OWASP 07
FALLOS EN LA AUTENTICACION

Álvaro García González

¿DE QUE TRATA?

Este punto trata sobre aquellos casos donde el atacante engaña al sistema para reconocer un usuario incorrecto o invalido como legítimo.

Vulnerabilidades

- Permitir ataques automatizados o por fuerza bruta porque no son bloqueados a tiempo (o no son bloqueados directamente)
- Permitir el uso de contraseñas débiles o conocidas como "admin" o "paso"
- Permitir en el registro usar contraseñas que se sabe que se han filtrado
- Permitir la recuperación de contraseñas con preguntas "basadas en conocimiento" (ej: pregunta de seguridad: ¿Cómo se llama tu perro?)
- Usar texto plano o con hash débiles para almacenar contraseñas
- La web NO tiene factor de autenticación doble o múltiple
- En la URL expone el identificador de la sesión, en un campo oculto o en alguna otra localización expuesta al cliente
- Reutiliza el mismo identificador de la sesión después del logearte correctamente

Maneras de prevenirlo

- Implementar y obligar el uso del doble (o múltiple) factor de autenticación
- Anima y habilita la opción de usar gestores de contraseñas
- Nunca despliegues una aplicación con contraseñas por defecto
- Implementa chequeos de contraseñas débiles (testea nuevas contraseñas contra la lista de las 10.000 peores contraseñas)
- Durante el registro o el cambio de contraseña, valídalas contra la lista de credenciales filtrada
- No fuerces a las personas a cambiar la contraseña al menos que haya habido una brecha (en ese caso sí, fuérzales)
- Asegúrate que en el login, en el cambio de contraseña y en la ruta de las APIs están protegidas contra los ataques de cuenta de enumeración usando siempre el mismo mensaje (usuario o contraseña incorrectos)
- Guardar en el log todos los fallos y las alertas cuando sepas o **creas** que estas sufriendo un ataque

Que se ve reflejado en nuestra aplicación

Nuestra aplicación final tiene **MUCHAS** vulnerabilidades

No bloquea los ataques por fuerza, permite contraseñas débiles, no tiene doble factor de autenticación, reutilizamos la misma sesión después de un login correcto, no consultamos la lista de las peores 10 mil contraseñas para el registro1, no chequeamos y prohibimos el uso de contraseñas filtradas, **no deshabilitamos la sesión durante el logout ni después de un periodo de inactividad,**

Aunque hay algunas vulnerabilidades que no tenemos como: recuperación de contraseñas inseguras (directamente no podemos recuperarla) ni mostramos la sesión al cliente en el URL ni en ningún otro sitio (excepción evidente, en la página detalle, que lo hacemos apropósito)