Alumno: Rodrigo Vila

Modulo 3 – Final

Consigna:

El ejercicio final de este módulo, corresponde a crear un informe relacionado a lo

aprendido en esta unidad y aplicando algunas medidas de seguridad aprendidas en otras unidades.

Seleccionar solamente UNA de las técnicas que se mostraron en esta unidad, y exponer cuáles podrían ser las formas de mitigación.

- Ingeniería Social
- Ataques de Autenticación
- Denial of Service (DoS)
- Ataques de Modificación

Técnica seleccionada:

Ataques de Autenticación.

También veremos Ingeniería Social como técnica colateral relacionada al robo de credenciales de autenticación.

En esta exposición trabajaré sobre 2 escenarios:

- Ingenieria social - Phising a través de correo electrónico
- Ataques de autenticación a un formulario de inicio de sesión web utilizando fuerza bruta.

En el último escenario mencionado intentaremos vulnerar la seguridad utilizando ataques de Fuerza bruta con diccionarios, lo que nos permitirá observar de manera práctica la aplicación de métodos que nos ayuden a mitigar estos ataques, haciendo difícil al atacante lograr su objetivo.

También veremos como luce un ataque de “Phishing” camuflado con ingeniería social y cómo podemos tratar de identificar y cuidarnos de este tipo de engaños.

Ingeniería social y Phishing:

Escenario:

Recibimos un e-mail que dice ser del equipo de Facebook para que “confirmemos nuestra información para mantener la cuenta segura”:

Acción requerida: Actualiza tu información de seguridad Recibidos ×

Rodrigo Vila <rodrigovila.it@gmail.com> 23:09 (hace 0 minutos)
para mí

Asunto: Acción requerida: Actualiza tu información de seguridad

De: Facebook noreply@facebook.com

**Hola [Rodrigo Vila],

Recientemente hemos actualizado nuestra política de seguridad y necesitamos que confirmes tu información para mantener tu cuenta segura.

Por favor, haz clic en el siguiente enlace para iniciar sesión y actualizar tu información de seguridad:

Iniciar sesión ahora

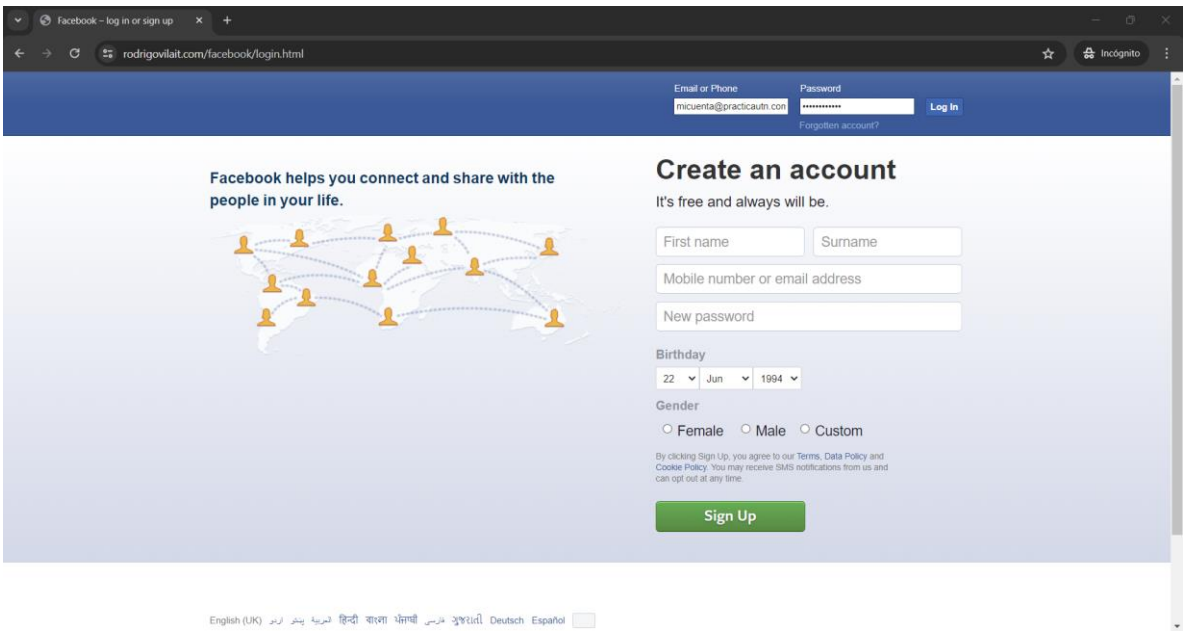
Si no actualizas tu información en los próximos 24 horas, podríamos suspender temporalmente tu cuenta por razones de seguridad.

Gracias por tu cooperación.

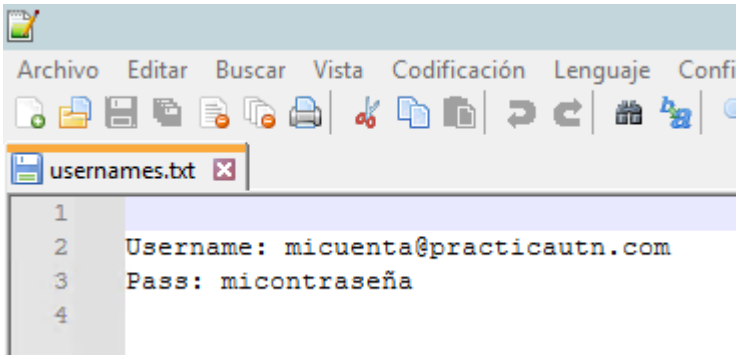
Atentamente, El equipo de Facebook.

Responder Reenviar

Procedemos a hacer click en el enlace y nos logueamos, ya que no queremos que nuestra cuenta sea suspendida, tal como dice el mail:



Le damos a Log In y pareció no haber pasado nada, nos volvió a llevar a la página original, repetimos el proceso y esta vez si entramos a nuestra cuenta y nos quedamos seguros porque todo funciona a la normalidad, pero en realidad lo que paso es esto:



Nuestros datos de autenticación han sido capturados por el sitio de phishing.

Al poco tiempo recibiremos un correo que han cambiado los datos de recuperación de la cuenta y probablemente no podamos volver acceder más a nuestra cuenta.

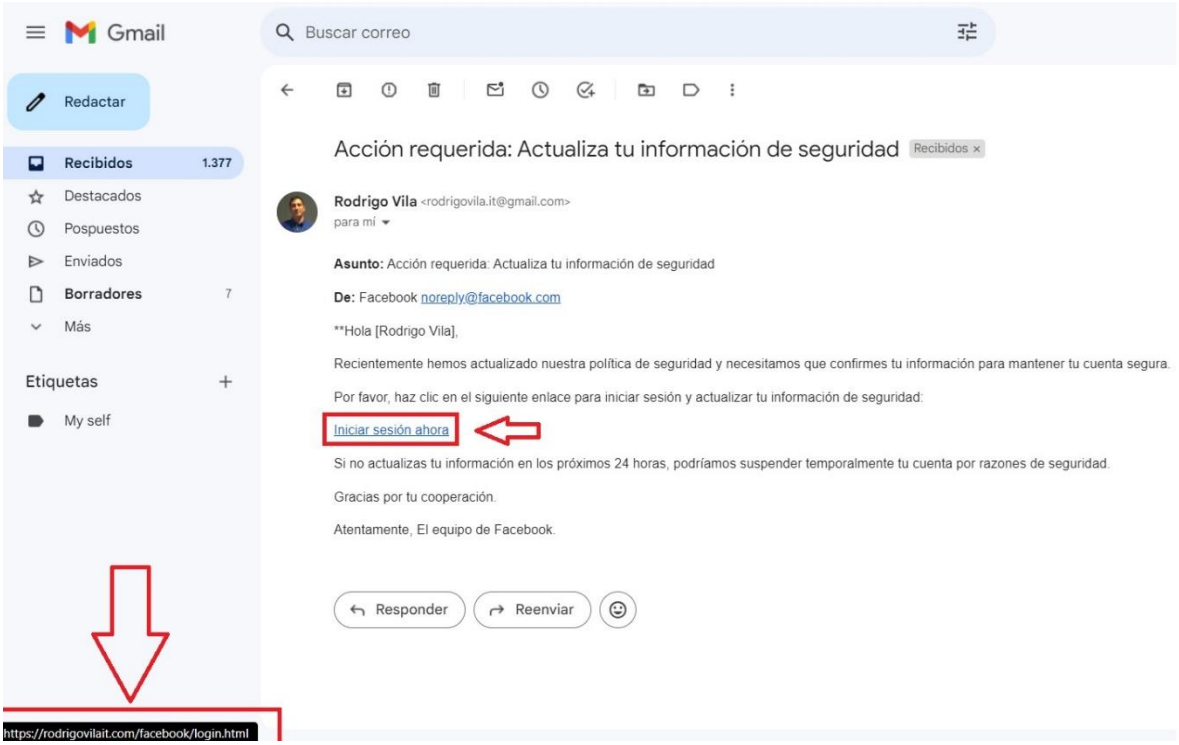
Como mitigar este tipo de ataques?:

Vamos a desglozar la información relevante de este correo electrónico que nos indicará si es falso o no.

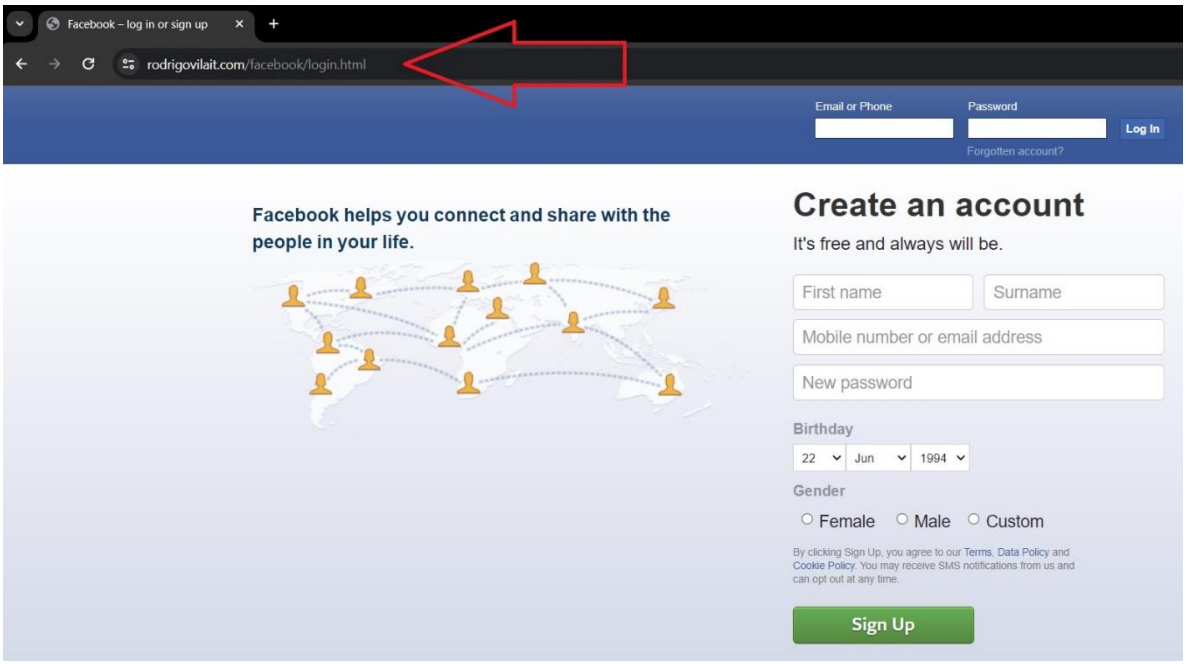
Primero que nada, el remitente:

Debemos fijarnos que el dominio del remitente no tenga faltas de ortografía, caracteres similares o duplicados al original, buscar inconsistencias sospechosas y aun así, no confiar por mas fidedigno que parezca, ya que hay servicios que permiten personalizar el remitente a través de los servidores SMTP por donde se envían estos correos.

Lo mismo se aplica para el cuerpo del mensaje, pero lo mas importante de todo, debemos fijarnos a dónde nos lleva el hipervínculo que nos proporciona. “Iniciar sesión ahora”:



Vemos que posando el click sobre el hipervínculo, el navegador nos muestra abajo a la izquierda la dirección donde nos llevara ese link. Debemos observar si se trata de la web original o nos lleva a otra dirección. Aun así, tampoco hay que confiarse solo en esto ya que nos pueden engañar utilizando enmascaramiento de URLs. Por eso si llegamos hacer click debemos observar bien hacia que web nos redirige:



Vemos que la URL no es la original de Facebook. También existen enmascaramientos de URL como mencioné antes. Asique debemos observar si la web tiene errores ortográficos, si la (en este caso red social) no modernizó su página de inicio, avisos de seguridad que nos avise nuestro navegador, etc. También podemos observar el certificado de la web si corresponde con la organización a la que estamos intentando loguear.

Para ayudar a mitigar un ataque de phishing como el expuesto anteriormente, donde se intenta engañar a los usuarios para que ingresen sus credenciales en una página falsa, se pueden seguir varias estrategias y medidas de seguridad:

1. Educación y Concienciación del Usuario

Capacitación Regular: Organizar sesiones de capacitación periódicas para educar a los usuarios sobre los riesgos de phishing, cómo reconocer correos electrónicos sospechosos y qué hacer si reciben un correo sospechoso.

Simulaciones de Phishing: Realiza simulaciones de ataques de phishing para evaluar la conciencia de seguridad de los usuarios y reforzar el entrenamiento.

Políticas de Seguridad: Implementa y comunica políticas claras sobre la seguridad del correo electrónico y el uso de credenciales.

2. Tecnología y Herramientas de Seguridad

Filtros de Spam y Anti-Phishing: Utilizar filtros de spam avanzados y herramientas anti-phishing en los servidores de correo para bloquear correos electrónicos sospechosos antes de que lleguen a los usuarios.

Navegadores Seguros: Asegurarse de que los navegadores de los usuarios estén actualizados y tengan habilitadas las funciones de seguridad como el filtro de navegación segura que advierte sobre sitios web sospechosos.

3. Medidas Técnicas Adicionales

Autenticación Multifactor (MFA): Implementar MFA para todas las cuentas de usuario. Esto añade una capa adicional de seguridad, ya que los atacantes necesitarían algo más que solo la contraseña para acceder a las cuentas.

Monitoreo y Análisis: Utilizar herramientas de monitoreo y análisis de seguridad para detectar comportamientos anómalos o patrones que puedan indicar un intento de phishing.

Certificados SSL/TLS: Asegurarse de que todos los sitios web legítimos utilicen HTTPS para cifrar el tráfico entre el navegador del usuario y el servidor web. Esto ayuda a verificar que el usuario está en el sitio correcto y no en una página falsa.

Protección contra Malware: Utiliza software antivirus y anti-malware en todos los dispositivos para detectar y bloquear amenazas potenciales.

4. Procedimientos de Respuesta a Incidentes

Plan de Respuesta a Incidentes: Desarrolla un plan de respuesta a incidentes específico para ataques de phishing, que incluya procedimientos claros para la identificación, contención, erradicación y recuperación de un ataque de phishing.

Notificación y Reporte: Establece un mecanismo para que los usuarios puedan reportar correos electrónicos sospechosos de phishing rápidamente. Actúa de inmediato para investigar y mitigar cualquier amenaza.

Análisis Forense: Realiza análisis forense de los incidentes de phishing para comprender cómo ocurrió el ataque y mejorar las defensas futuras.

5. Mejores Prácticas

No Compartir Información Sensible: Educa a los usuarios para que nunca compartan información sensible (como contraseñas) a través de correo electrónico o sitios no verificados.

Verificación de Identidad: Antes de ingresar credenciales, verifica siempre la URL del sitio web para asegurarse de que sea legítima.

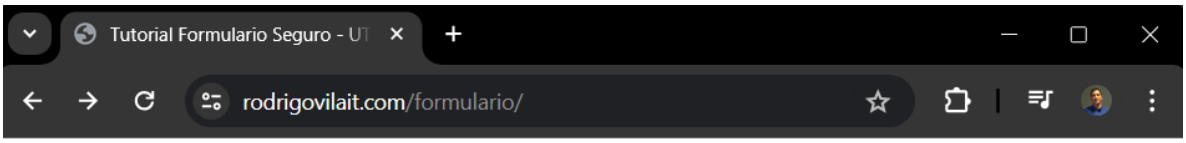
Desconfianza Proactiva: Fomenta una cultura de desconfianza proactiva, donde los usuarios son cautelosos y verifican cualquier solicitud de información personal o confidencial.

Implementar estas medidas puede ayudar a reducir significativamente el riesgo de ataques de phishing y proteger a los usuarios y la organización de posibles compromisos de seguridad.

Ataque a formulario de Login Web utilizando Fuerza bruta:

Escenario:

Utilizare un formulario que hice para ejercicios de unidades anteriores, pero esta vez modificado con registro y autenticación conectado a una base de datos.



UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Centro de e-Learning
Secretaría de Cultura y Extensión Universitaria

Formulario Seguro - UTN

Username:

Password:

Remember Me

Login

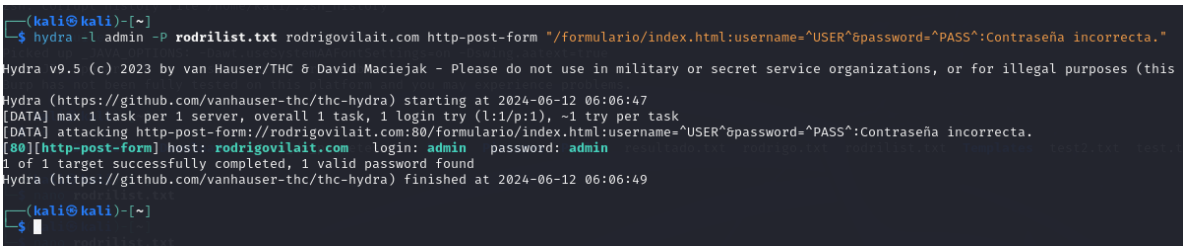
No tienes cuenta? Registrate

Primero creamos un usuario poco seguro, por ejemplo: Usuario admin – Contraseña: admin (un clásico usuario por defecto):

Ahora veremos como una herramienta de fuerza bruta, utilizando un diccionario de palabras y contraseñas comunes, puede vulnerar credenciales simples y por defecto:

En este caso utilizando la herramienta “Hydra”:

Acá podemos ver que encontramos la coincidencia:



Nos logueamos con las credenciales obtenidas:

Como mitigar este tipo de ataques?:

Primero que nada, como tanto hemos repetido, concientizar a los usuarios de crear contraseñas robustas. Para “ayudarlos” a que cumplan con una política de contraseñas robustas podemos hacer algunas cosas a través del código. Como por ejemplo: establecer un mínimo de caracteres necesarios más amplio, obligarlos a que deban incluir minúsculas, mayúsculas, números y símbolos:

```php
// Validación del nombre de usuario
if (empty($username) || strlen($username) < 5 || strlen($username) > 20) {
    echo "Error: El nombre de usuario debe tener entre 5 y 20 caracteres.";
    exit;
}

// Validación de la contraseña
if (empty($password) || strlen($password) < 8) {
    echo "Error: La contraseña debe tener al menos 8 caracteres.";
    exit;
}
if (!preg_match('/[A-Z]/', $password)) {
    echo "Error: La contraseña debe incluir al menos una letra mayúscula.";
    exit;
}
if (!preg_match('/[a-z]/', $password)) {
    echo "Error: La contraseña debe incluir al menos una letra minúscula.";
    exit;
}
if (!preg_match('/[0-9]/', $password)) {
    echo "Error: La contraseña debe incluir al menos un número.";
    exit;
}
if (!preg_match('/[!@#$%^&*(),.?":{}|<>]/', $password)) {
    echo "Error: La contraseña debe incluir al menos un símbolo.";
    exit;
}
```

Algunas prácticas de seguridad extras que podemos añadir:

1. Implementar Captchas

Descripción: Utiliza captchas para diferenciar entre humanos y bots.

Efectividad: Reduce significativamente los intentos automatizados de fuerza bruta.

Ejemplo: reCAPTCHA de Google.

2. Bloqueo de Cuenta después de Intentos Fallidos

Descripción: Bloquea temporalmente una cuenta después de un número específico de intentos fallidos.

Efectividad: Limita la capacidad de probar múltiples combinaciones de contraseñas en poco tiempo.

Ejemplo: Bloquear la cuenta durante 15 minutos después de 5 intentos fallidos.

3. Implementar Delays (Retrasos) después de Intentos Fallidos

Descripción: Añade un retraso creciente entre los intentos fallidos de inicio de sesión.

Efectividad: Desincentiva los ataques de fuerza bruta al aumentar el tiempo necesario para probar múltiples combinaciones.

Ejemplo: Aumentar el retraso en 5 segundos por cada intento fallido sucesivo.

4. Autenticación Multifactor (MFA)

Descripción: Añade una capa adicional de seguridad requiriendo un segundo factor de autenticación.

Efectividad: Hace que sea significativamente más difícil para los atacantes comprometer una cuenta, incluso si logran obtener la contraseña.

Ejemplo: Enviar un código SMS o utilizar una aplicación de autenticación como Google Authenticator.

5. Monitoreo y Alertas de Seguridad

Descripción: Monitorea los intentos de inicio de sesión y genera alertas para actividades sospechosas.

Efectividad: Permite una respuesta rápida a posibles ataques y la implementación de medidas adicionales.

Ejemplo: Alertar al administrador cuando hay múltiples intentos fallidos desde una misma IP.

Para desarrollar estos ejercicios se realizó a modo laboratorio:

- Web de phishing con fines educativos: https://rodrigovilait.com/facebook/login.html
- Formulario web securizado con php, conectado a una instalación de MySQL, con sistema de registro y pagina de visualización solo para usuarios registrados y autenticados: https://rodrigovilait.com/formulario/index.html

Caso real y opinión:

Fuente: https://elpais.com/tecnologia/2024-05-31/la-guardia-civil-investiga-un-posible-ciberataque-a-la-direccion-general-de-trafico.html

El ciberataque que sufrió la Dirección General de Tráfico (DGT) en España el mes pasado puso de manifiesto varias vulnerabilidades en su infraestructura tecnológica. Para evitar incidentes similares en el futuro, se pueden considerar varias medidas preventivas:

- Actualización y parcheo continuo: Es crucial mantener todos los sistemas y software actualizados con los últimos parches de seguridad. Esto ayuda a cerrar las brechas que los atacantes podrían explotar.

- Implementación de firewalls y sistemas de detección de intrusiones (IDS): Utilizar firewalls avanzados y sistemas de detección de intrusiones puede ayudar a identificar y bloquear intentos de acceso no autorizados antes de que comprometan los sistemas internos.

- Seguridad en la autenticación: Adoptar métodos de autenticación más robustos, como la autenticación multifactor (MFA), reduce el riesgo de que las credenciales comprometidas permitan el acceso no autorizado. Esto es especialmente relevante en instituciones con datos sensibles como la DGT.

- Capacitación del personal: La formación continua del personal en prácticas de ciberseguridad, como la identificación de correos electrónicos de phishing y otras tácticas de ingeniería social, es fundamental para prevenir ataques basados en el error humano.

- Copia de seguridad y planes de recuperación: Tener copias de seguridad actualizadas y un plan de recuperación ante desastres garantiza que, en caso de un ataque, los datos críticos puedan ser restaurados rápidamente, minimizando el impacto en las operaciones.

- Evaluaciones de seguridad regulares: Realizar auditorías y evaluaciones de seguridad de manera regular para identificar y corregir vulnerabilidades antes de que los atacantes puedan explotarlas. Esto incluye pruebas de penetración y análisis de vulnerabilidades.

- Monitoreo constante: Implementar soluciones de monitoreo de seguridad que puedan detectar actividades anómalas en tiempo real, permitiendo una respuesta rápida y efectiva ante posibles amenazas.

Adoptar estas medidas puede fortalecer significativamente la ciberseguridad de la DGT y reducir el riesgo de futuros ciberataques.

Contando un poco con mis palabras, un amigo que está por España trabajando y viviendo, me cuenta que es un desastre la infraestructura informática de los bancos y de los sistemas estatales dependiendo el municipio. Dado que entre municipios tienen relación de conectividad entre redes. Deberían establecer y cumplir con un estándar de seguridad nacional sobre las redes estatales.

Porque si logran acceder a los sistemas de un municipio vulnerable, desde estos sistemas es muy probable que puedan acceder a otros lugares que si pueden llegar a tener mas seguridad contra los intrusos, pero confían en la autenticación en sus sistemas de una PC ubicada en uno de los organismos que puede estar ya vulnerado.

Para finalizar este trabajo y dando mi perspectiva sobre este caso real expuesto, les falto algo fundamental: almacenar la información personal CIFRADA.

Rodrigo Vila.-