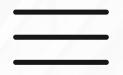




SEGURIDAD E INYECCIÓN SQL

Cheuk Kelly Ng Pante, Javier González de la Barreda Arimany y Samuel Toledo Hernández





INTRODUCCIÓN A LA CIBERSEGURIDAD

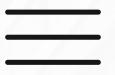


Se enfoca en

- Salvaguardar equipos, redes, software, sistemas críticos y datos contra amenazas digitales

Se emplean medidas y herramientas para:

- Resguardar información confidencial
- Prevenir el acceso no autorizado
- Evitar interrupciones en las operaciones empresariales



¿POR QUÉ ES IMPORTANTE LA CIBERSEGURIDAD?

Previene o reduce el costo de las brechas

- Organizaciones adoptan estrategias de ciberseguridad
- Reduciendo al mínimo las consecuencias no deseadas

Mantener una conformidad normativa

- Las empresas tienen la obligación de cumplir con requisitos normativos
- Reglamento General de Protección de Datos (GDPR) en Europa

Mitigar las ciberamenazas

- Las empresas se adaptan y se mantienen actualizadas con las medidas de ciberseguridad

INTRODUCCIÓN A LAS BASES DE DATOS

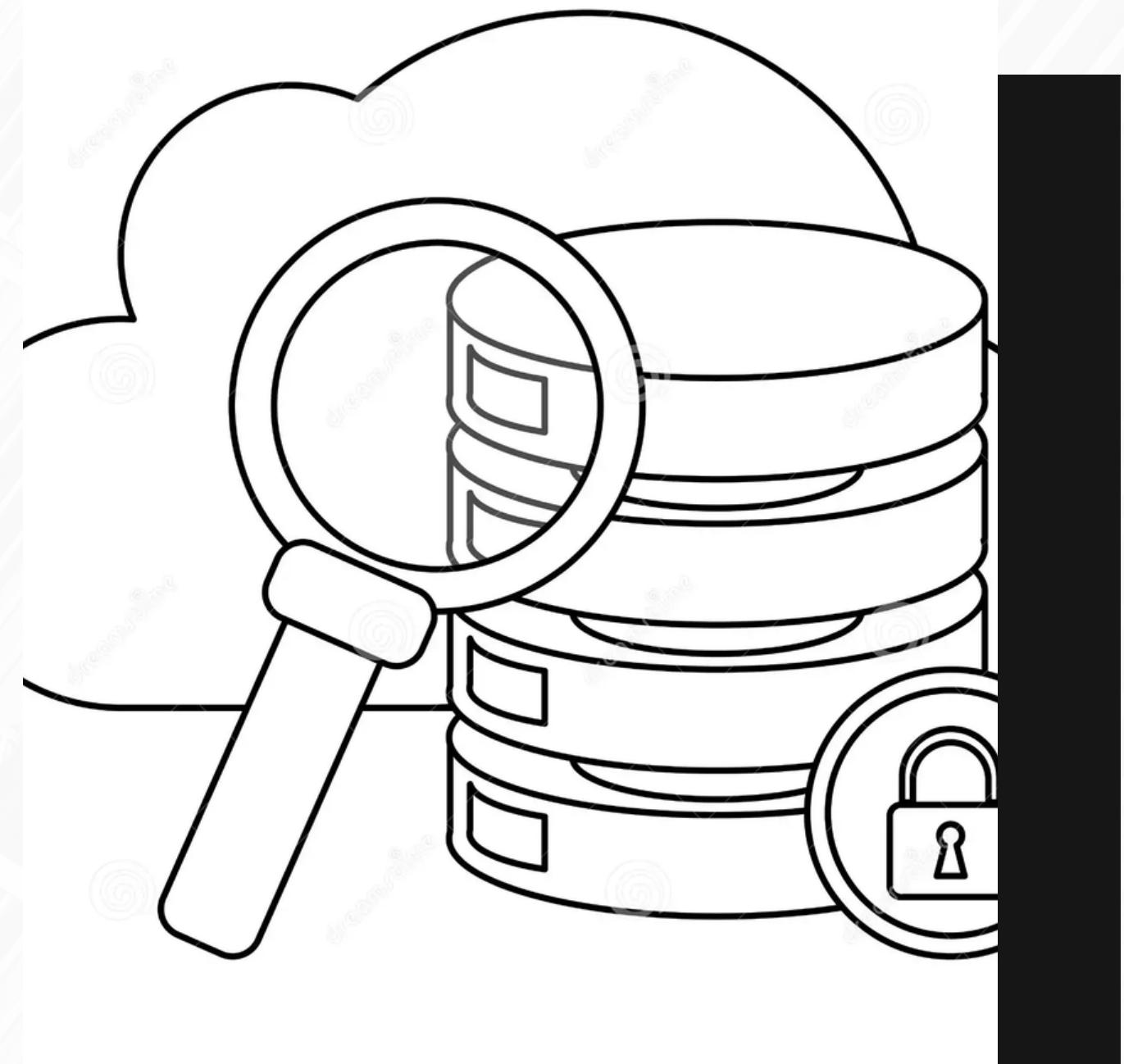
Consiste en

- Una colección de datos interrelacionados que representan información sobre una organización o área particular.

Están organizadas:

- Según el modelo de datos que definen la estructura, almacenamiento y manipulación de la información

Los sistemas de gestión de bases de datos (DBMS) son programas informáticos que gestionan, modifican, consultan y crean bases de datos.





SEGURIDAD DE BASES DE DATOS

Datos de la base de datos

- Información que abarca desde nombres y contraseñas hasta números de tarjeta de crédito

Sistema de gestión de bases de datos (DBMS)

- Papel fundamental al crear, administrar y manipular las bases de datos
- Esencial que esté actualizado, configurado y protegido de manera adecuada

Aplicaciones asociadas

- Los programas que se comunican con la base de datos deben validar y filtrar las entradas de los usuarios

Servidor de base de datos

- Deben de contar con protección física, sistemas de copia de seguridad, ...

Infraestructura informática

- Los medios a través de los cuales usuarios y aplicaciones se comunican con la base de datos deben de garantizar la seguridad y privacidad de las comunicaciones.

FORTALECER LA SEGURIDAD DE LAS BASES DE DATOS



Diseñar una arquitectura de base de datos segura que separe los datos sensibles de los no sensibles

Implementar un DBMS actualizado y configurado adecuadamente

Desarrollar una aplicación segura que utilice métodos de conexión seguros

Llevar a cabo pruebas de seguridad periódicas

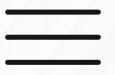
Impartir formación y concienciación a los usuarios y administradores de bases de datos



INYECCIÓN SQL

Inyección SQL

- Tipo de ciberataque que se aprovecha de los errores existentes en aplicaciones web para meter código malicioso y atacar bases de datos de SQL.
- Al introducir el código van con el fin de quebrantar las medidas de seguridad y privacidad y así acceder a datos protegidos



RIESGOS Y CONSECUENCIAS QUE CONLEVAN UNA INYECCIÓN SQL



Robos de datos sensibles

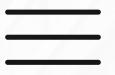
- El robo de datos puede ser utilizado para intenciones maliciosas, como llevar a cabo fraudes, robar identidades, ...

Modificación o eliminación de contenido de la base de datos

- Los atacantes pueden manipular o suprimir información almacenada en la base de datos

Escalada de privilegios

- Los atacantes pueden obtener privilegios de administrador o de usuario de la base de datos, permitiendo acciones que normalmente están fuera de alcance



TIPOS DE INYECCIÓN SQL

In-Band

- Tipo de inyección más común
- Obtención de información de la BBDD en la propia pantalla
- Mediante el propio canal que explota la vulnerabilidad

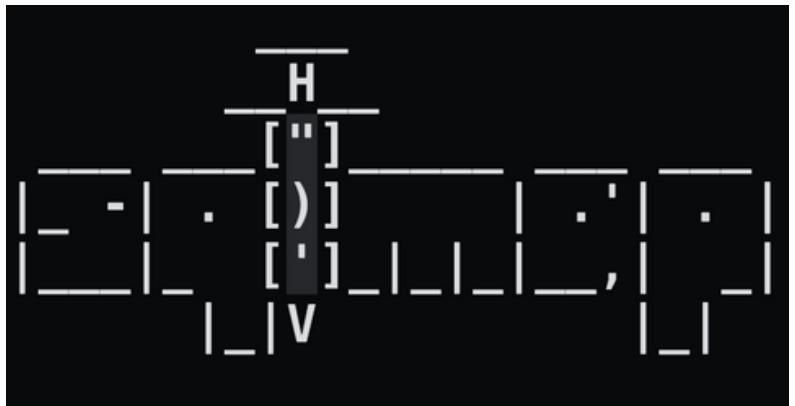
Basado en error

- Obtención de información de la BBDD mediante la inclusión de errores en la interacción con el cliente
- Estos errores revelan información sobre la estructura y el contenido de la BBDD

A ciegas

- Obtención de información de la BBDD sin que se muestre en el sitio web
- Pruebas de verdadero o falso

HERRAMIENTAS PARA LA IDENTIFICACIÓN DE VULNERABILIDADES



- ### SQLMap
- Open-Source en Kali Linux
 - Gran cantidad de payloads para explotar vulnerabilidades
 - No se requieren conocimiento profundos

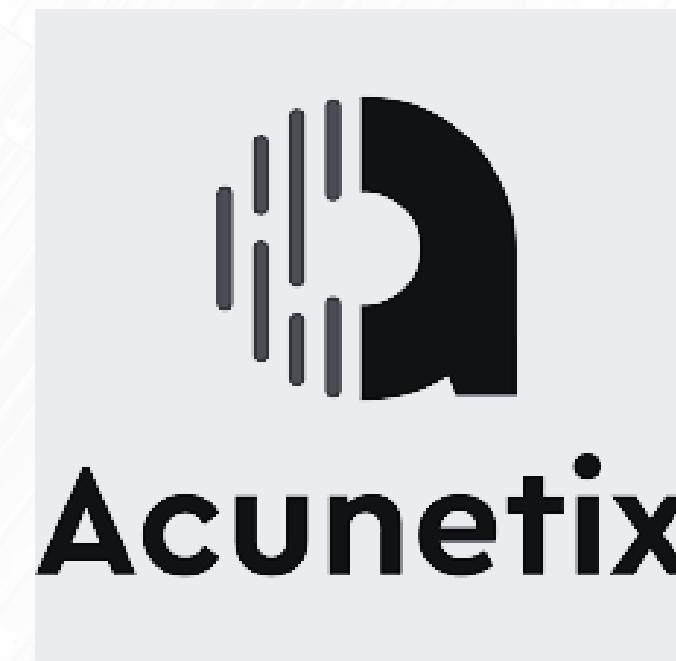
Welcome to the website Super IP (suip.biz)!

The most popular services:

- Determine your IP
- Determine CMS of Websites
- Black box WordPress vulnerability scanner online
- Detecting SQL injection flaws online
- Open ports and running services scanner (nmap) online

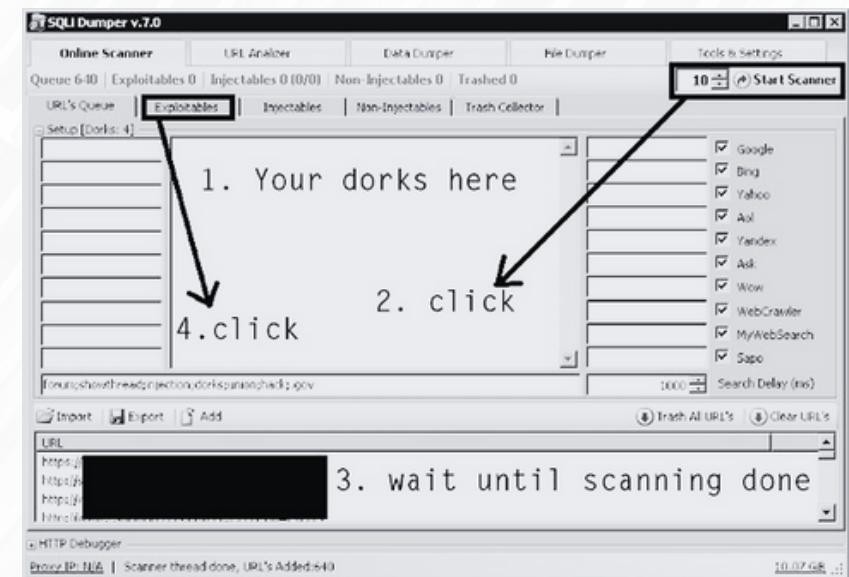
suIP.biz

- Acciones con direcciones IP
- Se ingresa la URL y se selecciona el tipo de inyección



Acunetix

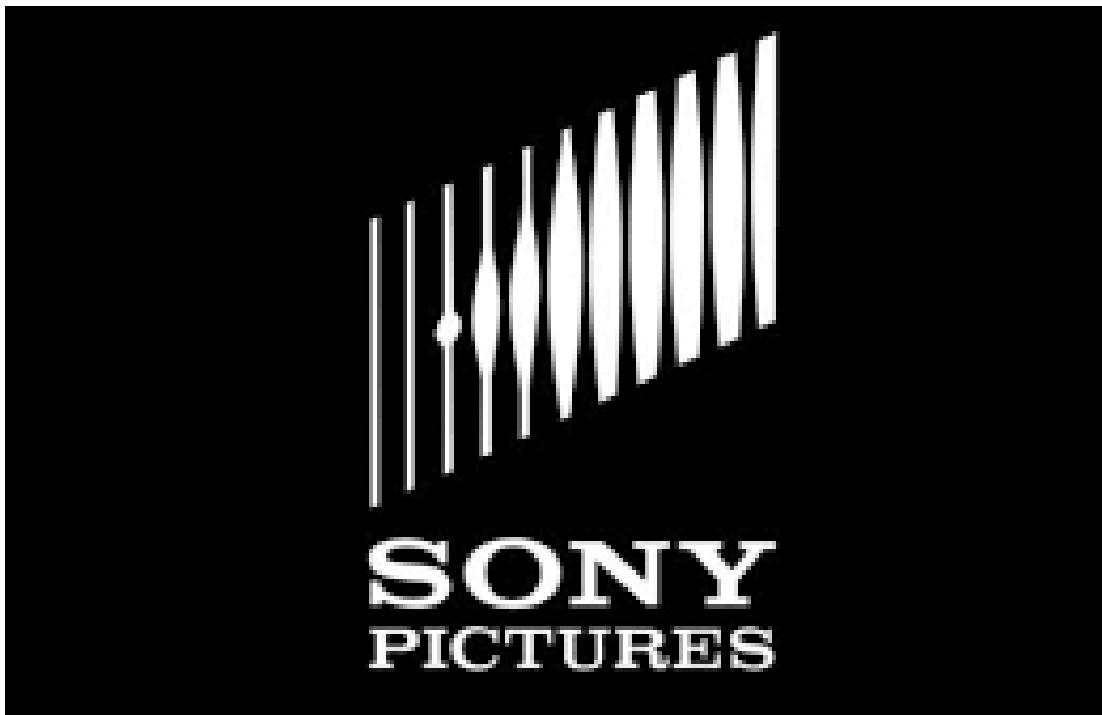
- Escaner de vulnerabilidades más duro
- AcuMonitor y AcuSensor
- C++
- Una de las soluciones más rápidas



SQLi Dumper

- Escanea apps web en busca de inyecciones SQL
- Utiliza un proceso con varios pasos en cada fase

EJEMPLOS DE CASOS REALES



Incidente en Sony Pictures

- Ataque 2011:
 - Atacante: Grupo de hackers LulzSec.
 - Objetivo: Sony Pictures, mediante inyección SQL.
- Impacto:
 - Fuga de información confidencial, correos y películas no estrenadas.
 - Afectación global en la industria del entretenimiento.

Brecha en Yahoo!

- Ataque 2012:
 - Atacante: D33Ds Company, aprovechando inyección SQL.
- Impacto:
 - Afectó a 450,000 usuarios de Yahoo! globalmente.
 - Víctimas incluyeron usuarios comunes y pequeñas empresas.
 - Los datos comprometidos incluyeron nombres de usuario, direcciones de correo electrónico y contraseñas.

Base de Datos de Salud de Estonia

- Ataque 2020
 - Atacante: Desconocido.
 - Objetivo: Base de Datos Central de Salud de Estonia.
 - Método: Ataque de inyección SQL.
- Impacto:
 - Compromiso potencial de historiales médicos de casi todos los ciudadanos.
 - Brecha a nivel nacional.
 - Daño financiero no revelado.
 - Sacudió la confianza pública.



BUENAS PRÁCTICAS

Consultas concatenadas

Sin parámetros:

`"SELECT * FROM users WHERE username = 'admin' AND password = '1234';"` 

Con parámetros:

`"SELECT * FROM users WHERE username = :username AND password = :password;"` 





BUENAS PRÁCTICAS

Utilizar tablas separadas para datos sensibles.

Utilizar funciones hash para almacenar contraseñas.

Utilizar procedimientos almacenados.

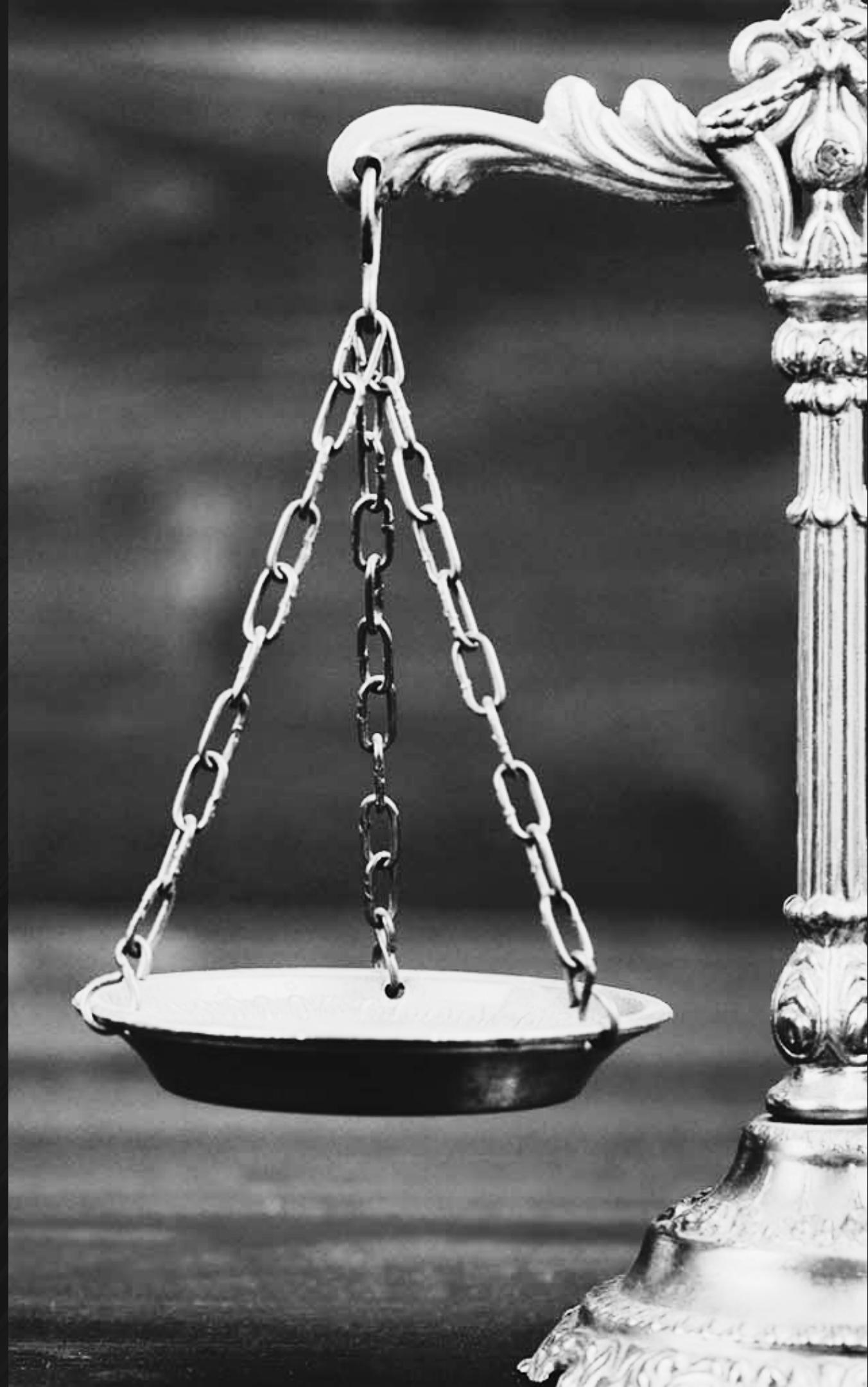
Utilizar cifrado para proteger los datos.

MARCO LEGAL

La Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Delitos penados

- 1.Robo de datos personales (artículo 197.1 del Código Penal).
- 2.Daños informáticos (artículo 264 del Código Penal).
- 3.Amenazas (artículo 169 del Código Penal).
- 4.Coacción (artículo 172 del Código Penal).



FUTURO DE LOS ATAQUES DE INYECCIÓN SQL

Desafío en Seguridad AI/ML

- Rápido avance tecnológico crea complejidades en seguridad.
- Ataques de inferencia en IA y Machine Learning (ML) son un desafío crítico.

Amenazas de Inferencia

- Ataques de membresía buscan datos de entrenamiento o comprender funcionamiento interno.

Contexto de ML

- Sistemas ML utilizan datos de entrenamiento para mejorar toma de decisiones.
- Despliegue de API públicas con datos sensibles.

Mitigación de Riesgos

- Limitaciones en API para detectar consultas maliciosas.
- Integración de pruebas de penetración en actividades regulares de seguridad.

GRACIAS

