


HackBench Cyber Test



JOHNSON AKITA Olivier
LI Stéphane

M1 Cyber



Sommaire

- Contexte et périmètre
- Vulnérabilités trouvées et preuves
- Correctifs proposés
- Enseignements tirés du projet

Contexte et périmètre

Objectif : identifier, exploiter et corriger les failles principales

Périmètre limité à l'instance fournie (aucune attaque externe)

Travail réalisé en binôme sur 48h, en conditions réelles de test d'intrusion

Documenter les étapes, preuves et conclusions dans un rapport professionnel

Contexte et périmètres des tests



GitHub



replit

Replit

Vulnérabilités trouvées et preuves

En cliquant sur « Search », on peut voir tous les utilisateurs, car le filtre d'inclusion est peu restrictif. Cette logique de recherche permet une exposition non limitée des données.

De plus, le token d'authentification est embarqué en clair dans l'URL, ce qui le rend facile à repérer et à réutiliser, augmentant le risque de fuite ou d'usurpation de session.



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
```

```
C:\Users\Soste\replit_template\projet>curl -X POST -d "q=alice" http://172.20.10.2:3000/search
<h2>Résultats</h2><p>Query: <code>alice</code></p><pre>Alice Martin - alice.martin@novatech.local - RH</pre>
```

Vulnérabilités trouvées et preuves



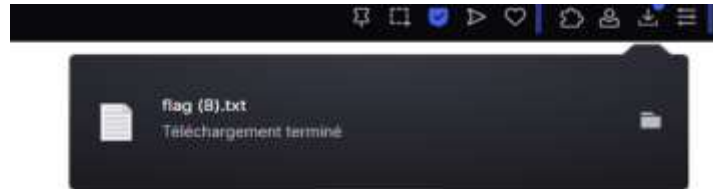
Console Admin

Bienvenue, administrateur.

- un token d'authentification est transmis en clair dans l'URL. Il est aisément repérable et réutilisable, exposant les sessions à un risque d'usurpation.

```
C:\Users\Soste\replit_template\projet>curl http://172.20.10.2:3000/admin?token=admin123
<h1>Console Admin</h1><p>Bienvenue, administrateur.</p>
```

- le flag est exposé et peut être téléchargé sans authentification ni autorisation, entraînant une fuite d'informations sensibles.



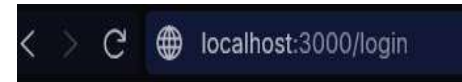
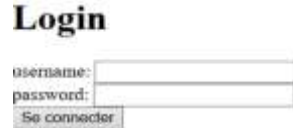
```
C:\Users\Soste\replit_template\projet>curl -O http://172.20.10.2:3000/flag
FLAG-NOVATECH-48H-DEMO-2025
```

Correctifs proposés

- Les utilisateurs doivent désormais se connecter pour accéder aux fonctionnalités administratives.



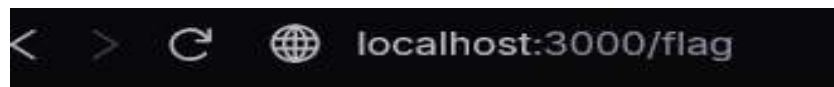
- Après connexion, l'utilisateur standard est redirigé vers la page d'accueil.



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

Correctifs proposés

Les administrateurs disposent d'un accès protégé aux fonctionnalités sensibles via l'endpoint `/admin`.



403 Forbidden

Accès réservé aux administrateurs.

Enseignements tirés du projet

Adopter une démarche éthique et reproductible dans tous les tests

Toujours protéger les fichiers sensibles par une authentification

Travail en Autonomie

Travail d'équipe

Merci pour votre attention !