

PHP SECURITY & VULNERABILITY INSPECTION CHECKLIST

GENERAL INFORMATION

Name: _____

Date: _____

Location: _____

PHP Configuration & Environment

- ☐ Yes ☐ No — PHP version is supported and receives security updates
- ☐ Yes ☐ No — Error reporting does not expose sensitive details
- ☐ Yes ☐ No — Dangerous PHP functions are restricted where appropriate
- ☐ Yes ☐ No — Production settings follow security best practices

Input Validation & Data Handling

- ☐ Yes ☐ No — User inputs are validated and sanitized appropriately
- ☐ Yes ☐ No — Database queries use parameterized statements
- ☐ Yes ☐ No — Output is escaped to prevent cross-site scripting
- ☐ Yes ☐ No — File uploads are restricted and validated

Authentication & Access Control

- ☐ Yes ☐ No — Passwords are securely hashed and stored
- ☐ Yes ☐ No — Administrative access requires appropriate authentication

☐ Yes ☐ No — User permissions follow least privilege principles

☐ Yes ☐ No — Session cookies use secure settings

Dependencies & Updates

☐ Yes ☐ No — PHP frameworks and libraries are supported

☐ Yes ☐ No — Dependencies are checked for known vulnerabilities

☐ Yes ☐ No — Unused packages and components are removed

☐ Yes ☐ No — Security patches are applied promptly

Server & File Security

☐ Yes ☐ No — Sensitive configuration files are protected

☐ Yes ☐ No — File and directory permissions are appropriately restricted

☐ Yes ☐ No — Secrets are excluded from public web directories

☐ Yes ☐ No — Directory listing is disabled where appropriate

Network & Application Protection

☐ Yes ☐ No — HTTPS is enforced for application traffic

☐ Yes ☐ No — Cross-site request forgery protections are implemented

☐ Yes ☐ No — Security headers are configured appropriately

☐ Yes ☐ No — Rate limiting helps protect sensitive endpoints

Logging & Incident Readiness

- ☐ Yes ☐ No — Security events are logged without exposing secrets
- ☐ Yes ☐ No — Logs are protected from unauthorized access
- ☐ Yes ☐ No — Alerts are configured for suspicious activity
- ☐ Yes ☐ No — Backup and incident response procedures are documented

FINAL NOTES

Inspector Name: _____

Inspector Email: _____

Inspection Date: _____

☐ I confirm this inspection was completed accurately

Powered by:  FIELD EAGLE www.fieldeagle.com