**Logo, company name

Description automatically generated**

**Security Assessment Report**

Version N.0

April 30, 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

The goal of this assignment was to find and fix security issues in a previous project.

## Assessment Scope

I used Visual Studio Code as a lightweight tool to edit this script since it is only a small python file along with GitHub as a repository for version control.

## Summary of Findings

Of the findings discovered during our assessment, 1 was considered High risks, 2 Moderate risks, 1 Low, and 1 Informational risk. The SWOT used for planning the assessment are broken down as shown in Figure 2.

Figure 1. Findings by Risk Level

A diagram of a swot

Description automatically generated with low confidence

Figure 2. SWOT

Explain which issues were used from above SWOT (which are addressed in this assessment).

Out of date third party libraries and auditing were the primary issues in this assessment. The library Python-dox is finicky and should be replaced altogether. For now to keep he script working we opted to update to the lates version since the 2016 version has known issues. Auditing is the next on the list. In creating a word document we run the risk of letting someone run malicious code when opening the word document. We need to keep track of those who edit the script.

## Summary of Recommendations

The majority of the script is made using the third-party dependency python-docx. It was out of date and had major security holes. It has since been updated so while not totally secure it has been mitigated. The next issue on the list would be adding a logging system to see what changes are made by who. This would make tracking much easier along with accountability to any malicious changes. (Datadog n.d.)

# Goals, Findings, and Recommendations

## Assessment Goals

The purpose of this assessment was to do the following:

* Determine if the application was securely maintained.
* Find what steps were needed to secure the application should it not be secured.

## Detailed Findings

The biggest and easiest weakness to address is the matter of outdated third-party libraries. This has a rating of high risk and easy in reference to table 1. The outdated library is open to security holes that can make it a risk to use.

Auditing is another issues in that any can edit this script and automatic create invoiced in a word document to send to a client (Datadog n.d.). It would not be a good idea to have someone be able to change to make it send malicious code to a client.

## Recommendations

To fix the outdated third-party libraries we simply had to update them to fill in that security hole. This is why it’s an Easy on the fix evaluation in table 2. This is not a permanent fix seeing as it would be better to have an entirely new library that is better maintained. Aspose.Words library seems like a good replacement as it sill have recent updates (aspose-words 23.4.0 n.d.).

Auditing this script would just be keeping a .txt file that would mark the changes, the users who made them along with the date and time. This would help keep track of what user did what and when.

# Methodology for the Security Control Assessment

**3.1.1 Risk Level Assessment**

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 |

**3.1.2 Tests and Analyses**

I plan to use Robot for the testing and analysis phase of this application. Robot seems to be the most widely used framework and would have the better documentation of my options (Robot Framework n.d.). This would help to make the testing development easier to navigate.

**3.1.3 Tools**

This was completed using windows PowerShell and, in the future, will be implementing Robot framework for testing.

# Figures and Code

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

A picture containing text, font, number, line

Description automatically generated

Figure 3: Scripted portion of the invoice.

# Works Cited

(Robot Framework n.d., 1)

(aspose-words 23.4.0 n.d.)