Introducción

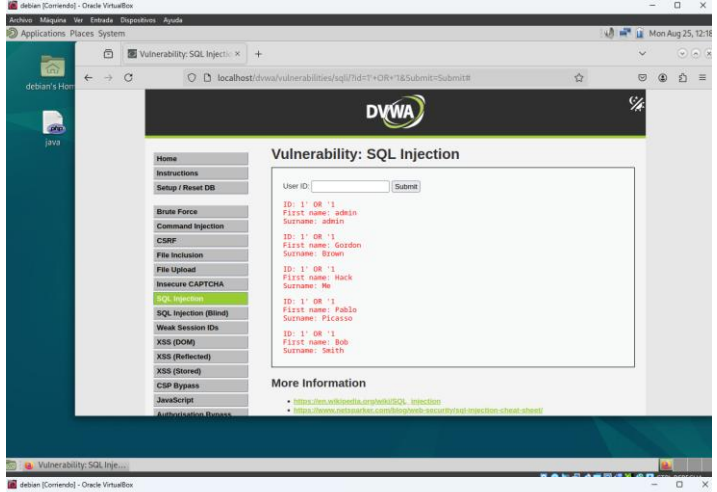
El objetivo de la prueba fue simular ataques reales, como inyección SQL, fuerza bruta y command injecction, para entender mejor como funciona estas vulnerabilidades y cual es el impacto de no proteger bien un sistema.

Descripción del ataque

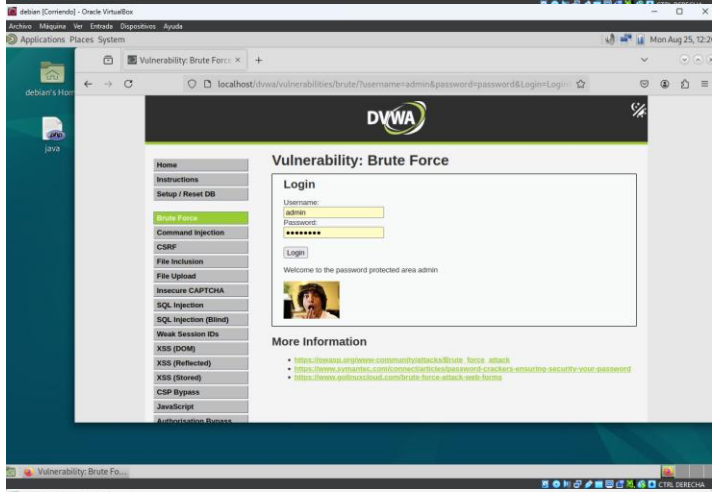
- En un entorno seguro (virtualbox) en debian, configuramos DVWA en un servidor y lo dejamos en nivel de seguridad bajo. Después hicimos diferentes pruebas:
- En SQL injection usamos comandos como: ‘1’ OR ‘1’=‘1 que nos proporción diferentes credenciales.
- En Brutal Force hicimos múltiples intentos en la pantalla de login hasta lograra acceder al sistema.
- Y en command injeccion usamos comandos como: 127.0.0.1;ls –la para ejecutar comandos directamente en el servidor.

a continuación implemento unas imágenes de los problemas.

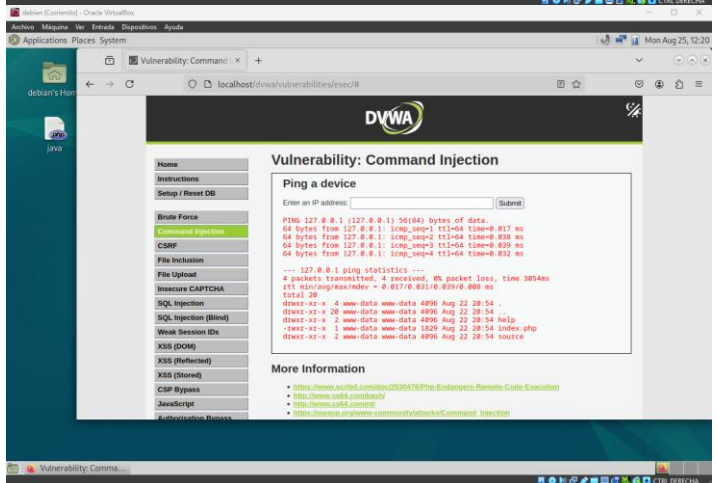
- SQL inyection:



- Brute force:



- Command inyection:



Impacto

- Estos ataques demuestran que: si un sstema no esta bien protegido, cualquier atacante puede robar información, acceder a cuentas de usuarios, y también tomar control del servidos inyectando comandos

esto seria un serio riesgo muy elevado para un servidor real de una empresa que contiene toda la información de la empresa o de los clientes, no solo a nivel económico ya que una mala defensa conlleva a multas muy altas sino también a la imagen y reputacion de la empresa.

Recomendaciones

- Para prevenir esto es necesario aplicar buenas practicas de seguridad, como por ejemplo implementar un doble factor de autenticación, y renforzar la defensa del servidor.

Conclusion.

- Esta practica me ayudo a comprender la importancia de seguridad en los servidores y lo frágil que pueden llegar a ser las defensas y como aveces es fácil superar la seguridad.

  por eso es fundamental la seguridad e implementar correctas prevenciones de seguridad para evitar estos problemas.