Sobre el cumplimiento de diferentes políticas de seguridad en [ENTIDAD FINANCIERA]

Consultoría realizada por:

Juan Luis Ruano Muriedas

José Joaquin Rojas Romero

Antonio José Suárez García

CONFIDENCIAL

Índice

CONFIDENCIAL

Resumen ejecutivo

Tras un exhaustivo estudio de su problema, **hemos detectado problemas** de seguridad en **ambas** de sus consultas.

En la ***Consulta 1***, se ha encontrado que varios de los usuarios **no cumplían las políticas de seguridad de contraseñas de la empresa,** viéndose así comprometida la seguridad de sus contraseñas. Para solucionar este problema recomendamos algún tipo de **charla con sus empleados** para asegurar el cumplimiento de las políticas de seguridad de la empresa o el uso de algún **sistema de autenticación passwordless** con firma digital.

En la ***Consulta 2***, se ha encontrado que una clave de 32 bits **no es lo suficientemente robusta** para garantizar la integridad de los mensajes cliente/banco.Tampoco recomendamos el **reparto de memorias físicas** como método seguro para el intercambio de claves. Para solucionar este problema, recomendamos **aumentar el tamaño de la clave** a, por lo menos, **64 bits**. En cuanto al **intercambio de claves** recomendamos el uso de **RSA**, el cual está probado como un método seguro para el intercambio de información.

A medida que su empresa continúa evolucionando, también lo hacen las necesidades de seguridad informática. Es por ello que queremos reiterarle nuestro compromiso de brindarle un **servicio de consultoría integral y personalizado** que se adapte a sus nuevos desafíos.

CONFIDENCIAL

Metodología y resultados

Consulta 1

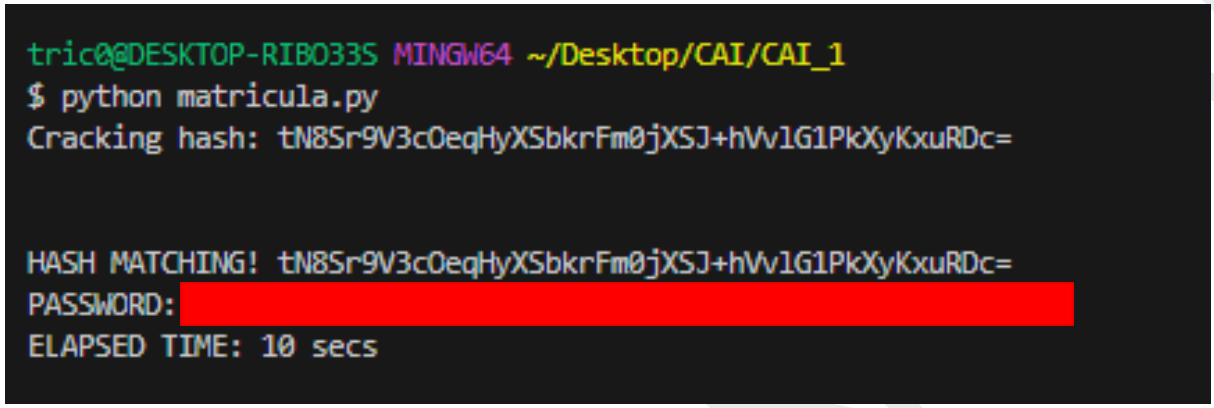
Tras el estudio de la *Consulta 1* hemos encontrado que varios de sus empleados **incumplen las condiciones** sobre las contraseñas que impone la política de seguridad de su empresa. En la siguiente tabla se expone cuáles de estas condiciones se incumplen, así como el tiempo empleado en descifrar las contraseñas. Más adelante se hablará de ellas una por una.

Nombre	Regla 1	Regla 2.a	Regla 2.b	Regla 2.c	Tiempo (s)
ragopi		Sin minúsculas			10
aretax		Sin mayúsculas			0
ampema					-
pezama					0

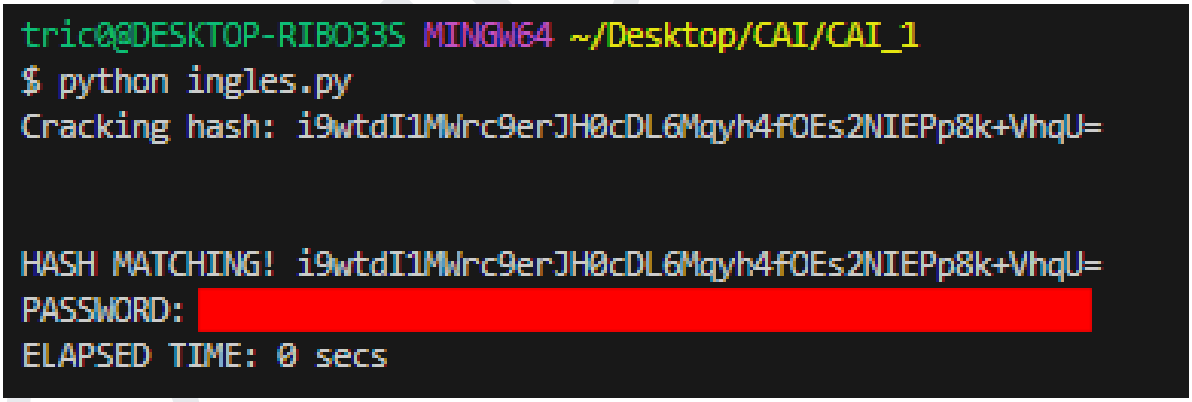
Para la comprobación de la seguridad de las contraseñas se han diseñado varios scripts en el lenguaje de programación Python donde los vectores de ataque son: **búsqueda acotada y diccionario**. Se parte del conocimiento del cifrado (SHA256 y base64).

CONFIDENCIAL

- La contraseña de **ragopi** ha sido obtenida mediante una **búsqueda acotada**, usando los comentarios emitidos en público por esa misma persona para acotar la búsqueda. Esta contraseña no cumple con el mínimo de caracteres requeridos, no contiene letras minúsculas y no contiene ningún carácter especial.



- La contraseña de **aretax** ha sido obtenida mediante un **ataque de diccionario** usando los comentarios emitidos en público por esa misma persona para acotar la búsqueda. Esta contraseña no contiene mayúsculas, no contiene números y tampoco contiene caracteres especiales.



- La contraseña de **pezama** ha sido obtenida mediante una **búsqueda acotada**, usando los comentarios emitidos en público por esa misma persona para acotar la búsqueda. Esta contraseña no contiene letras ni caracteres especiales.

```
tric0@DESKTOP-RIBO335 MINGW64 ~/Desktop/CAI/CAI_1
$ python fecha.py
Cracking hash: 95qamsyzWZO1Jq5/glwBO2u/ijcH7SF1DoS2ZCtAIzY=


HASH MATCHING! 95qamsyzWZO1Jq5/glwBO2u/ijcH7SF1DoS2ZCtAIzY=
PASSWORD: [redacted]
ELAPSED TIME: 0 secs
```

Consulta 2

Para la comprobación de la seguridad del tamaño de clave simplemente nos hemos basado en la seguridad que ofrece la ***Consulta 1*** en comparación a la ***Consulta 2***.

CONFIDENTIAL

Soluciones

En cuanto a la ***Consulta 1***, proponemos múltiples soluciones al problema de seguridad presente:

- En primer lugar, lo más esencial y sencillo es **modificar el formulario de registro** de los empleados para comprobar que las contraseñas cumplen las condiciones que establece la política de seguridad de la empresa. Esta solución es muy rápida y sencilla, tratándose de una simple modificación del código de la aplicación en la que sus empleados se registran. Además, debido a que la comprobación se realiza del lado del cliente, no implica carga de trabajo extra al servidor de la empresa.

- En segundo lugar, se recomienda que **hablen con sus empleados** del tema. En cualquier empresa, muchos empleados desconocen de las políticas de seguridad, ya sea por despiste o dejadez. Una solución simple y rápida que recomendamos es realizar algún tipo de charla con los empleados para invitarles a cambiar sus contraseñas por otras más seguras.

- En último lugar, recomendamos algún **sistema de autenticación passwordless** basado en firma digital. Estos sistemas han demostrado tener múltiples ventajas sobre los sistemas tradicionales que dependen de contraseñas. Ofrecen una mayor seguridad al estar basados en criptografía de clave pública, se elimina el riesgo de robo de contraseña por ataques de phishing o ingeniería social, la experiencia de usuario se ve simplificada al no tener que recordar y gestionar contraseñas y facilita la adopción de medidas de autenticación multifactor, como el uso de tokens o autenticación biométrica. En nuestra experiencia, combinar un sistema basado en firma digital con el uso de tokens ha demostrado ser un sistema completamente seguro y fácil de usar.

En cuanto a la ***Consulta 2***, nos gustaría proponer una solución a cada uno de los problemas presentes:

- En cuanto al **intercambio de claves**, realizarlo en cualquier formato físico es un modo muy inseguro e ineficiente de hacerlo. Los dispositivos físicos como las memorias USB o las memorias SD son fácilmente extraviables debido a su

CONFIDENCIAL

pequeño tamaño. Esto provocaría retrasos en la entrega de las claves a los clientes, al tener que generar nuevas claves en caso de que uno se extravíe, así como ser susceptible a ser robado por algún atacante. Además, tienen el costo añadido que conlleva tener que comprar múltiples memorias cada año, costo que aumenta conforme aumenta su negocio. Para solucionar este problema recomendamos el uso del envío de claves mediante RSA, el cual es comúnmente usado para estos casos. RSA ha sido demostrado múltiples veces como un método seguro para el intercambio de claves debido a su alta seguridad, su interoperabilidad y su eficiencia.

- En cuanto al **tamaño de las claves**, recomendamos aumentar su tamaño. En este caso al tener un cifrado menor para MAC (32 bits) posiblemente se esté empleando SHA1, MD5 o DES entre otros mecanismos de cifrado. Estos algoritmos pertenecen al pasado donde 32 bits eran robustos. En la actualidad se recomienda emplear un algoritmo de cifrado de mínimo 128 bits sin un excesivo coste computacional agregado, como SHA224, SHA256, SHA512 o similares. La actual MAC es sensible frente a ataques de: *Replay Attack, Multiple forgery attacks* y *Key replication attacks*. Aplicando un algoritmo de cifrado más robusto, como SHA224, conseguimos protegernos de *Multiple Forgery* y *Key Replication attacks*, mientras que añadiendo un *nonce* al mensaje nos defenderemos de los Replay attacks y Man in The Middle.

CONFIDENCIAL

Discusión y conclusiones

Para concluir nuestra consultoría, queremos resaltar la importancia crucial de la ciberseguridad en la era digital actual, especialmente para empresas como la suya. Es esencial incorporar en la planificación estratégica métodos sólidos para establecer normas de ciberseguridad y así protegerse de posibles ciberataques.

Una medida fundamental es el uso de contraseñas seguras y robustas, ya que estas son la base para la gestión, análisis e integración de la empresa, lo que en última instancia se traduce en una mayor rentabilidad. Sin embargo, crear contraseñas seguras no es una tarea sencilla. Los usuarios no pueden limitarse a utilizar información fácilmente recordable, como fechas de cumpleaños o dejar las contraseñas anotadas en lugares visibles, como debajo del teclado o en un Post-It.

Es imperativo seguir una Política de Seguridad para garantizar la fortaleza de las contraseñas. Además, durante nuestra consultoría hemos observado la necesidad de mantener actualizados los mecanismos de seguridad, ya que la obsolescencia facilita los ataques cibernéticos.

En última instancia, es mejor prevenir que lamentar. Por ello, recomendamos encarecidamente que las contraseñas relacionadas con la empresa sean utilizadas exclusivamente para fines corporativos, como cuentas de correo electrónico o aplicaciones web de la empresa, y no para uso personal. Esta práctica ayuda a mantener la seguridad de los datos corporativos y a prevenir posibles brechas de seguridad.

CONFIDENCIAL