



SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

CAI 1. CONSULTA SOBRE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE CONTRASEÑAS (Parte 1)

La empresa nos realiza una consulta sobre su **Política de Seguridad** respecto a los mecanismos de autenticación basados en contraseñas. Sobre dichas contraseñas indica que éstas:

1. Deben tener como mínimo 8 caracteres.
2. Deben 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: ! @ # \$ % & * ^ () - = { } [] \ : ; < > ? , . /

No existe mecanismo alguno que controle el cumplimiento de esta Política de Seguridad en dicha organización.

La base de datos de control de acceso a los sistemas de información de dicha organización contiene el nombre de los usuarios, su **username** y la contraseña cifrada mediante un **algoritmo de hashing seguro** para evitar que si alguien accede a dicha tabla no puede conocer dicha contraseña.

Se sospecha que las tres contraseñas de la tabla siguiente no cumplen con la Política de Seguridad de dicha organización,

Nombre usuario	Username	Contraseña
...
...
...

(Las contraseñas no aparecen pues se informará de ellas en la sesión de trabajo)

Las sospechas se fundamentan en que el primer usuario ha indicado a alguno de sus compañeros de trabajo que **“no se ha complicado la vida y ha puesto como contraseña una palabra rara del diccionario de la Real Academia de la Lengua”**, el segundo ha comentado que **“no se ha quebrado la cabeza y ha puesto una contraseña de las comunes que se ponen”**, y el último ha dicho que **“tiene puesta una contraseña jugando con algunas de las letras de su nombre y apellidos con un número al final”**. Consideren también que podrían estar diciendo alguna mentira.

Las consultas que nos presenta el cliente consisten en:

- a. **Indicar al cliente qué tecnología considera más oportuna para comprobar que dichas contraseñas no cumplen dicha Política de Seguridad, debería hacerse un análisis de las alternativas tecnológicas que existen y justificar la opción elegida. (Valoración 30%)**
- b. **Indicar al cliente cuál o cuáles de los usuarios incumple la Política de Seguridad de contraseñas mediante la correspondiente comprobación por la técnica seleccionada en el apartado a. Además, el cliente nos solicita que se le indique las reglas de la Política que podrían estar violando cada una de las contraseñas analizadas. Se valorará presentar las contraseñas originales y capturas del proceso seguido para conseguirlas. (Valoración 30%)**

El cliente final indica que valorará el análisis riguroso que se debe realizar de las diferentes alternativas tecnológicas que existen para llevar **dicha comprobación eficientemente** para evitar los problemas de incumplimiento de las Políticas de Seguridad.

Normas del entregable

- El plazo de entrega de dicha consultoría se acordado con el cliente que finalizará el próximo **día 20 de Octubre a las 23:59 horas.**
- En la segunda parte de la consultoría se informará del procedimiento para la entrega del trabajo.

Noticia relacionada:

- [Una filtración permitió ver la ubicación de más de medio millón de vehículos con localizador satelital en EEUU](#)