Incident handler's journal

CyberCrab™ – Advanced Threat Defense

Security Analyst Name: Sunay Sabriev

Date: September 25, 2025	**Entry:** #2
Description	An individual gained unauthorized access to approximately 50,000 customer records containing PII and financial information via a forced browsing attack. This exploited a vulnerability in the e-commerce web application, allowing URL modification (e.g., altering order numbers in purchase confirmation pages) to access and exfiltrate data. The attacker sent extortion demands, initially $25,000 and later $50,000 in cryptocurrency, including data samples for proof.
Tool(s) used	Web application logs, web server access logs, and the incident final report for analysis.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An external individual (attacker) exploiting a zero-day vulnerability; affected parties include the mid-sized retail company's employees, security team, and approximately 50,000 customers. ● **What** happened? Unauthorized data access and exfiltration through forced browsing, leading to extortion attempts via email with demands for cryptocurrency to prevent public data release. ● **When** did the incident occur?

	Initial extortion email on September 22, 2025, at 3:13 p.m. PT; follow-up on September 25, 2025; incident officially logged at 7:20 p.m. PT; investigation from September 28–31, 2025. ● **Where** did the incident happen? At the mid-sized retail company operating physical stores and e-commerce (80% of sales), specifically targeting the web application's purchase confirmation pages. ● **Why** did the incident happen? Due to a vulnerability allowing URL parameter manipulation without proper authentication or authorization checks, motivated by financial gain through extortion.
Additional notes	To prevent recurrences, the journal outlines actionable recommendations, which were adopted post-incident: • Perform routine vulnerability scans and penetration testing to identify flaws early. • Implement URL allowlisting to restrict access to approved patterns, blocking unauthorized requests. • Ensure only authenticated and authorized users can access sensitive content, mitigating broken access control risks. These measures reflect industry standards, such as those in the SANS Incident Handler's Handbook, which emphasizes policy updates and team training following resolution. Additional best practices include using indirect reference maps for URLs and rate limiting to deter automated attacks, though not explicitly noted in this journal entry.