Vulnerability: Path Traversal

Path traversal is a vulnerability that allows an attacker to access files and directories outside of the intended directory on a web server. This vulnerability can compromise the confidentiality and integrity of sensitive data and system files, and potentially allow an attacker to execute malicious code on the server.

Steps to Replicate the Vulnerability:

1. Set up a vulnerable page on the web server that includes a path traversal vulnerability. For example, create a page that allows users to view files on the server by specifying the file name in the URL, without properly validating the file name.

2. Create a file outside of the specified folder that you want to access (In this case Code folder), for example in the root directory or some other directory that is not accessible through the vulnerable page.

3. Access the vulnerable page using a web browser or an HTTP client like curl. Try to access the file outside of the specified folder by using ../ directory traversal components in the URL.

   Example: http://localhost:5050/../sensitiveInfo.txt

   If the vulnerability exists, the server should return the contents of the file-outside-specified-folder.txt file, which contains sensitive information.

Mitigation:

To mitigate the path traversal vulnerability, it is important to properly validate user input and sanitize file names before accessing them on the server. This can be done by checking that the file name only contains valid characters and does not include any directory traversal components. Additionally, it is important to limit the permissions of the web server user to prevent access to sensitive system files. Finally, it is recommended to use a web application firewall (WAF) to detect and block path traversal attacks.