- Título: Reporte de incidente de un ataque de inyección SQL

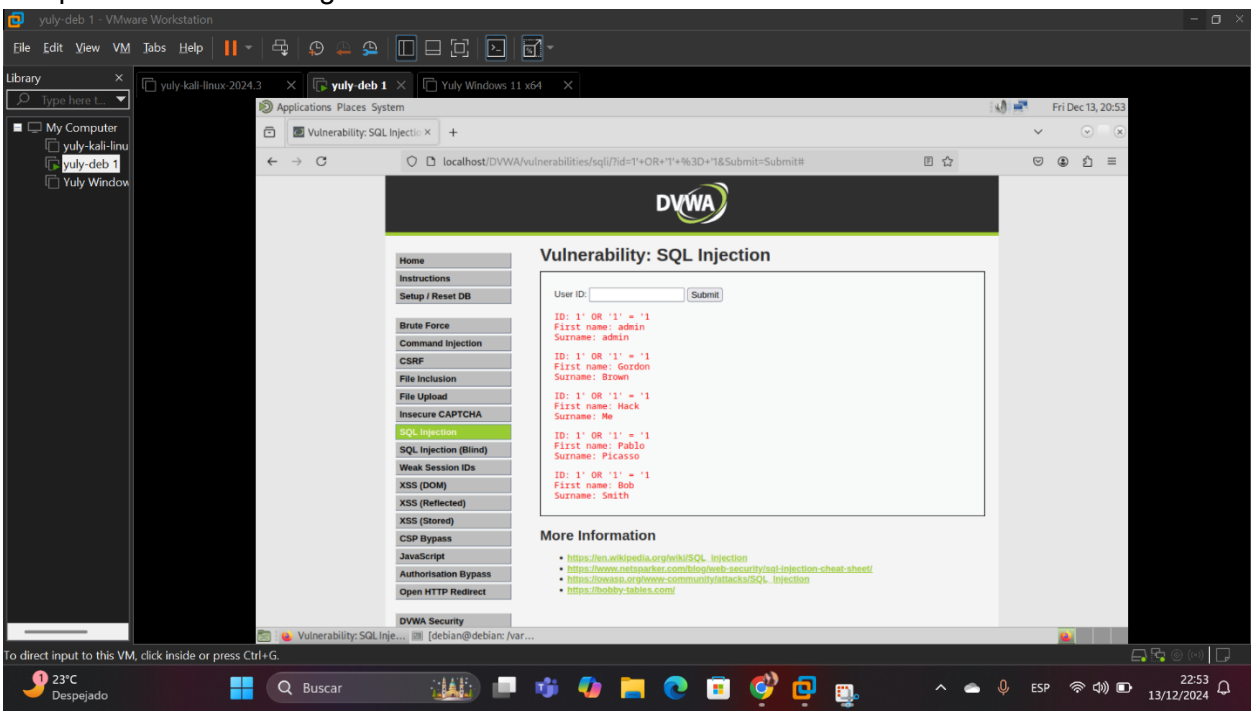
- Introducción: A continuación, se realiza el siguiente reporte debido a la identificación de un ataque en la aplicación web Damn Vulnerable Web Application (DVWA).

  (Esto se realizo en entorno seguro para dicha explotación).

- Descripción del incidente: Luego de colocar el código malicioso a través de los campos de entrada de la pagina web se vio de inmediato como los datos de esa pagina fueron expuestos y por ende vulnerados. Evidentemente esos datos se pueden corromper.

- Proceso de reproducción: Se uso el comando 1’ OR ‘1’ = ‘1 para así acceder a los datos de manera corrupta.

- Impacto del incidente: Esta corrupción de datos tiene un gran impacto para la seguridad. Ya que se pierde la integridad (el atacante puede modificar, eliminar etc.) y confidencialidad (exposición de datos), y cuando tengamos que tomar medidas también se pierde la disponibilidad de los datos (por tener que solucionar el problema). Estos son pilares de la ciberseguridad.



- Recomendaciones:

- ✓ Utilizar parámetros de consultas preparadas
- ✓ validación de entradas de usuarios
- ✓ Constantes pruebas de penetración
- ✓ realizar con regularidad auditorias de seguridad

- Conclusión: Dicho ataque deja ver que hay que tener políticas de seguridad robusta, lo cual es una tarea que siempre necesita supervisión, actualización, revisar vulnerabilidades, etc.
  No es algo que se configura y ya, es un proceso constante. Se tiene que contar con un equipo bien calificado, herramientas adecuadas, manera correcta de la respuesta a incidentes; así se minimiza los incidentes y por ende se protegen los datos críticos de una organización.