# Memoria de Prácticas

Daniel Carrera Bonilla.

## Revisión y sanitización de vulnerabilidades de inyección de código en sentencias SQL en PHP

### Motivación

#### ¿Cómo funciona una inyección SQL?

### Una **inyección SQL** es una técnica de ataque en la que un atacante inserta o "inyecta" código SQL malicioso en una consulta que la aplicación envía a la base de datos. Este tipo de ataque aprovecha las vulnerabilidades en la validación de entradas de usuario, permitiendo al atacante ejecutar comandos SQL no autorizados. Por ejemplo, si una aplicación web permite a los usuarios ingresar datos sin una adecuada sanitización, un atacante podría insertar código SQL en un campo de entrada, como un formulario de inicio de sesión, para acceder a información confidencial, modificar datos o incluso eliminar tablas completas. La prevención de inyecciones SQL incluye prácticas como el uso de consultas preparadas, la validación y sanitización de entradas de usuario, y la implementación de controles de acceso adecuados.

### Pasos seguidos para la sanitización y puesta a punto

#### Detección de posibles sentencias afectadas

Al contar con numerosos programas que se pueden ver afectados por este tipo de casos, sería inviable la búsqueda de estas sentencias de una forma manual. Es por ello, que gracias a un script en el lenguaje PYTHON se estableció la búsqueda y detección de estas, mediante búsquedas iterativas para las variables pasadas por GET o POST, y que posteriormente dichas variables se usasen en sentencias SQL.

#### Análisis y sanitización de las sentencias afectadas

La **sanitización y puesta a punto** en estos programas PHP se ha llevado a cabo principalmente utilizando las funciones odbc\_prepare y odbc\_execute. Garantizando la seguridad y eficiencia en la interacción con bases de datos. A grandes rasgos los pasos a seguir han sido:

1. **Establecimiento de la Conexión ODBC**: Primero, se debe establecer una conexión con la base de datos utilizando odbc\_connect(). Este paso asegura que la aplicación pueda comunicarse con la base de datos de manera segura.
2. **Preparación de la Consulta**: Utilizando odbc\_prepare(), se prepara una declaración SQL con parámetros. Esto permite que la consulta sea parametrizada, evitando la inyección de SQL. Por ejemplo:

$stmt = odbc\_prepare($conn, 'SELECT \* FROM usuarios WHERE nombre = ?');

1. **Ejecución de la Consulta**: Una vez preparada la consulta, se ejecuta con odbc\_execute(), pasando los valores de los parámetros. Esto asegura que los datos de entrada sean tratados como parámetros y no como parte del código SQL. Ejemplo:

$nombre = 'Juan';

odbc\_execute($stmt, array($nombre));

1. **Sanitización de Datos**: Aunque odbc\_prepare y odbc\_execute ayudan a prevenir la inyección de SQL, es importante sanitizar los datos antes de utilizarlos en la consulta. Esto puede incluir la eliminación de caracteres especiales y la validación de formatos. Todo ello se ha podido realizar mediante el uso de funciones como **trim, odbc\_decode** u **odbc\_encode**
2. **Manejo de Resultados**: Después de ejecutar la consulta, se pueden manejar los resultados utilizando funciones como odbc\_fetch\_array() para obtener los datos de manera segura y eficiente.

#### Test post sanitización: pruebas a nivel local de la sentencia y global del programa entero

### Después de la sanitización de datos, es crucial que se realicen pruebas exhaustivas tanto a nivel local como global para asegurar que las sentencias SQL y el programa entero funcionen correctamente. Inicialmente, se han ido probando los distintos programas y archivos utilizando archivos locales, que actúan como un entorno aislado. Estos archivos permiten ejecutar y verificar individualmente cada sentencia SQL sin afectar el entorno de producción.

### En casos más complejos, debido a la naturaleza de las funcionalidades y su interdependencia, se ha creado un entorno de pruebas más robusto. Este entorno cerrado nos ha permitido simular todas las funcionalidades del programa en un ambiente controlado. Aquí, se pueden realizar pruebas integrales que incluyen la inserción, eliminación, actualización y combinación de datos, garantizando que todas las operaciones se ejecuten correctamente y sin errores. Este enfoque asegura que cualquier cambio o actualización en el código no afecte los programas y datos en el entorno real, proporcionando una capa adicional de seguridad y confiabilidad antes de la implementación final.

### Pasos finales

#### Control de los cambios realizados: Excel y logs de cambios

### A medida que se iban aprobando los cambios, hemos procedido a documentar meticulosamente cada modificación tanto en el archivo Excel como en el log de cambios. En el Excel, hemos añadido nuevas filas y columnas para reflejar los ajustes realizados, asegurándonos de incluir detalles como la fecha, la descripción del cambio y el impacto esperado. Esta práctica ha permitido mantener una visión clara y organizada de la evolución del proyecto.

### Simultáneamente, en el programa que recoge los cambios en cualquier tipo de programa a nivel interno, hemos registrado cada actualización con precisión, proporcionando un historial detallado de las modificaciones. Este registro incluye información sobre quién solicitó el cambio, la razón detrás de la modificación y cualquier comentario adicional relevante. Al mantener ambos documentos actualizados, hemos garantizado una trazabilidad completa y una comunicación efectiva entre todos los miembros del equipo, facilitando la revisión y aprobación de futuros cambios.

## Control y revisión de procesos diarios, semanales y mensuales

## Desarrollo con WebFocus

### Desarrollo de procesos

#### Desarrollo proceso de carga de datos a través de fuente de datos csv

He llevado a cabo el desarrollo de nuevos procesos, que se suman a los ya existentes que son ejecutados cada día en un tramo horario específico.

Estos procesos vienen dados, o bien, por las necesidades especiales de algunos departamentos de la entidad que necesitan ser conocedores de dichos datos de forma diaria; o bien, por propia iniciativa del departamento que entiende que es necesario que esos datos estén disponibles.

De cualquiera de las formas el proceder del desarrollo de estos procesos se basa en primer lugar de saber y analizar la procedencia de los datos. Estos pueden venir de dados de documentos externos o bien de las tablas que se encuentran delegadas a los servicios informáticos de Madrid. En cualquiera de los casos, los datos deben ser procesados para que puedan ser almacenados y accedidos a través de las bases de datos internas de la entidad.

Cuando ya disponemos de las tablas en formato DB2, son manejables para nosotros. Ahí, entra el momento del análisis de qué es lo que estamos buscando. Debido a las numerosas posibilidades que se pueden encontrar en estas tablas, hay que ser meticulosamente cuidadosos a la hora de según qué campos se eligen y bajo que condiciones. Tras cualquier paso, se ha ido comprobando que los datos que se iban obteniendo podían casar con lo esperado.   
Otro de los condiciones a tener en cuenta especialmente, ha sido la elección de las fechas de los datos debido a los distintos casos que se podían dar.

En definitiva, he podido desarrollar diversos procesos que me han permitido poner a prueba mis conocimientos y destreza a la hora de afrontar problemas nuevos para mí. He tenido la oportunidad de trabajar en el desarrollo de procesos de distintos ámbitos como procesos que han involucrados propiedades, documentos legales, puntuaciones, movimientos, transferencias y operaciones de todas las clases.

## Mantenimiento de programas WebFocus y herramientas Report Caster

### Subida de procesos nuevos

Como comentamos en el punto anterior, uno de mis cometidos ha sido el desarrollo de nuevos procesos que se sumarían a los más de 50 procesos diarios que se reciben.

Una vez testeados y asegurado en línea que el funcionamiento del nuevo proceso es el esperado, se ha de proceder a la subida del mismo a la herramienta en línea IBI WebFocus, la cual se encargará de su ejecución en los tiempos y formas deseados.

En ella, se añade un nuevo proceso, configurándolo de forma que cuente con las especificaciones propias de este nuevo proceso. Teniendo que modificar para ello: su título, cuerpo del mensaje, su recurrencia (aunque sean procesos diarios se puede indicar de forma específica que haya días que no sean necesarios, por cualesquiera de las razones). También se modifica la distribución por el medio elegido de los resultados obtenidos tras la ejecución del mismo, por ejemplo, si son enviados por correo a quien o qué departamento/s quiero que lleguen dichos resultados.

### Mantenimiento y control de los distintos procesos y programas

#### Introducción

De igual forma, se cuentan con numerosos programas diarios, pero también cabe destacar que no son los únicos. Los procesos sobre los que he llevado el control se pueden clasificar como:

* Procesos diarios
* Procesos semanales o de fin de semana
* Procesos mensuales

##### Procesos diarios

Comentados anteriormente. Se ejecutan de forma diaria, programados a una cierta hora del día, ideada para que no existan conflictos entre ellos.

##### Procesos semanales o de fin de semana

Estos a diferencias de los diarios solo son ejecutados por normal general un día a la semana, o en algunos casos dos (sábado y domingo).

Son procesos que arrastran información que se van generando y guardando en las tablas a lo largo de la semana y cuyo procesamiento final se realiza al final de cada semana con el objetivo de actualizar la información semanalmente.

##### Procesos mensuales

Estos como su propio nombre indica son ejecutados de forma mensual con el objetivo, al igual que lo semanales, de actualizar mensualmente distintos ámbitos de la empresa y los datos que estos generan.

Cabe destacar que el control sobre estos procesos, al depender a su vez de otros muchos más pequeños (diarios y semanales) necesitan de un mayor control y consideración de condiciones para su correcta ejecución.

#### Control diario

#### Forma de actuación ante cualquier fallo

Día a día se deben recibir de forma general la confirmación vía correo electrónico de que los procesos se ejecutaron correctamente. Debido a los diversos factores que los condicionan, es posible que se reciba el correo, pero indicando su incorrecta ejecución o directamente ni se reciba.

Todo ello debe ser controlado de forma diaria, al igual que, en caso de contar con alguna falla, se debe proceder a su investigación de por qué el proceso no ha ido como se esperaba. De esta forma, cuando se detecten se ha de aislar el problema, identificado su origen y razonando su posible solución.

## Control de versiones (Gestión de Proyectos/Desarrollo)

### Motivación

Con el objetivo de llevar un control de los distintos cambios en programas, y de igual forma, para llevar control de la creación de nuevos, a través de un sistema interno se van anotando dichas acciones.

El control de todas las acciones que he ido realizando en el departamento es vital para una buena coordinación y seguimiento del trabajo tanto diario como general. En cualquier momento, dichas acciones pueden necesitar dar marcha atrás en cualquier cambio realizado. Revisar quién, cuándo y dónde ha realizado cualquier clase de modificación, ha creado nuevos archivos o cualquier otro tipo de acción realizada por los miembros del departamento es fundamental.

## Atención a peticiones interdepartamentales (SIGPEs)

### Introducción

### En nuestra organización, contamos con un sistema interno denominado **SIGPE**, que permite a cualquier departamento abrir una especie de ticket para enviar una solicitud a otro departamento. Este sistema facilita la comunicación y colaboración interdepartamental, permitiendo que las solicitudes, ya sean por problemas técnicos, necesidades operativas o peticiones específicas, sean gestionadas de manera eficiente y organizada. Al abrir un ticket en SIGPE, el departamento solicitante puede describir detalladamente la naturaleza de la solicitud, adjuntar documentos relevantes y establecer prioridades. El departamento receptor, por su parte, puede seguir el progreso de la solicitud, asignar tareas a los miembros del equipo y proporcionar actualizaciones sobre el estado de la petición.

### Asignación de peticiones

De forma general, en cada departamento, cuando llega una petición a través del sistema SIGPE, es fundamental que cada miembro del equipo sea conocedor de cuáles solicitudes deben encargarse. Esto se determina en función de su familiaridad con el tema o por otras razones específicas, como su experiencia previa o su rol dentro del departamento. Este enfoque asegura que las peticiones sean gestionadas por la persona más adecuada, optimizando así la eficiencia y la calidad de la respuesta.

En nuestro caso, las peticiones SIGPE se nos han ido asignando de manera gradual. Este método ha tenido como objetivo permitirnos aprender y conocer lo máximo posible sobre todos los tipos de funcionamientos internos del departamento. A través de esta exposición progresiva, hemos podido desarrollar una comprensión integral de los procesos y mejorar nuestras habilidades para gestionar una amplia variedad de solicitudes de manera efectiva.

## Extracción de datos complejos

### Otro de los casos que hemos encontrado frecuentemente son las peticiones de extracciones de datos complejos. A través de la apertura de SIGPEs, los distintos departamentos, en momentos puntuales, se enfrentan a la necesidad de obtener ciertos datos a los que no pueden acceder por sus propios medios. En estos casos, intervenimos nosotros, aprovechando nuestro acceso total a las diversas bases de datos. A través de un estudio previo, sus casos y necesidades, realizando un análisis previo de las tablas disponibles y evaluando las distintas posibilidades. A partir de este estudio, conformábamos la extracción correcta de los datos requeridos, asegurando que la información proporcionada cumpliera con sus expectativas y necesidades operativas. Proporcionándoles dichos datos en los formatos más idóneos para cada caso, siendo un caso común la generación de archivos EXCEL.

### Este proceso garantizaba que los departamentos pudieran obtener los datos necesarios de manera eficiente y precisa, facilitando así la toma de decisiones informadas y la resolución de problemas específicos.

## Uso y manejo en OFFICE 365: Word, Excel

### Durante nuestras tareas diarias, hemos debido aprender a manejar los distintos programas de Office 365 para diversas tareas y casos específicos. En Word, hemos utilizado herramientas de edición y formato para crear documentos profesionales, redactar informes y colaborar en tiempo real con otros miembros del equipo. La capacidad de insertar gráficos, tablas y comentarios ha sido esencial para mejorar la claridad y la presentación de la información.

### En Excel, el manejo ha sido más técnico y detallado, requiriendo el uso de funciones y casos específicos para realizar operaciones concretas. Me he desenvuelto en el uso de funciones para buscar y analizar datos de manera eficiente.

## Diseño y desarrollo de aplicaciones con herramientas de Bussiness Intelligence: Power BI

### Motivación

#### En nuestro departamento, contamos con una serie de proyectos desarrollados en la herramienta QlikView, los cuales necesitaban ser migrados a la aplicación Power BI. Esta migración se ha motivado por la necesidad de aprovechar las capacidades avanzadas de visualización y análisis de datos que ofrece Power BI, así como su integración con otras herramientas de Microsoft y su facilidad de uso para los usuarios finales.

#### Formación cursada

### Para poder adentrarnos en este proyecto de migración, hemos cursado un curso a través de la plataforma online UDEMY sobre Power BI. Esta formación nos ha proporcionado los conocimientos necesarios para entender las funcionalidades y características de Power BI, así como las mejores prácticas para la migración de datos y la creación de informes interactivos. A través de este curso, hemos adquirido habilidades en la conexión a diversas fuentes de datos, la transformación y modelado de datos, y la creación de visualizaciones dinámicas que facilitan la toma de decisiones basada en datos.

### Proceso seguido

#### Reuniones llevadas a cabo

Para asegurar el correcto funcionamiento del proyecto de migración a Power BI, hemos llevado a cabo reuniones semanales. Estas reuniones han sido fundamentales para conformar la plantilla del proyecto a través de la puesta en común de diferentes ideas y procedimientos. Durante estas sesiones, cada miembro del equipo ha tenido la oportunidad de aportar sus perspectivas y sugerencias, lo que ha permitido alcanzar un consenso sobre la dirección del proyecto. A través de este proceso colaborativo, hemos podido definir la idea final de manera efectiva. Además, estas revisiones semanales han sido cruciales para evaluar los avances, ajustar los pasos según sea necesario y asegurar que todos los aspectos del proyecto se desarrollen de manera coherente y alineada con los objetivos establecidos. Gracias a estas reuniones, hemos logrado conformar versiones más finales y refinadas de los proyectos, garantizando su éxito y funcionalidad.

## Conclusiones y valoraciones finales

Durante nuestras prácticas, he llevado a cabo una variedad de actividades que han contribuido significativamente a mí desarrollo profesional. Entre ellas se incluyen:

1. **Sanitización y puesta a punto en programas PHP**: He aprendido a validar y sanitizar datos utilizando funciones específicas como odbc\_prepare y odbc\_execute, asegurando la seguridad y eficiencia en la interacción con bases de datos.
2. **Desarrollo de procesos de carga de datos**: He desarrollado programas para la carga de datos desde archivos CSV a una tabla DB2, automatizando la actualización de información de inmuebles provenientes de SharePoint online.
3. **Atención a peticiones interdepartamentales (SIGPEs)**: He gestionado solicitudes internas mediante el sistema SIGPE, asignando tareas según la familiaridad y experiencia de los miembros del equipo, y aprendiendo gradualmente sobre los diferentes funcionamientos internos del departamento.
4. **Uso y manejo de Office 365**: He adquirido habilidades en el manejo de Word y Excel, utilizando funciones avanzadas para realizar operaciones concretas y mejorar la eficiencia en la gestión de datos.
5. **Diseño y desarrollo de aplicaciones con Power BI**: He migrado proyectos de QlikView a Power BI, participando en reuniones semanales para conformar la plantilla del proyecto y asegurar su correcto funcionamiento.
6. **Extracciones de datos complejos**: He atendido peticiones de extracciones de datos complejos, analizando las necesidades de los departamentos y proporcionando la información requerida de manera precisa y eficiente.

En definitiva, las prácticas realizadas han sido una experiencia enriquecedora que nos ha permitido adquirir conocimientos valiosos y desarrollar habilidades técnicas y profesionales. He aprendido a manejar herramientas y tecnologías clave, como PHP, Office 365 y Power BI, al igual que he mejorado mi capacidad para trabajar en equipo y gestionar proyectos. La exposición a diversas tareas y responsabilidades me ha proporcionado una comprensión integral de los procesos internos del departamento y me ha preparado para ser capaz de enfrentarme a desafíos futuros con confianza.

En general, las prácticas de empresa han sido altamente positivas. He tenido la oportunidad de aplicar todos aquellos conocimientos teóricos cosechados durante mi formación académica y universitaria en un entorno real, aprender de profesionales experimentados y contribuir activamente al éxito de los proyectos. La experiencia adquirida me ha permitido crecer tanto personal como profesionalmente, y estoy agradecidos por la oportunidad de haber participado en este programa de prácticas.