
Date: 1/19/2024	Entry: 4
Description	Review of the major security incident involving a data breach at the retail company.
Tool(s) used	Security incident tracking system, threat intelligence tools.
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who caused the incident? An individual gained unauthorized access to customer PII and financial data.• What happened? Unauthorized access to customer data affecting approximately 50,000 records.• When did the incident occur? The security incident occurred on December 28, 2022, with initial signs noted on December 22, 2022.• Where did the incident happen? The incident occurred within the e-commerce web application of the retail company.• Why did the incident happen? The incident happened due to a vulnerability in the web application that allowed a forced browsing attack.
Additional notes	The incident highlights the importance of proactive security measures, including routine vulnerability scans, penetration testing, and access control mechanisms to prevent similar incidents in the future.
