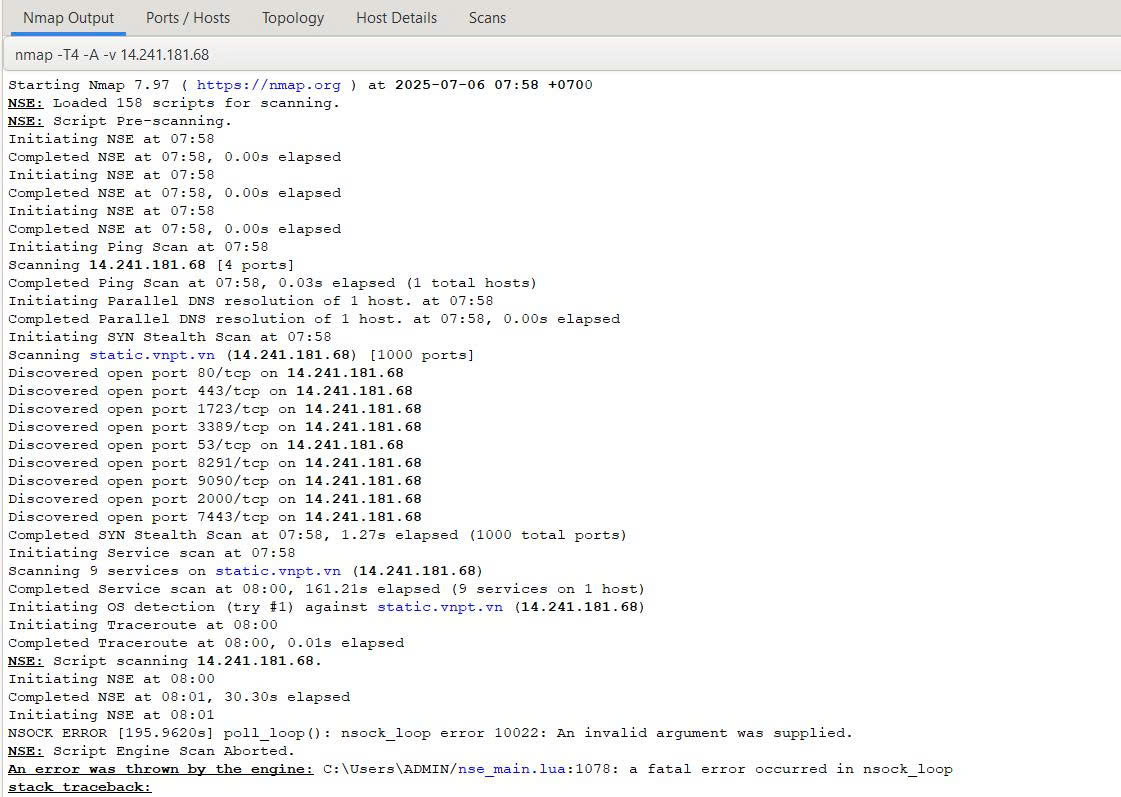
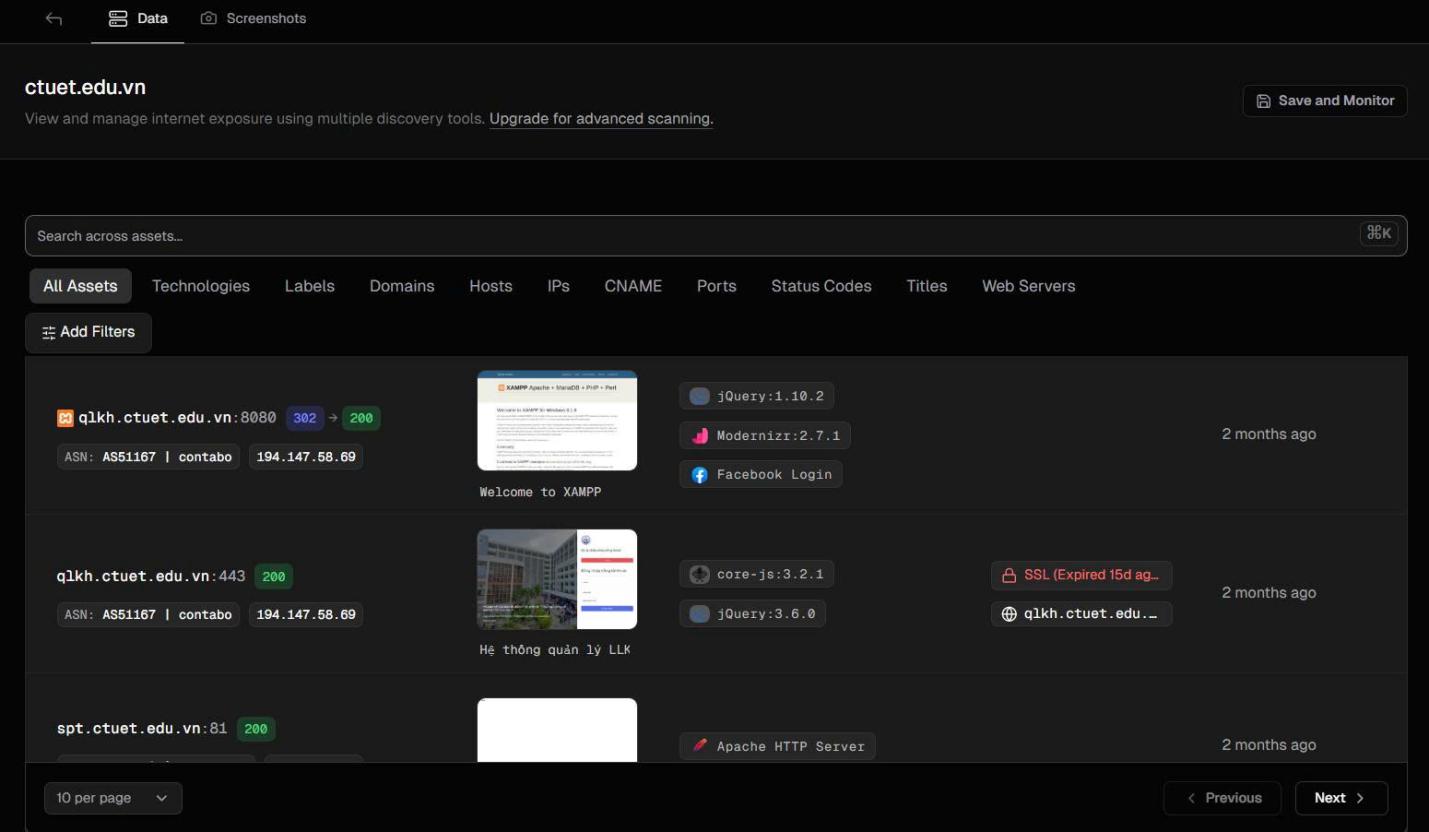
BÁO CÁO ĐÁNH GIÁ LỖ HỔNG BẢO MẬT WEBSITE STUDENT.CTUET.EDU.VN

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  | STT | Lỗ hổng bảo mật | Mô tả lỗi | Mức độ | Công cụ sử dụng |  |
|  | 1 | Tiết lộ thông tin máy chủ | Header HTTP hiển thị Apache → giúp kẻ tấn công xác định phần mềm và khai thác dễ hơn | Thấp | WhatWeb, Nmap http-headers |  |
|  | 2 | TRACE enabled | Máy chủ phản hồi TRACE → dễ bị tấn công XST (Cross Site Tracing) | Trung bình | Nmap --script http-methods |  |
|  | 3 | Directory listing /icons/ | Truy cập thư mục liệt kê tệp tin → có thể rò rỉ thông tin nếu lộ file cấu hình hoặc mã nguồn | Trung bình | Trình duyệt, Nmap http-enum |  |
|  | 4 | Dịch vụ RDP mở (3389/tcp) | Remote Desktop mở từ Internet → nguy cơ bị brute-force nếu không bảo vệ đủ mạnh | Cao | Nmap -p 3389, Shodan |  |
|  | 5 | Winbox MikroTik (8291/tcp) | Nếu giữ cấu hình mặc định → dễ bị chiếm quyền điều khiển thiết bị mạng nội bộ | Cao | Nmap -p 8291, MikroTik Tool |  |
|  | 6 | SSL dùng thuật toán yếu | Một số cipher như RC4, 3DES có thể đang hoạt động → giảm độ an toàn của kết nối HTTPS | Trung bình | Nmap ssl-enum-ciphers |  |





Thực hành lap3

