**Hack The Box Audit Progress**

Here is a summarized version of your Hack The Box Audit Report so far, integrating the provided screenshots and additional information.

**Hack The Box Audit Report**

**Project Name:** Hack The Box Audit  
**Prepared By:** Anuj Kulat & Syed Hussain  
**Date:** 12/2/2024

**Setup Overview**

1. **Hack The Box Account and Environment Setup:**
   * Created an account on Hack The Box and configured the testing environment with **Kali Linux**.
   * Connected to Hack The Box resources and established a secure connection using **VPN**.
2. **Command Basics:**
   * Learned how to use Vim commands for editing, including:
     + **Press esc** to exit edit mode.
     + **Type :** followed by **wq!** to save and quit.

**Stage 1: Initial Target Enumeration and Scanning**

1. **Target Machine Identification:**
   * Selected the target machine **"Instant"** with IP address **10.129.231.155**.
   * Confirmed the machine is online and available for interaction.
2. **Initial Nmap Scan:**
   * Conducted an **Nmap scan** on the target IP to identify open ports and services.
   * Recorded results, including filtered and closed ports, to establish a baseline for further analysis.
3. **Website Access and Analysis:**
   * Accessed the website associated with the target IP and performed an **Nmap scan** to gather additional data.
   * Observed active services and logged any potential vulnerabilities for exploration.
4. **Application Source Code Exploration:**
   * Decompiled the source code and reviewed critical files such as **AdminActivities.java**.
   * Focused on analyzing HTTP request handling, especially authorization headers, URL endpoints, and sensitive tokens.
5. **Configuration File Analysis:**
   * Analyzed **network\_security\_config.xml** to identify network domains allowed by the application, including instant.htb and swagger-ui.instant.htb.
   * Verified security configurations and noted any settings that could lead to vulnerabilities.

**Stage 2: Service Enumeration and Exploitation**

1. **Authorization and API Exploration:**
   * Accessed **Swagger UI** for the target API, reviewed available endpoints, and tested API interactions.
   * Successfully authenticated with Bearer token and examined endpoints for functions like adding users, listing users, and viewing profiles.
2. **Data Retrieval and Exploitation Attempts:**
   * Explored the **/admin/list\_users** API endpoint to retrieve user information such as emails, roles, and wallet IDs.
   * Investigated **log file access** through **/admin/read\_log** endpoint by providing log file names as query parameters.
   * Attempted **path traversal** by modifying log file names to access sensitive files (e.g., /etc/passwd).