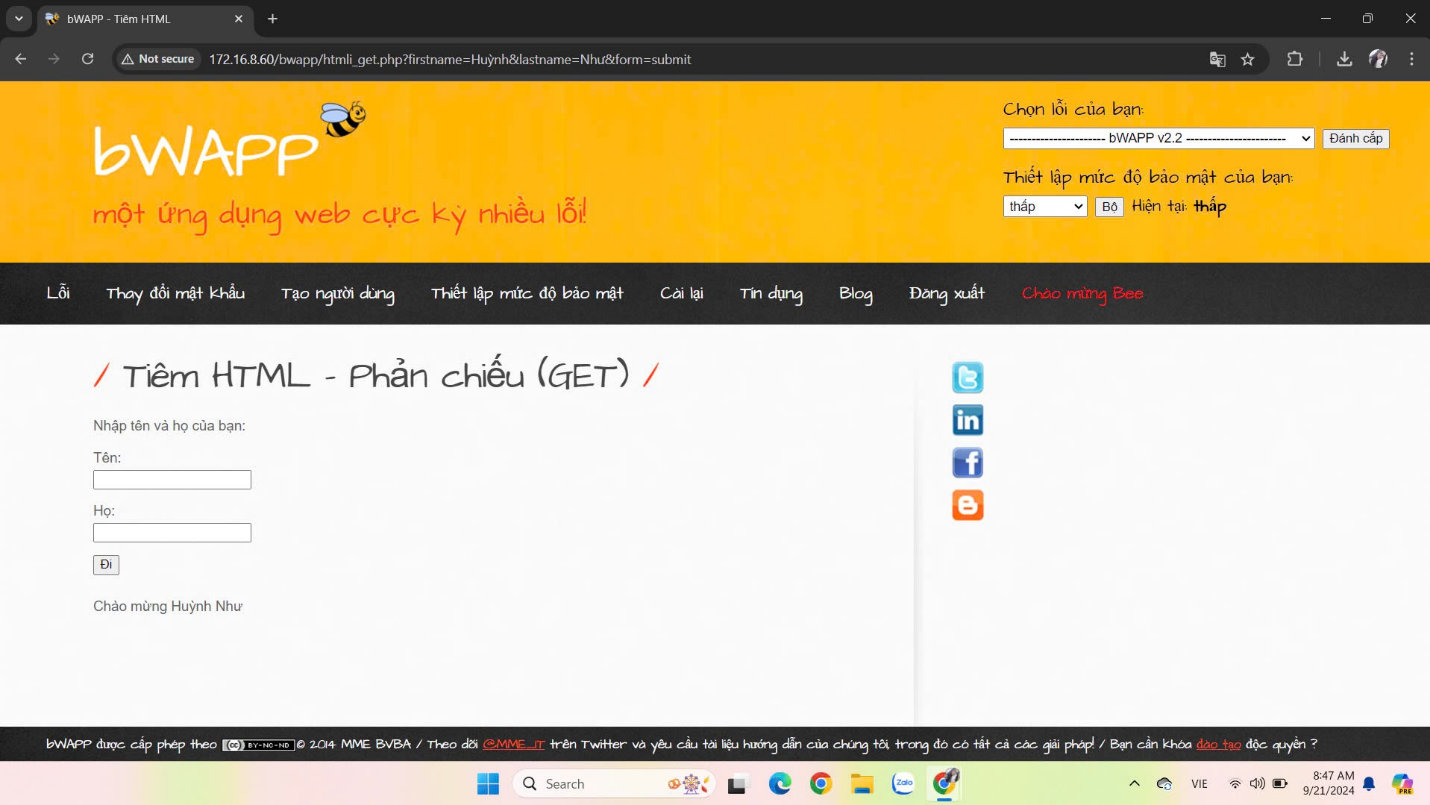
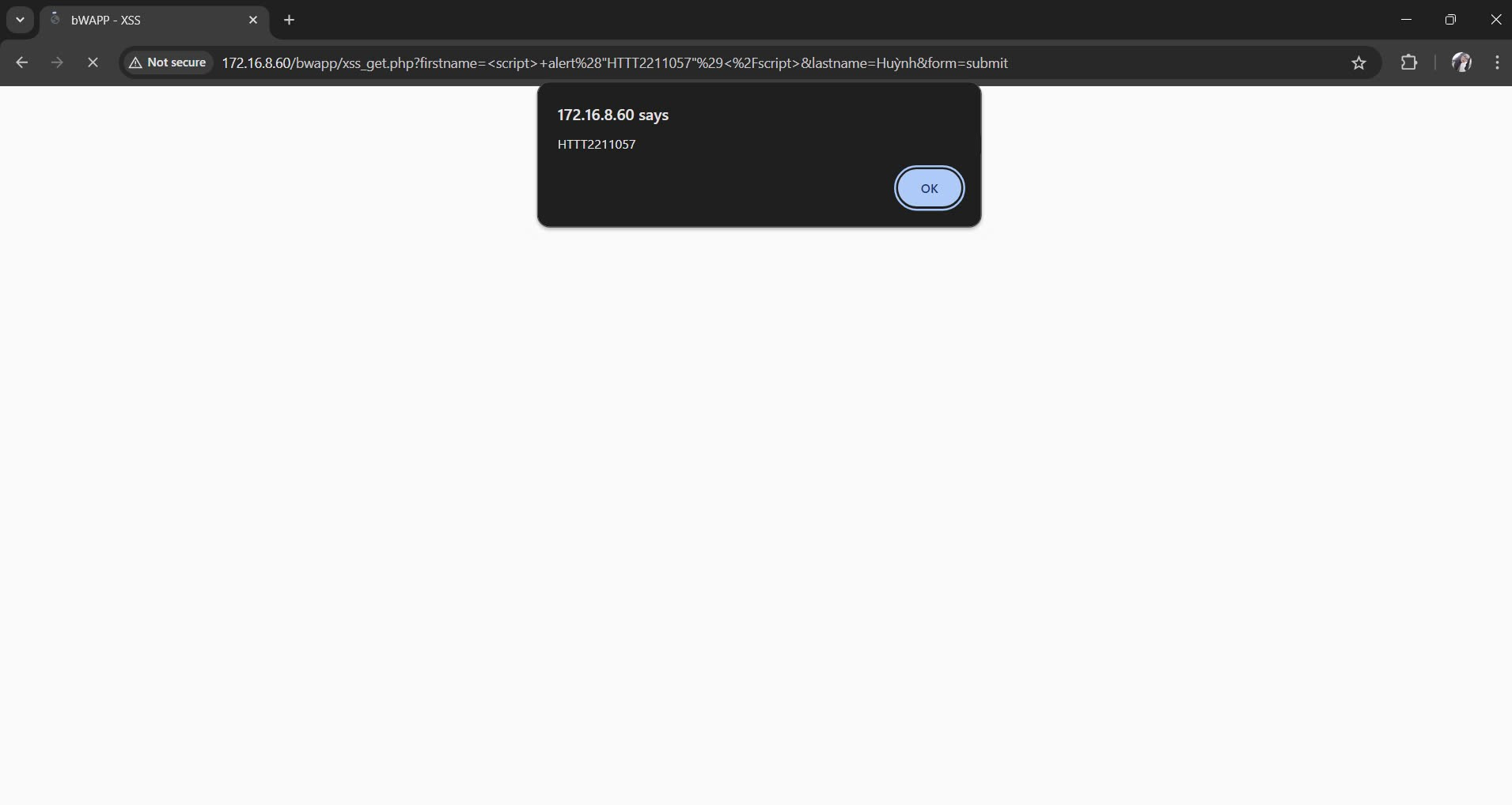
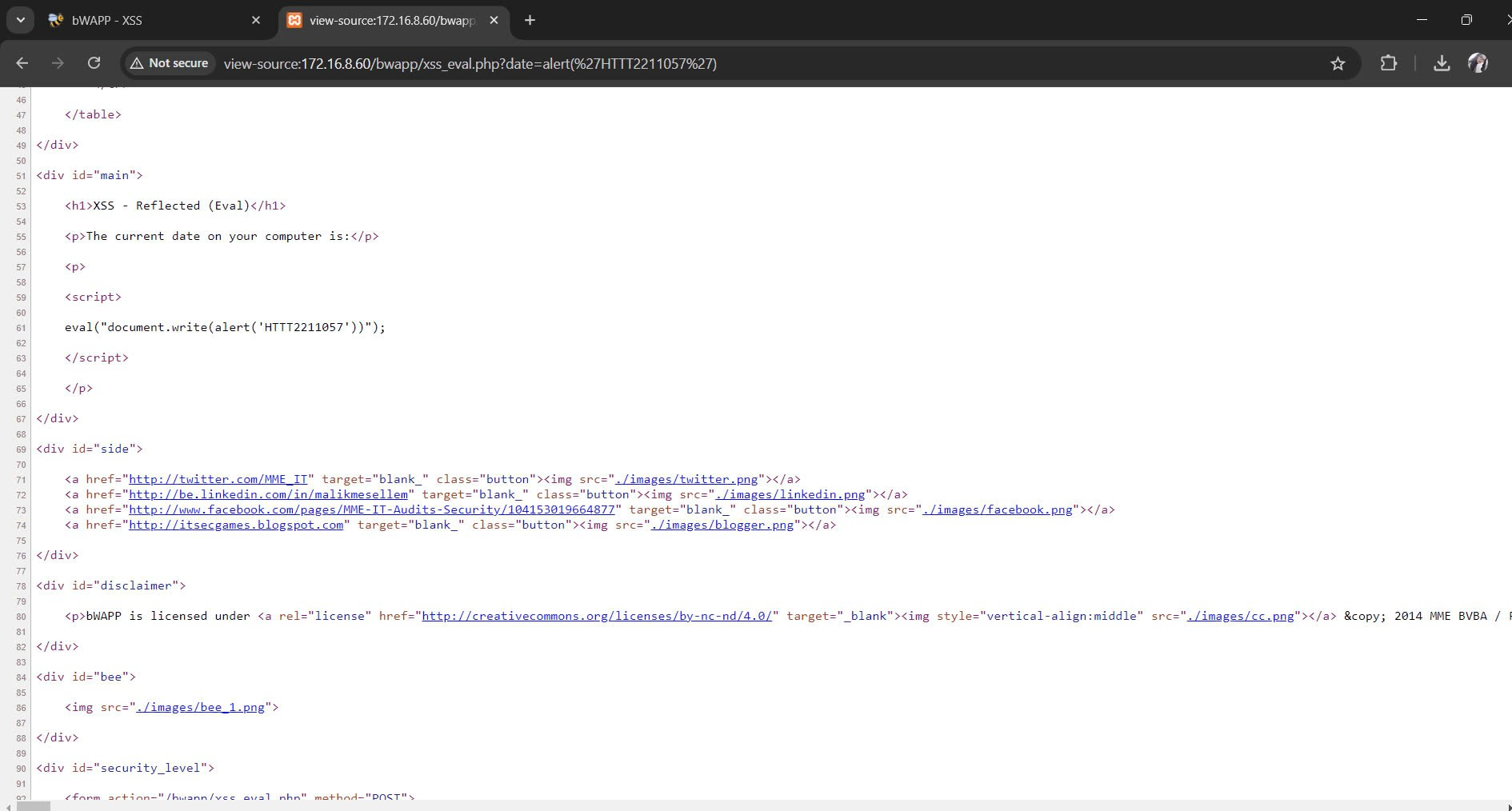
**THỰC HÀNH BUỔI 2**

1. Tấn công XSS phản xạ sử dụng phương thức GET (low)
2. Tấn công XSS phản xạ sử dụng phương thức GET (medium)

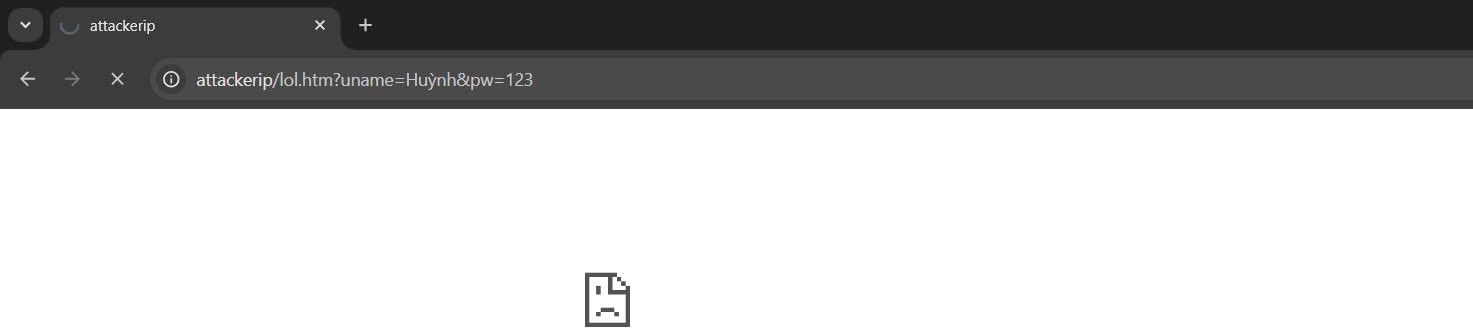


1. Tấn công XSS phản xạ sử dụng hàm EVAL (low)

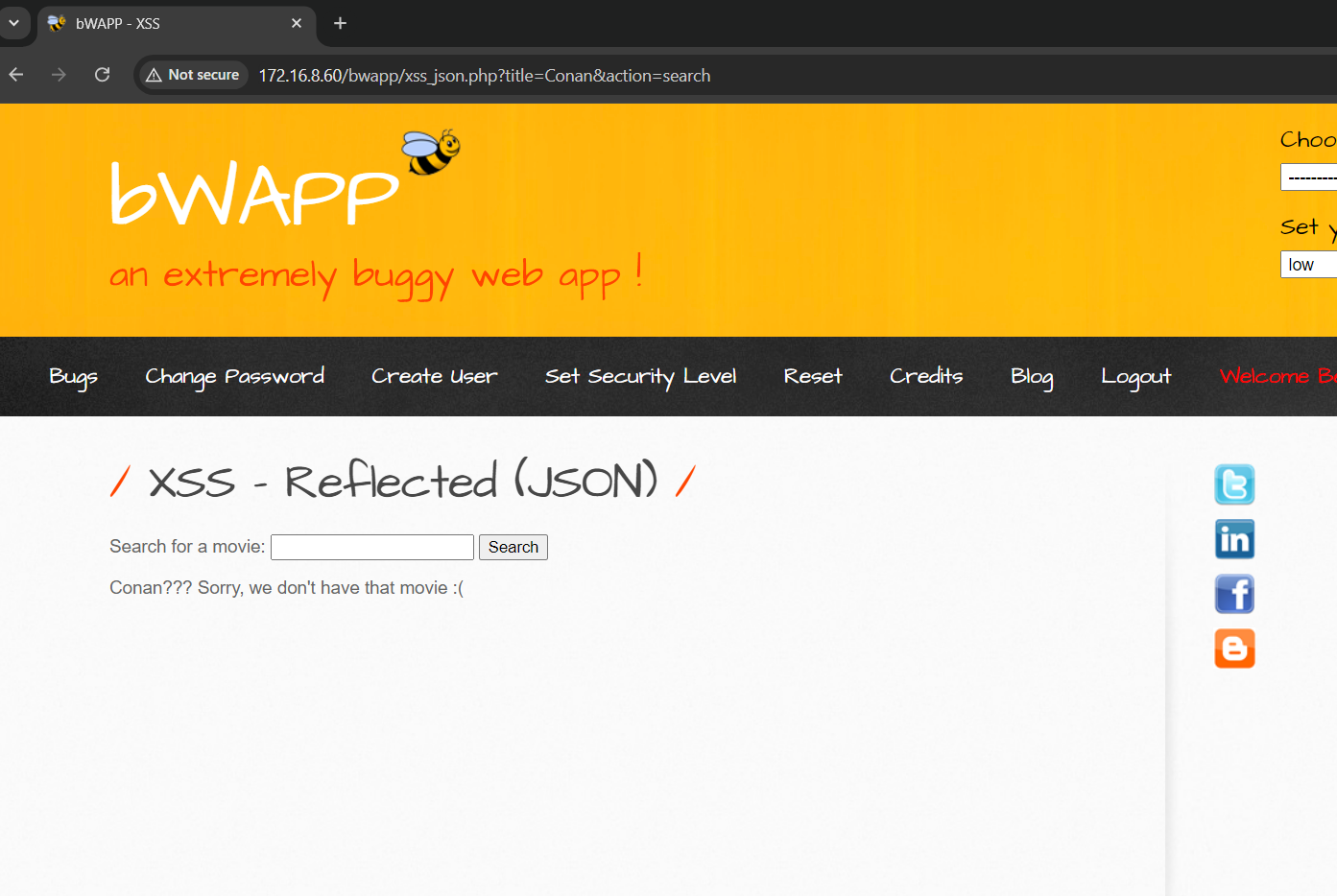


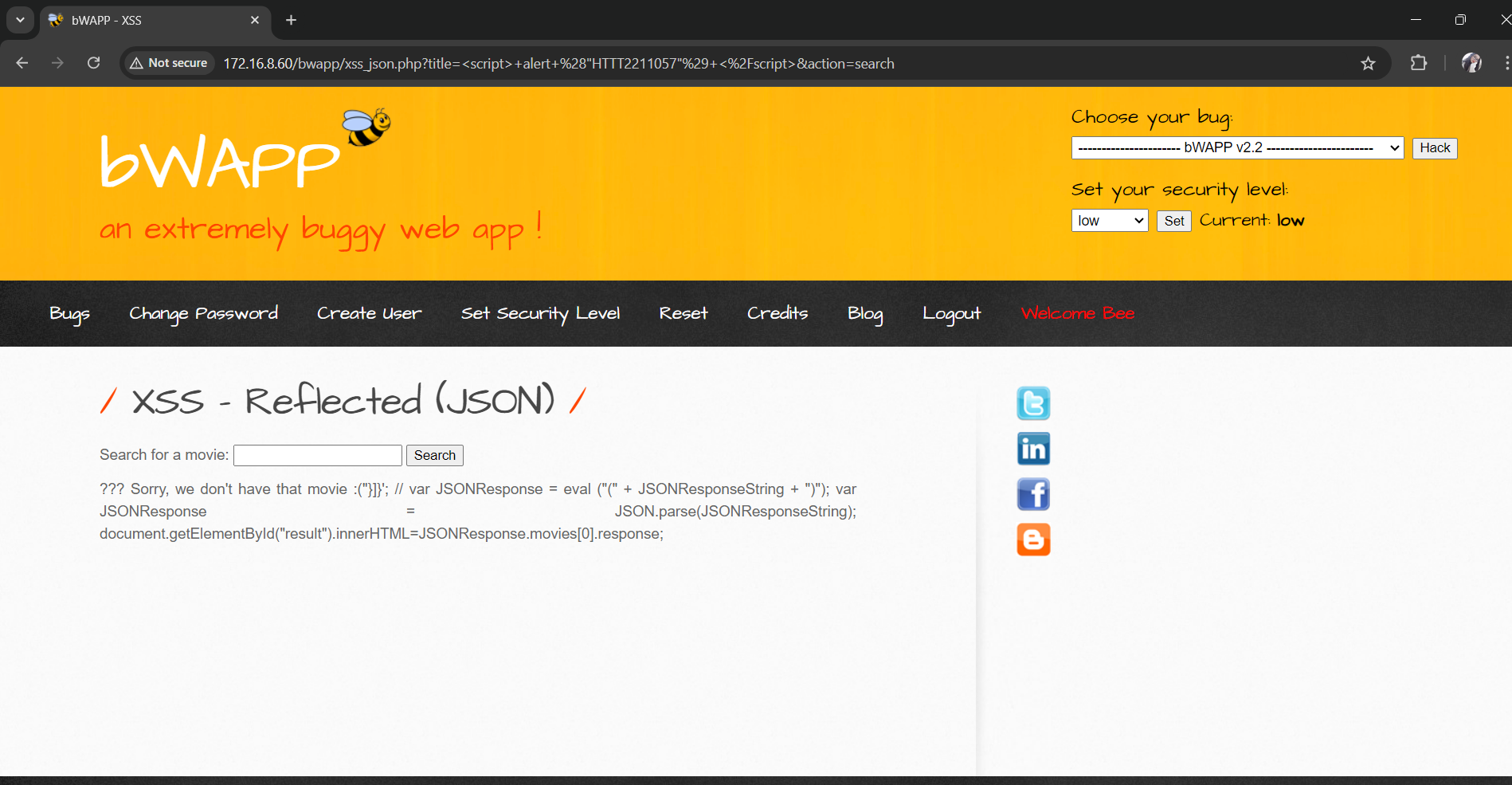
Thay date = alert(%HTTT2211057%)





1. Thực hành tấn công XSS phản xạ sử dụng chuỗi JSON (low)

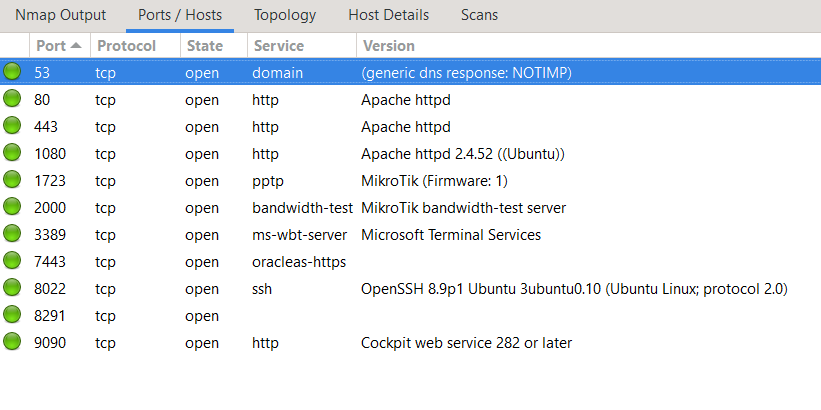




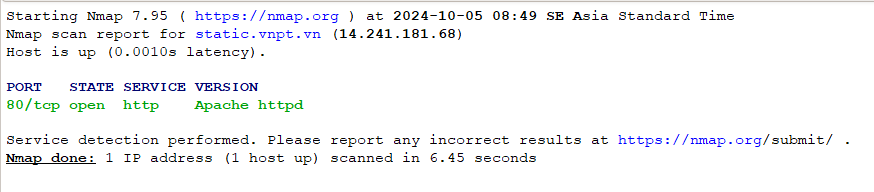
**THỰC HÀNH BUỔI 3**

1. *Khai thác thông tin thông qua quét mạng trên NMAP của website ctuet.edu.vn:*

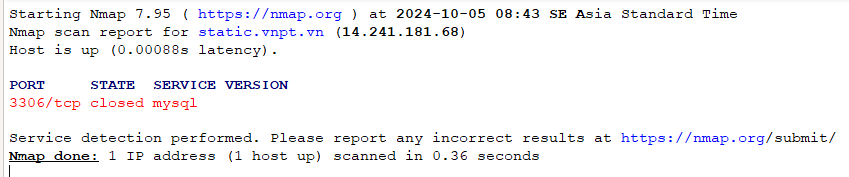
* Địa chỉ ID: 14.241.181.68
* Hệ điều hành: Linux 5.4
* Có 11 cổng dịch vụ đang mở:



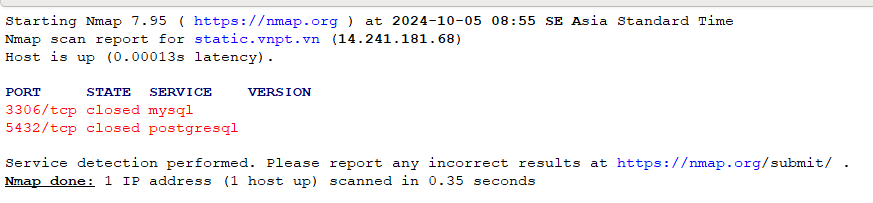
* Apache đang mở và sử dụng cổng 80:



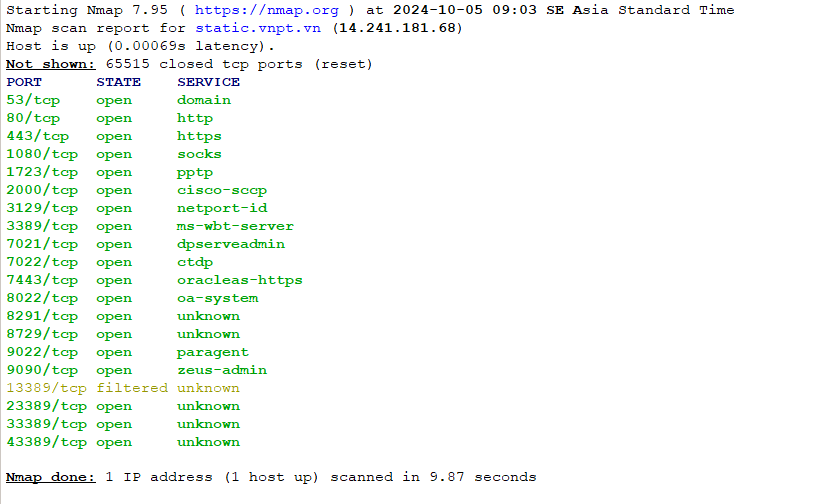
* Dịch vụ Mysql đang bị đóng:



* SQL:



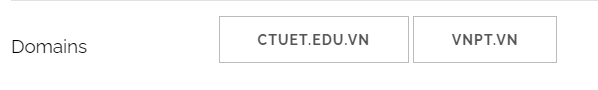
* Quét SYN còn gọi là quét tàng hình (Stealth Scan):

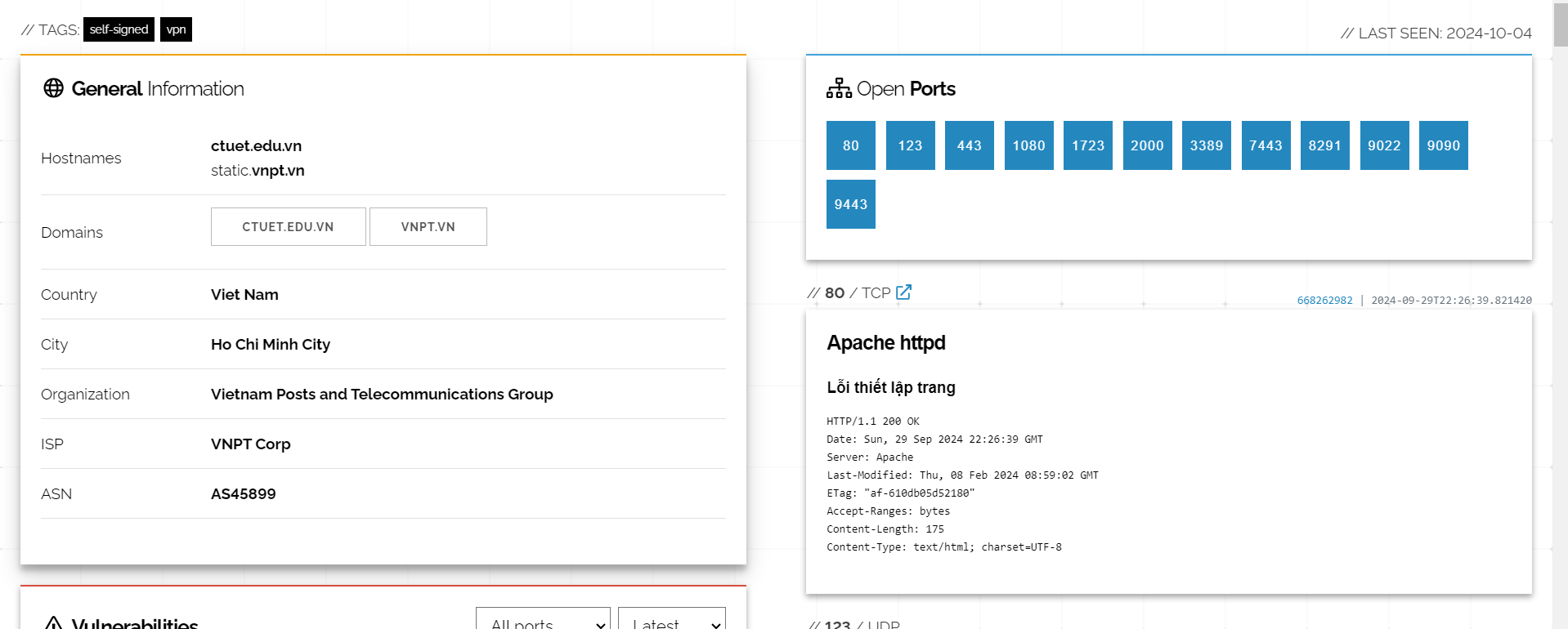


* Quét xmax:



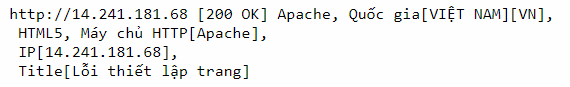
1. Khai thác thông tin trên Shodan
2. Tên miền:

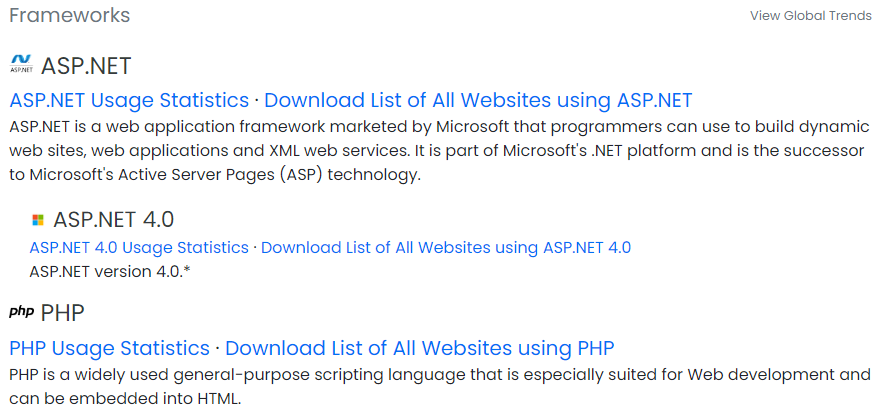


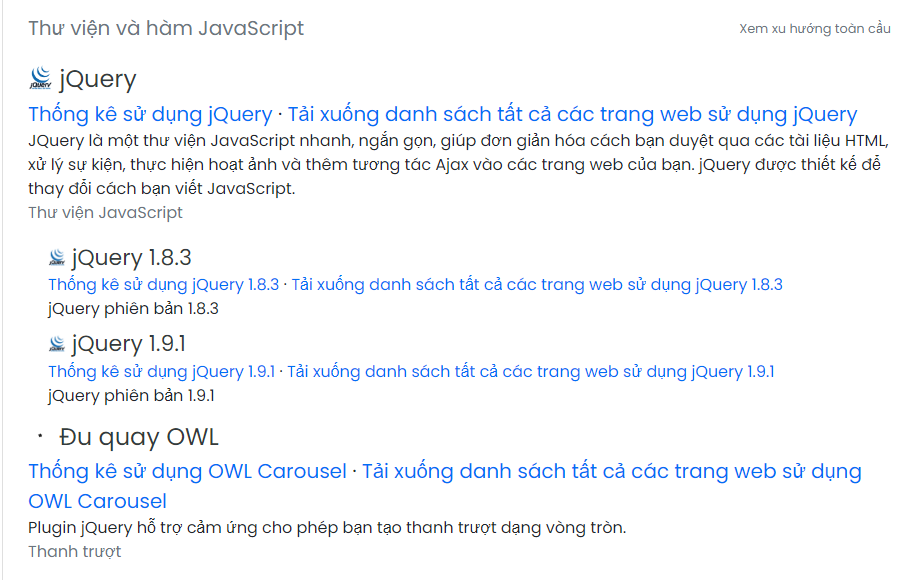


1. Subfinder:
2. Whatweb:

* Sử dụng ngôn ngữ HTML5



1. builtwith.com:



1. URLScan.io

