Tabla 13. Lista de Chequeo: Archivos y recursos

- Se deben gestionar de forma segura los datos que no sean confiables.
- Se deben almacenar los datos no confiables fuera del ***webroot*** de la aplicación teniendo unos permisos con unos límites bien definidos.

Descripción	Nivel		
	1	2	3
Verificar que las URL se re-direccionen y reenvíen sólo a destinos clasificados en la lista blanca, o mostrar una advertencia cuando se redirija a contenido potencialmente no confiable.	X	X	X
Verificar que archivos no confiables enviados a la aplicación no sean utilizados directamente por comandos de entrada/salida de archivos, especialmente para proteger contra manipulaciones de rutas, archivo local incluido, manipulación de tipo ***mime*** y vulnerabilidades de inyección de comandos de sistema operativo	X	X	X
Verificar que los archivos procedentes de fuentes no confiables sean validados para ser del tipo del cual se espera y sean analizados por escáneres antivirus para evitar la carga de contenido malicioso conocido.	X	X	X
Verificar que datos no confiables no se utilicen en funcionalidades de reflexión, cargado de clases o inserción para prevenir vulnerabilidades de inclusión de archivos remotos/locales.	X	X	X
Verificar que datos no confiables no se utilicen en recursos de dominios compartidos (**CORS**) para proteger contra el contenido remoto arbitrario.	X	X	X
Verificar que los archivos obtenidos de fuentes no confiables se almacenen fuera del webroot, con permisos limitados, preferiblemente con una fuerte validación.		X	X
Verificar que el servidor web o de aplicación se encuentre configurado por defecto para negar el acceso a recursos remotos o sistemas fuera del servidor web o de aplicación.		X	X
Verificar que el código de la aplicación no ejecuta datos cargados obtenidos de fuentes no confiables.	X	X	X
Verificar que no utiliza Flash, Active-X, Silverlight, NACL, Java del lado del cliente u otras tecnologías del lado del cliente que no sean soportadas de forma nativa a través de los estándares de navegador W3C.	X	X	X