Project

As a new level-one SOC analyst, I'm reviewing a major data breach that impacted over one million users in our mid-sized retail company. My primary objectives are to understand exactly what happened, when it occurred, analyze the company's response actions, and review future recommendations. Using my incident handler's journal, I'll carefully examine the final incident report to gain insights into the breach's lifecycle and help prevent similar security incidents in the future. This review is a critical part of my first week of training, allowing me to develop a deeper understanding of our company's security processes and potential vulnerabilities.

Incident handler's journal

Date: Record the date of the journal entry.	**Entry: 2** 3:13 p.m., PT, on December 22, 2022
Description	Description: Unauthorized access to customer PII and financial data through e-commerce web application vulnerability. Affected 50,000 records. Initial report on 12/22 dismissed as spam. Follow-up on 12/28 prompted investigation. Attacker used forced browsing, manipulating order numbers in URLs. Estimated financial impact: $100,000. Incident closed after thorough investigation.
Tool(s) used	Forced Browsing
The 5 W's	Capture the 5 W's of an incident. ● **Who** Malicious actor ● **What** data theft ransomware ● **When** 3:13 p.m., PT, on December 22, 2022 ● **Where** an organization ● **Why** Vulnerability in e-commerce web app allowed forced browsing attack by modifying order numbers in URLs. Attacker accessed

	thousands of purchase confirmation pages, exposing customer PII and financial data. Inadequate access controls and authentication led to this breach. Attacker's motive was financial gain, attempting to extort the company for cryptocurrency payment in exchange for not releasing the stolen data publicly.
Additional notes	● The forced browsing attack exploited a critical vulnerability in the e-commerce platform, highlighting the need for more robust input validation and access controls. ● Web application access logs were crucial in determining the scope of the breach, emphasizing the importance of comprehensive logging and monitoring practices.

INCIDENT FINAL REPORT

Executive summary

The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted.

Timeline

At approximately 3:13 p.m., PT, on December 22, 2022, an employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it.

On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000.

On the same day, the employee notified the security team, who began their investigation into the incident. Between December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft.

Investigation

The security team received the alert and traveled on-site to begin the investigation.

The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer

purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.

After confirming the web application vulnerability, the security team analyzed the web application access logs. The logs indicated that the attacker accessed the information of thousands of purchase confirmation pages.

Response and remediation

The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.

After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source showing an exceptionally high volume of sequentially listed customer orders.

Recommendations

To prevent future recurrences, we are taking the following actions:

Perform routine vulnerability scans and penetration testing.

Implement the following access control mechanisms:

Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range.

Ensure that only authenticated users are authorized access to content.