

Security Practice Checklist

- 1. Verify for Security Early and Often
- 2. Parameterize Queries
- 3. Encode Data
- 4. Validate All Inputs
- 5. Implement Identity and Authentication Controls
- 6. Implement Appropriate Access Controls
- 7. Protect Data
- 8. Implement Logging and Intrusion Detection
- 9. Use Security Frameworks and Libraries
- 10. Error and Exception Handling

DevSecOps Trigger Points

- Design review: Get security architectural review
- Code Reviews : Security Practice Checklist
- Pre-commit (IDE) or in Pull-Requests: Static scan analysis. Heed to high certainty+ high severity vulnerabilities.
- QA Integration: Dynamic scan analysis, heed high certainty and high severity vulnerabilities
- Production Acceptance : Production-safe dynamic testing
- Post-Production: RASP (runtime application self-protection) or Web Application Firewalls (WAFs need rules updated – automatic is better)

Want to know more? Drop us a line at sales_dev@whitehatsec.com!