

**Finding Name: No use of Whitelist Filters for file upload at Server-side**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Charanpreet | SRC | Project Co-lead | Ontrack | Payal and Jaspriya |  |
|  |  |  |  |  |  |

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

**Finding Description**

The web application uses whitelist filters at the client-side and does not employ them at the server side along with content type filters due. The client-side filters can be easily bypassed with the use of Burp suite and can be used to upload malicious files to the server that can make the server behave in an unpredictable manner.

**Risk Rating**  
Impact: Severe  
Likelihood: Unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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**

**Data Breach and Loss of Sensitive Information**

* Malicious files could lead to a data breach, compromising sensitive student, faculty, and administrative data. This could result in legal repercussions, financial loss, and damage to the institution's reputation.

**Service Disruption**

* A successful attack could disrupt the availability of the web application, affecting remote learning, administrative operations, and communication within the educational institution.

**Financial Costs**

* Remediation of a security breach, including system restoration, security enhancements, and potential legal fees or fines, could impose significant financial costs on the institution.

**Loss of Trust**

* Students, faculty, and parents may lose trust in the institution's ability to safeguard their information, potentially affecting enrollment and participation in remote learning programs.

**Affected Assets**

**Web Application and web server**

* Should a file with an unintended file extension, such as an executable file named 'malware.exe', be uploaded to the server, it has the potential to compromise both the web application and the server's integrity.

**Evidence**

**Step 1. The vulnerable piece of code can be found in FileHelper module in ‘file\_helper.rb’ file.**

A screenshot of a computer screen

Description automatically generated

**Remediation Advice**

## **Validate File Extensions**

Create a whitelist of permitted file extensions at the server side also that are necessary for your application's functionality. Reject all files that do not match the extensions on this list. For example, if your application only requires image uploads, your whitelist might include .jpg, .jpeg, .png, and .gif.

**References**

1. <https://www.opswat.com/blog/file-upload-protection-best-practices>
2. <https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html>
3. https://owasp.org/www-community/vulnerabilities/Unrestricted\_File\_Upload

**Contact Details**

Name: Charanpreet Singh

Teams Name: CHARANPREET CHARANPREET SINGH

University Email: [s221538173@deakin.edu.au](mailto:s221538173@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on.