Incident Handler's Journal – Entry #3

Lab Description:

In this activity, I reviewed a final incident report from a retail company that experienced a major data breach. The goal was to understand what happened during the incident, how the company responded, and what steps were recommended to prevent it from happening again.

Date: Record the date of the journal entry.	**Entry:** #3 **Date:** October 8, 2025
Description	I analyzed the company's final report and identified key details about the data breach, including the cause, response actions, and recommendations.
Tool(s) used	Final incident report
The 5 W's:	● **Who:** A cyber attacker exploited a vulnerability in the company's e-commerce website. ● **What:** Data breach exposing about 50,000 customer records containing personal and financial information. ● **When:** Attack discovered on **December 28, 2022**, starting around 7:20 p.m. PT. ● **Where:** The company's online retail system and web server logs. ● **Why:** A web app vulnerability allowed the attacker to manipulate order numbers in URLs to access customer data.
Additional notes:	The report showed how a small web app flaw led to a large data breach. The response focused on notifying customers, offering identity protection, and

	fixing the web vulnerability. Recommendations included routine vulnerability scans, penetration testing, and tighter access control.