Lista de Chequeo: Autenticación

- Existen sesiones de usuario únicas por conexión evitando compartidas.
- Las sesiones que ya no son necesarias deben establecerse a un estado inválidas, teniendo además un tiempo restringido mientras no se presente actividad contra la aplicación.

Descripción	Nivel		
	1	2	3
Verificar que no se utiliza un gestor de sesiones personalizado, o que, si el gestor de sesiones es personalizado, éste sea resistente contra los ataques más comunes.	X	X	X
Verificar que las sesiones se invalidan cuando el usuario cierra la sesión.	X	X	X
Verificar que las sesiones se invalidan luego de un período determinado de inactividad.	X	X	X
Verificar que las sesiones se invalidan luego de un período determinado de tiempo, independientemente de que se esté registrando actividad (timeout absoluto).		X	X
Verificar que todas las páginas que requieren autenticación poseen acceso fácil y visible a la funcionalidad de cierre de sesión.	X	X	X
Verificar que el identificador de sesión nunca se revele en las URLs, en los mensajes de error o registros de historial. Esto incluye verificar que la aplicación no es compatible con la reescritura de URL incluyendo el identificador de sesión.	X	X	X
Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión.	X	X	X
Verificar que sólo los identificadores de sesión generados por la aplicación son reconocidos como activos por ésta.		X	X
Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas.	X	X	X
Verificar que los identificadores de sesión almacenados en cookies poseen su atributo “path” establecido en un valor adecuadamente restrictivo y que además contenga los atributos "Secure" y "HttpOnly".	X	X	X
Verificar que la aplicación limita el número de sesiones concurrentes activas.	X	X	X
Verificar que una lista de sesiones activas esté disponible en el perfil de cuenta o similar para cada usuario. El usuario debe ser capaz de terminar cualquier sesión activa.	X	X	X
Verificar que al usuario se le sugiera la opción de terminar todas las otras sesiones activas después de un proceso de cambio de contraseña exitoso.	X	X	X