ISO 27001 Reporte de Incidente -Inyección SQL en DVWA

º Introducción

Mediante este informe detallamos como se ha podido explotar una vulnerabilidad en Damn Vulnerable Web Application (DVWA), el ataque consistió en hacer una inyección SQL a traves del puerto 80. Todo esto se llevo acabo en un entorno controlado con el fin de estudiar el impacto que esta vulnerabilidad puede llegar a tener.

º Descripción del Incidente

Durante el testeo de la seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL. Esta vulnerabilidad permite al atacante vulnerar la seguridad mediante la inyección de código SQL malicioso a traves de los inputs de la aplicación y de esta manera tener acceso a las bases de datos y a los datos existentes en las mismas.

º Método de Inyección SQL Utilizado

Para poder replicar y demostrar la vulnerabilidad encontrada, en el recuadro de USER ID: ingresamos el siguiente comando:

1 1' OR '1'='1

Al ingresar este comando en el input, el atacante logra eludir la autenticación mediante 'usuario' y 'contraseña' y de esta manera tener acceso a su información.

º Impacto del Incidente

Aunque el incidente ocurrió en un entorno controlado de pruebas, los efectos de una inyección SQL en un entorno de producción serían significativos. Los posibles impactos incluyen:

º Acceso no autorizado a datos sensibles º Alteración o eliminación de la base de datos º Escalamiento de privilegios, mediante alteraciones de la base de datos

Esto podría suponer un riesgo significativo para los servicios de DVWA, debido a la falta de confidencialidad, integridad y disponibilidad de los datos que almacena.

º Recomendaciones

Para la mitigación y prevención de inyecciones SQL, se sugieren las siguientes acciones:

º Sanitización de entradas: Asegurarse de que todas las entradas de usuario estén correctamente validadas y filtradas.

º Configuración segura: Deshabilitar la opción de mostrar errores de base de datos en entornos de producción para evitar que los atacantes obtengan información útil sobre el sistema

- Uso de Web Application Firewall (WAF): Implementar un firewall de aplicaciones web (WAF) para detectar y bloquear intentos de inyección SQL en tiempo real.

- Conclusión

La prueba de inyección SQL realizada a DVWA, comprobó la importancia de proteger las paginas web contra ataques comunes. Aunque este ataque se realizo en un entorno controlado, se deben aplicar los mismos principios de seguridad en entornos de producción y de esta manera prevenir ataques que comprometan la seguridad, confidencialidad y disponibilidad de la información.