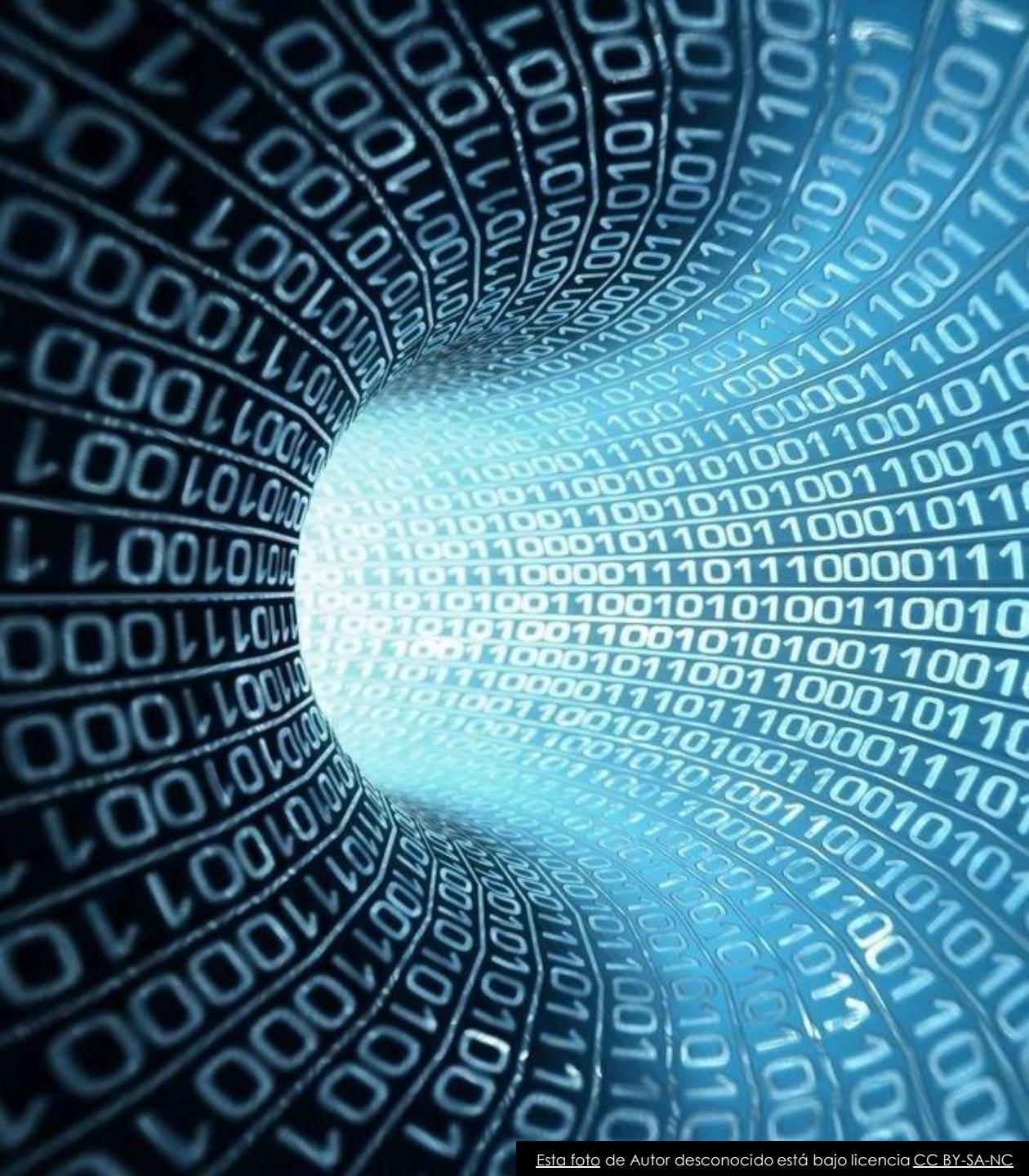


Bases de datos 2

Clase 4

Kevin Morán

bases2.fiusac@gmail.com



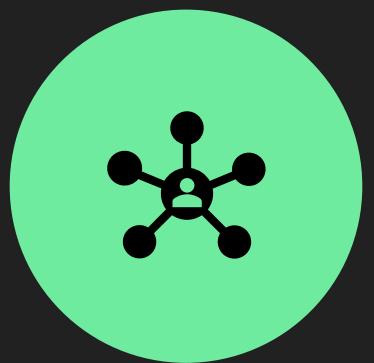
SEGURIDAD(2)

ORACLE®

D A T A B A S E

Seguridad de la información

- La seguridad informática es el área que se encarga de plantear normas, técnicas y procedimientos para proteger la información, a nivel de recursos de software, hardware y también humanos, en los que se apoyan los procesos críticos de una organización. La seguridad de la información está relacionada con el asegurar la **confidencialidad, integridad y disponibilidad** en la manipulación de la información, buscando minimizar riesgos y amenazas, con la aplicación de buenas prácticas, estándares y normativas de seguridad.



DISPONIBILIDAD: ASEGURAR QUE LOS USUARIOS AUTORIZADOS SIEMPRE TENGAN ACCESO A LA INFORMACIÓN QUE REQUIERAN. SE GARANTICE QUE LA INFORMACIÓN SEA PUNTUAL Y CON SUS RESPECTIVOS PRIVILEGIOS PARA ACcedER A LA INFORMACIÓN.



INTEGRIDAD: GARANTIZAR QUE LA INFORMACIÓN DEL SISTEMA NO SEA ALTERADA POR USUARIOS NO AUTORIZADOS CON EL FIN DE EVITAR LA PÉRDIDA DE CONSISTENCIA DE INFORMACIÓN.



CONFIDENCIALIDAD: BUSCA QUE LA INFORMACIÓN PRIVADA NO SE REVele A USUARIOS O TERCEROS NO AUTORIZADOS.

Normas / Estándares en seguridad en bases de datos

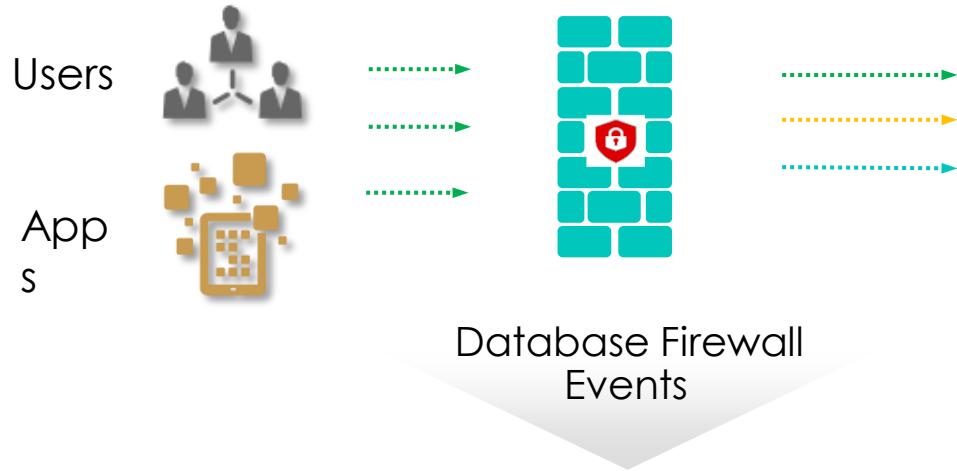
- COBIT: Objetivos de control para la información y tecnologías relacionadas. Es un conjunto de mejores prácticas y controles que permite auditar la gestión de los sistemas de información y tecnología desarrollado por la Asociación de Auditoría y Control del Sistema de Información ISACA.
- BIS: Instituto Británico de Estándares. Brinda normas que tiene como objeto la estandarización de procesos, enfocado en la característica de seguridad de la información: Auditoria, certificación y formación.
- Normas ISO: International Standards Organization. Proporciona normas para la administración, mantenimiento y continuidad de la seguridad de la información; enmarcada en las normas de la familia ISO/IEC 27000, como la ISO/IEC 27001 y su anexo ISO/IEC 27002.
- HIPAA: Health Insurance Portability and Accountability Act (Ley de Portabilidad y Contabilidad de los Seguros de Salud), conjunto de reglas relacionada con el manejo de la confidencialidad de la información.

Seguridad en base de datos Oracle

- La Base de datos Oracle dispone de opciones y soluciones, que facilitan el cumplimiento a regulaciones y normativas de seguridad, según la documentación oficial de Oracle, en su documentación técnica describe mecanismos de seguridad a nivel de:

Oracle Data Vault

- Sistema de Control de Accesos, Gestión de privilegios y Revisión de derechos de acceso a usuarios. Oracle permite el manejo de opciones de administración de usuarios, privilegios y roles. Para esto adicionalmente cuenta con el producto de seguridad Oracle Database Vault".



[Home](#) [Secured Targets](#) [Firewalls](#) [Hosts](#) [Settings](#)[Home](#) > [Secured Targets](#) > Register Secured Target**Secured Targets**[Targets](#)[Groups](#)[Access Rights](#)**Monitoring**[Audit Trails](#)[Enforcement Points](#)**Register Secured Target****New Secured Target Name ***

Linux

Description

OEL 6.0

Secured Target Location *

192.168.56.30

Secured Target Type *

Oracle Database

User Name

IBM DB2 LUW

Password

Microsoft SQL Server

Enter Password

Add Secured Target Addresses**Hostname / IP Address****Port Number****Service Name**

Sybase ASE

MySQL

Sybase SQL Anywhere

Microsoft Windows

Microsoft Active Directory Server

Oracle Solaris

Oracle ACFS

Linux

- Predefined reports
- Interactive browsing
- Build custom reports
- Report scheduling and notification
- Report attestation

ORACLE® Audit Vault Server

Home Secured Targets Reports Policy Settings

Home > Reports > Compliance Reports

Built-in Reports

- Audit Reports
- Compliance Reports
- Specialized Reports
- Custom Reports
- Uploaded Reports
- Interactive Reports

Report Workflow

- Report Schedules
- Generated Reports

Quick Links

- Audit Trails
- Enforcement Points

Payment Card Industry (PCI) Reports

Gramm-Leach-Bliley Act (GLBA) Reports

Health Insurance Portability and Accountability Act (HIPAA) Reports

Sarbanes-Oxley Act (SOX) Reports

Data Protection Act (DPA) Reports

To associate Secured Target(s) with this Compliance Category, click on the Go button **Go**

Activity Overview	Digest of all captured audit events for a specified period of time			
Data Access	Details of audited read access to data for a specified period of time			
Data Modification	Details of audited data modifications for a specified period of time			
Database Schema Changes	Details of audited DDL activity for a specified period of time			

Policy

Audit Settings

Firewall Policy

Alerts

Alerts

Quick Links

Audit Trails

Enforcement Points

Modify Alert

Name * NonHRAppAccessJOBS

Secured Target Type Oracle Database

Severity * Critical

Threshold (times) * 1

Duration (min) * 0

Group By (Field) - Select Field -

Status * Disabled

Description
Alert me when non-HR app is accessing HR.JOBS table

51 of 255

Condition *

```
:TARGET_OBJECT like '%JOBS%' and :USER_NAME NOT LIKE '%HR%'
```

Condition - Available Fields

ACTION_TAKEN

AV_TIME

CLIENT_HOST_NAME

CLIENT_IP

CLUSTER_TYPE

COMMAND_CLASS

ERROR_CODE

ERROR_MESSAGE

EVENT_NAME

EVENT_STATUS

EVENT_TIME

NETWORK_CONNECTION

OSUSER_NAME

SECURED_TARGET_NAME

TARGET_OBJECT

TARGET_OWNER

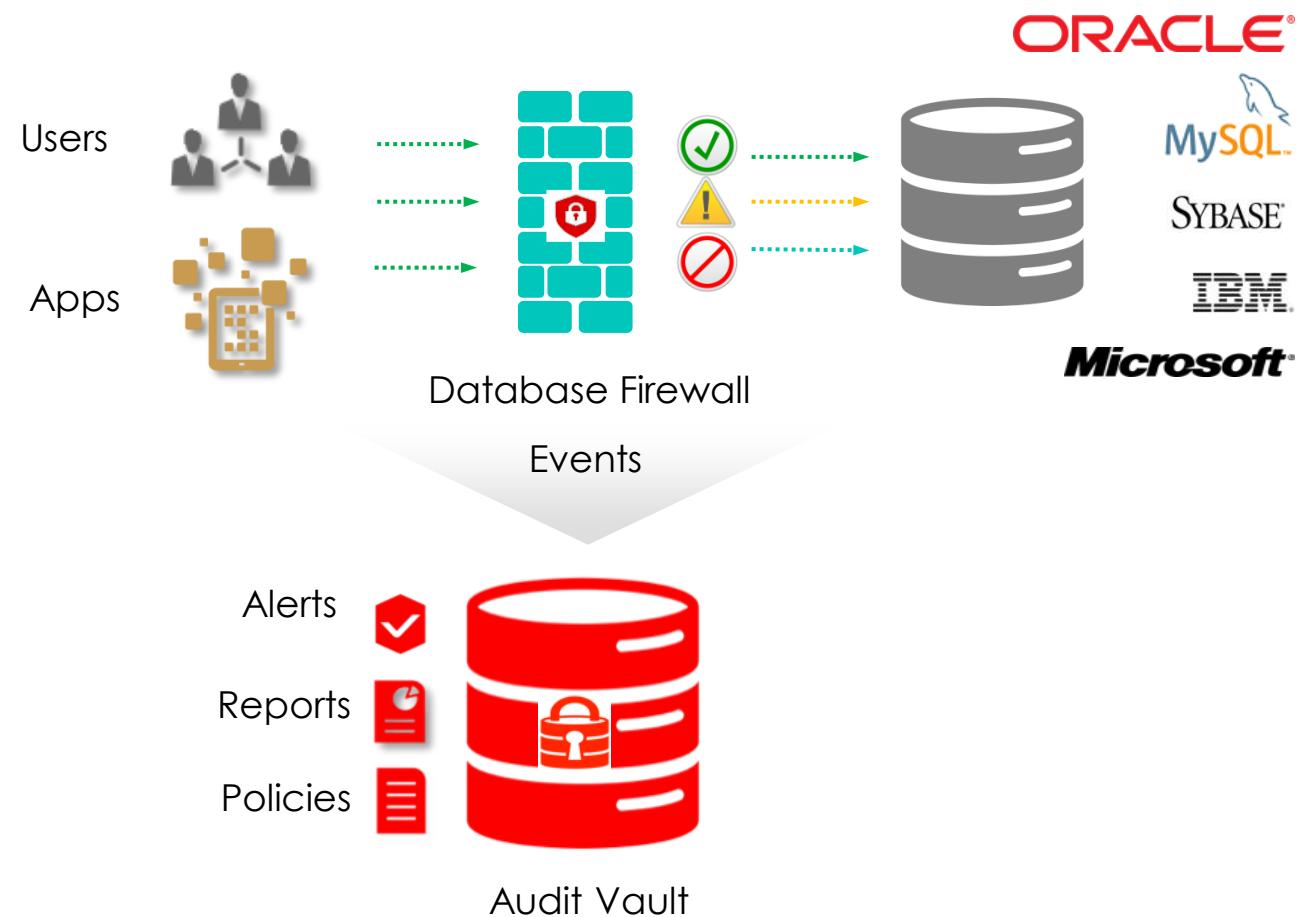
TARGET_TYPE

THREAT_SEVERITY

USER_NAME

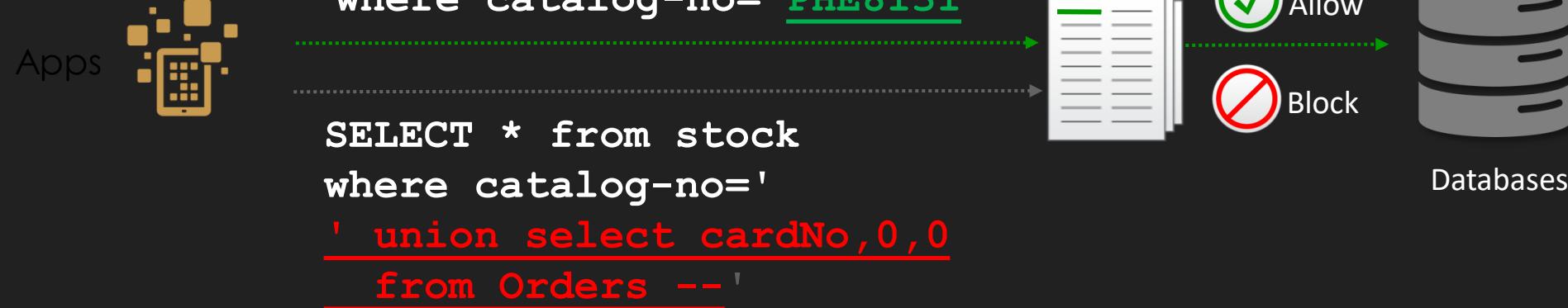
DATABASE FIREWALL

- Monitor user activity from network
- Detect and block unauthorized activity
- Detect and block SQL injection attacks
- Advanced grammatical SQL analysis
- Positive and negative security model
- Scalable software appliance



DATABASE FIREWALL

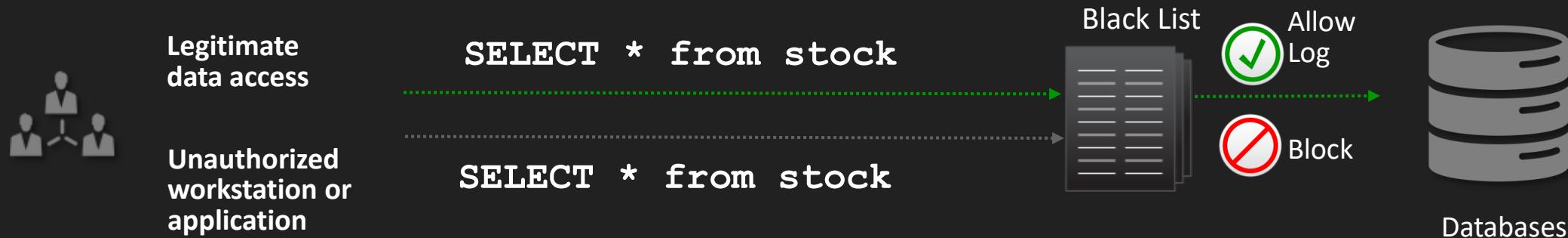
Anomaly detection and threat blocking with positive security model



Block out-of-policy SQL statements from reaching the database
Automated white list generation for any application
Define permitted SQL behavior per user or application

Database Firewall

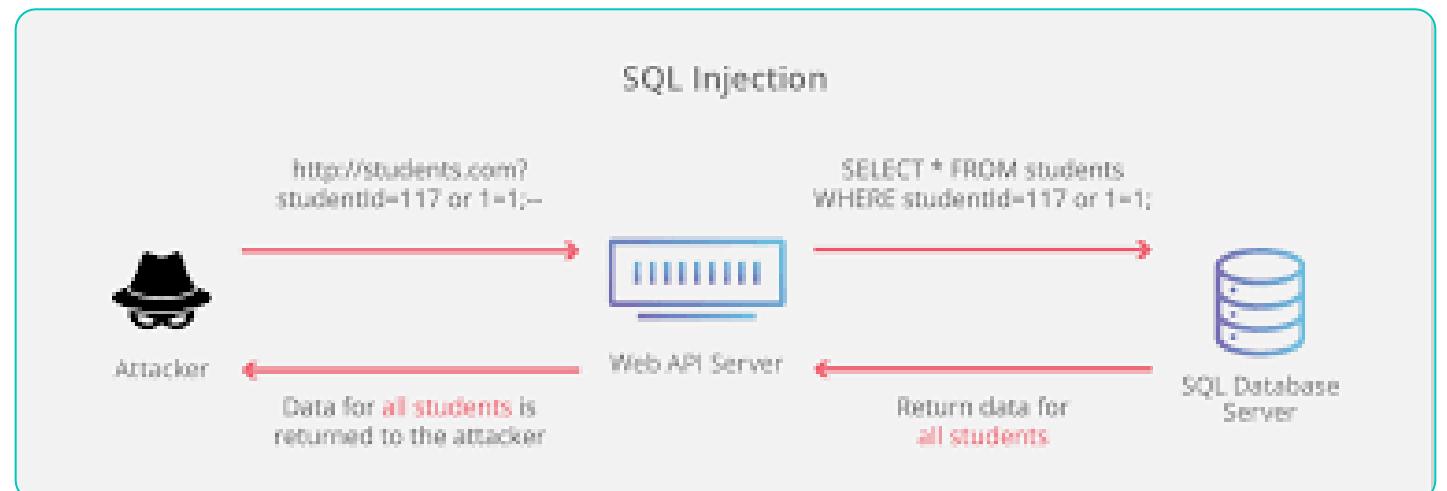
Enforcing behavior with negative security model



Block specific unauthorized SQL statements, users or object access
Blacklist on session factors: IP address, application, DB user, OS user

SQL injections

- Para protección contra ataques de SQL Injection, Oracle dispone del productos como “Bind Variables”, que permite el manejo de datos dinámicos dentro de instrucciones de consulta SQL; Oracle cuenta con opciones para validar las direcciones IP desde donde se puede acceder a la información. Soluciones como Oracle Virtual Private Database (VPD) y Oracle Label Security (OLS), disminuyen la cantidad de información que puede ser afectaba por SQL Injection.



Sin variables Bind:

```
int subsidiary_id;
Statement command = connection.createStatement(
        "select first_name, last_name"
        + " from employees"
        + " where subsidiary_id = " + subsidiary_id
    );
```

Con variables Bind:

```
int subsidiary_id;
PreparedStatement command = connection.prepareStatement(
        "select first_name, last_name"
        + " from employees"
        + " where subsidiary_id = ?"
    );
command.setInt(1, subsidiary_id);
```

Ver también la documentación de la clase: [PreparedStatement](#).

Auditoría

- Gestión de Comunicaciones y Operaciones, Registro de auditorías, Supervisión de uso del sistema, Protección de la información de registro. Para esto Oracle cuenta con mecanismos de activación de pistas de auditorías. Cuenta con una serie de comandos para auditar los cambios en la base de datos, tanto DDL (create, alter, drop) como DML (insert, update, delete)

Controles Criptográficos.

- Controles Criptográficos. Oracle dispone de controles a este nivel como: Transparent Data Encryption (TDE) que permite la encriptación transparente de datos. Network encryption: Para el cifrado de red, con estándares de encriptación (RC4, DES, AES). Integrity of information: Asegurando que los mensajes no se modifiquen en su tránsito. Strong authentication, soportando diferentes métodos de autenticación como Kerberos, RADIUS (Remote Authentication Dial-In User Service), Secure Sockets Layer (with digital certificates), PKI .

Vulnerabilidades en bases de datos

- Mecanismos de seguridad débiles en la configuración de perfiles. Perfiles con demasiados privilegios y que no son utilizados
- Autenticación como usuario administrador SYSDBA, sin asignación de contraseña. Una vez instalada la base de datos Oracle, se crea por defecto el usuario que creó la Base de datos rol SYSDBA. Este usuario puede acceder la base de datos sin necesidad de usar contraseña.
- Usuarios y contraseñas creados por defecto en la instalación de Oracle, algunos con privilegios de DBA, y que facilitan el acceso de atacantes cuando no son cambiados o eliminados.

Vulnerabilidades en bases de datos (2)

- Algoritmos de verificación de contraseña débiles, que permiten al atacante la fácil identificación de credenciales usuarios, permitiendo acceder e penetrar en la seguridad de la Base de datos. <https://howsecureismypassword.net/>
- Debilidades en los aplicativos que faciliten ataques de SQL Injection , como cadenas de conexión a la base de datos con usuario y contraseña explicitas en el código fuente , sentencias SQL construidas dinámicamente , mensajes de error que revelen información de la Base de datos. Otro aspecto que facilita los ataques SQL Injection, es el bajo nivel de seguridad en los procedimientos realizados por el lenguaje de programación propio de ORACLE, PL/SQL.
- Desbordamiento de buffer, causadas por fuentes de entrada masivas con valores diferentes o muy superiores a los que se espera en la aplicación. Se debe tener en cuenta la actualización de parches en el software de la base de datos que brinda el proveedor, para solucionar vulnerabilidades encontradas en sus versiones.

Vulnerabilidades en bases de datos (3)

- Utilización de mecanismos débiles de cifrado de la información de la base de datos.
- Débil configuración de privilegios a usuarios sobre objetos de la base de datos o sistema.
- Proceso TNS listener (transparent network substrate) desprotegido, ya que es posible acceder de forma fácil a información de la instancia de la Base de datos (bases de datos almacenadas, IP de servidores de Base de datos, puertos).

Vulnerabilidades en bases de datos (4)

- Falta de capacitación en las políticas de seguridad de la empresa a los usuarios de la base de datos en la administración de contraseñas.
- Falta de mecanismos de monitoreo en la base de datos débiles, que permitan identificar a tiempo posibles fallas y aplicar las correcciones respectivas.
- Débil configuración de mecanismos de auditoria, que no faciliten el rastreo de ataques y detectar amenazas de seguridad, esto coloca en alto riesgo la seguridad de los datos.

Vulnerabilidades en bases de datos (5)

- Cuando los datos críticos del negocio en la base datos no cuentan con controles y mecanismos de seguridad de cifrado dejándola expuesta a amenazas.
- Configuraciones de respaldo débiles, que no permitan ejecutar la recuperación rápida y con la menor pérdida posible de información en caso de falla o ataque a la información.

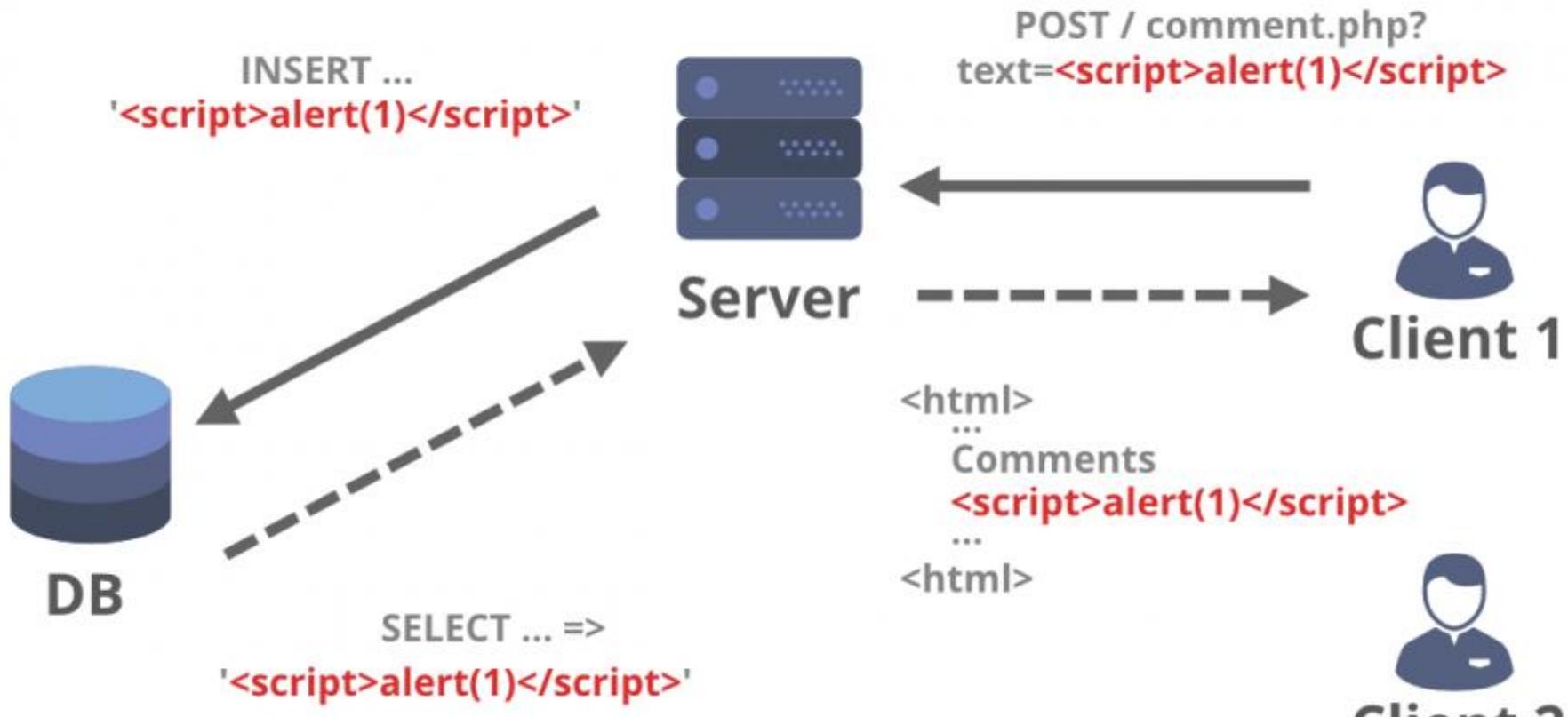
Tipos de ataques



Ataques por técnicas de inyección de scripts

- Este tipo de ataque se presenta al injectar código o datos en una línea de comando o consulta; Entre estos tipos de ataques se encuentran: Cross site scripting (XSS), Cross site request forgery (CSRF) y clickjacking.
 - Cross site scripting (XSS): consiste en introducir código Javascript a una aplicación WEB con vulnerabilidades, con la finalidad de robar información, apropiarse de sesiones activas, corromper el navegador web y como consecuencia afectar la integridad del sistema.
 - Un ejemplo de este tipo de ataques es la suplantación de identidad o phishing, a través del direccionamiento del acceso a páginas, sitios web, servidores, este tipo de ataque se basa en la confianza del usuario tiene sobre el sitio frecuentado.
 - Cross site request forgery (CSRF): falsificación de petición en sitios cruzados. En este tipo de ataque CSRF, usa un usuario o dirección IP de usuarios validados para el sistema, generando que el usuario realice acciones no deseadas en sitios remotos. Este tipo de ataque, dado que se realiza con un usuario propio, dependiendo de los privilegios con lo que cuente el usuario en el sistema sería la magnitud del ataque que puede causar.
 - Clickjacking: este tipo de ataque pretende engañar al usuario para que accedan a través de un clic sobre links. De esta forma el atacante obtiene información, logrando causar ataques de tipo CSRF (Cross-site request forgery).Este tipo de ataque superpone páginas, en lugares donde habitualmente el usuario accede.

Cross Site Scripting(XSS)



Ataques de Path Transversal

- Los ataques que se basan en esta técnica, van dirigidos a lograr conseguir acceso a ficheros del servidor, carpetas fuera de donde se encuentra alojada la aplicación, explota la vulnerabilidad que se ocasiona cuando no existe seguridad en cuanto a la validación de usuarios en la aplicación, o no cuenta con controles de manejo de errores controlados, que impidan la salida de errores por defecto, que normalmente muestran rutas del archivo afectado donde se provocó el error. De esta forma se accede a ficheros a los cuales un usuario no debería tener acceso, logrando acceder a información crítica.

```
<?php
$template = 'blue.php';
if ( isset( $_COOKIE['TEMPLATE'] ) )
    $template = $_COOKIE['TEMPLATE'];
include ( "/home/users/phpguru/templates/" . $template );
?>
```

```
GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../etc/passwd
```

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache
```

```
root:fi3sED95ibqR6:0:1:System Operator:/bin/ksh
daemon:*:1:1::/tmp:
phpguru:f8fk3j10If31.:182:100:Developer:/home/users/phpguru/bin/csh
```

Ataques de inyección de SQL

- Los ataques de inyección SQL consisten en la modificación de datos de ingreso a través de inserción de consultas o sentencia SQL.
- Con este tipo de ataque se pretende por lo general obtener información la base de datos, modificar datos, realizar operaciones de administración, entre las acciones más buscadas se destacan
 - Saltar restricciones de acceso.
 - Elevar privilegios.
 - Obtención de información de la base de datos
 - Detener servicios de del gestor de base de datos.
 - Ejecución de sentencias SQL dentro del servidor

Ataques de inyección SQL

- Esta técnica se basa en ejecutar operaciones directamente a la base de datos. Este tipo de técnica, aprovecha debilidades en:
 - Comprobación de parámetros de entrada
 - Comprobación de parámetros utilizados en códigos SQL
 - Construcción de sentencias SQL, dinámicas
 - En la construcción de código PL/SQL en el caso de Oracle

Con esta técnica se posibilita al atacante:

- Acceder a información sin autorización de la base de datos tales como registros y objetos.
- Elevación de privilegios, accediendo con credenciales de usuarios con mayores privilegios y alterando permisos.
- Denegación de servicio, la modificación de sentencias SQL, puede llevar a cabo acciones que provoquen destrucción a nivel de: borrado de datos y/o objetos, detener servicios. Al igual que ejecutar sentencias que generen lentitud en las respuestas del sistema hasta colapsarlo.
- suplantación de usuarios: cuando el atacante puede acceder a la información de credenciales de usuarios, es posible que pueda tomar alguna y ejecutar procesos usando las credenciales robadas

Ataques de inyección de ficheros

- Este tipo de ataques permite la inclusión de archivos remotos o locales, debido a debilidades en el código de programación de la aplicación, por falta de filtros. Esto permite que se puedan modificar parámetros o archivos del sistema, comprometiendo la seguridad. Por ejemplo modificación de archivo de contraseñas. Este tipo de ataques puede darse por inclusión de archivo remotos, inclusión de archivos locales o Webtrojans. Estos últimos que se dan cuando la página permite subir archivos como imágenes, documentos, pdf, videos y no cuentan con mecanismo de comprobación del tipo de archivo enviado, permitiendo la llegada al servidor de archivos malintencionados.

Tarea no. 2

- Investigar sobre las pruebas de seguridad en una base de datos (Pruebas de caja negra y pruebas de caja blanca) y presentar recomendaciones para la realización de dichas pruebas en una organización.
 - Definición
 - Ejemplos
 - Ventajas
 - Desventajas
- Entrega: Lunes 14/06 11:59 p.m.

Nota: Recordar no solo copiar y pegar, si no que utilizar opiniones personales.