SQL Injection Incident Report

1. Introduccion

Instalamos e integramos DVWA Damn Vulnerable Web Application a nuestra maquina debian. Integramos la base de datos MariaDB para configurar DVWA. esto con el intento de ejecutar una SQL Injection en esta aplicación web.

2. Incident Description

Al instalar y configurar un usuario con todos los privilegios a esta base de datos, logramos la una vulnerabilidad de SQL.

3. Reproduction Process

Al ingresar a http://localhost/DVWA logramos una injection SQL de 1' OR '1=1 en la página de login. Y logramos acceso al usuario root/admin.

4. Incident Impact

Con la inyección que utilizamos logramos conseguir los usuarios y contraseñas necesarias para poder modificar la base de datos. Incluso pudimos haber borrado o copiado la información para beneficiarnos como hacker malicioso.

5. Recommendations

Mi mayor recomendación es usar una WAF para identificar y bloquear tráfico malicioso.

6.Conclusion

Una inyección SQL puede llegar a ser fatal para una empresa. Un hacker veterano pudiera modificar la base de datos incluso borrar toda la información crítica de una empresa si logra el acceso de root/admin. En mi punto de vista es una vulnerabilidad que se tiene que priorizar. SQL es una de las vulnerabilidades mas conocidas en el mundo de ciberseguridad. Mitigar y configurar la aplicación web es imperativo para la funcionalidad y reputación de una empresa.