# Final Report Review Summary

## Goal 1: Identify exactly what happened

An attacker exploited a vulnerability in the company’s e-commerce web application using a forced browsing attack. By modifying order numbers in the purchase confirmation page URLs, they accessed and exfiltrated personal identifiable information (PII) and financial information of customers. Approximately 50,000 customer records were compromised.

## Goal 2: Identify when it happened

- Initial email threat received: December 22, 2022, at 3:13 p.m. PT  
- Second email (with data sample): December 28, 2022  
- Security team notified and began investigation: December 28, 2022  
- Incident investigation conducted: December 28–31, 2022  
- Incident officially reported and closed after investigation

## Goal 3: Identify the response actions the company took

- On-site investigation by the security team  
- Identified and confirmed the web vulnerability  
- Reviewed web server access logs  
- Publicly disclosed the breach with help from the PR team  
- Offered free identity protection services to affected customers

## Goal 4: Identify future recommendations

- Routine vulnerability scans and penetration testing  
- Allowlisting of specific URLs to prevent unauthorized access  
- Require authentication for access to sensitive content/pages