for reverse engineering and conducted an initial assessment of common vulnerabilities, particularly in weak authentication and database security. The next step will be finalizing the platform selection and starting the reverse-engineering process.

Delta Over Existing Knowledge

This project will contribute to the field by identifying **previously unknown vulnerabilities** in LIMS platforms and providing **tangible security solutions**. The success of this project will lead to better-secured systems for managing sensitive research data, setting a precedent for enhanced cybersecurity in laboratory management software.

Expected Outcome and Timeline

By the end of Week 4, we will present a prototype demonstrating the security improvements applied to the LIMS platform. The documentation will compare the state of the system before and after implementing the security enhancements, with clear evidence of reduced vulnerability.

Backup Plan: If the project faces unexpected challenges (e.g., issues with reverse engineering or implementation), a backup plan will focus on producing theoretical analyses and recommendations for securing LIMS platforms.

Applications in Broader Contexts

The security measures developed in this project can be applied to other **data management systems** in sensitive fields like **healthcare, pharmaceuticals, and academic research**, where the protection of sensitive data is crucial. This project can also inform **cybersecurity standards** for laboratory software and other systems that handle critical research data.

Individual Tasks and Contributions

Each team member is expected to contribute at least **5 hours of quality work per week**.

Task	**Person Responsible**	**Hours Contributed**	**Duration**
Research LIMS platforms	Laasya Vajjala	5 hours	Week 1
Research common vulnerabilities	Surya Pramod Vadapalli	5 hours	Week 1
Reverse engineering	Laasya Vajjala	5 hours	Week 2
Vulnerability analysis	Surya Pramod Vadapalli	5 hours	Week 2
Implement MFA	Laasya Vajjala	5 hours	Week 3
Secure database and encryption	Surya Pramod Vadapalli	5 hours	Week 3
Testing and penetration simulations	Laasya Vajjala	5 hours	Week 4
Documentation and final report	Surya Pramod Vadapalli	5 hours	Week 4

References

- Singh, A. K., & Saxena, R. (2019). "Cybersecurity in Laboratory Information Management Systems: Vulnerabilities and Defenses." *Journal of Information Security*, 10(4), 321-335.

- Turner, B., & Bailey, J. (2021). "Securing Digital Health: Encryption and Authentication Solutions in Health IT." *International Journal of Medical Informatics*, 144, 104298.

- Zhao, Y., et al. (2020). "Reverse Engineering for Security Analysis of Web-Based LIMS Systems." *IEEE Access*, 8, 23012-23022.

- Parker, M., & Lee, W. (2021). "Multi-Factor Authentication: A Review of Implementations in Secure Systems." *IEEE Security and Privacy*, 19(2), 34-42.

- Caldwell, T. (2022). "Database Security in LIMS: Challenges and Solutions." *Cybersecurity Journal*, 11(3), 48-59.

- Hart, K., & Mills, D. (2020). "Data Encryption: Best Practices for Securing Research Data." *Journal of Data Security*, 9(5), 102-115.

Reverse Engineering Laboratory Information Management Systems (LIMS)

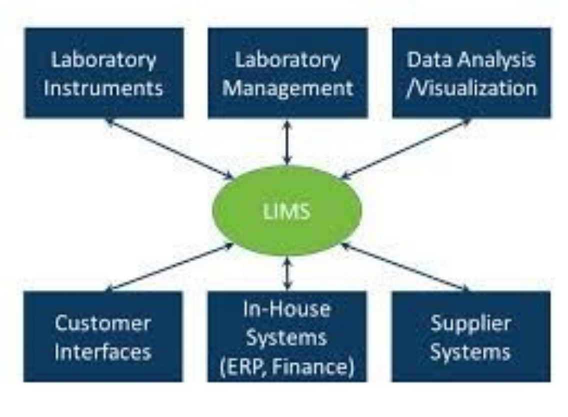
•••

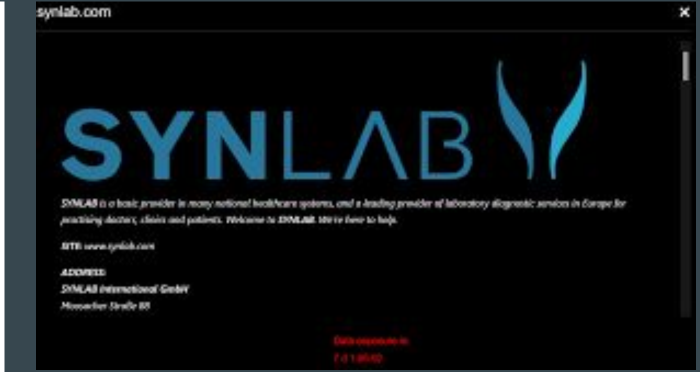
by Laasya Vajjala & Surya Pramod Vadapalli

Master of Science in Computer Science, Washington State University

Context and Background

Laboratory Information Management Systems (LIMS) are vital for managing research data and workflows in scientific environments. However, these systems face significant security challenges, often lacking robust protections against cyber threats. Recognizing the vulnerability of LIMS to unauthorized access and data manipulation, our project focuses on improving the security of these systems to safeguard sensitive research data.




synlab.com

SYNLAB

SYNLAB is a basic provider in many national healthcare systems, and a leading provider of laboratory diagnostic services in Europe for practising doctors, clinics and patients. Welcome to SYNLAB. We're here to help.

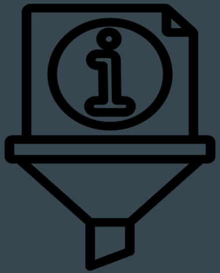
SITE: www.synlab.com

ADDRESS:
SYNLAB International GmbH
Moosacher Straße 88

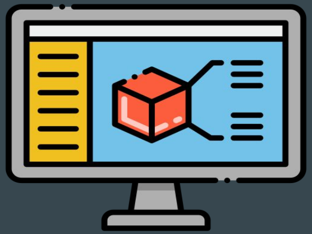
Data exposure in:
[illegible]

Project Goals and Objectives

- Reverse-engineer a LIMS platform to identify specific vulnerabilities.
- Implement advanced security measures, including multi-factor authentication (MFA), encrypted data storage, and secure database access.
- Validate the effectiveness of these measures through rigorous security testing.



Information extraction

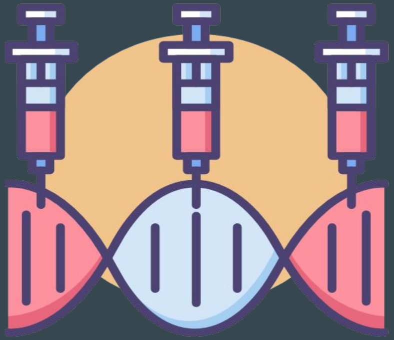


Modeling

Review

Importance of the Project

Security in LIMS has often been deprioritized in favor of functionality, leaving research data at risk. By prioritizing security, our project will protect sensitive information, reduce vulnerability to cyber-attacks, and contribute broadly to the field of cybersecurity within laboratory management software.



Project Approach and Team Roles

We will execute this project using an agile development process, allowing for regular updates and feedback through weekly sprints. Our approach includes:

- **Week 1:** Research and selection of an appropriate LIMS platform (Laasya) and initial analysis of common vulnerabilities (Surya).
- **Week 2:** Reverse-engineering the platform to understand its structure (Laasya) and identify security gaps (Surya).
- **Week 3:** Implementation of critical security measures: MFA (Laasya) and database access and encryption (Surya).
- **Week 4:** Conduct security testing through simulated cyberattacks, (Laasya) and finalize documentation (Surya).

Expected Outcomes

By project end, we aim to deliver:

- A prototype demonstrating applied security enhancements, showing the LIMS platform’s reduced vulnerability.
- Comprehensive documentation detailing the system's security state pre- and post-implementation, backed by evidence of successful testing and risk reduction.

Thank You
Any questions?