reporte de incidentes

Introducción:
Este reporte documenta el proceso de un ataque de inyección SQL ejecutado en la aplicación Damn Vulnerable Web Application (DVWA), un entorno diseñado para prácticas de seguridad web. La inyección SQL es una vulnerabilidad que permite a un atacante ejecutar comandos SQL maliciosos en la base de datos de una aplicación, lo que puede provocar la exposición, alteración o eliminación de datos sensibles.

Descripción del Incidente:
El ataque de inyección SQL se llevó a cabo en el nivel de seguridad "Bajo" en DVWA. El objetivo fue explotar una vulnerabilidad en el formulario de autenticación para obtener información no autorizada de la base de datos. DVWA, al carecer de una validación robusta de entradas en este nivel, permite la manipulación directa de las consultas SQL.

Proceso de Reproducción:

1. Acceder a DVWA e iniciar sesión.
2. Navegar a la sección de SQL Injection en la aplicación.
3. En el campo de entrada de usuario, se ingresó el payload SQL **“ ‘ OR ‘1’ = ‘1’ – “** para modificar la consulta SQL ejecutada por la aplicación.
4. Al enviar el formulario, se realizó la inyección, lo que resultó en la extracción de datos sin autenticación.

Impacto del Incidente:
Este ataque permitió el acceso a información almacenada en la base de datos de DVWA sin autorización, incluyendo posibles datos de usuarios. Si esta vulnerabilidad estuviera presente en una aplicación en producción, podría comprometer la integridad de la información y la privacidad de los usuarios.

Recomendaciones:

1. Implementar validaciones y sanitización de entradas para prevenir inyecciones SQL.
2. Utilizar consultas preparadas o procedimientos almacenados en lugar de concatenación de strings en las consultas SQL.
3. Mantener los sistemas actualizados con parches de seguridad.

Conclusión:
La explotación exitosa de esta vulnerabilidad en DVWA demuestra los riesgos de la inyección SQL en aplicaciones web. Este tipo de pruebas es esencial para identificar y mitigar riesgos de seguridad en entornos reales.