Star Health VDP Report Format

Vulnerability Title

Local File Inclusion (LFI) via filename Parameter on Home Page – https://example.com/home

Vulnerable URL / Affected Area

https://example.com/home (Home Page)

Affected Parameter / Form

filename parameter

Vulnerability Description

The filename parameter on the Home Page (https://example.com/home) is vulnerable to a Local File Inclusion (LFI) attack. An attacker can manipulate this parameter by sending a POST request with directory-traversal payloads such as ../../../../../../etc/passwd. Due to missing input validation and sanitization, the server processes the malicious path and returns contents of sensitive system files, exposing critical server information.

Severity - Critical

Risk Rating - High

CVE Reference - CVE-2023-31904

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

CVSS Score - 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L)

Vulnerability Classification

Broken Access Control

Impact Analysis

LFI allows attackers to load arbitrary files from the server by altering the filename parameter. Successful exploitation may disclose sensitive files, configuration details, credentials, or even enable remote code execution depending on server configuration.

Steps to Reproduce

1. Navigate to the Home Page: https://example.com/home
2. Select any file from the available selection area.
3. Intercept the request using Burp Suite Proxy.
4. Send the request to the "Repeater" tab.
5. Modify the "filename" parameter to: ../../../../../etc/passwd
6. Observe the response displaying sensitive file contents.

Recommended Mitigation Steps

- Validate and sanitize all user-supplied input.
- Avoid using raw user input in file inclusion functions; implement whitelisting.

- Use predefined mappings or fixed absolute file paths.
- Restrict file access permissions to safe directories only.
- Keep software and server components updated.

References

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion
https://brightsec.com/blog/local-file-inclusion-lfi/
https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/