SQL injection en DVWA

Introducción

El presente documento detalla el descubrimiento de una vulnerabilidad de seguridad crítica de tipo Inyección de SQL (SQL Injection. Esta vulnerabilidad permite a un atacante eludir los controles de acceso a los datos y extraer información sensible de la base de datos subyacente.

Descripción del Incidente

El campo de entrada "User ID" no valida los datos proporcionados por el usuario antes de procesarlos en una consulta a la base de datos. Un atacante puede insertar código SQL malicioso en este campo para manipular la consulta original.

Al introducir la carga útil (payload) ' OR '1' = '1, la consulta SQL ejecutada en el servidor se altera. La consulta original probablemente se asemeja a:

SELECT first_name, last_name FROM users WHERE user_id = '[INPUT]';

Al inyectar la carga útil, la consulta se convierte en:

SELECT first_name, last_name FROM users WHERE user_id = '' OR '1' = '1';

La condición '1' = '1' siempre es verdadera, lo que provoca que la cláusula WHERE se evalúe como cierta para todos los registros de la tabla users. Como resultado, en lugar de devolver un solo usuario, la base de datos devuelve la lista completa de todos los usuarios almacenados.

Proceso de Reproducción

- *Navegación*: Acceder a la aplicación y navegar a la sección "SQL Injection" desde el menú lateral.
- *Identificación del campo*: Localizar el campo de entrada de texto etiquetado como "User ID".
- *Inyección*: Introducir la siguiente cadena de texto en el campo "User ID": 1' OR '1' = '1
- *Envío*: Hacer clic en el botón "Submit".

Impacto del incidente

La explotación de esta vulnerabilidad tiene un impacto crítico en la seguridad de la aplicación y sus datos, afectando los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Recomendaciones

- *Principio de mínimo privilegio*: configurar la cuenta de la base de datos que utiliza la aplicación web con los permisos mínimos necesarios. Por ejemplo, si la aplicación solo necesita leer datos de una tabla, la cuenta no debe tener permisos de escritura (UPDATE, INSERT) o eliminación (DELETE, DROP).
- *Manejo de errores genéricos*: configurar la aplicación para que no muestre mensajes de error detallados de la base de datos al usuario final. Estos errores pueden proporcionar a los atacantes información valiosa sobre la estructura de la base de datos.

Conclusión

La vulnerabilidad de Inyección de SQL identificada es de severidad crítica y expone a la aplicación a un riesgo significativo de compromiso total de la base de datos. Permite la extracción no autorizada de datos sensibles y abre la puerta a la manipulación o destrucción de la información.