




Reporte del incidente

 Propietario	 Ayala Arroyo Raúl
 Etiquetas	

Título del Reporte

Vulnerabilidad de Inyección SQL en Damn Vulnerable Web Application (DVWA)

Introducción

Este reporte describe una vulnerabilidad de inyección SQL identificada en la aplicación web Damn Vulnerable Web Application (DVWA). El objetivo es demostrar cómo esta vulnerabilidad permite la explotación para acceder a datos confidenciales almacenados en la base de datos de la aplicación. Este incidente se documenta conforme a la norma ISO 27001 para la gestión de incidentes de seguridad de la información.

Descripción del Incidente

Se identificó una vulnerabilidad de inyección SQL en la funcionalidad de DVWA, específicamente en el campo `User ID` de la sección **SQL Injection**. La vulnerabilidad permite a un atacante modificar la consulta SQL enviada al servidor, lo cual da acceso no autorizado a la información de usuarios almacenada en la base de datos.

Proceso de Reproducción

1. Configuración del Entorno:

- Antes de acceder a la aplicación, se realizaron los siguientes pasos en la terminal para preparar el entorno y configurar DVWA correctamente.

```
bash
Copiar código
# Cambiar al directorio donde se almacenará DVWA.
```

```
cd /var/www/html

# Instalar wget y unzip para descargar y descomprimir el archivo DVWA.
sudo apt-get install wget unzip

# Descargar el archivo comprimido de DVWA y descomprimirlo.
sudo wget https://storage.googleapis.com/breathecode/virtualbox/DVWA.zip
sudo unzip DVWA.zip

# Renombrar la carpeta descargada para simplificar su nombre.
sudo mv DVWA-master DVWA
```

2. Configurar el Archivo de DVWA:

- Cambiar al directorio de configuración de DVWA y preparar el archivo de configuración.

```
bash
Copiar código
# Moverse al directorio de configuración de DVWA.
cd /var/www/html/DVWA/config

# Copiar el archivo de configuración de muestra para crear el archivo de configuración principal.
sudo cp config.inc.php.dist config.inc.php
```

- Editar el archivo `config.inc.php` para asegurar que las credenciales de la base de datos sean correctas:

```
php
Copiar código
$_DVWA['db_user'] = 'root';
$_DVWA['db_password'] = 'tu_contraseña_de_root';
$_DVWA['db_database'] = 'dvwa';
```

3. Configurar la Base de Datos en MariaDB:

- Crear la base de datos `dvwa` y configurar el usuario de base de datos.

```
bash
Copiar código
# Acceder a MariaDB como usuario root.
sudo mariadb -u root -p

# Dentro de MariaDB, ejecutar los siguientes comandos SQL:
CREATE DATABASE dvwa;
CREATE USER 'root'@'localhost' IDENTIFIED BY 'tu_contraseña';
GRANT ALL PRIVILEGES ON dvwa.* TO 'root'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

4. Ajustar los Permisos:

- Configurar los permisos de DVWA para que el servidor web tenga acceso adecuado a los archivos y carpetas.

```
bash
Copiar código
# Cambiar el propietario y grupo de los archivos de DVWA a
www-data.
sudo chown -R www-data:www-data /var/www/html/DVWA/
```

```
# Asignar permisos de lectura, escritura y ejecución adecuados.  
sudo chmod -R 755 /var/www/html/DVWA/
```

5. Reiniciar Apache:

- Reiniciar el servidor web Apache para aplicar todos los cambios.

```
bash  
Copiar código  
sudo systemctl restart apache2
```

6. Acceso a la Aplicación:

- Abrir un navegador e ir a <http://localhost/DVWA/setup.php>.
- Hacer clic en "Create / Reset Database" para inicializar la base de datos de DVWA.

7. Prueba de Inyección SQL:

- Iniciar sesión en la aplicación DVWA en <http://localhost/DVWA> con las credenciales:
 - **Usuario:** `admin`
 - **Contraseña:** `password`
- Cambiar el nivel de seguridad a "Low" desde la pestaña **DVWA Security**.
- Navegar a la sección **SQL Injection**.
- En el campo `User ID`, ingresar el siguiente payload de inyección SQL:

```
sql  
Copiar código  
1' OR '1'='1
```

- Hacer clic en **Submit** para ejecutar la inyección.

8. Resultados de la Inyección SQL:

- La inyección SQL fue exitosa, mostrando la siguiente información confidencial de los usuarios:

ID	First Name	Surname
1' OR '1'='1	admin	admin
1' OR '1'='1	Gordon	Brown
1' OR '1'='1	Hack	Me
1' OR '1'='1	Pablo	Picasso
1' OR '1'='1	Bob	Smith

Impacto del Incidente

Esta vulnerabilidad permite a un atacante acceder y visualizar información confidencial de los usuarios de la aplicación, lo cual representa una seria violación de la seguridad de los datos. Un atacante con este acceso podría explotar la vulnerabilidad para realizar otras consultas SQL maliciosas, modificar datos o extraer información sensible. Esto pone en riesgo la integridad y confidencialidad de la base de datos.

Recomendaciones

Para mitigar y resolver esta vulnerabilidad, se recomiendan las siguientes acciones:

1. **Validación de Entradas:** Implementar una validación de entradas robusta que asegure que los datos ingresados por el usuario no contengan caracteres maliciosos.
2. **Uso de Consultas Preparadas (Prepared Statements):** Las consultas preparadas permiten separar el código SQL de los datos de entrada, evitando que las entradas maliciosas afecten la consulta.
3. **Restricciones de Privilegios:** Limitar los privilegios del usuario de la base de datos usado por la aplicación para evitar accesos no autorizados a información sensible.

4. **Deshabilitar Errores Detallados en Producción:** Asegurarse de que los mensajes de error detallados no se muestren en entornos de producción para evitar que un atacante obtenga información sobre la estructura de la base de datos.

Conclusión

La vulnerabilidad de inyección SQL en DVWA es un riesgo significativo de seguridad que expone información confidencial de los usuarios. Esta práctica ha permitido identificar la vulnerabilidad y simular un ataque SQL exitoso. Es crucial implementar las medidas recomendadas para prevenir este tipo de ataques y proteger la seguridad de la información en aplicaciones web.