

**Finding Name: Unsanitized input**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Manasa Vallaboju | SCR | Team member | Ontrack |  | NO |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

A vulnerability in the file reading functionality of the code located in the path api/submission/portfolio\_evidence\_api.rb allows for directory traversal. An attacker may be able to browse directories and access arbitrary files on the system by using the File.read function to read a file without properly sanitizing the input.

A path traversal attack, referred to as a directory traversal attack, seeks to get access to files and directories that are kept outside of the designated folder. Access to arbitrary files and directories stored on the file system, such as application source code, configuration, and other crucial system files, may be gained by modifying files with "dot-dot-slash (../)" sequences and their variations, or by using absolute file paths.   
  
When a program is run with rights that the user giving the path shouldn't have, the ability to access and modify an arbitrary path creates vulnerabilities. A path traversal vulnerability on a website would provide people access to private files on the server that hosts it.

**Risk Rating**  
Impact: Major  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

The program and the business as a whole are seriously at danger from the directory traversal vulnerability. Attackers might be able to access sensitive files on the system, which could result in the disruption of corporate operations, compromising of system integrity, and illegal access to private data.

**Affected Assets**

Affected Assets: The api/submission/portfolio\_evidence\_api.rb file's file reading capability is compromised by the vulnerability.

**Evidence**

The code sample that is available under the route api/submission/portfolio\_evidence\_api.rb is vulnerable. A directory traversal vulnerability may arise from the code snippet's use of the File.read function without sufficient input sanitization.

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

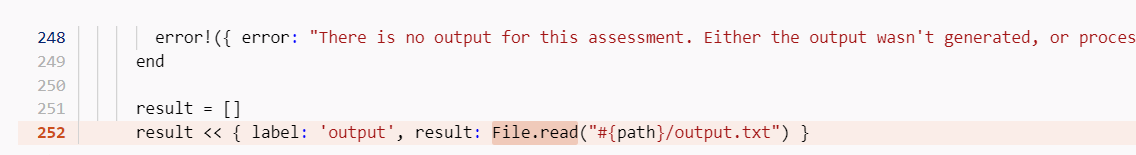
Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

****

**Remediation Advice**

Apply input validation and sanitization to guarantee that user-supplied data is thoroughly cleaned before being utilized as a file path.

Limit file access to trusted, secure locations by using a whitelist strategy.

To avoid directory traversal attacks and automatically sanitize input, think about utilizing a file handling function offered by the framework.

Continually patch and upgrade the program and its supporting files to address vulnerabilities that have been identified.

<https://github.com/Vizzuality/trase/commit/ea5b147b311eca7620abb44b2f7828fe091d1046?diff=split#diff-ecc850a9bd24b21c936da45280c7bb36b90c24882be1343607a6a7bd97a6313eL-1>

[**https://cwe.mitre.org/data/definitions/23.html**](https://cwe.mitre.org/data/definitions/23.html)

**References**

* **OWASP Path Traversal: https://owasp.org/www-community/attacks/Path\_Traversal**
* [**https://cwe.mitre.org/data/definitions/23.html**](https://cwe.mitre.org/data/definitions/23.html)
* [**https://learn.snyk.io/lesson/directory-traversal/?\_gl=1\*5j1scw\*\_ga\*MTEyMDYxMzE4OS4xNzAyNDc3OTgz\*\_ga\_X9SH3KP7B4\*MTcxMzA4NDI3MS4yOS4xLjE3MTMwODQyNzMuMC4wLjA**](https://learn.snyk.io/lesson/directory-traversal/?_gl=1*5j1scw*_ga*MTEyMDYxMzE4OS4xNzAyNDc3OTgz*_ga_X9SH3KP7B4*MTcxMzA4NDI3MS4yOS4xLjE3MTMwODQyNzMuMC4wLjA)**.**

**Contact Details**

Name: Manasa Vallaboju

Email: s223001068@deakin.edu.au

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.