**Logo, company name

Description automatically generated**

**Security Assessment Report**

May 1, 2023

Table of Contents

[1. Summary 3](#_Toc127779445)

[1. Assessment Scope 3](#_Toc127779446)

[2. Summary of Findings 3](#_Toc127779447)

[3. Summary of Recommendations 4](#_Toc127779448)

[2. Goals, Findings, and Recommendations 4](#_Toc127779449)

[1. Assessment Goals 4](#_Toc127779450)

[2. Detailed Findings 5](#_Toc127779451)

[3. Recommendations 5](#_Toc127779452)

[3. Methodology for the Security Control Assessment 5](#_Toc127779453)

[4. Figures and Code 7](#_Toc127779454)

[4.1.1 Process flow of System (this one just describes the process for requesting) 7](#_Toc127779455)

[4.1.2 Other figure of code 7](#_Toc127779456)

[5. Works Cited 7](#_Toc127779457)

# Summary

Executive Summary Here: changes were made to an old project to make it more secure.

## Assessment Scope

This was a WinForms project that was a mock ticket purchasing page done in Visual Studio.

## Summary of Findings

Of the findings discovered during our assessment, 6 were considered High risks, 2 Moderate risks, 6 Low, and 0 Informational risks. The SWOT used for planning the assessment are broken down as shown in Figure 2.

Figure 1. Findings by Risk Level

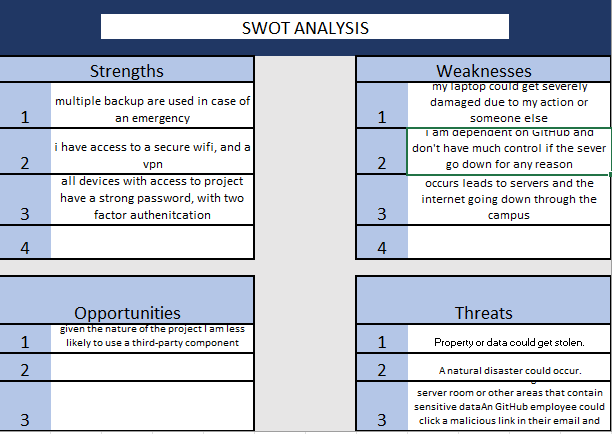


Figure 2. SWOT

Major issues that were discovered in my assessment include destruction of property, the possibility of not having Wi-Fi or even a secure connection. This highlighted the importance of having multiple backups in case an event outside of my control hinders the completion the project.

## Summary of Recommendations

**As of now, there are multiple backups, stored in the cloud as well as now my laptop. Events are now logged to a file, though current implementation could be improved. A security test are being performed from the Snyk extension on Visual Studio.**

# Goals, Findings, and Recommendations

## Assessment Goals

The purpose of this assessment was to do the following:

* To ensure that application was secure.
* Using Snyk, eliminate any potential vulnerabilities in code.

## Detailed Findings

The possible threats that were identify focus on possible property damage. This included water damage, theft, malware, or any other thing that could physically render my laptop inoperable like an act of God. Possible threats include things I could not control like servers, the internet going down. This includes the lack of a secure internet connection. There were also noticeable weaknesses also, but were focused on human errors like forgetting passwords, accidentally deleting files.

## Recommendations

Most of the threat that listed above could have mitigated by utilizing multiple forms of backups like cloud storage. This like malware and an unsecure internet connection could be solved by using a VPN and antivirus. All online services have a form of password recovery.

# Methodology for the Security Control Assessment

**3.1.1 Risk Level Assessment (delete this text: you don’t have to change 3.1.1)**

Each Business Risk has been assigned a Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1 apply to risk level assessment values (based on probability and severity of risk). While Table 2 describes the estimation values used for a risk’s “ease-of-fix”.

Table 1 - Risk Values

| Rating | Definition of Risk Rating |
| --- | --- |
| High Risk | Exploitation of the technical or procedural vulnerability will cause substantial harm to the business processes. Significant political, financial, and legal damage is likely to result |
| Moderate Risk | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to organization. |
| Low Risk | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment |
| Informational | An “Informational” finding, is a risk that has been identified during this assessment which is reassigned to another Major Application (MA) or General Support System (GSS). As these already exist or are handled by a different department, the informational finding will simply be noted as it is not the responsibility of this group to create a Corrective Action Plan. |
| Observations | An observation risk will need to be “watched” as it may arise as a result of various changes raising it to a higher risk category. However, until and unless the change happens it remains a low risk. |

Table 2 - Ease of Fix Definitions

| Rating | Definition of Risk Rating |
| --- | --- |
| Easy | The corrective action(s) can be completed quickly with minimal resources, and without causing disruption to the system or data |
| Moderately Difficult | Remediation efforts will likely cause a noticeable service disruption   * A vendor patch or major configuration change may be required to close the vulnerability * An upgrade to a different version of the software may be required to address the impact severity * The system may require a reconfiguration to mitigate the threat exposure * Corrective action may require construction or significant alterations to the manner in which business is undertaken |
| Very Difficult | The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling   * An obscure, hard-to-find vendor patch may be required to close the vulnerability * Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity * Corrective action requires major construction or redesign of an entire business process |
| No Known Fix | No known solution to the problem currently exists. The Risk may require the Business Owner to:   * Discontinue use of the software or protocol * Isolate the information system within the enterprise, thereby eliminating reliance on the system   In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by IS Management, to validate that security incidents have not occurred |

|  |  |  |
| --- | --- | --- |
| **risk** | **Risk value** | **Ease of fix** |
| **Laptop get stolen/damaged** | **Moderate** | **Very difficult** |
| **Forgets password** | **Low** | **easy** |
| **Natural disaster** | **High** | **No known fix** |
| **Severs/ internet go down** | **Moderate** | **Very difficult** |
| **Unsecure Wi-Fi** | **Moderate** | **Easy** |
| **Malware** | **High** | **Very difficult** |
| **File deletion** | **Low** | **Easy** |
| **Used libraries become outdated** | **moderate** | **Easy** |

**3.1.2 Tests and Analyses**

This was completed using Black box testing.

**3.1.3 Tools**

This was completed using Snyk.

# Figures and Code

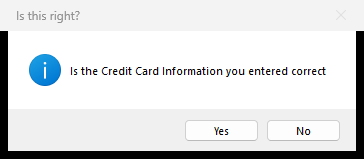
Insert any pictures here (including of major code issues or code that was used as a tool – can just screenshot and add link to github). This section must include at least 4 figures or code portions:

### Process or Data flow of System (this one just describes the process for requesting), use-cases, security checklist, graphs, etc.

Diagram

Description automatically generated





This application is more or less a mock shopping site, so the flow chart represents that. The use presses a button to purchase a ticket, that leads to another page the enter payment info, then it asks to confirm then the application closes. During the entire process it logs all event handlers and successful transitions.

### Other figure of code

HERE

# Works Cited

IT Supply Chain. “Third-Party Access and Cyber Security Vulnerabilities.” *IT Supply Chain*, 23 Sept. 2020, https://itsupplychain.com/third-party-access-and-cyber-security-vulnerabilities/.

“What Is Error Logging in C++.” *Rollbar*, 18 July 2022, https://rollbar.com/guides/cpp/cpp-error-logging/.