ACTIVIDAD 31

SQL INJECTION

¿Qué es la inyección SQL (SQLi) y cómo prevenirla?

La inyección SQL (SQLi) es un tipo de ataque de inyección que permite ejecutar sentencias SQL maliciosas. Estas sentencias controlan un servidor de base de datos detrás de una aplicación web. Los atacantes pueden aprovechar las vulnerabilidades de inyección SQL para eludir las medidas de seguridad de la aplicación.

¿Cómo y por qué se realiza un ataque de inyección SQL?

Para realizar un ataque de inyección SQL, un atacante primero debe encontrar entradas de usuario vulnerables dentro de la página o aplicación web. Una página o aplicación web con una vulnerabilidad de inyección SQL utiliza dichas entradas de usuario directamente en una consulta SQL.

EJEMPLOS

1-

```
GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users
WHERE uname='test' HTTP/1.1
Host: testphp.vulnweb.com
```

```
2-
GET http://testphp.vulnweb.com/artists.php?artist=1 HTTP/1.1
Host: testphp.vulnweb.com
```

```
3-
<?php

$offset = $_GET['offset']; // ¡Cuidado, no hay validación en la entrada de datos!
$query  = "SELECT id, name FROM products ORDER BY name LIMIT 20 OFFSET $offset;";
$result = pg_query($conn, $query);

?>
```

SINTAXIS:

```
$usuario = $_POST['usuario'];
$contraseña = $_POST['contraseña'];
$sql = "SELECT * FROM usuarios WHERE usuario = '$usuario' AND
contraseña = '$contraseña'";
Si un atacante ingresa en el campo "usuario" el siguiente valor:
```

```
' OR '1'='1
La consulta SQL resultante sería:

sql
Copiar
Editar
SELECT * FROM usuarios WHERE usuario = '' OR '1'='1' AND contraseña =
'';
```

Mis propias palabras:

Es una forma de obtener informacion de una base de datos y poder aprovechar de sus vulnerabilidades al compartir un link, o algun boton, que al ser interactuado por el usuario nos abre digamos una puerta a esa base de datos:

INDEX

El archivo index.html es uno de los elementos más importantes al crear una web. Este archivo sirve como la puerta de entrada de cualquier sitio web. Es el encargado de mostrar la página principal de una web cuando alguien visita la dirección del sitio

Para que sirve?

Carga automática de contenido:
Los servidores web están programados para buscar el archivo index.html automáticamente cuando alguien ingresa a la página principal. Esto permite que el sitio web cargue de forma rápida y ordenada.
Facilita la navegación:
Este archivo hace que los usuarios puedan ver la página de inicio sin tener que escribir el nombre del archivo completo en la URL. Por ejemplo, basta con poner www.ejemplo.tld en lugar de www.ejemplo.tld/index.html, haciendo la navegación más cómoda y directa.
Mejora el SEO y la experiencia de usuario:
Tener una estructura clara en la web facilita que los motores de búsqueda (como Google) puedan entender el contenido del sitio. Esto ayuda a que tu página sea más fácil de encontrar para los usuarios y se muestre correctamente en los resultados de búsqueda.

EJEMPLO CLARO:
Ejemplo claro: Si alguien entra a www.dominio.tld, el navegador automáticamente buscará un archivo llamado **index.html**. Si no encuentra este archivo, puede que muestre un error o el contenido de las carpetas, lo cual no es muy amigable para los usuarios y no da una buena imagen del sitio.

Sintaxis

INDICE(matriz; núm_fila; [núm_columna])

La forma de matriz de la función INDICE tiene los siguientes argumentos:

matriz Obligatorio. Es un rango de celdas o una constante de matriz.

Si matriz contiene solo una fila o columna, el argumento núm_fila o núm_columna correspondiente es opcional.

Si matriz tiene varias filas y columnas, y solo usa núm_fila o núm_columna, INDICE devuelve una matriz de dicha fila o columna completa.

fila Obligatorio, a menos que núm_columna esté presente. Selecciona la fila de la matriz desde la cual devolverá un valor. Si se omite núm_fila, núm_columna es obligatorio.

núm_columna Opcional. Selecciona la columna de la matriz desde la cual devolverá un valor. Si se omite núm_columna, núm_fila es obligatorio.

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Página Principal - Mi Sitio Web</title>
</head>
<body>
  <header>
    <h1>Bienvenido a Mi Sitio Web</h1>
    <p>Explora nuestros servicios y productos.</p>
  </header>

  <main>
    <section>
      <h2>Servicios</h2>
      <p>>Ofrecemos una variedad de servicios para ayudarte en tu proyecto web.</p>
    </section>
    <section>
      <h2>Contacto</h2>
      <p>¿Tienes preguntas? Ponte en contacto con nosotros</p>
    </section>
  </main>

  <footer>
    <p>&copy; 2024 Mi Sitio Web. Todos los derechos reservados.</p>
  </footer>
```

```
</body>
</html>
```

Mis propias palabras:

Un index es la parte principal de una pagina web, es el acceso y es lo que se muestra al momento de dar click a un enlace, entre mejor sea su estructura, la carga sera mas rapida

TRANSACCION

En programación, una transacción es una secuencia de operaciones o acciones que se tratan como una unidad lógica indivisible, garantizando la integridad y consistencia de los datos. Se asegura que todas las operaciones dentro de la transacción se completen con éxito o, en caso de fallo, ninguna se realiza, manteniendo el estado de los datos en un estado consistente.

Beneficios de utilizar transacciones:

Integridad de los datos:
Las transacciones ayudan a mantener la consistencia y la integridad de los datos al asegurar que las operaciones se realicen en su totalidad o ninguna.
Recuperación de errores:
En caso de error, las transacciones permiten revertir los cambios realizados, evitando la corrupción de los datos.
Simplificación del desarrollo:
El uso de transacciones simplifica el desarrollo de aplicaciones que requieren la gestión de múltiples operaciones relacionadas.
Gestión de la concurrencia:
Las transacciones ayudan a controlar la concurrencia, evitando problemas causados por acceso simultáneo a los datos.

SINTAXIS BASICA:

```
BEGIN TRANSACTION;
-- Operaciones de la transacción
UPDATE empleados SET salario = salario * 1.10 WHERE departamento = 'Ventas';
INSERT INTO historial_salarios (empleado_id, antiguo_salario, nuevo_salario) SELECT id, salario, salario * 1.10 FROM empleados WHERE departamento = 'Ventas';
COMMIT;
```

Ejemplos de transacciones en programación:

Transferencia bancaria:

Cuando se transfiere dinero de una cuenta a otra, la operación de débito en la cuenta fuente y crédito en la cuenta destino deben ser consideradas como una única transacción atómica.

Compra en línea:

Al realizar una compra en un sitio de comercio electrónico, la transacción implica la validación del pago, el procesamiento del pedido, la actualización del inventario y la notificación al cliente.

Actualización de una base de datos:

Modificar varios registros en una base de datos, como actualizar la información de productos o usuarios, puede ser parte de una transacción para garantizar que los cambios se hagan de forma coherente y consistente.

Gestión de recursos:

En sistemas que manejan recursos limitados (como impresoras o conexiones a una red), la gestión de estos recursos puede ser encapsulada en una transacción para asegurar que se asignen de forma correcta y evitar conflictos.

Registro de empleados o nómina:

En sistemas de gestión de recursos humanos, la creación, actualización o eliminación de registros de empleados, así como el cálculo de la nómina, pueden ser parte de una transacción.

Reservas de hotel o avión:

En sistemas de reserva, la transacción implica la verificación de disponibilidad, la asignación de habitaciones o asientos, la confirmación de la reserva y la notificación al cliente.

Procesamiento de pedidos en línea:

La creación de un pedido en línea, el cálculo de impuestos y envío, y la actualización del inventario pueden ser parte de una transacción.

Mis propias palabras:

Entendi que un transaccion es una operacion en sql que nos ayuda a completar algun movimiento de datos de forma segura ya que agregas condiciones para asegurarte que realizas la operacion en el lugar correcto.