Title: Directory Listing Vulnerability

Reported by: Abdulmajeed Alghamdi

Instructor: Atharva Bhamburkar

Date Discovered: 10/22/2025

Date Reported: 10/22/2025

Executive Summary:

While browsing the website a directory listing vulnerability was identified. This vulnerability allows unauthorized visibility of files and directories that should not be publicly accessible.

Discovery Method:

The vulnerability was discovered using browser developer tools (F12) while inspecting the "Sources" tab. This revealed a directory structure that displayed a list of files and folders, indicating a lack of adequate access controls. Additionally, the type of server operating system and its version were noticeable from the information exposed, providing potential attackers with useful data for exploitation.

Vulnerability Classification:

Name: Directory Listing Vulnerability

Definition: occurs when a web server is misconfigured to allow users to view a list of files and directories in a web directory, which should be restricted.

Risk: Exposes sensitive files and directories to unauthorized users, making it easier for attackers to gather information for further exploits. This visibility increases the risk of data breaches and can facilitate more severe attacks on the system.

Affected URL:

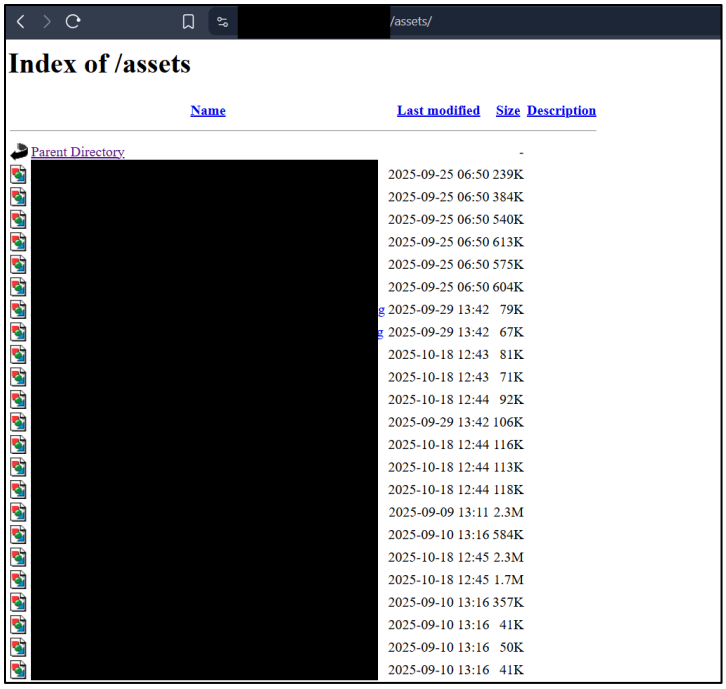
- https:/[redacted]/assets

Affected systems / components

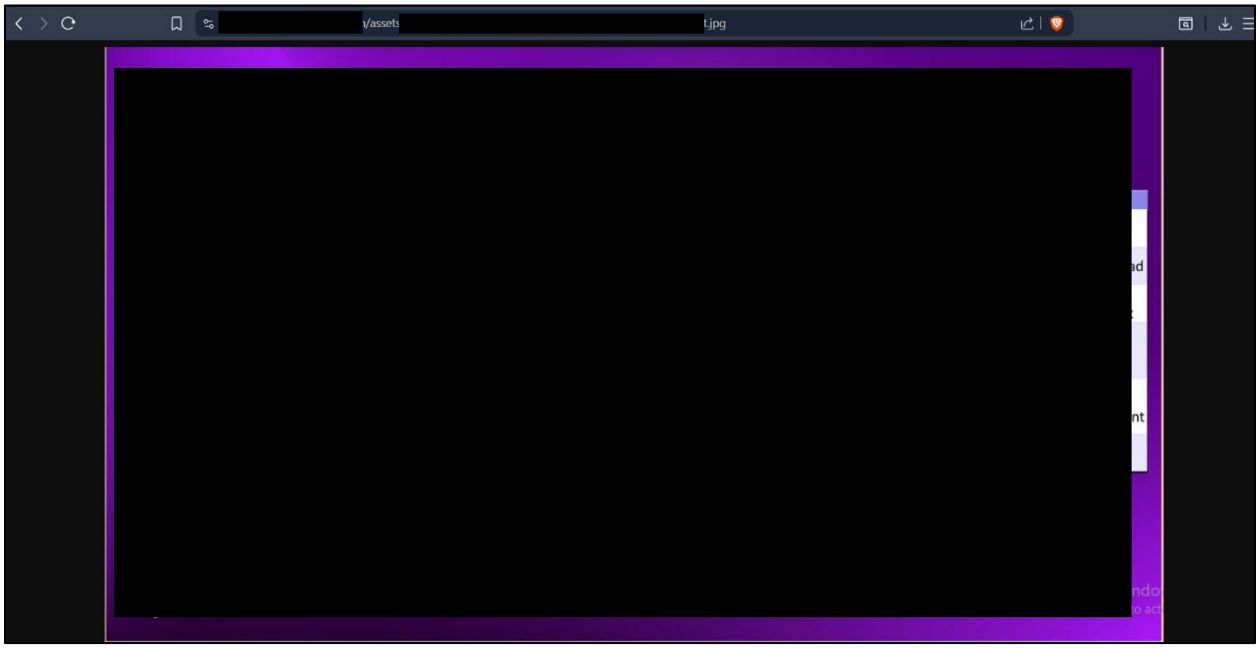
Web Application: Misconfigured web application that allow directory listing can expose sensitive directories and files.

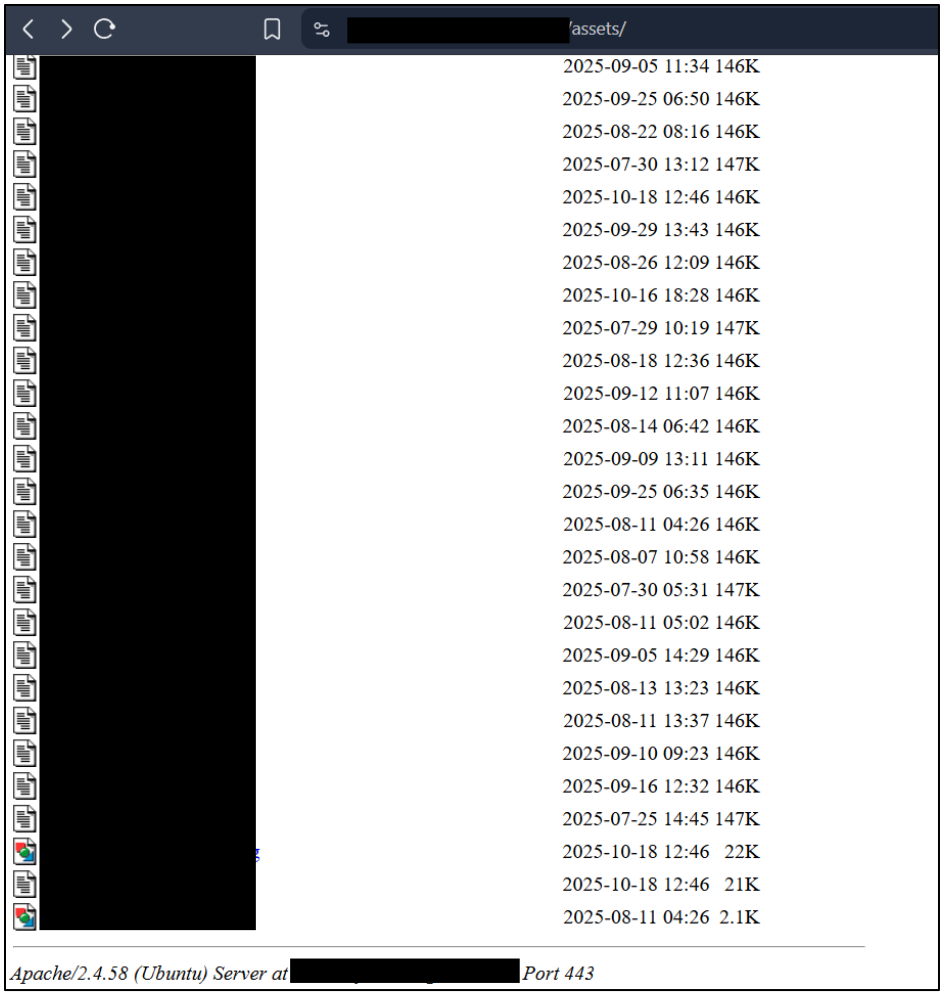
Evidence:

Allowed accessing the directory of assets and showing all the files uploaded and can be accessed.



Example of one of the pictures that is in the directory





Lastly, once reaching the bottom of the directory, the type of server operating system and its version were noticeable from the information exposed, providing potential attackers with useful data for exploitation.

Mitigation and Recommendation

- Disable Directory Listing: Configure the web server to prevent directory listings.
- Implement Access Controls: Ensure that access is restricted to necessary files only.