Contents

**[A.](#_Toc80894576)****[Điểm yếu vận hành khai thác](#_Toc80894576)** [2](#_Toc80894576)

**[1.](#_Toc80894577)****[Hardcode tài khoản trong source trên github](#_Toc80894577)** [2](#_Toc80894577)

**[2.](#_Toc80894578)****[Mở dịch vụ quản trị SSH qua Internet](#_Toc80894578)** [3](#_Toc80894578)

**[B.](#_Toc80894579)****[Lỗ hổng](#_Toc80894579)** [3](#_Toc80894579)

**[1.](#_Toc80894580)****[Lỗ hổng tấn công từ chối dịch vụ DOS Slowloris](#_Toc80894580)** [3](#_Toc80894580)

**[2.](#_Toc80894581)****[Lỗ hổng API thiếu xác thực tài khoản](#_Toc80894581)** [4](#_Toc80894581)

**[3.](#_Toc80894582)****[Lỗ hổng nhiều API không phân quyền truy xuất dữ liệu](#_Toc80894582)** [7](#_Toc80894582)

**[4.](#_Toc80894583)****[Lỗ hổng thiếu kiểm tra File extension khi Upload](#_Toc80894583)** [8](#_Toc80894583)

**Đánh giá ATTT website Vaccom**

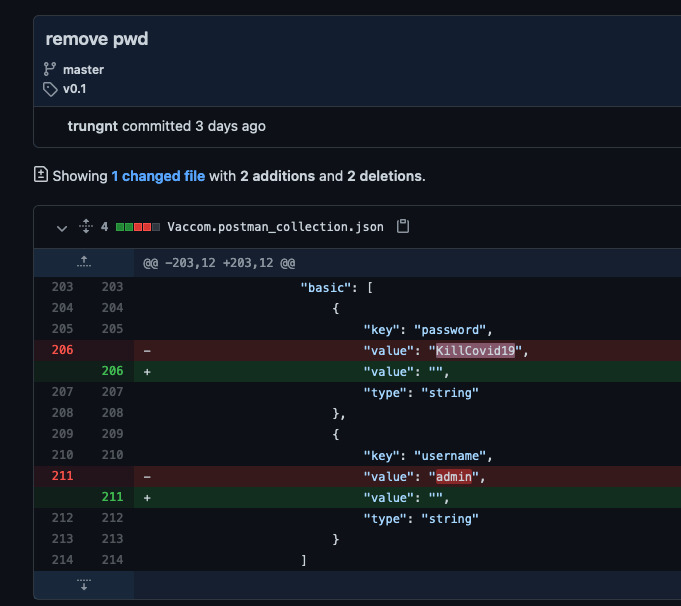
# **Điểm yếu vận hành khai thác**

## **Hardcode tài khoản trong source trên github**

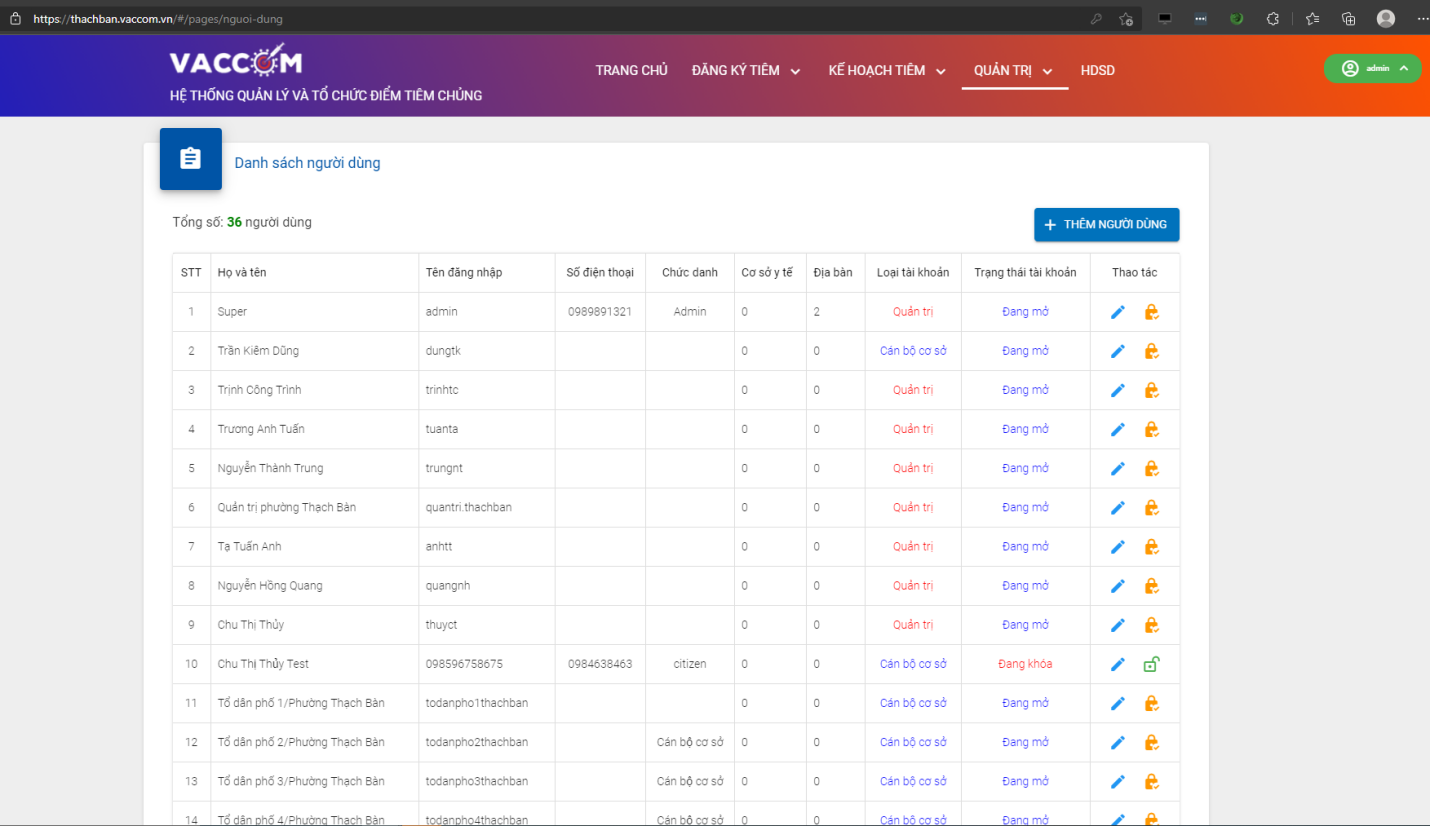
**Vị trí lỗi:** File Vaccom.postman\_collection.jon

Rủi ro: Lộ tài khoản admin portal đang sử dụng được thực tế của hệ thống

*Mật khẩu bị hardcode và lộ*



*Tài khoản admin đăng nhập thành công vào web portal (hiện đã đổi mật khẩu tạm để tránh bị tấn công)*

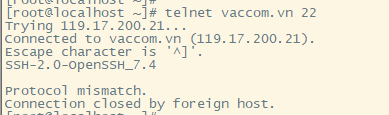


## **Mở dịch vụ quản trị SSH qua Internet**

**Vị trí lỗi:** Firewall mềm, dịch vụ SSHD trên máy chủ

**Rủi ro:** Tấn công bruteforce tài khoản từ Internet vào máy chủ dịch vụ

*Dịch vụ SSH mở port quản trị 22 ra Internet*

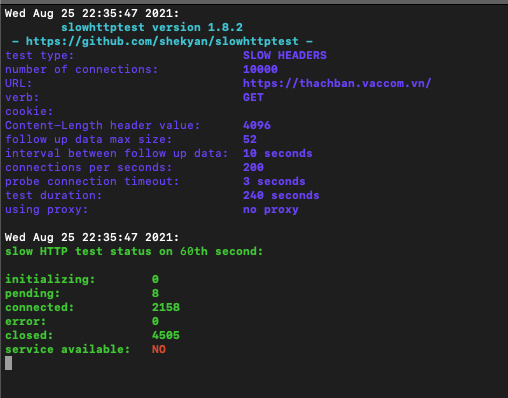


# **Lỗ hổng**

## **Lỗ hổng tấn công từ chối dịch vụ DOS Slowloris**

**Rủi ro:** Tấn công từ nguồn tài nguyên có hạn vào website, gây gián đoạn dịch vụ

*Từ nguồn là laptop cá nhân, gửi ~ 6.6k connections vào website gây gián đoạn dịch vụ vào 22:35 ngày 25/8*



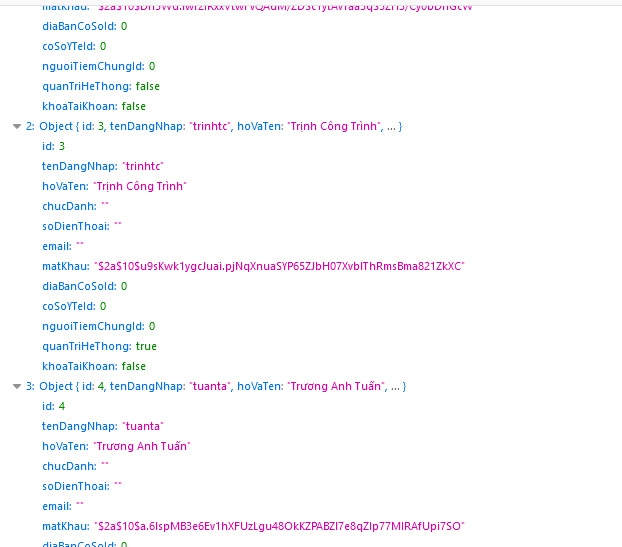
## **Lỗ hổng API thiếu xác thực tài khoản**

**Vị trí lỗi:** /rest/v1/app/get/

**Rủi ro:** Lộ thông tin truy xuất được từ API trên bao gồm thông tin user quản trị hệ thống, nội dung trả về bao gồm cả pass mã hóa; người đăng ký tiêm (thông tin cá nhân):

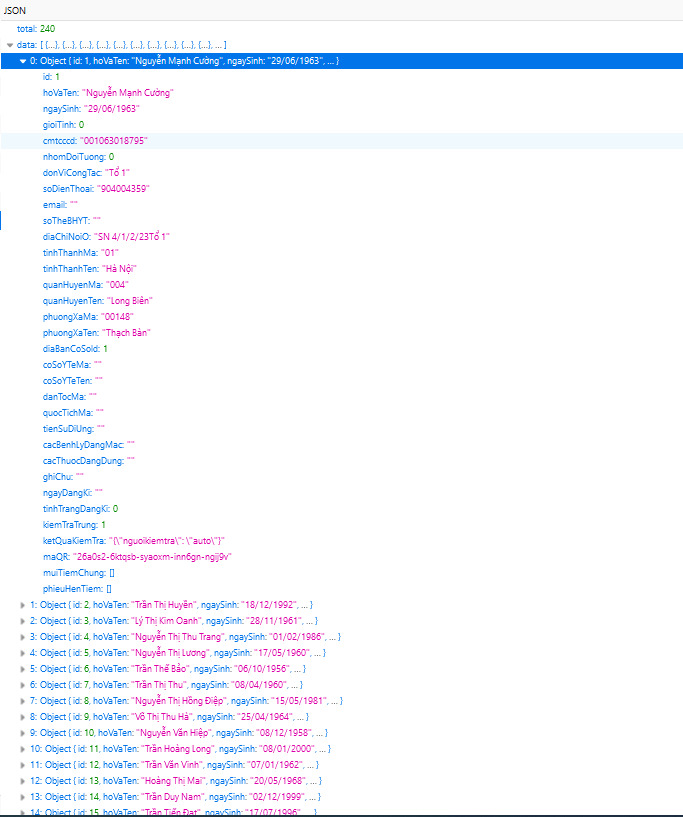
*Thông tin quản trị viên*

*<https://thachban.vaccom.vn:8080/rest/v1/app/get/nguoidung?page=0&size=20>*



*Thông tin người tiêm*

*<https://thachban.va5ccom.vn:8080/rest/v1/app/get/nguoitiemchung?cmtcccd=&nhomdoituong=&ngaydangki=&hovaten=&diabancosoid=&cosoytema=&tinhtrangdangky=1&kiemtratrung=&page=0&size=50>*



## **Lỗ hổng nhiều API không phân quyền truy xuất dữ liệu**

**Vị trí lỗi:** Tại nhiều API, tối thiểu có

/add/nguoitiemchung

/update/nguoitiemchung/{id}

/delete/nguoitiemchung/{id}

/update/nguoitiemchung/tinhtrangdangky

/delete/nguoitiemchung

/add/diabancoso

/update/diabancoso/{id}

/delete/diabancoso/{id}

/add/cosoyte

/update/cosoyte/{id}

/delete/cosoyte/{id}

/add/phieuhentiem

/update/phieuhentiem/{id

/delete/phieuhentiem/{id}

/add/lichtiemchung

/update/lichtiemchung/{id}

/delete/lichtiemchung/{id}

/get/lichtiemchung

/add/muitiemchung

/update/muitiemchung/{id}

/delete/muitiemchung/{id}

**Rủi ro:** Người dùng thường có thể truy xuất, sử dụng các API đặc quyềncủa quản trị viên như thêm sửa xóa lịch tiêm, người tiêm, địa bàn, cơ sở…. trên toàn bộ hệ thống

## **Lỗ hổng thiếu kiểm tra File extension khi Upload**

**Vị trí lỗi:**

/rest/v1/upload/one

/rest/v1/upload/multi

**Rủi ro:** Upload webshell lên máy chủ, làm bàn đạp để tấn công leo thang vào CSDL

