Risk Assesment-Path traversal

After analyzing the path traversal vulnerability in the web server, it has been determined that the overall risk associated with the vulnerability is "High".

The likelihood of the vulnerability being exploited is assessed as "High". This is because the vulnerability is relatively easy to exploit and can be done with commonly available tools, such as curl or a web browser. Additionally, the vulnerability can be discovered and exploited by both attackers with low and high skill levels, which further increases the likelihood of exploitation.

The impact of the vulnerability is assessed as "High". If exploited, the vulnerability allows an attacker to access files outside the intended directory, potentially leading to a data breach or unauthorized access to sensitive information. This can result in reputational damage, loss of trust, and financial loss for the organization.

The base CVSS score for the vulnerability is 7.5, indicating that the vulnerability is considered "High" severity. This score is based on the following metrics:

Attack Vector: Network (AV:N)
Attack Complexity: Low (AC:L)
Privileges Required: None (PR:N)
User Interaction: None (UI:N)
Scope: Unchanged (S:U)
Confidentiality: High (C:H)
Integrity: None (I:N)
Availability: None (A:N)
The base CVSS string for the vulnerability is:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

The relevant CWE value for the vulnerability is CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

The impact of the vulnerability on a web application's security posture under ASVS is significant.
The vulnerability violates several ASVS requirements, including ASVS V2.1.1: Verification Requirements, V2.2.2: Session Management Requirements, and V5.1.2: Directory Enumeration Prevention Requirements. Additionally, the vulnerability is related to CWE-22, which maps to ASVS V10.3: Path Traversal Prevention Requirements.