Instalación de DVWA en una Máquina Virtual para Prácticas de Inyecciones SQL

Introducción

Mediante este informe se indica el proceso de instalación del Damn Vulnerable Web Application (DVWA) en una máquina virtual Debian para prácticas de inyecciones SQL.

Método de inyección SQL utilizado

Como identificación de usuario para replicar y demostrar la vulnerabilidad, se colocó en “User ID” la siguiente información:

1’ OR ‘1’=’1

Esta carga útil explota la vulnerabilidad para modificar la consulta SQL original de tal manera que devuelve la identificación de usuario almacenada en la tabla de usuarios, específicamente para el usuario 1’ OR ‘1’=’1. Al ejecutar con éxito esta inyección SQL, se obtienen las credenciales del usuario objetivo sin autorización.

Impacto del incidente

El impacto de este incidente podría permitir a un atacante acceso a información confidencial y la posibilidad de poder extraer cualquier dato que considere de utilidad. Asimismo, podría modificar, borrar o poner en riesgo información almacenada que se considere sensible. Esta situación representaría un riesgo desde el punto de vista de la triada de la ciberseguridad (confidencialidad, integridad y disponibilidad) suministrada por DVWA.

Recomendaciones

Basado en los hallazgos mencionados se sugiere:

- Implementar un firewall de aplicaciones web para detectar y bloquear patrones de inyección comunes antes de que lleguen al servidor.
- Desactivar mensajes de error detallados mediante la configuración del servidor para que no muestre errores de SQL al usuario final. Estos errores dan pistas al atacante sobre la estructura de tu base de datos.
- Realizar auditorías de seguridad periódicas que permitan identificar y mitigar riesgos.
- Capacitar a los usuarios sobre buenas prácticas para concientizar sobre potenciales riesgos.

Conclusiones

Es importante maximizar esfuerzos para evitar vulnerabilidades del DVWA, mediante sistemas cifrados que dificulten la penetración por parte de agentes externos que quieran interrumpir el normal desempeño. Esto se puede lograr mediante la vigilancia y mantenimiento constantes del sistema para detectar fallas y tomar las acciones que sean necesarias de manera inmediata.