Vulnerability Assessment

Vulnerability: Path traversal

Likelihood: High
Reason: This attack is easy to perform with a tool such as burpsuite, but it requires basic knowledge of the file system of the web server's OS and HTTP request to use this attack effectively.

Impact: Critical
Reason: This vulnerability allows the attacker to access files outside of the directory of the web application. Combined with the PUT request and DELETE request which are enabled for this web application, they allow the attacker to add and delete files in the affected web server. This could allow attacks that could compromise the confidentiality, integrity, and availability of web application files on the server such as creating and executing PHP files, vandalizing HTML files, and navigating the system and reading sensitive files.

Overall Risk: High

Base CVSS Score: 9.0(Critical)

Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

Attack Vector:
Network – This attack on the web application occurs over the internet.

Attack Complexity:
Low – Attack can be performed on demand by inserting a directory path pattern in the URI of the HTTP request using the burpsuite tool.

Privileges Required:
Low- Most of the files on the system can be read using this attack, but modifications, additions or deletions of files using the PUT or DELETE option can be done only within the directory of the system user running the web application.

User Interaction:
Required – The attacker must interact with the web application by sending a HTTP request to perform the attack.

Scope:
Changed – Since remote code execution is possible by creating and running PHP files, it could be used to access other systems through the vulnerable web server.

Confidentiality:
High – This attack allows the attacker to read sensitive files outside and inside the web application directory.

Integrity:
High – This attack can affect almost all the files in the web application directory but little outside of it. (E.g., This attack can still be used to write files into the /tmp folder in Linux)

Availability:
High – Using the DELETE request, web pages can be deleted only from the web application's directory but still greatly affects its availability.

CWE:
This attack is related to CWE-23: Relative Path traversal, which is the member of CWE Category 1345 (A01:2021- Broken Access Control, OWASP Top 10 2021)

ASVS:
The path traversal vulnerability shows that the web application violates requirement 4.1.3 according to the version 4.0.3 of ASVS since there are no mechanisms set to enforce access control to sensitive files on the web server except for the file permissions set at the OS level.

References:
MITRE, CWE-23: Relative Path Traversal Link:
https://cwe.mitre.org/data/definitions/23.html

MITRE, CWE CATEGORY: OWASP Top Ten 2021 Category A01:2021 - Broken Access Control Link: https://cwe.mitre.org/data/definitions/1345.html

FIRST, Common Vulnerability Scoring System Version 3.1 Calculator Link:
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

OWASP, OWASP Application Security Verification Standard 4.0.3: V4.1 General Access Control Design Page no: 36