



Cybersecurity Incident Report

EXECUTIVE SUMMARY

A recent security assessment conducted by WeHackApps, LLC identified serious security weaknesses within Full Sail University's Full Sail One (FSO) application. These weaknesses allow unauthorized individuals to access and manipulate sensitive university data, including the ability to alter stored information and gain elevated access to restricted user accounts. Because the affected system contains student and staff records, including academic and personal information, the risk to the university is significant.

If exploited, these vulnerabilities could lead to data exposure, operational disruption, regulatory penalties, and reputational harm. The issues were determined to have existed approximately six months before discovery, increasing the likelihood of potential misuse. Immediate corrective action is required to reduce institutional risk and protect university stakeholders.

CONTACT INFORMATION

Report Data:

February 6, 2026

Report Author

Name: Kayla Hodge

Job Title: Information Security Manager

Phone: 555-555-5555

Chief Information Security Officer

Name: Jack Norman

Phone: 555-555-5544

Organization: Full Sail University

Email: kmhodge@fullsail.edu

Title: Chief Information Security Officer

Email: ciso@fullsail.edu

Stakeholder

Name: Mary Pentessa

Title: Lead Penetration Tester

Company: WeHackApps, LLC

Email: mpentessa@wehackapps.com

INCIDENT DESCRIPTION**Date and Time of Discovery**

February 3, 2026, at 14:45 Eastern Standard Time

Resolution Time

At the time of this report, the security issues have not been fully resolved. The Full Sail University Security Team has established an estimated resolution date of no later than February 28, 2026, at 18:00 Eastern Standard Time. Security teams are actively working to remediate the identified vulnerabilities and reduce ongoing risk.

Physical Location of Affected Systems

Primary data center for Full Sail University

Number of Physical Locations Affected

One physical location was affected. The incident is isolated to the primary data center.

Number of Systems Affected

Four production systems supporting the Full Sail One (FSO) application were identified as affected.

Number of Users Affected

Potential exposure includes approximately 18,500 students and 220 faculty and staff members with active FSO accounts.

Length of Time Incident Has Persisted

The vulnerabilities have been present since the last major update to the Full Sail One (FSO) application, indicating the incident persisted for approximately six months before discovery.

Discovering Party

Penetration testing team contracted from WeHackApps, LLC.

Validating Party

Full Sail University Security Team

Additional Information

At this time, it has not been confirmed whether unauthorized external parties exploited the identified vulnerabilities before they were discovered. This report documents the confirmed existence of security weaknesses identified during the penetration test. Full Sail University Security Teams will continue their investigation to determine whether a data breach occurred and will provide additional updates as more information becomes available.

Impact/Potential Impact

The following outlines the potential impacts to Full Sail University if the identified vulnerabilities are exploited. Each impact describes the associated risk and the specific vulnerabilities that could lead to the outcome.

Loss of Data/Data Compromise:

Injection vulnerabilities could allow unauthorized modification or extraction of student data stored within the FSO application. If privilege escalation is achieved through broken access control, attackers could access restricted records, including academic and personal information. Exploitation of these vulnerabilities could result in unauthorized disclosure or permanent loss of institutional data.

System Damage:

Both injection attacks and broken access control could be used to alter application functionality or disrupt system operations. Successful exploitation may result in partial or complete system outages, preventing students and staff from accessing the FSO platform for academic and administrative purposes.

Financial Loss:

Financial impacts could include costs associated with incident response, forensic investigations, and remediation efforts. Additional losses may result from delayed academic services, increased support staffing, or required system restoration. Regulatory penalties and legal expenses could further increase both operational and capital expenditures.

Public Relations Impact:

Full Sail University is recognized for its focus on technology-driven education. A security incident involving student and staff data could negatively affect the institution's reputation and erode trust among students, faculty, and prospective applicants. This loss of confidence may impact enrollment decisions and the university's ability to attract and retain qualified faculty members.

Regulation Violation:

Full Sail University is subject to compliance requirements related to the protection of sensitive student and staff information. These requirements include, but are not limited to, FERPA, GLBA, GDPR, and applicable privacy regulations. Failure to adequately protect this data could result in regulatory violations, financial penalties, and increased oversight.

Sensitivity of Information Involved

☐ **Public** – This information is intended for unrestricted access and doesn't pose a risk to the university if disclosed.

***Examples of Public Information:** Academic calendars, general university announcements, and publicly available program descriptions.*

☒ **Internal Use Only** – Unauthorized access to this information could disrupt university operations and internal workflows, but doesn't typically include regulated personal data.

***Examples of Internal Use Information:** Internal system notifications, staff-to-student communications, internal scheduling data, and non-public operational information within the FSO application.*

☒ **Restricted or Confidential (Privacy Policy Violation)** – This level includes information that is protected by university privacy policies and applicable regulations. Unauthorized access to this data could result in privacy violations and institutional risk.

***Examples of Restricted or Confidential Information:** Student personally identifiable information (PII), academic records, grades, enrollment information, and staff account details maintained within the FSO application.*

☒ **Unknown** – This category accounts for information whose sensitivity or exposure level can't be determined without additional analysis or testing.

Example of Unknown Information: Information stored in systems or applications connected to the FSO platform that have not yet been fully assessed.

The Full Sail One (FSO) application processes multiple types of information with varying sensitivity levels. Restricted and confidential information represents the highest level of sensitivity due to the nature of the data involved. At this time, some information classifications remain undetermined pending further review of system integrations and data flows.

Mitigation

Injection Vulnerabilities

- Review all application inputs and backend database queries associated with the Full Sail One (FSO) application. (1-2 Months)
- Implement secure coding practices, including input validation and parameterized queries, to prevent unauthorized manipulation of database commands. (2-3 months)
- Restrict database permissions to ensure application accounts operate with the minimum access required. (2-3 weeks)
- Increase logging and monitoring of database activity to detect anomalous behavior during the remediation period. (1 month)
- Develop and deploy a corrective software update addressing injection-related vulnerabilities within **30 days**. (30 days)
- Conduct regression testing and follow-up penetration test to validate that injection vulnerabilities have been successfully remediated. (6-9 months)

Broken Access Control

- Perform a comprehensive review of authentication and authorization logic within the FSO application. (2-4 months)
- Enforce role-based access control (RBAC) to ensure users can only access functions and data appropriate to their assigned role. (3-4 months)
- Validate access controls on the server side to prevent privilege escalation and unauthorized data access. (2 months)
- Review and update existing user roles and permissions to align with the principle of least privilege. (2-3 weeks)
- Disable inactive accounts and remove unnecessary privileges from existing accounts. (2-3 weeks)
- Deploy an updated access control configuration within **30 days**. (30 days)

- Validation testing to confirm vulnerabilities have been successfully remediated. (6-9 months)

Individuals Notified of Incident

The following individuals and groups have been notified of the security vulnerabilities:

Gary Jones, President of Full Sail University

Jack Norman, Chief Information Security Officer

Full Sail Security Team, Full Sail University Information Security Team

Sign-Off

Name (PRINT): _____ Title: _____

Signature: _____ Date: _____