|  |
| --- |
| Gopher Industries - Nutrihelp |
| Identified Vulnerabilities Report |
|  |

|  |
| --- |
| Lachlan Adams  9-19-2024 |

Statement of Intent

Overview

This Document contains all vulnerabilities located via the “Vulnerability\_Scanner\_V1.1” python program. This program searches for 10 different vulnerabilities, all of which are mostly due to lack of user input validation / sanitisation. Refer to “Vulnerability Report” for additional information on each vulnerability and the potential damage caused for each specific vulnerability not getting patched.

Acronyms and Abbreviations

|  |  |
| --- | --- |
| **Acronym** | **Meaning** |
| OS | Operating System |
| XXS | Cross-Site-Scripting |

Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Dates** | **Version** | **Author** | **Comments** |
| 19/09/2024 | 1 | Lachlan Adams |  |
|  |  |  |  |

## Setting up the environment and downloading the repository:

### Python Download:

For Windows and Mac OS’s, the below links can be used to take you to the relevant python downloads page. From there, select the latest stable release and click “download”. Then begin the installation of the newly downloaded file and keep all settings default.

**Windows OS:** <https://www.python.org/downloads/>

**Mac OS:** <https://www.python.org/downloads/macos/>

**Linux OS:** Downloading and installing python for Linux can easily be done through the terminal in 5 simple steps.

1. Open the terminal form the Linux device
2. Run “sudo apt update”
3. Run “sudo apt install python3”
4. If prompted, type “y” to confirm installation.
5. Run “python3 --version” to confirm installation and current version.

Python is also available for download through the Microsoft store.

A screenshot of a computer

Description automatically generated

### Installing Git:

To clone a GitHub repository, “Git” must first be installed to run the “git” command. Use the link attached below to access the downloads page from their website.

Linux, Windows & Mac: <https://git-scm.com/downloads>

Select your relevant OS from the options provided, then install Git on your device

### Cloning the Nutrihelp-API GitHub repository:

With Git installed, open your file browser as demonstrated below.

A screenshot of a computer

Description automatically generatedHolding the windows key and pressing “E” will also work.

On **Linux**, select any file icon.

On Mac, click on the “file explorer” icon on the task bar.

Navigate to the location you would like to clone a repository to. Then right click and select terminal from the list of options.  
A screenshot of a computer

Description automatically generated

Into the terminal type “git clone <https://github.com/Gopher-Industries/Nutrihelp-api>“

A computer screen with white text

Description automatically generated

## How to use the Vulnerability Scanner tool:

Navigate to the “Vulnerability\_Tool” folder and copy the latest version of the vulnerability tool.

A screenshot of a computer

Description automatically generated

Paste a copy of the tool in a folder you wish to check file vulnerabilities for

A screenshot of a computer

Description automatically generated

Open a new terminal in this location as showed previously, then type “python3 Vulnerability\_Scanner\_V1.1.py” into the terminal. Dependant on the latest version of the program, type in the name of the file you copied over.

A screenshot of a computer

Description automatically generated

This program allows you to select any JavaScript file within the directory. After selection is made, the program will display if any of the 10 vulnerabilities were located.

# Vulnerabilites identified:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **File location** | **File name** | **Vulnerability** | **Vulnerability patched?** | **Identified By** |
| /controller | loginController.js | Insecure Token Generation | Yes | Lachlan Adams |
| /routes | imageClassification.js | Insecure File Handling | Yes – partially, only Jpeg or png files are allowed to be uploaded | Lachlan Adams |
| /routes | imageClassification.js | Insecure File Upload | Yes | Lachlan Adams |
| /test | signuptest.js | Insecure Token Generation | No fix needed; this is within the testing area – does not impact the API | Lachlan Adams |
| /test | test-helpers.js | Insecure Token Generation | No fix needed; this is within the testing area – does not impact the API | Lachlan Adams |
|  |  |  |  |  |
|  |  |  |  |  |

**ImageClassification** -file has been changed to allow for .png or .jpeg file only. This prevents attackers uploading scripts that execute on delivery. I have attached a screenshot of the file before and after changes.

A screen shot of a computer program

Description automatically generated

Changed file

A screen shot of a computer program

Description automatically generated

**loginController.js** – I have changed the method in which the MFA token is generated. As my vulnerability scanner had detected that the file was week due to Insecure Token Generation. I changed the relevant lines of code to use a different method. Which cannot be predicted by an attacker. Below is the line of code I changed to allow for this new method.

A screenshot of a computer program

Description automatically generated