Secure Software Development Checklist Exercise

Instructions:

1. Carefully read the scenario and features below.
2. Use the Secure Software Development Checklist to evaluate the system and make note of what has / has not been implemented.
3. Consider what could be implemented for each missing feature.
4. Feel free to refer to the section regarding recent events, if you need inspiration to get started.

Scenario:

Your team has developed the "*AutoBot*", an autonomous robot designed to deliver packages in smaller cities. It uses:

- GPS for navigation.
- A mobile app for user interaction and delivery requests.
- Cloud-based backend for route optimization and updates.
- Embedded Linux OS on the robot.
- APIs for third-party information (Traffic, weather, etc).

Features implemented:

- Basic input validation on API endpoints.
- HTTPS is used for all communication.
- User login requires email and password.
- Kubernetes used for deployment with auto-scaling
- Protected and disabled all unused ports on the robot.
- Automatic code and security analysis before being pushed to production.

Recent events (hints):

- A security researcher found an unauthenticated API that allows route overrides.
- A Power failure caused a critical outage and data loss for multiple robots.
- Logs show repeated failed login attempts and no alerts were raised.
- Management assumes that developers follow OWASP best practices.