Informe de la Fase 2 - Auditoria de Seguridad

1. Introducción

En esta fase se ha seleccionado y analizado una vulnerabilidad en la configuración del servidor web Apache. Se ha explotado la vulnerabilidad para demostrar su impacto y se han implementado medidas correctivas para mitigarla.

2. Vulnerabilidad Seleccionada

Se identificó que la opción "Indexes" estaba habilitada en la configuración de Apache, lo que permitía la exploración de directorios web.

3. Explotación

Se realizó un escaneo con Gobuster, confirmando que los directorios eran accesibles sin autenticación. Esto podría exponer archivos sensibles.

4. Medidas Correctivas

- Se editó el archivo de configuración /etc/apache2/apache2.conf.

- Se deshabilitó la opción "Indexes" en los directorios afectados.

- Se reinició el servicio Apache para aplicar los cambios.

- Se verificó que el acceso a directorios no mostrara su contenido.

5. Herramientas Utilizadas

- Gobuster: Enumeración de directorios.

- Nmap: Detección de servicios.

- Curl: Verificación de accesibilidad de directorios.

- Apache2: Modificación y configuración del servidor web.

6. Conclusión

La vulnerabilidad ha sido corregida, reduciendo el riesgo de exposición de archivos en el servidor. Se recomienda continuar con auditorías periódicas y aplicar las mejores prácticas de seguridad en la configuración del servidor web.