Max Montlleo Rodríguez

ISO 27001 Compliant Incident Management

Reporte - SQL Injection Vulnerability

Introducción

Este informe detalla la identificación y “explotación” de las vulnerabilidades de la DVWA. La prueba estuvo hecha en un ambiente controlado (máquina virtual sencilla) para demostrar las debilidades de dicha web.

Descripción del incidente

Durante la prueba/asalto de la DVWA, se descubrió la opción de atacar con “SQL Injection” en un apartado de la misma web. Después de establecer la dificultad de la misma en “low” (baja) se procedió a ello. Este ataque permite que, con una línea de “código” muy concreta, se desestabilice el proceso “normal” o esperado de los campos de llenado para el registro de usuarios y se pueda leer la base de datos de los mismos.

Metodo de “SQL Injection” usado

Para demostrar la vulnerabilidad se usó el codigo:

<<1’ OR ‘1’=’1>>

Este “payload” permite que devuelva una lista de los usuarios y su información básica. Es una buena manera de obtener, sin autorización, información útil para poder evitar otro ciberataque de una manera más fácil.

Impacto del Incidente

Como ya se ha comentado, con esta técnica el atacante puede obtener acceso a información confidencial. En niveles superiores, incluso puede modificar y/o eliminar información.

Recomendaciones

Creemos que la seguridad puede ser mejorado con las siguientes conductas:

-Aumentando los mínimos de los “inputs” de los usuarios con parametros seguros anti-SQL.

-Haciendo pruebas regularmente.

-Educar a los usuarios/trabajadores para poder mitigar los ataques o, al menos, prevenir futuros ataques aún más graves si este mismo (SQL) se ha llevado a cabo con éxito.

Conclusiones

La identificación de la posibilidad del ataque “SQL Injection” y su llevada a término nos evidencia que hay vulnerabilidades. Por lo tanto, es importante una seguridad proactiva y una buena concienciación para evitar casos graves y reales en un futuro cercano.