Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: November 12, 2024	**Entry:** 004
Description	Reviewed the final report of a significant **data theft** incident that impacted the company, resulting in the unauthorized access and exfiltration of sensitive customer data. The attack exploited a vulnerability in the e-commerce platform, allowing unauthorized access to over one million customer records. The goal of this review was to understand the incident's life cycle, identify the root cause, and examine the response actions taken by the organization.
Tool(s) used	• Incident Report Documentation • Web Server Logs (if available for future investigation) • Threat Intelligence sources (for context on similar incidents)
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by an external attacker who exploited a vulnerability in the company’s e-commerce platform.

	• **What** happened? The attacker exploited the vulnerability in the web application to gain unauthorized access to sensitive customer data. This data was then exfiltrated, affecting over one million users. • **When** did the incident occur? The breach occurred on December 22, 2022, and it was detected on December 28, 2022. • **Where** did the incident happen? The breach primarily affected the e-commerce platform and customer databases. • **Why** did the incident happen? The attacker exploited an unpatched vulnerability in the web application, specifically performing a **forced browsing** attack. This allowed them to access sensitive customer data and exfiltrate it.
Additional notes	**Root Cause:** The root cause of the incident was identified as a vulnerability in the e-commerce platform, which allowed the attacker to perform **forced browsing**. By manipulating the URL string of a purchase confirmation page, the attacker was able to gain unauthorized access to customer transaction data. **Response Actions:** Upon detection of the breach, the company took immediate action by isolating the affected systems to prevent further data exfiltration. The web application vulnerability was patched, and the affected users were notified. Additionally, the organization worked with the public relations team to disclose the breach to customers and offered free identity protection services to mitigate the impact.

	Recommendations for Future Prevention: To prevent similar incidents in the future, the following recommendations were made: ● **Routine Vulnerability Scanning and Penetration Testing:** Regular vulnerability scans and penetration tests will be conducted to identify and address potential security weaknesses before they can be exploited. ● **Access Control Mechanisms:** The company will implement stronger access control measures, such as **allowlisting** to restrict access to specific URLs and ensuring that only authenticated users can access sensitive data.