Introduction

This report details the vulnerabilities discovered in the [redacted]University (FSU) FSO application during a penetration test conducted by WeHackApps, LLC. The penetration test was authorized by [redacted], Chief Information Security Officer (CISO) of [redacted] on November 24th, 2023.

Executive Summary

On November 24th, 2023, [redacted] University's FSO application was subjected to a penetration test by WeHackApps, LLC. The test revealed that the application was vulnerable to a variety of injection attacks and had broken access control. These vulnerabilities allowed users to manipulate data on the backend database and elevate privileges to access other user account data. The vulnerabilities have existed in the FSO application since the last software update six months prior.

These vulnerabilities pose a significant risk to [redacted] University. The injection attacks could allow malicious actors to manipulate student PII and grades, which could lead to identity theft or academic fraud. The broken access control could allow malicious actors to gain unauthorized access to restricted data and systems.

OWASP Top 10 Category	Vulnerability	Significance
Injection flaws (A1: Injection)	Injection attacks could allow attackers to manipulate student PII and grades.	This could lead to identity theft or academic fraud.
Broken access control (A02: Broken Access Control)	Broken access control could allow attackers to gain unauthorized access to sensitive data and systems.	This could lead to data breaches, system outages, and financial losses.

Date and Contact Information

- Date of the report: November 27th, 2023
- Author of the report: Kyle Ford, Information Security Manager, [redacted] University
- Author's contact information: 555-867-5309 ISM@[redacted]
- Name of the organization's security: officer [redacted], [redacted]University
- Organization's security officer contact information: 555-555-1234 ciso@[redacted]
- Stakeholders involved: Johnny Hacksalot, Lead Penetration Tester, WeHackApps, LLC

Incident Description

- Date and time that the security incident was discovered: November 24th, 2023.
- Has the security incident been resolved: No
- Physical location of the affected system or information: FSO application
- Number of physical locations affected: 1.
- Number of systems affected by the security incident: 1.
- Number of users affected by the security incident: All users of the FSO application.
- How long the incident has persisted: Six months.

- Who discovered what: WeHackApps, LLC discovered the vulnerabilities during a penetration test.
- Who validated what: [redacted] internal security team verified the vulnerabilities.
- Additional information: The vulnerabilities have not been exploited to date.

Impact/Potential Impact

- Loss of Data/Data Compromise: The vulnerabilities could allow malicious actors to manipulate student PII and grades.
- System Damage: The vulnerabilities could allow malicious actors to damage or disable the FSO application.
- Financial Loss: The university could be liable for damages if student PII is compromised.
- Public Relations impact: The university's reputation could be damaged if a security breach is made public.
- Damage to the Delivery or Integrity of Information: The vulnerabilities could allow malicious actors to disrupt the delivery of education services.
- Regulation Violation: The university could be fined for violating data privacy regulations.
- Information Security Policy or Procedure Violation: The university's information security policies and procedures were violated.
- Other Unknown Risks: There is a risk that the vulnerabilities could be exploited in ways that we do not yet understand.

Sensitivity of information/information involved.

- Restricted or Confidential: Student PII and grades

Mitigation

[redacted] University is taking the following steps to mitigate the security incident:

- Working with WeHackApps, LLC to develop a patch for the vulnerabilities.
- Updating the FSO application with the patch.
- Providing additional security training to employees.
- Conducting regular penetration tests on the FSO application.

Notification

[redacted] University has notified the following individuals of the security incident:

- [redacted], President of [redacted] University
- [redacted], CISO of [redacted] University
- [redacted] Security Team

Sign-Off Information

Name/Title: Kyle Ford Title: Information Security Manager, [redacted] University

Signature: Kyle Ford

Name/Title:

Signature: