

Vulnerabilidad SQL Injection

Este reporte identificó y explotó una de las vulnerabilidades de Inyección SQL dentro del entorno DVWA.

El objetivo es ver cómo puedo manipular consultas SQL mediante la entrada del usuario para extraer información sensible desde la base de datos.

Descripción del Incidente

Dentro de "SQL Injection", encuentro un formulario que me permite consultar información de usuarios.

La inyección realizada (1' OR '1'='1) me permitió recuperar todos los registros de la tabla de usuarios, confirmando la vulnerabilidad.

La aplicación me devolvió como resultado múltiples usuarios existentes en la base de datos, demostrando que la consulta SQL fue manipulada exitosamente.

Esta inyección SQL permite:

- Lectura de información sensible, como usuarios, contraseñas.
- Modificación o eliminación de datos.
- De ocasionarse dentro de un entorno real, incluso:
 - Ejecución de comandos del sistema.
 - Compromiso total del servidor.

Conclusión

El payload 1' OR '1'='1 permitió recuperar toda la información de la tabla de usuarios, confirmando la explotación.

Recomendaciones

Se recomienda implementar controles de seguridad adecuados para evitar que esta vulnerabilidad sea explotada en un entorno real.

