Rapport d’audit – HackBench Cybernova 2025

Consultants : Colin, Hugo
Entreprise : Cybernova – Équipe Red/Blue Team
Date : 20–21 octobre 2025
Durée : 48h
Application cible : Intranet RH Demo – NovaTech
Environnement : ExpressJS (Replit)

1. Contexte de la mission

L’entreprise fictive NovaTech soupçonne la présence de failles sur son intranet interne RH. Dans le cadre du HackBench organisé par Cybernova, l’objectif était de reproduire une situation réelle d’audit de sécurité. L’application ExpressJS hébergée sur Replit comporte plusieurs endpoints : **/** – page d’accueil **/search** – recherche d’utilisateur **/admin** – console d’administration **/flag** – ressource sensible

2. Méthodologie

L’audit a été conduit en quatre phases principales :

Phase	Objectif	Outils
Reconnaissance	Identifier les endpoints exposés	curl, navigateur web
Exploitation	Tester les points d’entrée vulnérables	curl
Validation	Obtenir et prouver l’accès au flag	curl
Analyse	Formuler les correctifs adaptés	Documentation technique

3. Constat et preuves

Endpoint /search : absence de validation du paramètre q — fuite potentielle d’informations internes.
Endpoint /admin : jeton administrateur statique en clair dans l’URL — risque d’usurpation.
Endpoint /flag : accès public non protégé au fichier flag — compromission critique.

4. Analyse des vulnérabilités

Vulnérabilité	Gravité	Impact
Absence d’authentification sur /flag	Critique	Exfiltration de données confidentielles
Token admin statique et en clair	Élevée	Usurpation d’accès administrateur
Entrée utilisateur non validée dans /search	Moyenne	Fuite d’informations ou injection
Manque de journalisation	Faible	Absence de traçabilité

5. Recommandations

■ Implémenter une authentification serveur pour /admin et /flag (sessions, JWT, etc.). ■ Supprimer le token statique et interdire la transmission de secrets par URL. ■ Valider et filtrer les entrées utilisateur. ■ Journaliser les accès aux endpoints sensibles (IP, user agent, timestamp). Mettre à jour Express et séparer le fichier flag.txt dans un répertoire non public.

6. Conclusion

L’audit a permis de mettre en évidence plusieurs vulnérabilités majeures sur l’intranet RH simulé. La compromission du flag prouve l’absence de contrôle d’accès effectif. Les correctifs proposés permettront de renforcer la sécurité tout en respectant les bonnes pratiques OWASP.

Niveau de risque global : Élevé
Flag obtenu : ■
Remédiations : en cours par l’équipe Blue Team.