[PAN] Ataques de reconstrucción de bases de datos (Resumen)

Adversary Quering

Adeversary Quering o “Consulta Contradictoria” puede parecer un tipo de ataque bastante inocente, pero puede incurrir en riesgos de privadidad mediante el uso de inferencia. Para prevenir este tipo de ataques se recomienda rechazar las consultas que se puedan considerar peligrosas. El problema de esto es que los rechazos también pueden filtrar información. Por ejemplo, si tenemos una base de datos de salarios, se rechaza una consulta que pueda revelar el salario de un usuario en particular, pero si el atacante hace una consulta para saber cual es el máximo de los salarios de todos los empleados y después realiza una consulta para saber cual es el salario más alto de todos los usuarios menos el que se ha especificado y resulta ser este el más alto, la nueva respuesta a la consulta devolverá una cifra diferente, indicando al atacante cual era el sueldo del empleado en cuestión.

Ataques de reconstrucción de base de datos

Este tipo de ataques están orientados a bases de datos “Curadas”. Que una base de datos esté curada significa que cuando se realiza una consulta, los datos pasan por un “Curador” antes de ser publicadas para anonimizar los datos que se consideren críticos. Generalmente para curar una base de datos se recomienda evitar mostrar datos que sean demasiado detallados.