



HACKATHON

**CYBER  
CHALLENGE**

DU 24 AU 26 AVRIL

2025

[www.smi-cyber.com](http://www.smi-cyber.com)



## Hackathon

Défiiez vos limites, sécurisez le futur.

# LISTE DES EXERCICES (PARTIE 2)



**Analyse de Logs (200 points)** : Détectez une compromission de comptes utilisateurs.



**Web Vulnerability & Patching (200 points)** : Exploitez une faille et sécurisez l'application.

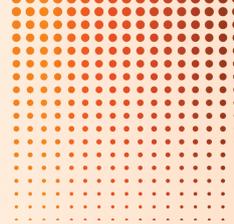


**Présentation (100 points)** : Les équipes défendront leur travail devant un jury composé de professionnels du secteur.



## Hackathon

Défiiez vos limites, sécurisez le futur.



# Votre objectif est simple

Résolvez chaque défi en appliquant vos connaissances en sécurité offensive et défensive.

## Règles générales

- Lisez attentivement les consignes de chaque exercice.
- Utilisez les outils et techniques adaptés à chaque situation.
- Documentez vos démarches et résultats pour expliquer vos découvertes et solutions.
- Vous les soumettrez par mail à la fin du challenge l'adresse suivante : [hackathon@rhopenlabs.africa](mailto:hackathon@rhopenlabs.africa)



## EXERCICE 1 : ANALYSE DE LOGS & DÉTECTION DE COMPROMISSION (50 POINTS)

### MISE EN SITUATION :

L'entreprise RHdata utilise plusieurs solutions logicielles qui partagent une même base de données. Seule une de ces applications est accessible via Internet. Récemment, l'entreprise a détecté des connexions suspectes : certains utilisateurs ont accédé au système depuis des emplacements inhabituels. Aucune intrusion physique n'a été constatée, ce qui laisse penser que la fuite provient de l'application web.

**Votre mission** est d'analyser les logs pour identifier les utilisateurs compromis et comprendre comment cette fuite a pu se produire.

### CONSIGNES :

- Accédez à la plateforme Wazuh via l'URL qui vous sera fournie: [wazuh](#)
- Connectez-vous avec les identifiants qui suivent:
  - username: **RHLabs**
  - password: **!Hacker@12**
- Appliquez un filtrage des logs en sélectionnant une période temporelle précise : **Mar 26 2025 de 17:30:00 à 18:00:00**



## EXERCICE 1 : ANALYSE DE LOGS & DÉTECTION DE COMPROMISSION (50 POINTS)

- Si vous n'êtes pas familier a wazuh, sur ce lien vous avez une description en image sur comment appliquer le filtre temporelle: [Filtrer les logs](#)

### INSTRUCTIONS :

- 1** Analysez les logs d'authentification généré par Wazuh.
- 2** Identifiez les **utilisateurs** ayant accédé au système depuis des localisations inhabituelles.
- 3** Déterminez les **comptes compromis**.
- 4** Proposez une **correction pour sécuriser** l'application web concernée.



## EXERCICE 2 : VULNÉRABILITÉ WEB & SÉCURISATION (100 POINTS)

### MISE EN SITUATION :

Suite à l'analyse des logs, vous avez confirmé que les identifiants des utilisateurs ont été compromis. L'enquête a révélé que la faille provient d'une vulnérabilité dans l'application web.

**Votre mission** est d'exploiter cette vulnérabilité, de récupérer le flag, puis de proposer un correctif pour sécuriser l'application.

### INSTRUCTIONS :

**1** Interagissez avec l'application web accessible ici: [application web](#). Une fois cela fait trouvez un moyen d'exploiter la faille identifiée à l'exercice 4

**2** Proposez une **solution** pour corriger cette faille

**NB : L'application à patcher est disponible dans le dossier ressources fourni.**