OWASP LatamTour
Chile 2011

The OWASP Foundation
http://www.owasp.org

OWASP
Seguridad de Acceso a Datos
2011

David Sutherland
Socio Consultor Datactiva

dsutherland@datactiva.cl

Temario

- Introducción.
- Control de Acceso.
- Seguridad en el Desarrollo
  - Construcción: Persistencia de Datos.
  - Testing: Encriptación y Enmascaramiento de datos.
  - Producción: Perfiles y Roles, Limitación de Recursos.
- Conclusiones

2

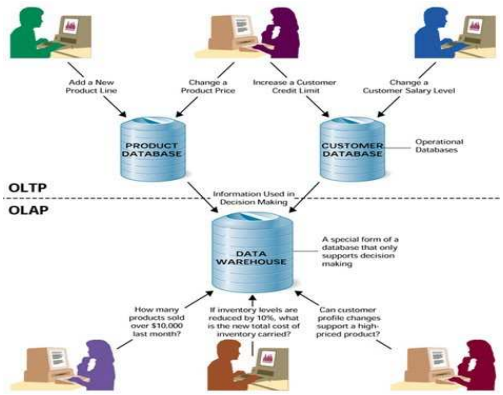
Introducción

- Los servidores de Base de Datos, poseen uno de los recursos más importantes de una compañía: los datos.
- Ellos almacenan información vital del negocio, detalle de clientes, información financiera, información de recursos humanos, etc.

3

Control de Acceso

- El control de acceso es uno de los puntos importantes dentro de la Seguridad. Esto se debe llevar a cabo en diversas áreas:



- ✓Sistema Operativo
- ✓Sistema de Base de Datos
- ✓Entornos de desarrollo
- ✓Aplicaciones de usuario
- ✓Aplicaciones Remotas

4

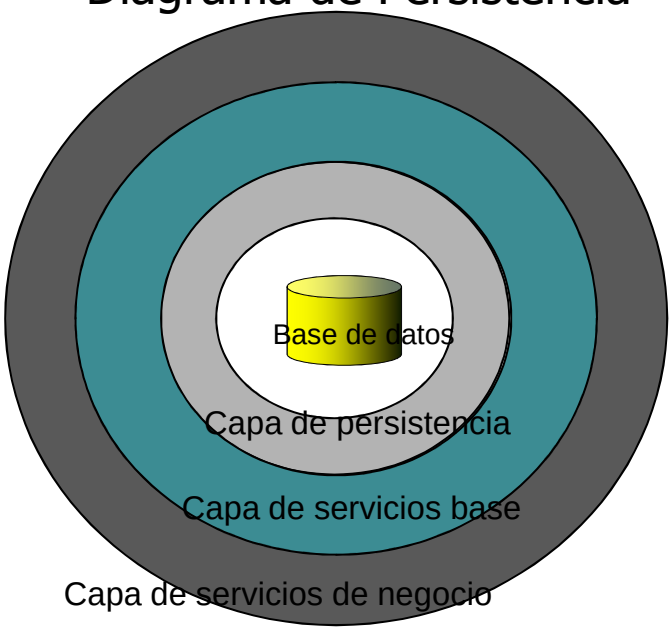
Seguridad en la Construcción
Ofuscamiento y Persistencia de Datos

- El ofuscamiento permite ocultar información acerca de cómo están desarrolladas las aplicaciones, y a qué datos acceden. También es posible, en algunos sistemas, encriptar o dejar en código de máquina el código fuente.

- La persistencia permite controlar el acceso a los datos a niveles discretos y con distintos privilegios.
  - ✓ Servicios que accedan a una cierta porción de datos
  - ✓ Operaciones bien definidas y acotadas
  - ✓ Reutilizados por las distintas áreas de la organización.

5

Diagrama de Persistencia



6

Seguridad en Testing

Encriptación y Enmascaramiento de datos.

- La encriptación de datos permite ocultar la información contenida en la base de datos, haciéndola ininteligible para quien no tenga la clave de desencriptación.
- El enmascaramiento permite ocultar algunos datos sensibles de una base de datos, para uso de pruebas, así como de toma de muestras de datos.

7

Alternativas de Encriptación.

- Encriptación en la base de datos:
  - Definición (en su creación) de columnas de datos encriptadas.
  - Servicios y funciones de encriptación propias del motor de base de datos.
- Encriptación de los Respaldos.

Enmascaramiento
¿Qué es?

Es la acción de proteger datos de clientes, financieros o de la compañía; para crear nuevos datos legibles, los cuales retendrán las propiedades de los datos, como son ancho, tipo y formato.

Rut	Nombre	Apellido	Nro. Cuenta	Banco
15.234.454-1	Carlos	Allendes	3456789-7	Boston
10.567.555-5	José	Castillo	6756778-8	International
11.534.888-k	David	Sutherland	3455656-0	London Bank

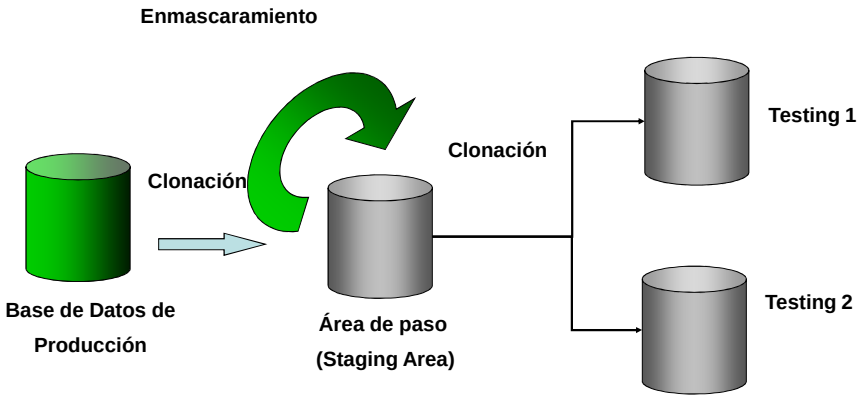
Rut	Nombre	Apellido	Nro. Cuenta	Banco
15.234.454-1	David	Allendes	3333333-1	Boston
10.567.555-5	José	Sutherland	8888888-5	International
11.534.888-k	Carlos	Castillo	7777777-3	London Bank

Enmascaramiento
¿Para qué?

Cuando los datos son compartidos con terceros, sin revelar información importante.

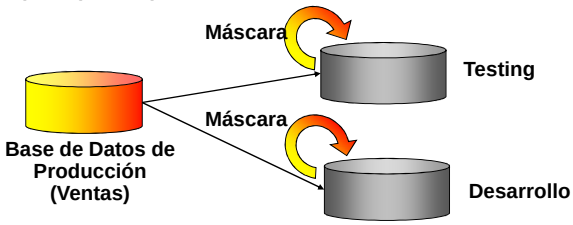
Para proteger la data confidencial en ambientes de test, QA o cuando los datos son usados por desarrolladores.

Modelo de Despliegue

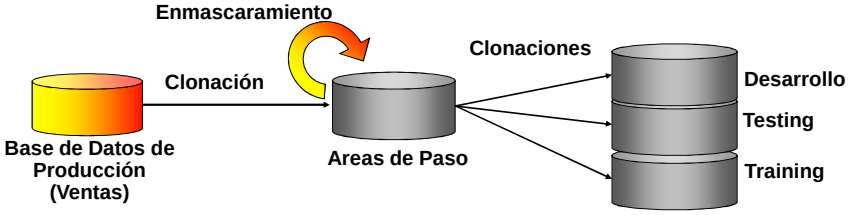


Modelo de Despliegue

Sin área de paso (directo) :



Utilizando Area de Paso (Staging Area):



Un algoritmo simple de enmascaramiento

1. Detectar tablas a enmascarar, ¿Cómo?, revisando aquellas que tengan típicamente más hijos.
2. Para cada una de esas tablas (habitualmente no más de 5) definir el tipo y forma de enmascaramiento hacer:
    3. Para cada fila i de la tabla hacer
        - 3.1 Asignar a las columnas con un formato fijo (ej. Tarj. Crédito) , un valor aleatorio (con ese formato)
        - 3.2 Leer fila j y k aleatoriamente
        - 3.3 Intercambiar columnas definidas entre filas i, j y k
        - 3.4 Grabar fila i con nuevos valores
4. Fin.

13

Otras Formas

- **Enmascaramiento Compuesto:**
  Conjunto de columnas enmascaradas juntas,
  Ej: ciudad, país, dirección, teléfono, código postal.
- **Enmascaramiento condicionado:**
  Especifica un formato de máscara distinto para cada condición, Ej: un formato de máscara diferente de acuerdo al código de país.
- **Clonado Integrado + Flujo de enmascaramiento:**
  - Crea BDD clonada para test a partir de BD productiva.
  - Soporte para SQL post-clonación, ej: cambio de password.

Máscaras definidas por el usuario

- Organizaciones con necesidades especializadas de enmascaramiento pueden crear formatos de máscaras definidas por ellos mismos.
- Estos formatos se definen utilizando herramientas del motor de base de datos, proveyendo un alto grado de flexibilidad en la generación de formatos de máscaras apropiados para la industria. Por ejemplo, instituciones financieras utilizan complejos algoritmos para generar números de cuenta para evitar fraudes.
- Con los formatos definidos, estas instituciones pueden generar números de cuentas ficticias para reemplazar los datos originales, sin dejar de lado el estándar de seguridad.

Enmascaramiento Determinista

- Algunas organizaciones tienen la obligación de proporcionar enmascaramiento coherente dentro, y a través de las bases de datos (enmascaramiento determinista).
- Por ejemplo, una empresa puede mantener un número de cliente en una relación de gestión de clientes de su CRM, una aplicación financiera de su ERP y un data warehouse personalizado.

Enmascaramiento Compuesto

- Consiste en el enmascaramiento de datos que se componen de dos o más elementos.
- Por ejemplo, una dirección compuesta, se puede conformar por una dirección, ciudad, código postal y país. En este caso, las aplicaciones esperan que el enmascarado sea coherente, es decir, los elementos de datos que componen la dirección resultante deben conservar el tipo y la estructura válida.



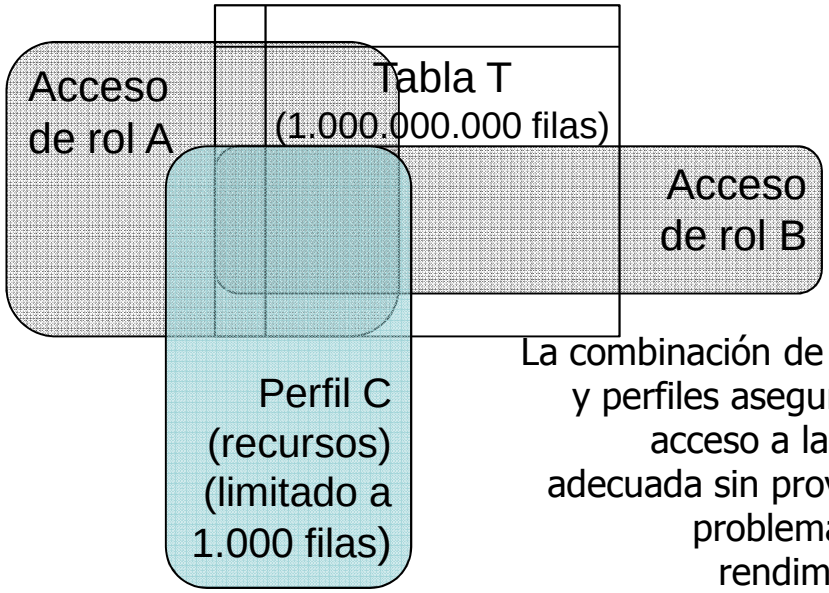
Seguridad en Producción

Perfiles y Roles, Limitación de Recursos

- Los Perfiles y Roles permiten definir el alcance y las limitaciones que tendrá un usuario o un grupo de usuarios en una base de datos.
- Se definen accesos sobre porciones de la base de datos con distintos privilegios.
- Los recursos se pueden limitar en términos de cantidad de sesiones, cantidad de espacio, uso de la CPU, etc.

18

Roles y Perfiles



La combinación de roles y perfiles asegura un acceso a la data adecuada sin provocar problemas de rendimiento

19

Conclusiones

- Es posible implementar seguridad en el acceso a los datos, a través de la Persistencia de Datos y el Ofuscamiento de código fuente, encriptación y enmascaramiento de los datos, así como del establecimiento de Roles, Privilegios y Limitación de Recursos.
- Justificación: necesidad creciente de compartir datos de producción con usuarios internos y externos, con una variedad de propósitos comerciales, tales como: Testing de productos, Testing de aplicaciones e Investigación de mercado.
- OWASP, es una organización que promueve el estudio y la investigación acerca de nuevas tecnologías y mejores prácticas enfocadas hacia la administración y optimización en la seguridad del acceso a los datos.

20


Muchas Gracias!
dsutherland@datactiva.cl
The OWASP Foundation
www.owasp.cl