



HACKATHON

**CYBER**  
**CHALLENGE**

FROM APRIL 24 TO 26

2025

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



# LIST OF EXERCISES (PART 2)



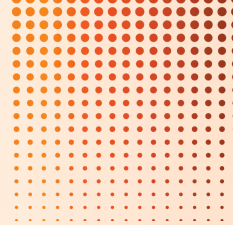
**Log Analysis (200 points)** : Detect a user account compromise.



**Web Vulnerability & Patching (200 points)** : Exploit an vulnerability and secure the application.



**Presentation (100 points)** : The teams will present and defend their work before a panel of industry professionals.



## Your Objective is Simple

Solve each challenge by applying your knowledge of offensive and defensive security.

## General Rules

- Carefully read the instructions for each exercise.
- Use the appropriate tools and techniques for each situation.
- Document your steps and results to explain your findings and solutions.
- Submit them via email at the end of the challenge to the following address: [hackathon@rhopenlabs.africa](mailto:hackathon@rhopenlabs.africa)



## EXERCISE 1 : LOG ANALYSIS & COMPROMISE DETECTION (200 POINTS)

### SCENARIO

RHdata uses multiple software solutions that share the same database. Only one of these applications is accessible via the Internet. Recently, the company detected suspicious logins: some users accessed the system from unusual locations. No physical intrusion was reported, suggesting that the breach originated from the web application.

**Your Mission :** Analyze the logs to identify compromised users and understand how this data breach occurred.

### GUIDELINES :

- Access the Wazuh platform via the provided URL :  
[wazuh](#)
- Log in using the following credentials :
  - username: **RHLabs**
  - password: **!Hacker@12**
- Filter the logs by selecting a specific time period:
  - Date : **Mar 26 2025**
  - Time range : **17:30:00 à 18:00:00**



## EXERCISE 1 : LOG ANALYSIS & COMPROMISE DETECTION (200 POINTS)

- If you are not familiar with Wazuh, you can refer to this step-by-step guide with images on how to apply the time filter : [Filter Data for Last 24 Hours in Wazuh](#)

### INSTRUCTIONS :

- 1 Analyze authentication logs generated by Wazuh.
- 2 Identify **users** who accessed the system from unusual locations.
- 3 Determine **compromised accounts**.
- 4 Propose a **security fix to protect** the affected web application.



## EXERCISE 2 : WEB VULNERABILITY & PATCHING (200 POINTS)

### SCENARIO

Following the log analysis, you confirmed that user credentials were compromised. The investigation revealed that the breach originated from a vulnerability in the web application.

**Your Mission** is to determine and exploit the vulnerability in the web application to retrieve the flag. Then propose a security fix to mitigate the vulnerability and protect the application.

### INSTRUCTIONS :

1

Interact with the web application available at: [web application](#). Once done, name the vulnerability and find a way to exploit the vulnerability identified in Exercise 4.

2

Propose a **fix to patch the vulnerability** and secure the application.

**Note :** The application to be patched is available in the provided resources folder