Cybersecurity Incident Response Report

Student Portal Application Security Case Study

An incident report documenting critical injection and broken-access-control findings in a university student portal application (fictional case scenario), their potential impact, and a phased remediation plan.

FERPA | Incident Response | Vulnerability Analysis | Injection | Broken Access Control | Remediation Planning

AT A GLANCE

Scenario	Third-party penetration test of a university student portal application finds two critical vulnerabilities, validated by the internal security team
Findings	Injection vulnerabilities enabling database query manipulation; broken access control enabling privilege escalation and account modification
Exposure	3 application servers, 1 backend database, ~18,000 students, faculty and staff; present for ~6 months
Outcome	Formal incident documentation with impact analysis, information sensitivity classification and a phased 2-week to 6-month remediation plan

Sean Richard

sean@autom8ionlab.com · linkedin.com/in/a8l-sean-richard · +1.352.818.9694

Portfolio edition based on original Full Sail University coursework. The university, application, vendor and roles are a fictional course scenario, not a real institution. Substantive project content is preserved.

01 — INCIDENT SUMMARY

Two critical findings in the student portal application

This report documents the results of a recent security assessment conducted on the University's student portal application. The University contracted a third-party penetration testing firm to perform security testing on the application. During this assessment, the firm identified two critical security vulnerabilities: injection vulnerabilities and broken access control.

These findings were reviewed and validated by the University Security Team and confirmed to be legitimate. The vulnerabilities have existed within the portal application since the last software update approximately six months ago. At this time, there is no confirmed evidence that these vulnerabilities were actively exploited; however, the risks posed by these issues are significant. University security teams are actively working to remediate these vulnerabilities and prevent potential compromise of sensitive information.

REPORT PARTIES

Report date **February 16, 2026**	Report author **Information Security Manager, the University**	Approving executive **Chief Information Security Officer, the University**
Discovering party **Lead Penetration Tester, external testing firm**	Validating party **University Security Team**	Notified **University President · CISO · Information Security Team**

02 — INCIDENT DESCRIPTION

Timeline, scope and affected systems

ATTRIBUTE	DETAIL
Date and time of discovery	February 10, 2026 at 14:15 Eastern Standard Time
Resolution time	Not fully resolved at the time of this report. Temporary mitigation controls have been implemented. Full remediation is expected no later than March 16, 2026.
Physical location of affected systems	Primary university data center
Physical locations affected	One (primary data center only)
Systems affected	Three application servers and one backend database system
Users affected	Approximately 18,000 students, faculty, and staff
Length of time incident has persisted	Approximately six months, since the last portal application update
Discovering party	External penetration testing firm
Validating party	University Security Team

Injection vulnerabilities allowed manipulation of backend database queries, while broken access control enabled unauthorized privilege escalation and modification of other user accounts. There is currently no confirmed evidence of data exfiltration; however, the investigation remains ongoing.

03 — IMPACT

Impact and potential impact

Loss of data / data compromise	Injection attacks and broken access control could allow unauthorized access to student records, grades, and personal identifiable information (PII).
System damage	Exploitation of these vulnerabilities could result in database corruption or extended system outages affecting students and faculty.
Financial loss	Potential financial impact includes remediation costs, compliance penalties, delayed academic operations, and additional staffing expenses.
Public relations impact	As a technology-focused institution offering cybersecurity programs, a breach would negatively impact the institution's reputation and student trust.
Regulation violation	Potential violations of FERPA and institutional privacy policies due to exposure of student academic and personal data.

Information security policy violation	Failure to enforce secure coding standards and access control policies.
Other unknown risks	Undiscovered exploitation or lateral movement to other internal systems.

04 — SENSITIVITY

Sensitivity of information involved

☐ **Public**
General university schedules and publicly available content.

☐ **Internal use only**
Internal communications and non-public system configuration data.

■ **Restricted or confidential — affected**
Student PII, grades, enrollment records, and account data.

■ **Unknown — affected**
Potential access to additional systems or sensitive institutional data not yet identified.

05 — MITIGATION

Phased remediation plan

Injection vulnerabilities

Immediate implementation of input validation and parameterized queries	**2 weeks**
Secure code review of all database interaction points	**1 month**
Deployment of application-level monitoring and intrusion detection	**1 month**
Emergency software patch to address confirmed vulnerabilities	**30–45 days**

Broken access control

Implementation of role-based access control (RBAC)	**2–3 months**
Enforcement of least-privilege access model	**6 months**
Review and removal of inactive or unnecessary accounts	**1 month**
Security testing prior to all future application updates	**Ongoing**