***Summary of findings from different stages***

**Stage 1: Vulnerability Assessment**

* Identified security vulnerabilities in SSL certificates, Node.js, OpenJDK, and Apache HTTP servers.
* Categorized vulnerabilities using CWE (Common Weakness Enumeration) and OWASP standards.
* Assessed business impact, such as potential data breaches, unauthorized access, and compliance risks.

**Stage 2: Nessus Integration**

* Nessus, a vulnerability scanning tool, was integrated into the system.
* It helps in **early detection, automated incident creation, risk prioritization, remediation, and compliance monitoring**.
* Nessus assigns risk scores to vulnerabilities, assisting in prioritizing fixes.

**Vulnerability Report Highlights**

* **SSL Certificate Misconfiguration (CWE-295)** → Can lead to **Man-in-the-Middle (MitM) attacks**.
* **Outdated Node.js Versions (CWE-1104, CWE-400, CWE-352, CWE-20)** → Risk of **arbitrary code execution, DoS, and CSRF attacks**.
* **OpenJDK Vulnerabilities (CWE-21502)** → Potential **data leaks and privilege escalation**.
* **Apache HTTP Server Enumeration (CWE-200)** → Increases the risk of **information leakage and reconnaissance attacks**.

**Tools Used**

* **Nessus** → Vulnerability scanning.
* **Suricata/Zeek** → Intrusion detection.
* **ELK Stack (Elasticsearch, Logstash, Kibana)** → Log analysis.
* **Prometheus & Grafana** → Monitoring and alerting.