
Example Summary:

A penetration testing firm “WeHackApps, LLC” was hired to perform a penetration test in the Full Sails FSO Platform. During this penetration test, it became known that the FSO platform was vulnerable to broken access and injection attacks. This means that attackers can increase their privileges within the environment and inject malicious code into it. This can result in the attacker gaining additional privileges which can manipulate other user accounts or the attacker can modify our database information. This could take us out of compliance with many regulations which could result in fines. With these vulnerabilities being in the system for six months the remediation of these is extremely important. On top of the remediation of these vulnerabilities ensuring that these vulnerabilities haven’t been taken advantage of by attackers is extremely important. The internal security team will review logs to ensure there hasn’t been a breach.

Date and Contact Information:

Date of the Report:
09/09/2024

Author of the Report:
Michael Kohronas - Information Security Manager

Author’s Contact Information:
Phone: 561-951-1769
Email: Mkohronas@student.fullsail.edu

Organization Security Officer:
Jack Norman

Stakeholders Involved:
Johnny Hacksalot - Lead Penetration Tester - WeHackApps, LLC

Incident Description:

Date and Time that the Security Incident was Discovered?: 01/01/2024

Has the security incident been resolved: This security incident has not been resolved. The incident is still under review by the security team. The security team needs to identify if the vulnerability was taken advantage of by an attacker. Then mitigate the vulnerabilities from the system.

The physical location of the affected system or information: Full Sail University in Winter Park, FL

Number of physical locations affected: One physical database affected

Number of systems affected by the security incident: One Physical Location affected

Number of users affected by the security incident: All students (15,500) and All Faculty (660)

How long the incident has persisted: 6 months without being noticed

Who discovered what: Discovered by WeHackApps, LLC whilst performing a penetration test

Who validated what: The internal security team at Full Sail validated the test results.

Any other additional important information about the security incidents: The incident was detected by WeHackApps, LLC and it is currently unknown if the vulnerability has been taken advantage of by any attackers at this moment.

Impact/Potential Impact:

Loss of Data/Data Compromise:
These vulnerabilities in the system allow for loss of data or data compromise due to the ability of the attacker to escalate privileges in the system. With higher privileges, they can view other people's accounts and information overall compromising the information. Depending on the skill of the attacker it can result in the loss of data as well.

System Damage:
An attack on the Fullsails system could prevent the website from being accessible meaning that students or faculty couldn't attend or host their classes.

Financial Loss:
Fullsail would experience Financial Loss. This would happen partly due to loss of reputation. With an attack like that being heard students who may have applied there previously may not due to that reason. It can also make it harder for the school to receive the accreditations it needs to have to be considered a reputable school.

Public Relations Impact:
Depending on the severity of the attack it could ruin many of fullsails public relations. Fullsail currently has many partnerships working with them to help promote jobs for their students as well as give their students a higher level of education. With the bad publicity, people may pull out of partnerships with the school or decide to end relations with them.

Damage to the Delivery or Integrity of Information
The integrity of information can be ruined due to a student modifying grades within the database. As part of the vulnerability allows for modification of the database without permission this could invalidate the student's current grades if not able to be recovered through logs.

Regulation Violation
Many regulations will fine you for violating their requirements. In the case of Fullsail, they deal with a lot of PII students. If there is broken access control or injection within the environment this could cause financial loss and depending on the severity of the infraction more severe punishment.

Sensitivity of Information Involved:

Public: Public information is not sensitive as the information is already out there and discoverable by the general public. For example: Full Sail Holidays

Internal Use Only: Information within Fullsail that is restricted to faculty or students only. For Example: FSO assignment submission, FSO messages, Emails, and Feedback.

Restricted or confidential (Privacy Policy Violation): Restricted or Confidential information pertains to the PII of the student or faculty at fullsail. This information is protected by policies or regulations that prevent the disclosure of this information. This information is usually illegal or restricted to disclose. For Example: Student grades should only be known by the student and the teacher. Disclosure of a student's grade is restricted by school policy.

Unknown: Unknown sensitivity of information refers to information that is managed or stored in a different location but pertains to Fullsail. This could pertain to O'Riley Learning, LinkedIn Learning, and other platforms for students.

Mitigation:

Broken Access Control:

- Implementation of least privilege mindset (4 months)
- Implementation of RBAC (6 months)
- Implementation of a user access management process (3 months)
- Minimize Cross-Origin Resource Sharing (2 months)
- Limit the access APIs have (2 months)
- Implement proper logging for access control (4 months)
- Model Access controls should enforce record ownership (3 months)

Injection:

- Ensure the use of safe APIs (6 months)
- Use server-side input validation (4 months)
- Ensure that inputs have length and character parameters (1 month)
- Use SQL controls such as "LIMIT" within queries (2 months)
- Ensure an SQL output error doesn't display on the html page (2 months)

Individuals Notified of the Incident:

Jack Norman - Chief Information Security Officer (CISO)

Gary Jones - President of Full Sail University

Information Technology Department at Full Sail - Full Sail Information Security Team

---

Sign-Off Information:

Name: Michael Kohronas Signature: _____ Date: 09/09/24

Name: _____ Signature: _____ Date: _____
