1. Priorités immédiates (T = 0 → 30 min)

1. **Isoler** l'instance vulnérable (empêcher toute exploitation supplémentaire)
    - Mettre l'application **hors ligne** depuis Replit (Stop / Disable).
    - Si impossibilité : restreindre l'accès (mettre protection par mot de passe Replit / rendre le repl privé).
2. **Préserver les preuves** (evidence) avant toute modification lourde
    - Sauvegarder `flag.txt` (localement).

Notifier les responsables (manager, référent sécurité) et activer l'équipe d'intervention.

---

2. Containment (T = 30 min → 2 h)

- **Bloquer l'accès public** :
    - Stopper le service Replit OU activer une page de maintenance.
    - Si service doit rester UP pour tests, configurer une restriction IP ou HTTP Basic Auth (temporaire).
- **Changer tous les secrets exposés** (si réels) — ici : retirer token hardcodé du repo et du code (remplacer par placeholder).
- **Surveiller** les logs (si disponibles) : noter IPs, timestamps, user-agents des requêtes vers `/admin` et `/flag`.

---

3. Eradication (T = 2 h → 4 h)

- **Corriger la configuration** minimale avant réouverture :
    - Retirer `flag.txt` du répertoire public ou le servir uniquement après authentification.

    - Remplacer le token codé en dur par une authentification par session (express-session) ou par vérification côté serveur (hashed secret).
    - Ajouter validation stricte sur `q` (whitelist, longueur ≤ 64, échapper tout affichage).
- **Appliquer patchs tests** sur une branche isolée (feature/fix-auth) et valider en local.
- **Valider la suppression d'accès direct** : tester `/flag` et `/admin` ne doivent pas être accessibles anonymement.

---

4. Recovery & Validation (T = 4 h → 8 h)

- **Vérification post-remediation** :
    - Rejouer les tests de l'attaque (recherche, admin token, flag) — consigner résultats.
    - Vérifier logs d'accès et confirmer absence d'anomalies après patch.
- **Rotate secrets** : remplacer clés/jetons utilisés pendant l'incident.

---

5. Communication (immédiat puis 24 h)

- **Message court aux stakeholders** : résumé de l'impact, actions prises et état (« containment réalisé, investigation en cours »).
- **Rapport technique** (24 h) : chronologie, preuves (hashes, captures), recommandations et plan de mitigation.
- **Transparence sur IA** : documenter l'usage d'IA dans rapport (outil + prompts).

---

6. Preuves & audits

- Conserver dossier `evidence/` immuable (read-only copy). Inclure : `commands.txt`, captures d'écran, `flag.sha256`.
- Ne pas mettre `evidence/flag.txt` dans un repo public ; ne pousser que `flag.sha256` et captures.
- Signer électroniquement (ou checksum) le dossier de preuves si requis.

---

7. Rôles & responsabilités (rapide)

- **Incident lead** : coordonne actions, decisions de mise hors ligne.
- **Tech lead (Dev)** : applique containtment et correctifs code.
- **Forensic / Evidence** : collecte et protège preuves.
- **Comms / Manager** : notifications & rapport aux stakeholders.

---

8. Checklist de sortie d'urgence

- Service isolé / restriction appliquée
- Copies des preuves sauvegardées
- Token secret retiré
- Authentification appliquée sur `/admin` et `/flag`
- Tests d'exploitation rejoués et échoués (preuve)
- Rapport préliminaire remis au manager