Redacted Security Report – Responsible Disclosure

Author: Aathithya Shanmuga Sundaram
Date of Disclosure: 24-03-2025
Affected System: *Student Feedback Platform (Internal Web Application)*

1. Executive Summary

During a structured security review of an internal web-based **Student Feedback Platform**, I identified an input-handling weakness that could allow unauthorized manipulation of feedback submissions.

This issue does **not** expose sensitive data publicly, but it directly affects **data integrity** and the **accuracy of faculty evaluation records**.

The vulnerability was reported privately to the institution following responsible disclosure practices.

2. Nature of the Vulnerability (Redacted)

A flaw in the platform's **input validation and request-handling logic** enabled the following:

- Submission of **tampered or artificially modified feedback data**
- The ability to submit feedback using **incorrect or mismatched student identifiers**
- Manipulation of stored feedback values without authentication checks

Technical details, payloads, and endpoint structures have been intentionally omitted to ensure safe public disclosure.

3. Potential Impact

Integrity Risks

- Faculty performance metrics could be **distorted** due to manipulated feedback entries.
- Duplicate or inconsistent records could be created under existing student identifiers.

Operational Risks

- Manual reviews may be required to correct manipulated entries.
- Trust in academic evaluation workflows could weaken.

Compliance Risks

- Although no PII was directly exposed, improper input validation may create **non-compliance concerns** under institutional data protection policies.

4. How the Issue Was Identified (High-Level Summary)

The vulnerability surfaced during a routine assessment where I evaluated:

- Client-side validation controls
- Server-side request handling
- Data submission patterns
- Response behaviors to malformed input

No exploitation beyond **minimal proof-of-concept testing** was performed.

All tests stayed inside the bounds of ethical, non-destructive verification.

5. Proof-of-Concept (Redacted)

A controlled test demonstrated that:

- The system accepted **unexpected input structures**.
- The backend did not fully verify the legitimacy of the submitted identifiers.

All technical payloads, request formats, and URLs have been removed for public safety.

6. Remediation Recommendations

Technical Controls

- Enforce **server-side validation** for all fields
- Implement **strict identifier verification**
- Add **duplicate record prevention logic**
- Perform **security header hardening**
- Enable **input sanitization & backend filtering**

Process Improvements

- Conduct periodic security audits on academic platforms
- Implement feedback submission rate limits
- Maintain a documented vulnerability reporting pipeline

8. Acknowledgment of Responsible Disclosure

I performed this analysis as an educational exercise with the intention of helping the institution improve system safety and integrity.

Recognizing responsible disclosures:

- Encourages a proactive security culture
- Demonstrates the institution's commitment to cybersecurity
- Strengthens trust among students and faculty
- Reflects positively on the cybersecurity program and its students

9. Author Statement

I remain available to collaborate with the technical team to provide clarification, assist with remediation, or validate the applied fix once implemented.

– Aathithya Shanmuga Sundaram
Responsible Disclosure Contributor