CAI 1 - CUMPLIMIENTO DE DIFERENTES POLÍTICAS DE SEGURIDAD EN ENTIDAD FINANCIERA

CONFIDENCIAL

Contexto de la Consulta 1: Una entidad financiera dispone de una **Política de Seguridad** que indica que los **mecanismos de autenticación** se basan en la existencia de contraseñas, y especifica un conjunto de condiciones que éstas deben cumplir:

1. **Debe tener como mínimo 8 caracteres.**
2. **Debe tener al menos un carácter de cada uno de los siguientes tres grupos:**
   a. **Letras (mayúsculas y minúsculas): A, B, C, … a, b, c …**
   b. **Caracteres numéricos: 0, 1, 2, 3, … , 8, 9**
   c. **Símbolos: ! @ # $ % & *^( ) - = { } [ ] \ : ; < > ? , . /**

La base de datos de control de acceso a los sistemas de información de dicha empresa contiene una tabla con el nombre de los usuarios, su ***username,*** la contraseña cifrada mediante un ***algoritmo de hashing seguro*** para evitar que si alguien accede a dicha tabla no puede conocer dicha contraseña y tiene también un campo **salt** que podría ser añadido como **prefijo o sufijo** a dicha contraseña para el almacenamiento seguro de la misma.

No disponen de mecanismo alguno que controle el cumplimiento de esta Política de **Seguridad** en dicha empresa. **Se sospecha por parte de la Dirección de la empresa que las 4 contraseñas de** la tabla siguiente no cumplen con la Política de Seguridad de dicha organización.

Nombre	Username	Contraseña[1]	Salt	Comentarios de empleados en público[2]
Ramón Gómix Piesco	ragopi	tN8Sr9V3cOeqHyXSbkrFm0jXSJ+hVvlG1PkXyKxuRDc=	39	*"… he puesto como contraseña la matrícula de mi nuevo coche"*
Arturo Rendo Taxore	aretax	i9wtdI1MWrc9erJH0cDL6Mqyh4fOEs2NIEPp8k+VhqU=	40	*"…mi contraseña es una palabra de la lengua inglesa en minusculas"*
Amalia A. Pearse Mariso	ampema	AGZXmYdx6x73XQom+IJK+Z2ov09yYdOk2JZwgoamGOs=	51	*" …mi contraseña es de las más comunes que se ponen seguida de dos números"*
Pedro Martteis Zausco	pemaza	95qamsyzWZOlJq5/glwBO2u/ijcH7SFlDoS2ZCtAlzY=	18	*"…mi contraseña es* ***la fecha de nacimiento de uno de sus hijos"***

Consulta 1. Informar al cliente cuál o cuáles de los usuarios incumple la Política de Seguridad de contraseñas mediante la correspondiente comprobación por la técnica seleccionada, e indicar las reglas de la Política que podrían estar violando cada una de las contraseñas analizadas. Recomendar una solución organizativa y/o técnica al cliente (oportunidad de negocio) para evitar todos estos problemas de incumplimiento de la Política de Seguridad de contraseñas y mejorar la misma.

Contexto de la Consulta 2: También, de acuerdo con la estrategia de aseguramiento de la información ***Security by design*** la entidad financiera publica en su Web que la integridad de las transferencias financieras, a través de la aplicación se pueden descargar los clientes, se hará de **"forma segura"** usando **Códigos de Autenticación de Mensajes (MAC)** de los mensajes realizados por el cliente al servidor del banco con **claves secretas de un tamaño de 32 bits.** Dicha entidad entrega a los clientes cada año un dispositivo físico (*pendrive, smartcard*, SD memory, …) que contiene dicha clave para realizar todas las gestiones financieras que deseen durante el año.

La **Política de Seguridad propuesta** de la entidad especifica **que todas las transmisiones de información de la entidad con los clientes deben ser íntegras (no hay todavía preocupación por la confidencialidad),** evitando los posibles ataques. No obstante, la entidad tiene dudas razonables sobre la **robustez del algoritmo de generación de MAC y las claves usadas para los MAC por dicha aplicación para dispositivos móviles**. El mensaje representa las transferencias financieras que se hacen en dicha entidad, el primer número la cuenta origen, el segundo la cuenta destino y el tercero la cantidad que se desea transferir. Y en este caso se ha empleado para el MAC una clave de 32 bits. Los mensajes recibidos son los siguientes:

Cliente 1:
Mensaje: 34567893 987344 120
MAC: F7HZhdhQlaNZ4HsQ7PEB9XAMGYK1ToVmNwX0hw8p4Tk=
Cliente 2:
Mensaje: 34567894 986454 10
MAC: 865etFtdcUpKTaDKHJyJ57V45kojGX8ozs4VsRs1nj8=
Cliente 3:
Mensaje: 34537895 957769 110
MAC: QFpV6BaR5CCl8HE/Afx93pPlp+t/bsY/2P6aricsAYA=

Consulta 2. Informar al cliente si es seguro el tamaño de clave que está usando para preservar la integridad de las transmisiones justificando la razón de ello. En caso de que no sea seguro el tamaño de clave usado, realizar una recomendación acerca del tamaño de clave que se considera adecuado desde un punto de vista de la capacidad computacional. Recomendar posibles mejoras en el proceso de entrega de claves a los clientes.
MUY IMPORTANTE: El cliente nos requiere para sus procesos de Auditoría Externa que se le justifique razonadamente el tamaño de clave que recomiendan los consultores del Security Team.

Política de desarrollo y entrega:

- Cada ***Security Team*** generará una sola entrada en el **Diario de grupo** con el detalle de la respuesta técnica aportada al cliente para las dos consultas. En la entrada del Diario se deben recoger evidencias del proceso, herramientas y pruebas realizadas, así como de las respuestas a las consultas planteadas. No se entregan las contraseñas y las claves encontradfas en el informe al cliente, sino que se envían mediante un **mensaje seguro (el mensaje de Curso es seguro) a la persona de INSEGUS que dirige la sesión de trabajo.**
- Las consultas se desarrollarán en la sesión de trabajo dispuesta al efecto, y en el tiempo indicado desde el comienzo de la sesión hasta las 12:30 horas.

[1] Codificación Base64
[2] Consideren también que podrían estar diciendo alguna mentira.