# Fiche de Bonnes Pratiques – OWASP Top 10

## 1. Règles générales

- Valider toutes les entrées utilisateur.
- Utiliser HTTPS partout.
- Ne jamais exposer de secrets.

## 2. Authentification et sessions

- Hash (bcrypt / Argon2).
- Timeout 15 minutes.
- Cookies : HttpOnly, Secure, SameSite.

## 3. Contrôle des accès

- RBAC (admin/user).
- 403 en cas d’accès interdit.
- Validation côté serveur.

## 4. Validation des entrées

- Requêtes préparées.
- Échapper les sorties.
- Limiter la longueur.

## 5. Sécurité des dépendances

- npm audit / pip-audit.
- Mises à jour régulières.
- Pas de libs obsolètes.

## 6. Configuration serveur

- Pas d’erreurs détaillées en prod.
- Ports inutiles fermés.
- Versions récentes.

## 7. Logging et monitoring

- Logs horodatés.
- Pas de mots de passe.
- Alertes en cas de comportement suspect.