Path Traversal in URL in AgeVolt Portal prior to version 0.1

Short Description

A directory traversal vulnerability (CVE-2022-38485) exists in the AgeVolt Portal prior to version 0.1 that leads to Information Disclosure. A remote authenticated attacker could leverage this vulnerability to read files from any location on the target operating system with web server privileges.

CVSS:3.1 score = 6.8 (Medium)

Details

By using special elements such as `../` separators, it is possible to escape outside of the restricted location to access files that are elsewhere on the system. In the screenshot below you can see that through this vulnerability we were able to read a text file `test.txt` that is in the `/tmp` directory.

Mitigation

- **Input Validation and Sanitization**:
  - Implement strict input validation to ensure that uploaded file names or paths only contain allowed characters and conform to a predefined format.
  - Sanitize user input to remove or escape characters that could be used for path traversal, such as ".." or "../../."
- **Use Whitelists**:
  - Maintain a whitelist of allowed file types and extensions for uploads. Only permit files that match the whitelist.
  - Apply strict file type checks to ensure that the content of uploaded files matches their declared type.
- **File Upload Directory Restrictions**:

- Store uploaded files in a dedicated, restricted directory that is separate from sensitive system files. This reduces the risk of unauthorized access to critical files.