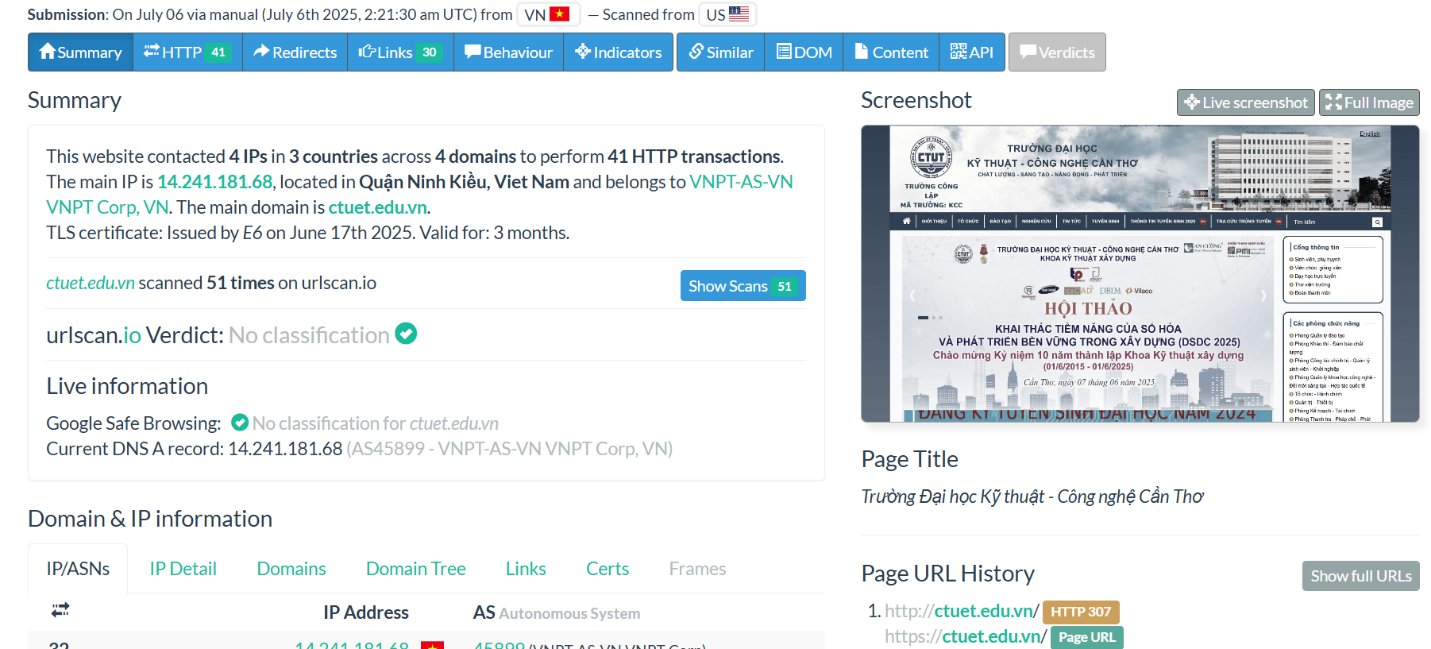
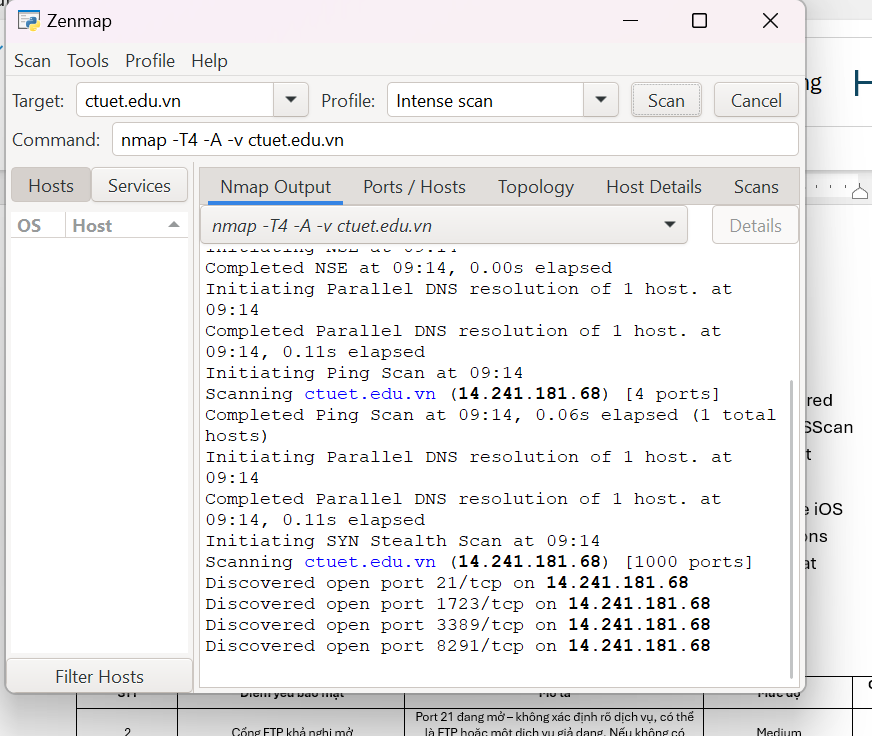
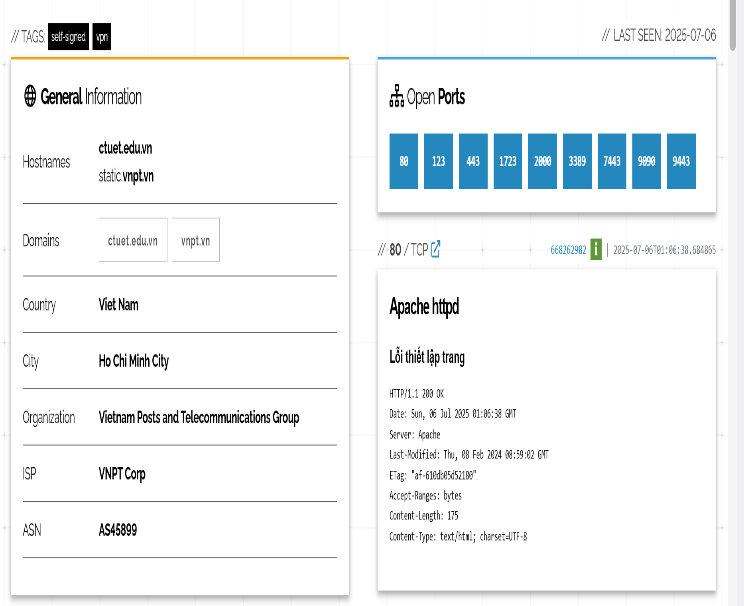
**Bài thực hành 2:**

****

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Điểm yếu bảo mật** |  | | **Mô tả** | **Mức độ nghiêm trọng (Critical, High, Medium, Low)** | **Công cụ sử dụng** |
| 1 | Lộ thông tin máy chủ |  | | Thông tin cấu hình máy chủ cho phép hacker đánh giá năng lực xử lý của máy chủ, từ đó đưa ra một số phương án tấn công | Low | thực hiện URL: |
| 2 | Dịch vụ FTP công kha |  | | Cổng 21 mở – nếu không có cấu hình xác thực bảo mật hoặc SSL thì dễ bị khai thác bằng brute force hoặc sniffing thông tin đăng nhập. | Medium | Nmap |
| 3 | Web Server |  | | Máy chủ chạy HTTP (port 80) và HTTPS (port 443) – cần kiểm tra kỹ phiên bản và các plugin để phát hiện lỗ hổng như XSS, SQLi, RCE, v.v. | Medium | Nmap |
|  | | | Tổng số lỗ hổng: 0 ;Critical: 0 ; High: 0 ; Medium: 0; Low: 1 | | | |