

INFORME TÉCNICO DE INCIDENTE DE SEGURIDAD-SQL INJECTION

Datos del Incidente

- .Fecha del reporte: 3 de junio de 2025
- .Sistema afectado: DVWA (Damn Vulnerable Web Application)
- .Descripción breve: Un atacante logro acceder a todos los registros de la base de datos a través de un campo vulnerable en la URL /vulnerabilities/sqli/.

Detalle tecnico

- .Payload usado: 1' OR '1'='1
- .Resultado: Acceso completo a datos de todos los usuarios almacenados.
- Ubicación exacta de la vulnerabilidad: Campo User ID en el modulo "SQL Injection" de DVWA
- .Causa raiz: Falta de validacion de entradas de usuario

Evaluación del Impacto

- .Confidencialidad: Comprometida, el atacante accede a todos los usuarios.
- .Integridad: No comprometida en este caso, pero podría ser si se inyectan comandos de estructura.
- Disponibilidad: No afectada.

Recomendaciones

- .Usar consultas preparadas para todas las interacciones con bases de datos.
- Filtrar y sanear toda la entrada del usuario.
- .Implementar políticas de control de acceso y monitoreo
- .Usar herramientas de acceso autorizado

