Write-up DBS401: Group 6

👋 Welcome to my write-up!

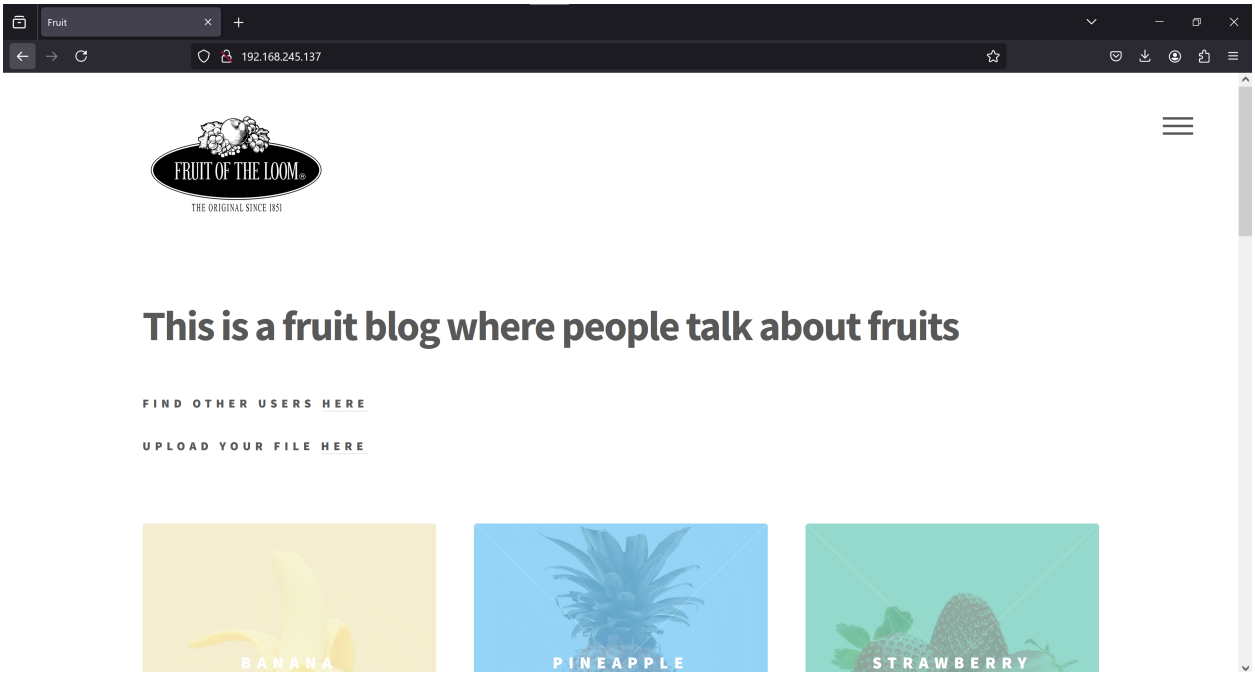
🔧 Tools: Burp Suite

🗂️ Flags' Completion Table

Flag Number	**Vulnerability's Name**	**Done**	**Flag**
1	Path Traversal	Got Flag Only	{flag1_path_traversal}
2	File Upload	Got Flag Only	{flag2_file_upload_priv_esc}
3	IDOR	yes	flag3

📝 Description

- A fruit blog website



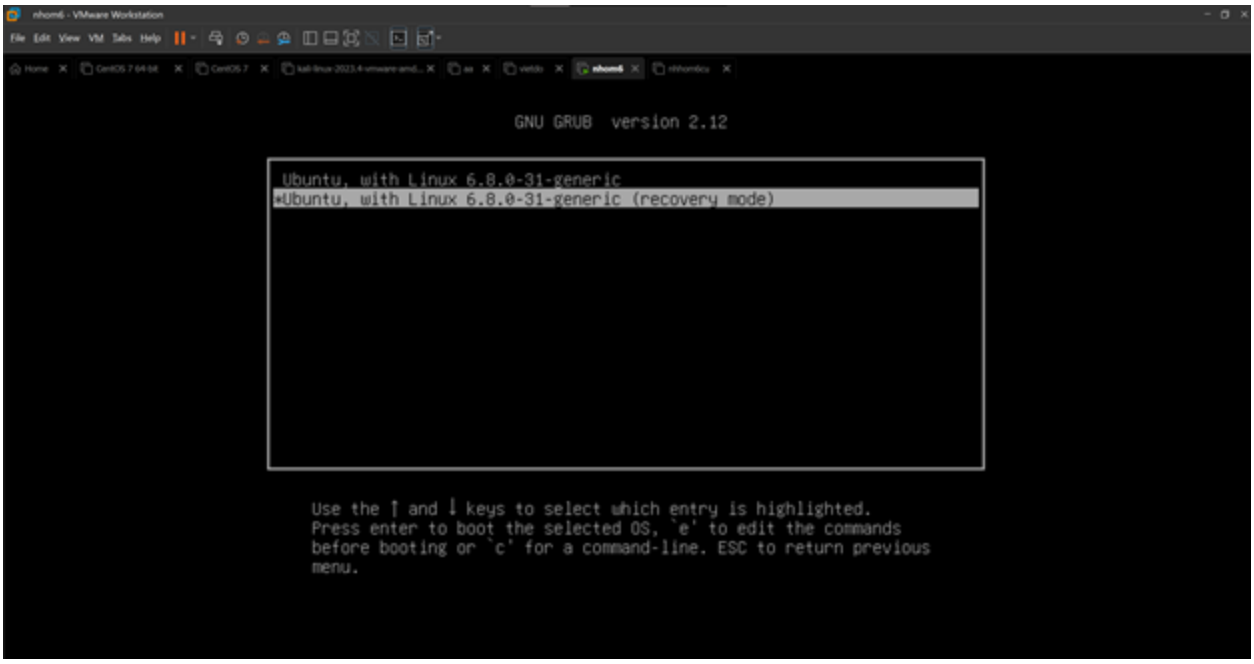
✅ Detailed Analysis

Vulnerability 1: OS Misconfiguration Leads To Unauthorized Root Access

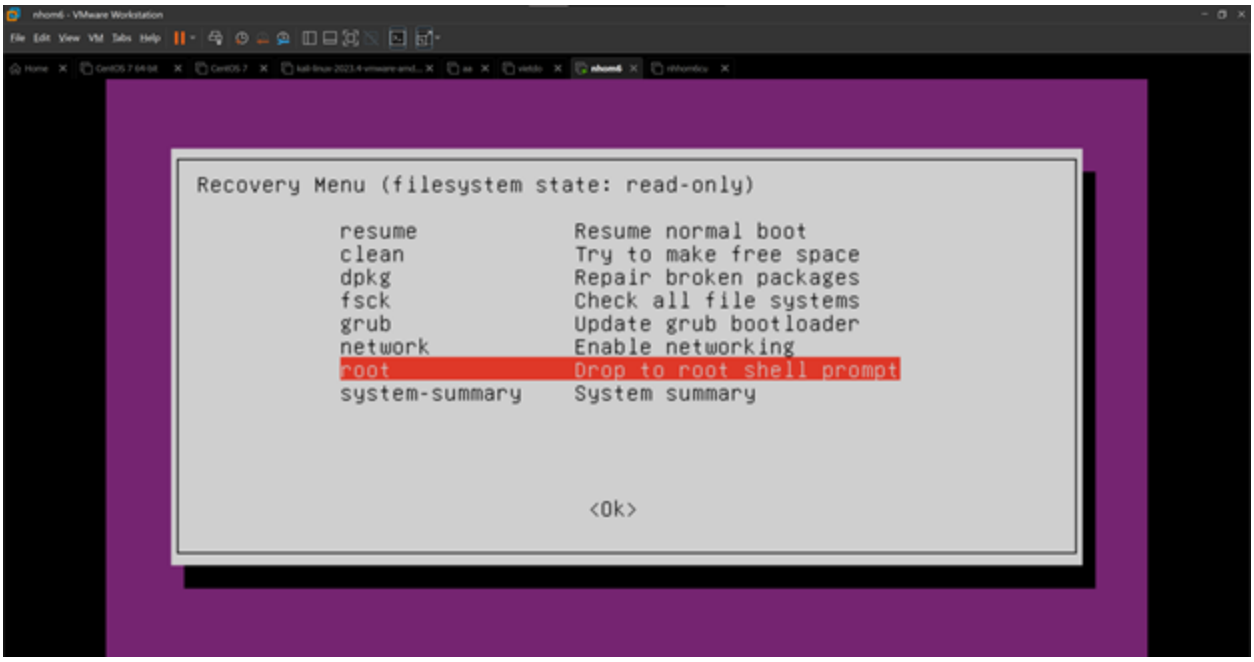
By accessing the recovery mode, an unauthorized person can gain root access without needing the root password because the owner of this machine forgot to set **GRUB Password**. This allows unauthorized person to change any system settings, view or modify all files, and potentially compromise any data stored on the machine.

Step to reproduce

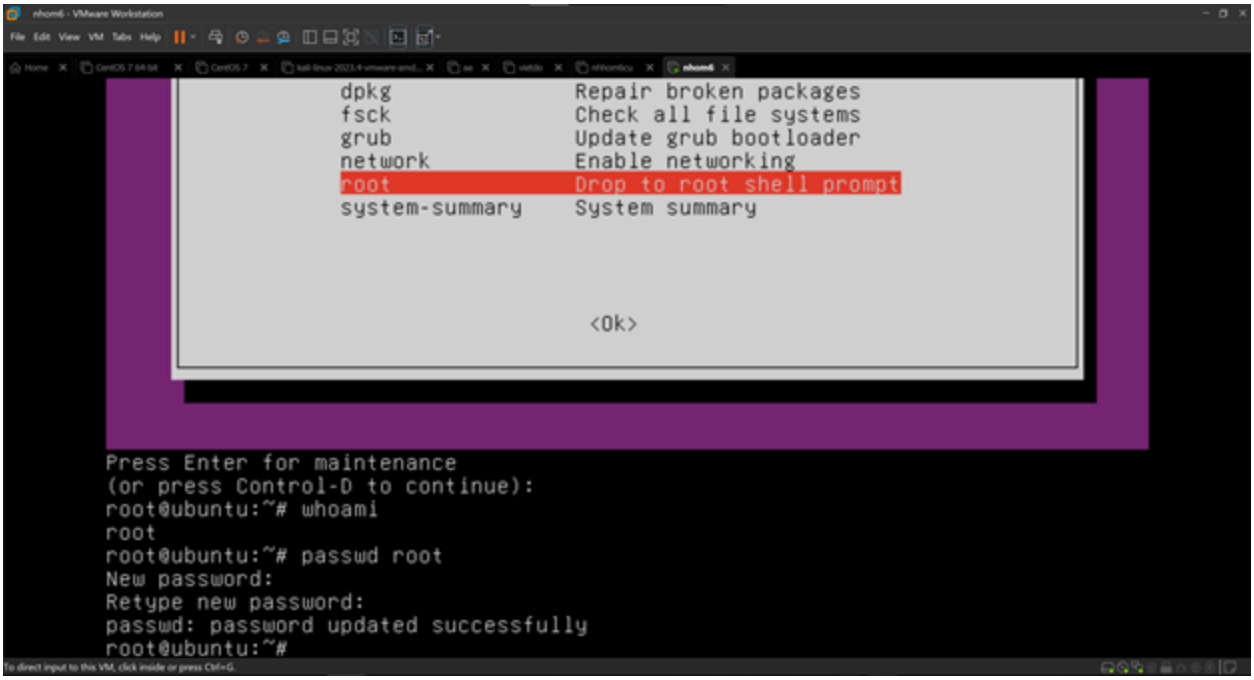
- **Reboot Your System**: Restart your computer.
- **Access GRUB Menu**: Hold down the `Shift` key during boot to access the GRUB menu. If you're using UEFI, you might need to press `Esc` instead.
- **Select Recovery Mode**



- **Select Root Shell Prompt**: After booting into recovery mode, you will be presented with a menu. Select the option "Drop to root shell prompt" or "root".



- Change password of root and we can get fully access to the machine

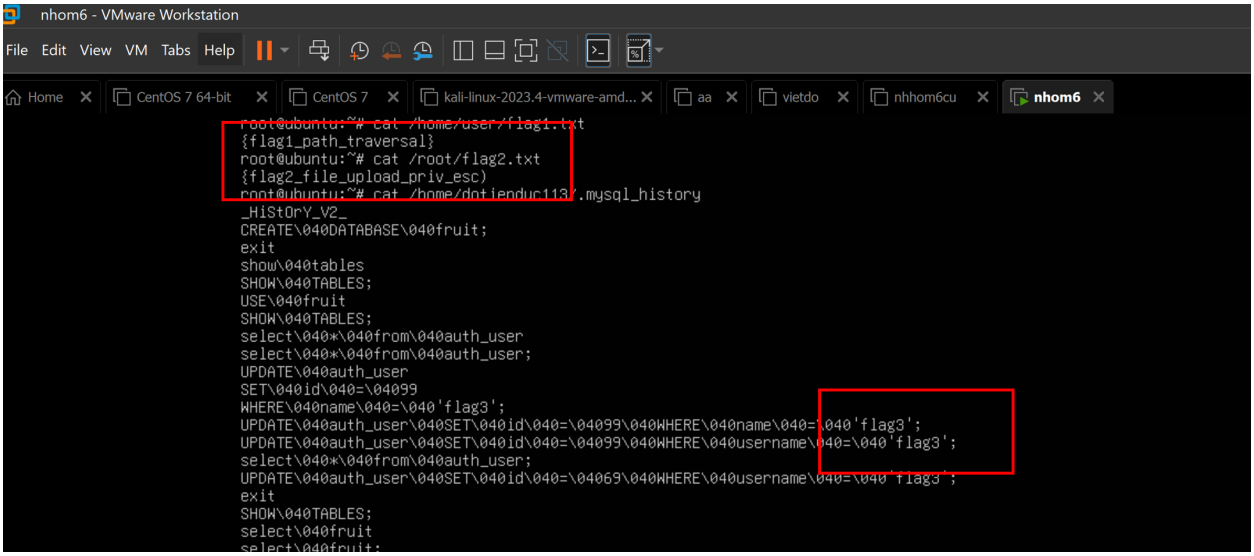


- According to hint that Group 6 provided, we can know exactly where the flags are

CTF: Cấu tạo máy sẽ giống 1 bài CTF cơ bản flag{....}
Flag1: ở /home/user
Flag2: ở /root
Flag3: tự tìm

Note: flag3 sẽ ko theo định dạng flag{...} mà chỉ là flag3

- So we can get all the flags at ease



🚩 **Flag 1:** {flag1_path_traversal}

🚩 **Flag 2:** {flag2_file_upload_priv_esc}

🚩 **Flag 3:** flag3

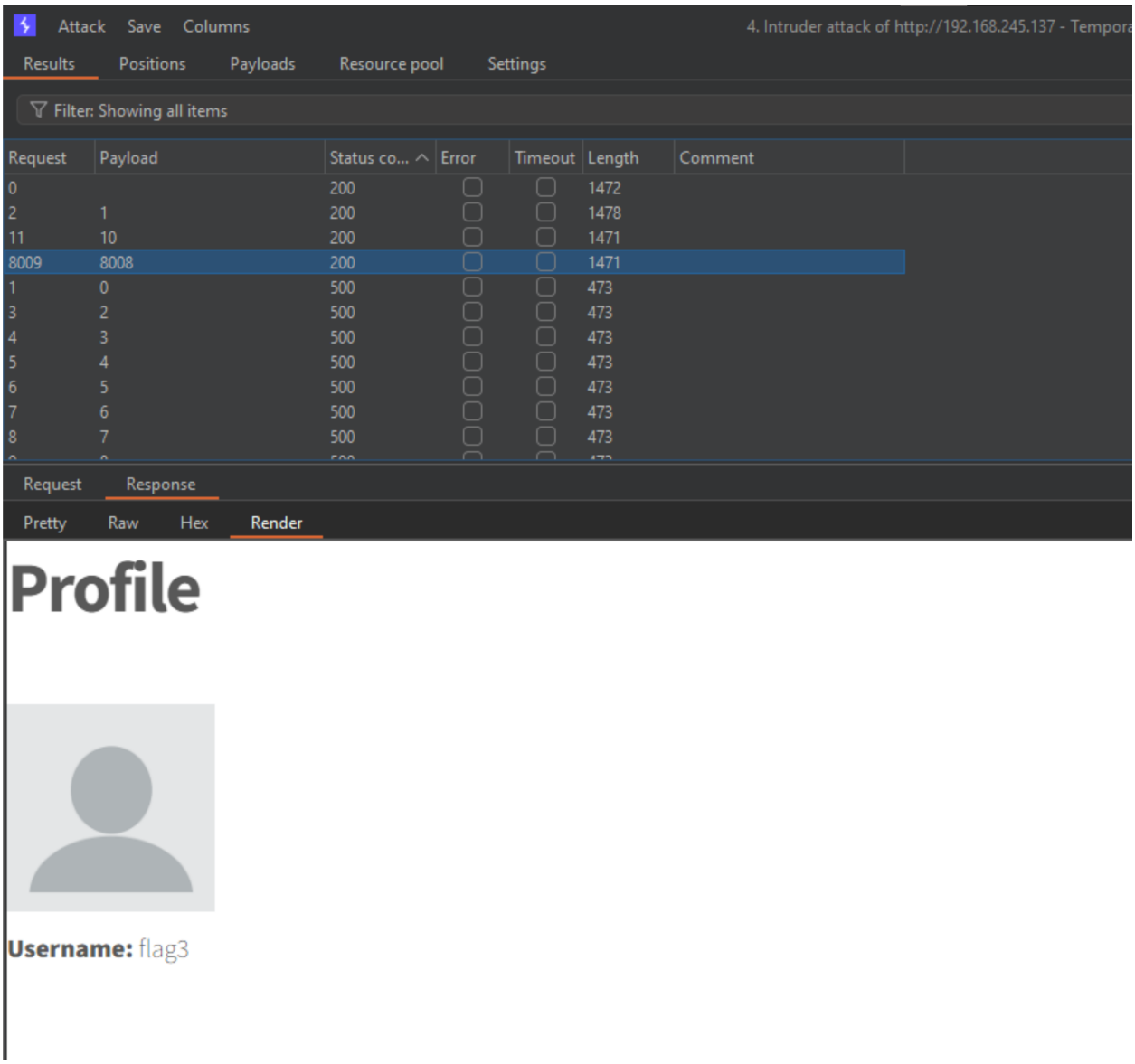
✅ Normal Solution

Vulnerability 2: IDOR

During the registration and login process, we examined the user information function. It was observed that the web application manages user IDs in a

predictable manner. For instance, accessing a user's details can be done via a URL like `http://192.168.245.137/user/id=8008`, which suggests the presence of an IDOR vulnerability.

- To confirm this, we utilized the intruder feature of the Burp Suite tool to test. Our tests revealed that the application indeed suffers from an IDOR vulnerability, as it allowed us to view the information of a few users. One of them is flag.



🚩 **Flag 3:** flag3