Web Directory Listing Vulnerability – icons/ Folder Remediation

# Overview

When a web server (like Apache or Nginx) has directory listing enabled, anyone can access a folder and view all the files inside it without authentication. This poses a security risk, especially if the folder is system-related, such as the default icons/ directory used by the OS.  
  
The icons/ folder typically contains icons used by the server’s default user interface. If exposed, it can lead to information disclosure and may assist an attacker in mapping the system.

# Identification

This issue is usually detected through vulnerability scans or manual checks.  
  
Example:  
http://<server\_ip>/icons/  
Directory Listing is Enabled  
  
This indicates that the autoindex module is active and the configuration allows listing the contents of the icons/ directory.

# Step-by-Step Remediation Process

## 1. Raise RITM to Unix Team

First, raise a Request Item (RITM) to the Unix team to verify the server’s configuration.  
  
Check the file: /etc/httpd/conf.d/autoindex.conf (or similar), and locate this section:

Alias /icons/ "/var/www/icons/"  
<Directory "/var/www/icons">  
 Options Indexes FollowSymLinks  
</Directory>

If Options Indexes is present, directory listing is enabled. To remediate:  
  
- Either comment out the block:

# Alias /icons/ "/var/www/icons/"  
# <Directory "/var/www/icons">  
# Options Indexes FollowSymLinks  
# </Directory>

Or remove the Indexes directive to prevent listing.  
  
Action: Clearly mention in the RITM that the /icons/ directory should be secured by disabling directory listing.

## 2. Notify Application Team

Email the application team responsible for the server to:  
- Inform them about the vulnerability and the planned configuration changes.  
- Request validation or confirmation if any application component depends on the icons/ path.

## 3. Apply Remediation Across Environments

### a. UNIT and INTG Environments

- Request the Unix team to apply the fix.  
- After changes are implemented, test the result:  
 http://<server\_ip>/icons/ should return 403 Forbidden or 404 Not Found.

### b. QA Environment

- Notify the QA team (e.g., ACCO QA team) to perform a health check post-remediation.  
- Ensure that application functionality remains unaffected.

### c. Production Environment

- Once validation in lower environments is successful:  
- Inform the application team and coordinate for validation in Production.  
- Request the Unix team to implement the same remediation.

# Post-Remediation Validation

After the fix, verify by accessing:  
http://<server\_ip>/icons/  
  
Expected result:  
- 403 Forbidden or  
- 404 Not Found  
  
Check server logs to ensure there are no errors related to the change.

# Conclusion

While the icons/ directory may seem harmless, exposing it through directory listing can lead to security risks. Proper coordination between Unix, App, and QA teams helps ensure the vulnerability is remediated safely without affecting the application.