# **Project Status Report**

## **Purpose**

The Project Status Report is a document that Project Managers may use as a means of regular reporting on the status of a project.

|  |  |
| --- | --- |
| Project Name: | StreamList React App |
| Week #: | 4 |
| Prepared By: | Zachary Harrison, Gizelle Samuels, Charles Taggart, Armando Perez |

## **Project Status Table**

|  |  |  |
| --- | --- | --- |
| **Project Team Member** | **Project/Organization Role** | **Contributions this Week** |
| Zachary Harrison, Gizelle Samuels, Charles Taggart, Armando Perez | Project Manager and Designer | Coordinated tasks, enhanced security with PCI DSS compliance, and improved authentication using OAuth |
| Zachary Harrison, Gizelle Samuels, Charles Taggart, Armando Perez | Assistant Project Manager and Designer I | Conducted security assessments using CodeGPT to identify vulnerabilities |
| Zachary Harrison, Gizelle Samuels, Charles Taggart, Armando Perez | Assistant Project Manager and Designer II | Integrated OAuth for authentication and API authorizations |
| Zachary Harrison, Gizelle Samuels, Charles Taggart, Armando Perez | Assistant Project Manager and Designer III | Managed GitHub repository, reviewed security patches, and monitored compliance |

## **1. Project Status Details**

### **1.1. Issues Report**

* **API Setup Challenges:** Initial difficulties in securing API calls with OAuth authentication. Resolved by properly configuring access tokens and permissions.
* **PCI DSS Compliance Implementation:** Ensured that payment handling adheres to PCI DSS standards, requiring encryption and secure storage practices.
* **OAuth Integration:** Encountered issues with token expiration, resolved by implementing automatic refresh mechanisms.
* **Code Security:** Discovered vulnerabilities in the payment processing logic, mitigated with CodeGPT-assisted security reviews.
* **Data Persistence Concerns:** Addressed issues with secure user session storage by utilizing encrypted tokens.

### **1.2. Risk Management Report**

* Implemented PCI DSS best practices to ensure secure handling of payment data.
* Added OAuth-based authentication to prevent unauthorized access to sensitive information.
* Utilized CodeGPT for automated security checks and vulnerability detection in the application code.
* Enhanced fraud detection measures by monitoring payment transactions and API calls.

### **1.3.** **Lessons Learned**

One key takeaway was the necessity of early security planning. Integrating OAuth from the beginning helped streamline authentication and authorization processes. Additionally, using CodeGPT provided real-time insights into potential vulnerabilities, improving overall security and maintainability. Moving forward, we will incorporate automated security testing into our development pipeline to ensure continued compliance with industry standards.

## **2. Milestone Deliverables scheduled for completion of the project**

Table 2

| Checkpoint Deliverables | Due Date | % Completed | Status |
| --- | --- | --- | --- |
| Checkpoint 1 (Week 2: Sections 1 through 14 First Draft) | 2/10/2025 | 100% | Completed |
| Checkpoint 2 (Week 3: Sections 1 through 20 Second Draft) | 2/17/2025 | 100% | Completed |
| Final Project Submission and Presentation (Week 5) | 3/3/2025 | 80% | Pending |

## **3. Project Recommendations**

* Continuing to refine PCI DSS compliance and ensuring adherence to best practices.
* Implementing additional security testing to identify potential vulnerabilities.
* Enhancing OAuth token management to further improve authentication security.
* Automating security reviews with CodeGPT to catch vulnerabilities early in development.

## **4. Project Budget/Financial Status**

|  |  |  |  |
| --- | --- | --- | --- |
| **Budget Item** | **Planned Budget** | **Actual Cost (if applicable)** | **Variance/Explanation** |
| API Subscription | $0 | $0 | N/A |
| Development Tools | $0 | $0 | Free online resources used |

## **5. Project Decision Process**

Decisions were made collaboratively through weekly meetings. Disagreements were resolved by majority vote or by consulting project guidelines. Open communication was emphasized, with each team member encouraged to raise concerns and propose solutions. Security-related decisions were reviewed collectively, with CodeGPT providing insights into potential vulnerabilities.

## **6. Objectives for Next Checkpoint**

1. Finalize PCI DSS compliance and conduct security testing.
2. Complete OAuth implementation and ensure seamless authentication.
3. Automate security reviews with CodeGPT and address flagged vulnerabilities.
4. Prepare the final project demonstration video.
5. Submit GitHub repository for final review and documentation.

**7.References**

* Payment Card Industry Security Standards Council. (2022). PCI security standards overview. Retrieved from <https://www.pcisecuritystandards.org>
* OAuth 2.0 Authorization Framework. (2023). Internet Engineering Task Force (IETF) RFC 6749. Retrieved from <https://www.ietf.org/rfc/rfc6749.html>
* OpenAI. (2024). Using AI to enhance secure coding practices. Retrieved from <https://openai.com>