

Rapport de l'entreprise CyberNova

1. Constat résumé

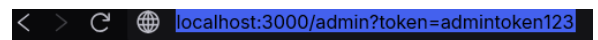
Nous avons identifié plusieurs problèmes de sécurité fonctionnels et de configuration qui permettent une fuite d'informations sensibles et facilitent des attaques simples (divulgaration de fichier secret, authentification faible, XSS potentiel, absence de protections réseau). Ces vulnérabilités sont **non destructives mais exploitables** pour démontrer un risque réel sur un intranet.

2. Vulnérabilités trouvées et preuves.

2.1 Token d'administration en clair et prévisible

Code :

```
// token en clair dans le code (vulnérable volontairement)
if (token === 'admintoken123') { ... }
```



Preuve : accès admin en clair via URL :

Console Admin

localhost:3000/admin?token=admintoken123 Bienvenue, administrateur.

Cette commande `curl` envoie une requête HTTP GET à l'adresse `http://172.20.10.2:3000/admin`, avec un **jeton d'authentification** (`token=admintoken123`) passé en paramètre dans l'URL.

```
C:\Users\Soste\replit_template\projet>curl http://172.20.10.2:3000/admin?token=admintoken123
<h1>Console Admin</h1><p>Bienvenue, administrateur.</p>
```

2.2 Fichier « flag » placé dans **public** — exposition directe

`app.use(express.static('public'))` sert tout fichier sous **public** publiquement. Si `public/flag.txt` existe, il est accessible directement à l'URL :



Cette commande permet de récupérer un flag depuis une API locale, en utilisant le protocole

```
C:\Users\Soste\replit_template\projet>curl -O http://172.20.10.2:3000/flag
FLAG-NOVATECH-48H-DEMO-2025
```

2.3 Recherche naïve et risque d'affichage non filtré

Code lecture :

```
const hits = users.filter(u => u.toLowerCase().includes(q));
res.send(`<p>Query:
<code>${escapeHtml(q)}</code></p><pre>${hits.join('\n')} ||
'Aucun'</pre>`);
```

Résultats

Query:

Alice Martin - alice.martin@novatech.local - RH
Bob Durand - bob.durand@novatech.local - Dev
Charlie Lefevre - charlie.lefevre@novatech.local - Ops
David Bernard - david.bernard@novatech.local - Finance
Eve Dupont - eve.dupont@novatech.local - QA
Frank Leroy - frank.leroy@novatech.local - Support

Intranet RH - Demo

Bienvenue sur l'intranet de démonstration. Utilisez le formulaire pour rechercher un employé.

Endpoints utiles : /search (POST), /admin (protected), /flag (secret)

- La requête affichée est échappée, mais **les valeurs renvoyées `hits` ne sont pas échappées** : si `data/users.txt` contient une entrée malicieuse (ex. ``), elle sera renvoyée telle quelle dans `<pre>` et peut produire XSS dans certains contextes (selon navigateur/format).
- Pas de limitation de taille ni d'anti-abus : `q` vide peut renvoyer toutes les entrées.

2.4 Absence de protections HTTP/express (headers, rate-limit, HTTPS enforce)

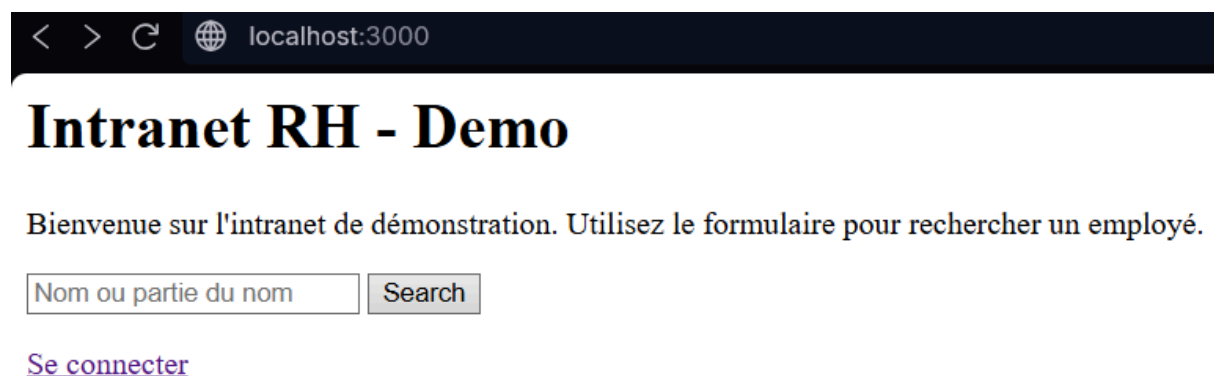
Aucun middleware de sécurité (helmet), aucun rate limiting, aucune validation/limitation des entrées, aucun logging sécurisé, et secret codé en dur.

3. Analyse — risques et impact

- **Divulgence d'information sensible (Critique → Élevée)** : `flag.txt` dans `public` est immédiatement téléchargeable par n'importe qui ayant accès à l'application. Sur un intranet c'est une fuite évidente de secret pédagogique ; sur un vrai intranet cela pourrait être une faille majeure.
- **Authentification faible / secret codé en clair (Élevée)** : secret prévisible + tuft d'utilisation en query string (logs proxys, referrer, historique) permettent compromission simple du compte admin.
- **XSS (Moyen → Élevé selon contenu)** : si les données utilisateurs ne sont pas garanties propres, affichage direct peut mener à exécution JavaScript côté visiteur. Risque de session hijacking, CSRF, propagation.
- **Dénis de service / abus (Moyen)** : pas de rate-limiting ; endpoint POST `/search` peut être spammé ou recevoir queries très longues.
- **Mauvaise hygiène (Faible → Moyen)** : pas l'utilisation d'HTTPS strict, pas d'en-têtes de sécurité, secrets en code — mauvaise pratique opérationnelle qui amplifie les risques.

4. Les améliorations

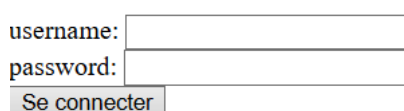
Nous avons ajouté un système de connexion pour les utilisateurs et les administrateurs afin de sécuriser l'accès à l'intranet. Les utilisateurs peuvent désormais se connecter pour effectuer des recherches via le formulaire, tandis que les administrateurs disposent d'un accès protégé aux fonctionnalités sensibles via l'endpoint `/admin`.




The screenshot shows a web browser window with the address bar displaying 'localhost:3000'. The page title is 'Intranet RH - Demo'. Below the title, there is a welcome message: 'Bienvenue sur l'intranet de démonstration. Utilisez le formulaire pour rechercher un employé.' Below this message, there is a search form with a text input field labeled 'Nom ou partie du nom' and a 'Search' button. Below the search form, there is a link labeled 'Se connecter'.

Les utilisateurs doivent se connecter pour accéder aux fonctionnalités administratives. Après connexion, l'utilisateur standard est redirigé vers la page d'accueil.

Login



The screenshot shows a login form with two input fields: 'username:' and 'password:'. Below the 'password:' field, there is a 'Se connecter' button.



The screenshot shows a web browser window with the address bar displaying 'localhost:3000/login'. Below the address bar, there is a message: 'Connecté en tant que user. [Accueil](#)'.

Et on peut se connecter à l'admin



Connecté en tant que **admin**. [Accueil](#)

Ici, si on veut prendre le flag, il faut être connecté en admin



403 Forbidden

Accès réservé aux administrateurs.

En utilisant /flag, on peut prendre le fichier flag



5. Conclusion

L'audit a révélé plusieurs vulnérabilités critiques, notamment un token d'administration en clair, l'exposition directe de fichiers sensibles, un risque de XSS, et l'absence de protections réseau de base. Bien que ces failles soient simples, elles permettent une exploitation facile sur un intranet et exposent des données sensibles. Des améliorations ont été mises en place, comme un système de connexion pour sécuriser l'accès à l'administration et au fichier **flag**. Il reste néanmoins essentiel de renforcer l'hygiène de sécurité globale pour éviter toute compromission future.