**Risk Assessment**

**1. Overall Risk Assessment:** High  
 - This vulnerability poses a high risk due to its potential impact on the confidentiality and integrity of sensitive data. Exploiting path traversal can grant unauthorized access to critical files, compromising the security and privacy of the system.

**2. Likelihood of Exploitation:** High

**3. Reasoning for Likelihood Assessment:**

- Path traversal vulnerabilities are commonly exploited due to their relative simplicity to exploit and the potential for significant impact. Attackers can easily manipulate input to access unauthorized files on the server.

**4. Impact of Exploitation:** High

**5. Reasoning for Impact Assessment:**

- Exploiting this vulnerability could lead to severe consequences, such as unauthorized access to sensitive files, exposure of confidential information, potential data breaches, or even the execution of malicious code on the server. This directly affects the confidentiality, integrity, and availability of the system.

**CVSS Score:**

- Base CVSS Score: 7.5 (High)

**Base CVSS String:**

- Attack Vector: Network (N)

- The attack occurs over a network, requiring no local access.

- Attack Complexity: Low (L)

- Path traversal vulnerabilities often involve straightforward manipulation of input.

- Privileges Required: None (N)

- Attackers do not need any privileges to exploit this vulnerability.

- User Interaction: None (N)

- No user interaction is necessary for exploitation.

- Scope: Unchanged (U)

- The vulnerability does not impact other components/systems.

- Confidentiality: High (H)

- Exploiting this vulnerability can lead to unauthorized access to sensitive files.

- Integrity: None (N)

- Exploitation does not impact data integrity directly.

- Availability: None (N)

- Exploitation does not directly impact system availability.

**Relevant CWE Values:**

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

- This vulnerability aligns with CWE-22, which refers to improper limitation of a pathname to a restricted directory, commonly known as 'Path Traversal.' CWE-22 precisely describes the risk associated with allowing unauthorized access beyond the intended directory structure.

**Impact on ASVS:**

- Exploiting this vulnerability could bypass authentication, access sensitive data, or compromise session management and data protection mechanisms.

- This vulnerability would violate ASVS requirements such as:

- V9: Authentication (ASVS Level 2, 3)

Exploiting this vulnerability might bypass authentication mechanisms, leading to unauthorized access.

- V10: Session Management (ASVS Level 2, 3)

It could compromise the session management system, potentially allowing an attacker to hijack sessions.

- V11: Access Control (ASVS Level 2, 3)

It undermines access controls, enabling unauthorized access to sensitive files.

- V12: Data Protection (ASVS Level 2, 3)

Exploiting this vulnerability could lead to the exposure of sensitive data, violating data protection measures.