Week 3: Advanced Security and Final Reporting

1. Basic Penetration Testing

In the final week, I conducted basic penetration testing to simulate common attack vectors and evaluate the effectiveness of the security measures implemented in Week 2.

- Simulated attacks included:
  - Unauthorized access attempts
  - Broken authentication scenarios
  - Parameter tampering

These tests confirmed that the JWT-based authentication middleware, input validation, and password hashing mechanisms were functioning correctly and successfully preventing exploitation. The application demonstrated improved resilience against basic attack patterns.

---

2. Logging and Monitoring

To improve security visibility and support potential incident response, I integrated logging functionality using a logging library.

- All login attempts were recorded, including both successful and failed attempts.
- Error messages and access anomalies were logged for further review.
- Logs were stored in both the console output and a dedicated security log file.

This logging setup enables early detection of suspicious behavior, brute-force attempts, or intrusion patterns, and facilitates auditability for system administrators.

---

3. Security Best Practices Checklist

Based on the security enhancements and learnings from the internship, I compiled a Security Best Practices Checklist to guide future development and ensure long-term protection of the application:

- ✅ All user inputs are validated and sanitized

- ✅ Passwords are securely hashed and salted before being stored
- ✅ Token-based authentication (JWT) is used to secure all API routes
- ✅ Security headers enforced using helmet middleware
- ✅ HTTPS configured for encrypted communication (where applicable)
- ✅ Server does not expose software version information
- ✅ Developer comments and sensitive data are removed from production code
- ✅ Security logs are maintained for activity monitoring and auditing

---

✅ Summary

Week 3 centered on validating the security posture of the application through penetration testing, enhancing system observability with logging and monitoring, and consolidating security knowledge into a best practices checklist.

Across the three weeks, the internship project successfully covered:

- 🔍 Identifying and addressing vulnerabilities
- 🔐 Implementing effective security measures
- 🛡️ Testing defenses under attack simulations
- 📝 Documenting improvements for sustainable security

This structured approach ensured that the application evolved into a more secure and reliable system, aligning with industry-standard cybersecurity principles.