**1. Basic Penetration Testing**

* **Tools Used:** Nmap and browser-based testing methods.
* **Outcome:** Identified common vulnerabilities (e.g., open ports, misconfigured services, insecure endpoints) and verified that Juice Shop is intentionally vulnerable for training purposes.
* **Finding:** Confirmed the importance of regular scanning to detect exposure points early.

**2. Basic Logging Implementation**

* **Tool Used:** winston Node.js logging library.
* **Outcome:** Configured logs to be written both to the console and to a persistent file (security.log).
* **Finding:** Logging allows for tracking security-related events, which helps in incident detection and forensic analysis.

**3. Security Checklist Creation**

* **Practices Included:**
  + Input validation to prevent injection attacks.
  + HTTPS for secure data transmission.
  + Hashing and salting passwords to protect stored credentials.
* **Finding:** These best practices align with OWASP recommendations and can significantly reduce common web application risks.

**4. Application to OWASP Juice Shop**

* Implemented and tested the checklist items on the Juice Shop application.
* Validated that following security best practices can mitigate many of the vulnerabilities exploited during testing.