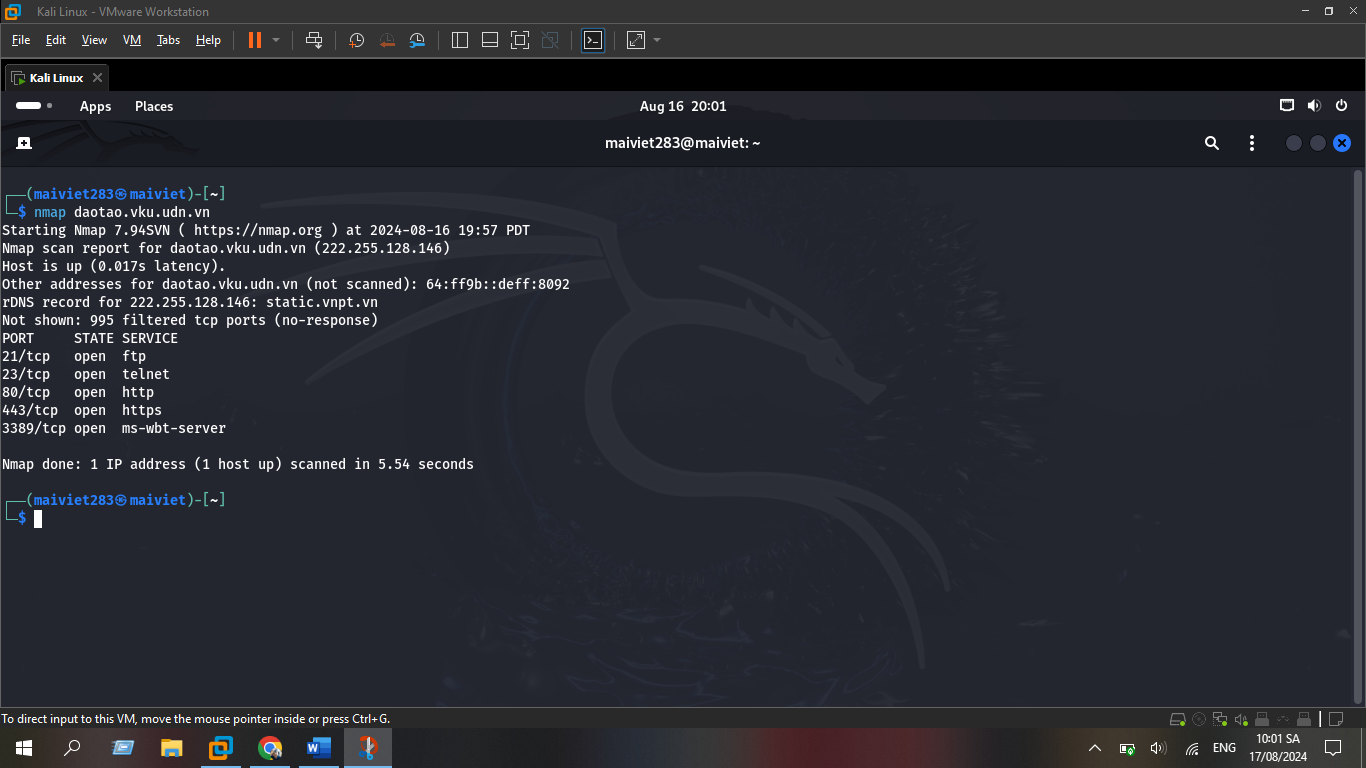
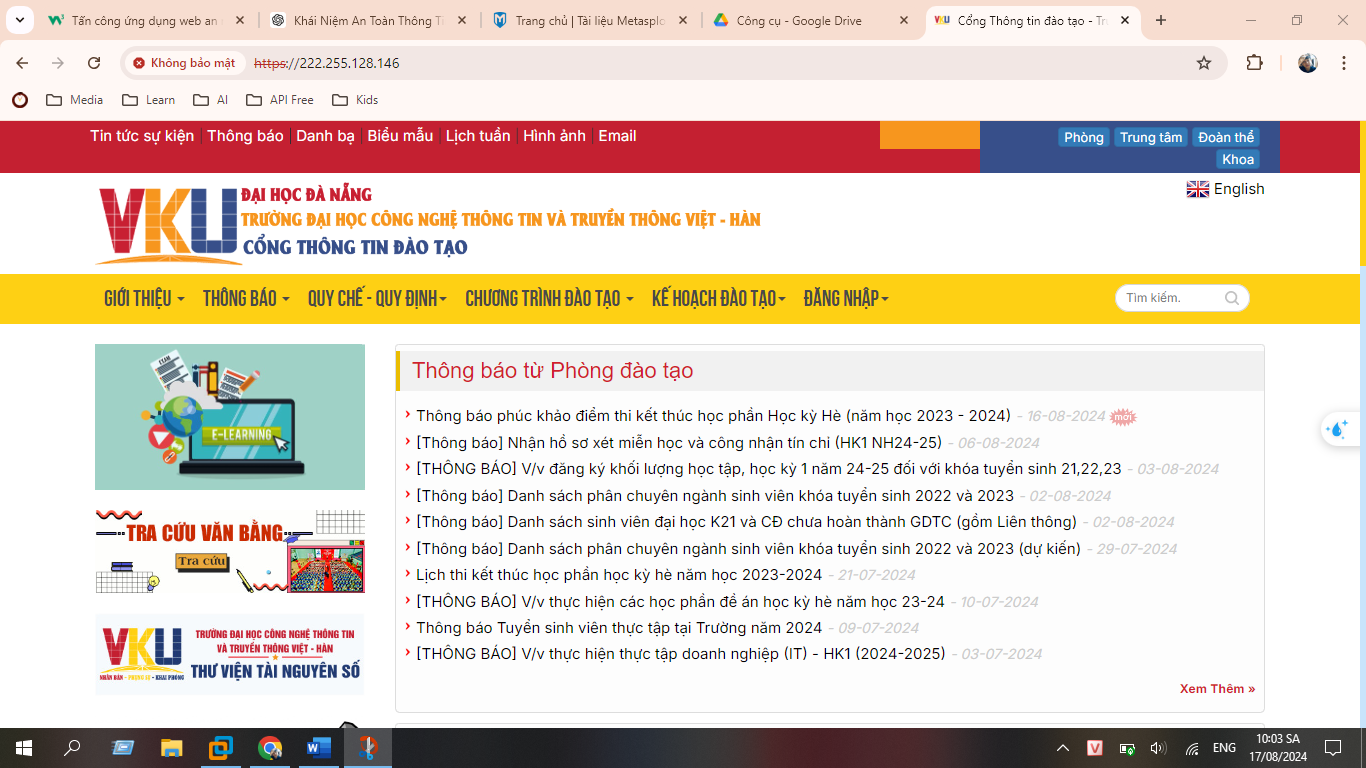
**Nhóm Lốc Xoáy**

**Câu 1 : IP Public là gì ?**

Nhóm em đã sử dụng công cụ nmap trên Kali Linux đã tìm ra được trang daotao.vku.udn.vn có ip là 222.255.128.146





**Câu 2 : Port Mở**



Các Port đang mở là 21, 23, 80 ,443, 3389

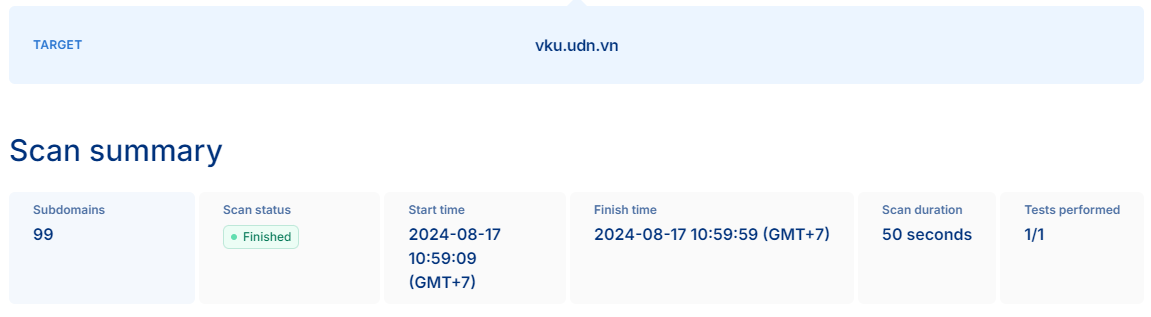
**Câu 3 : Các dịch vụ đang chạy ?**

Các dịch vụ được mở : ftp, telnet, http, https, ms-wbt-server



**Câu 4 : Sub domain là gì ?**

Nhóm em đã sử dụng công cụ Pentest-Tools

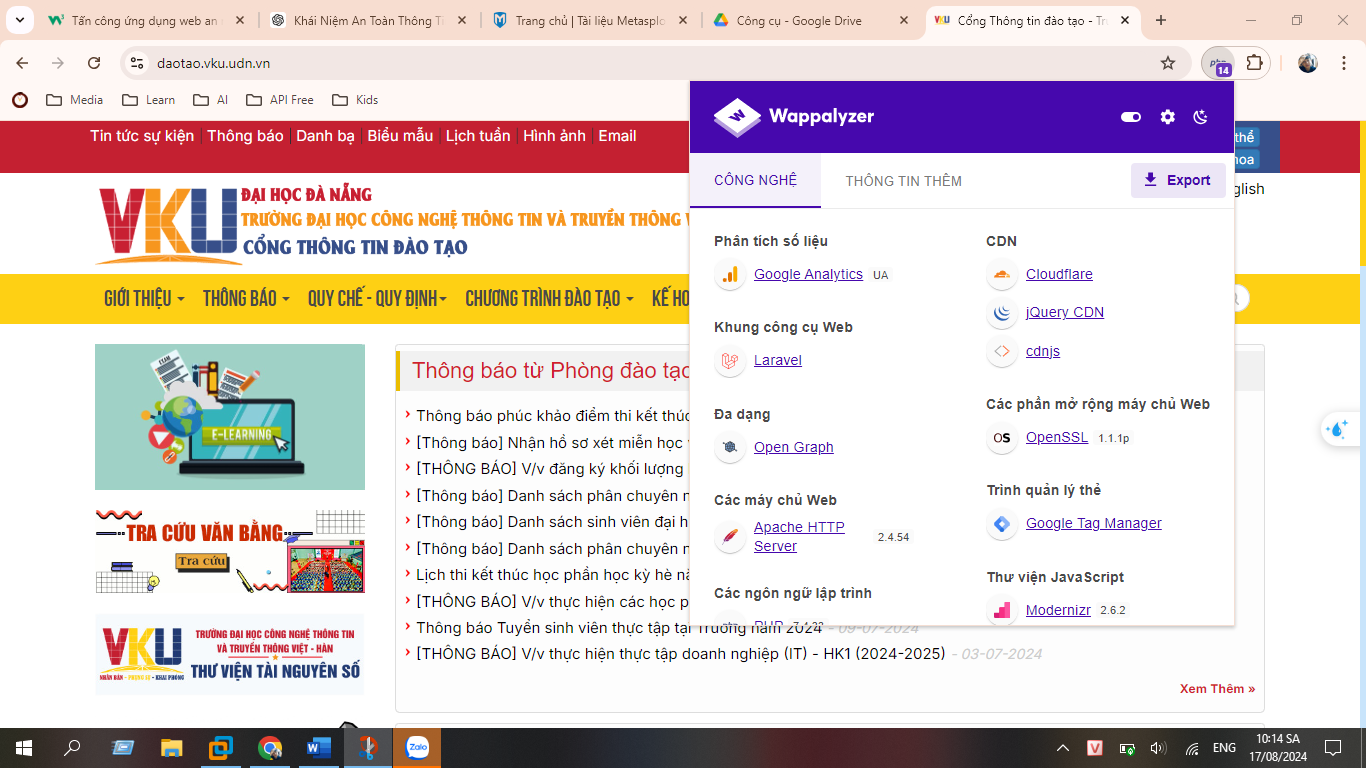


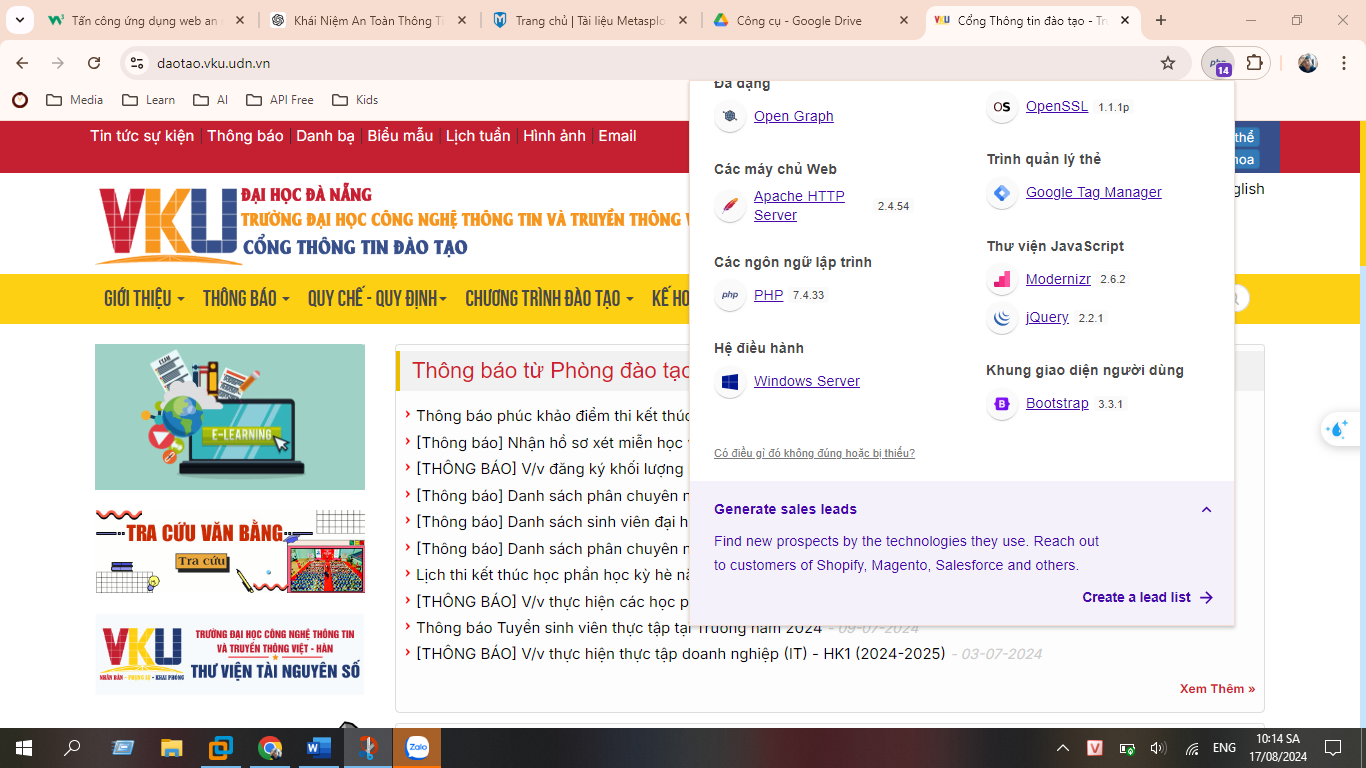
Quét được 99 sub domain

| **Hostnamein ascending order** | **Sort byIP Addressin ascending order** |
| --- | --- |
| piwik.cdn.vku.udn.vn | 0.0.0.0 |
| quiz.matomo.vku.udn.vn | 0.0.0.0 |
| piwik.portal.vku.udn.vn | 0.0.0.0 |
| lag-1.piwik.vku.udn.vn | 0.0.0.0 |
| forum.piwik.vku.udn.vn | 0.0.0.0 |
| archive.piwik.vku.udn.vn | 0.0.0.0 |
| uat.piwik.vku.udn.vn | 0.0.0.0 |
| sql.piwik.vku.udn.vn | 0.0.0.0 |
| stats.matomo.vku.udn.vn | 0.0.0.0 |
| app.matomo.vku.udn.vn | 0.0.0.0 |
| piwik.cs.vku.udn.vn | 0.0.0.0 |
| vsl.ce.vku.udn.vn | 61.14.233.104 |
| www.vku.udn.vn | 103.97.126.141 |
| vku.udn.vn | 103.97.126.141 |
| meet.vku.udn.vn | 222.255.128.147 |
| elearning.vku.udn.vn | 222.255.128.148 |
| portal.vku.udn.vn | 222.255.128.155 |
| cs.vku.udn.vn | 222.255.128.155 |
| global.vku.udn.vn | 222.255.128.155 |
| my.vku.udn.vn | 222.255.128.155 |
| de.vku.udn.vn | 222.255.128.155 |
| lib.vku.udn.vn | 222.255.128.243 |
| online.vku.udn.vn | 222.255.130.102 |
| oj.vku.udn.vn | 222.255.130.106 |
| meeting.vku.udn.vn | 222.255.130.107 |
| dashboard.vku.udn.vn | 222.255.130.150 |
| crm.vku.udn.vn | 222.255.130.150 |
| cdn.vku.udn.vn | 222.255.130.150 |
| lms.vku.udn.vn | 222.255.130.150 |
| beta.vku.udn.vn | 222.255.130.150 |
| mail.vku.udn.vn | 222.255.130.150 |
| ib.piwik.vku.udn.vn | N/A |
| 34.piwik.vku.udn.vn | N/A |
| wwwroot.matomo.vku.udn.vn | N/A |
| tv.matomo.vku.udn.vn | N/A |
| eportal.matomo.vku.udn.vn | N/A |
| sonarqube.piwik.vku.udn.vn | N/A |
| certauth.matomo.vku.udn.vn | N/A |
| minio.matomo.vku.udn.vn | N/A |
| develop.matomo.vku.udn.vn | N/A |
| development.piwik.vku.udn.vn | N/A |
| account.piwik.vku.udn.vn | N/A |
| webapp.piwik.vku.udn.vn | N/A |
| hec.piwik.vku.udn.vn | N/A |
| hk.piwik.vku.udn.vn | N/A |
| matomo.www.vku.udn.vn | N/A |
| clients.matomo.vku.udn.vn | N/A |
| temporary.piwik.vku.udn.vn | N/A |
| engage.matomo.vku.udn.vn | N/A |
| ip.matomo.vku.udn.vn | N/A |
| download.matomo.vku.udn.vn | N/A |
| tech.piwik.vku.udn.vn | N/A |
| uk.matomo.vku.udn.vn | N/A |
| abc.piwik.vku.udn.vn | N/A |
| matomo.online.vku.udn.vn | N/A |
| matomo.portal.vku.udn.vn | N/A |
| api1.piwik.vku.udn.vn | N/A |
| socket.matomo.vku.udn.vn | N/A |
| www-acc.piwik.vku.udn.vn | N/A |
| statistics.matomo.vku.udn.vn | N/A |
| ww2.matomo.vku.udn.vn | N/A |
| stores.matomo.vku.udn.vn | N/A |
| piwik.vku.udn.vn | N/A |
| get.matomo.vku.udn.vn | N/A |
| tn.piwik.vku.udn.vn | N/A |
| preprod.matomo.vku.udn.vn | N/A |
| matomo.lib.vku.udn.vn | N/A |
| nextcloud.matomo.vku.udn.vn | N/A |
| webdisk.matomo.vku.udn.vn | N/A |
| xbrl.piwik.vku.udn.vn | N/A |
| dev3.piwik.vku.udn.vn | N/A |
| vc.piwik.vku.udn.vn | N/A |
| links.matomo.vku.udn.vn | N/A |
| s2.piwik.vku.udn.vn | N/A |
| lag-62.matomo.vku.udn.vn | N/A |
| eng.matomo.vku.udn.vn | N/A |
| alert.piwik.vku.udn.vn | N/A |
| ticket.piwik.vku.udn.vn | N/A |
| press.matomo.vku.udn.vn | N/A |
| tls.matomo.vku.udn.vn | N/A |
| cgi.piwik.vku.udn.vn | N/A |
| relay1.piwik.vku.udn.vn | N/A |
| api-test.matomo.vku.udn.vn | N/A |
| bbb.matomo.vku.udn.vn | N/A |
| asia.piwik.vku.udn.vn | N/A |
| next.matomo.vku.udn.vn | N/A |
| server.matomo.vku.udn.vn | N/A |
| piwik.lms.vku.udn.vn | N/A |
| cdn.matomo.vku.udn.vn | N/A |
| portalapp.matomo.vku.udn.vn | N/A |
| feedback.matomo.vku.udn.vn | N/A |
| survey.piwik.vku.udn.vn | N/A |
| ppe.piwik.vku.udn.vn | N/A |
| res.piwik.vku.udn.vn | N/A |
| zabbix.matomo.vku.udn.vn | N/A |
| ci.matomo.vku.udn.vn | N/A |
| external.matomo.vku.udn.vn | N/A |
| quote.matomo.vku.udn.vn | N/A |
| adminvault.piwik.vku.udn.vn | N/A |

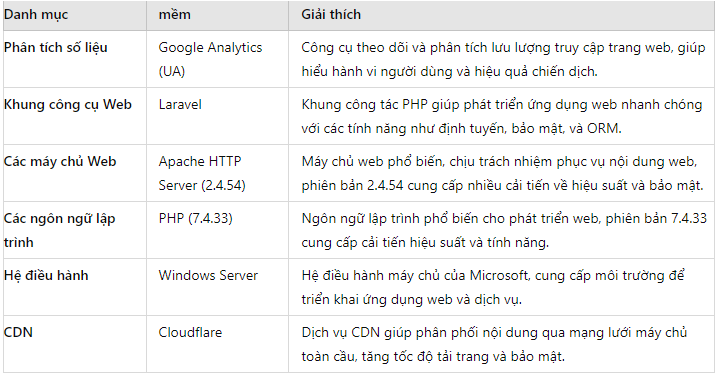
**Câu 5 : CMS là gì ?**

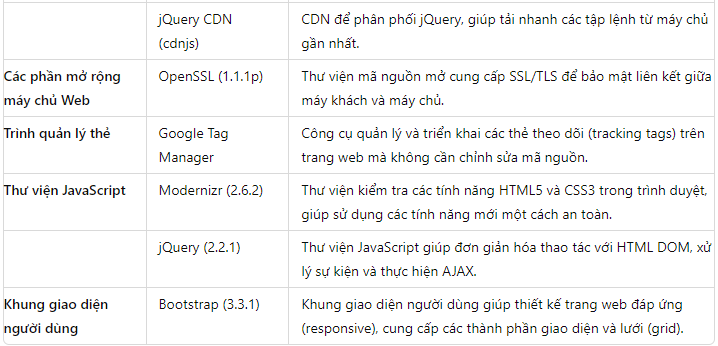
Nhóm em đã sử dụng wappalyzer extension để xem



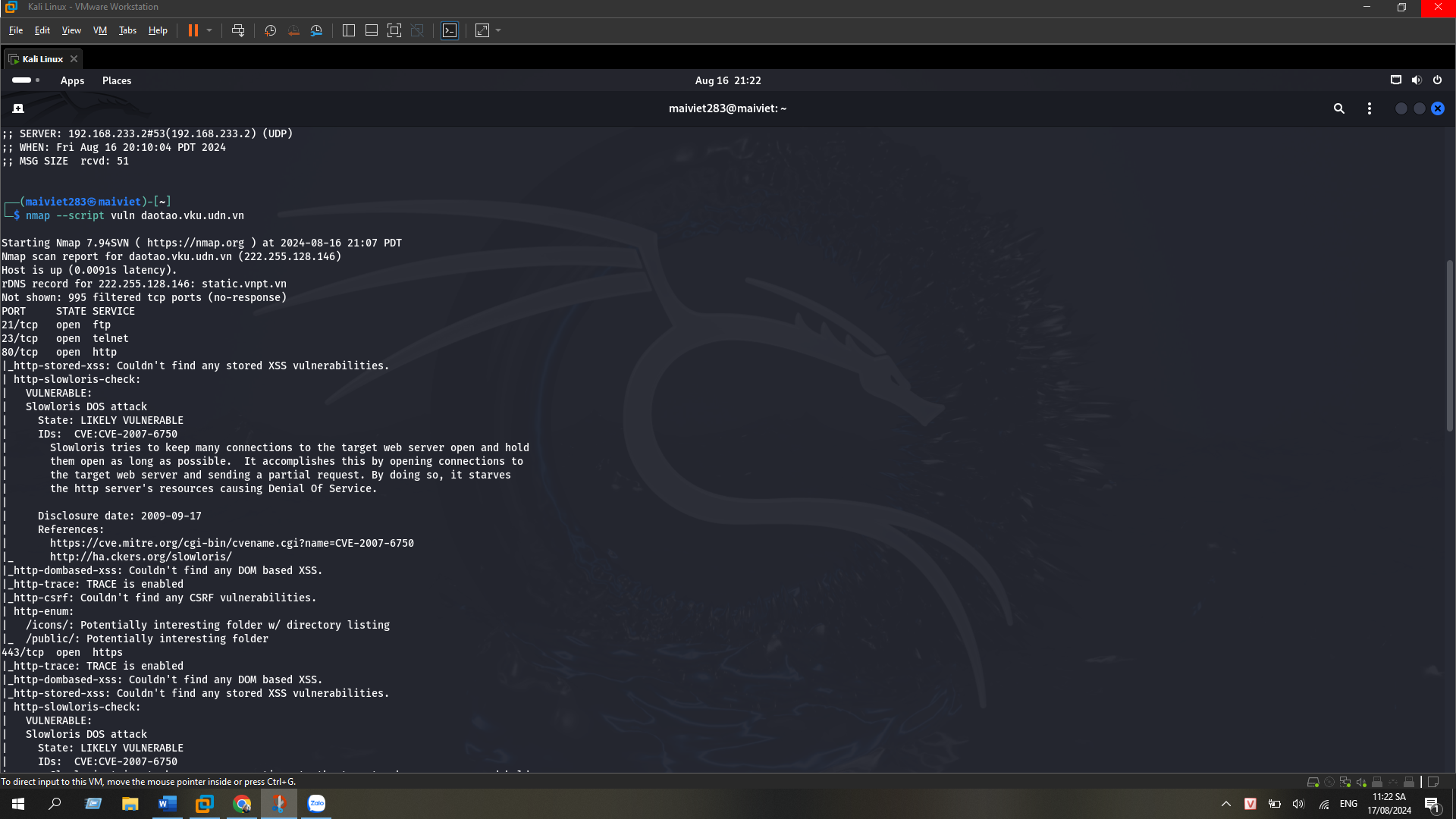


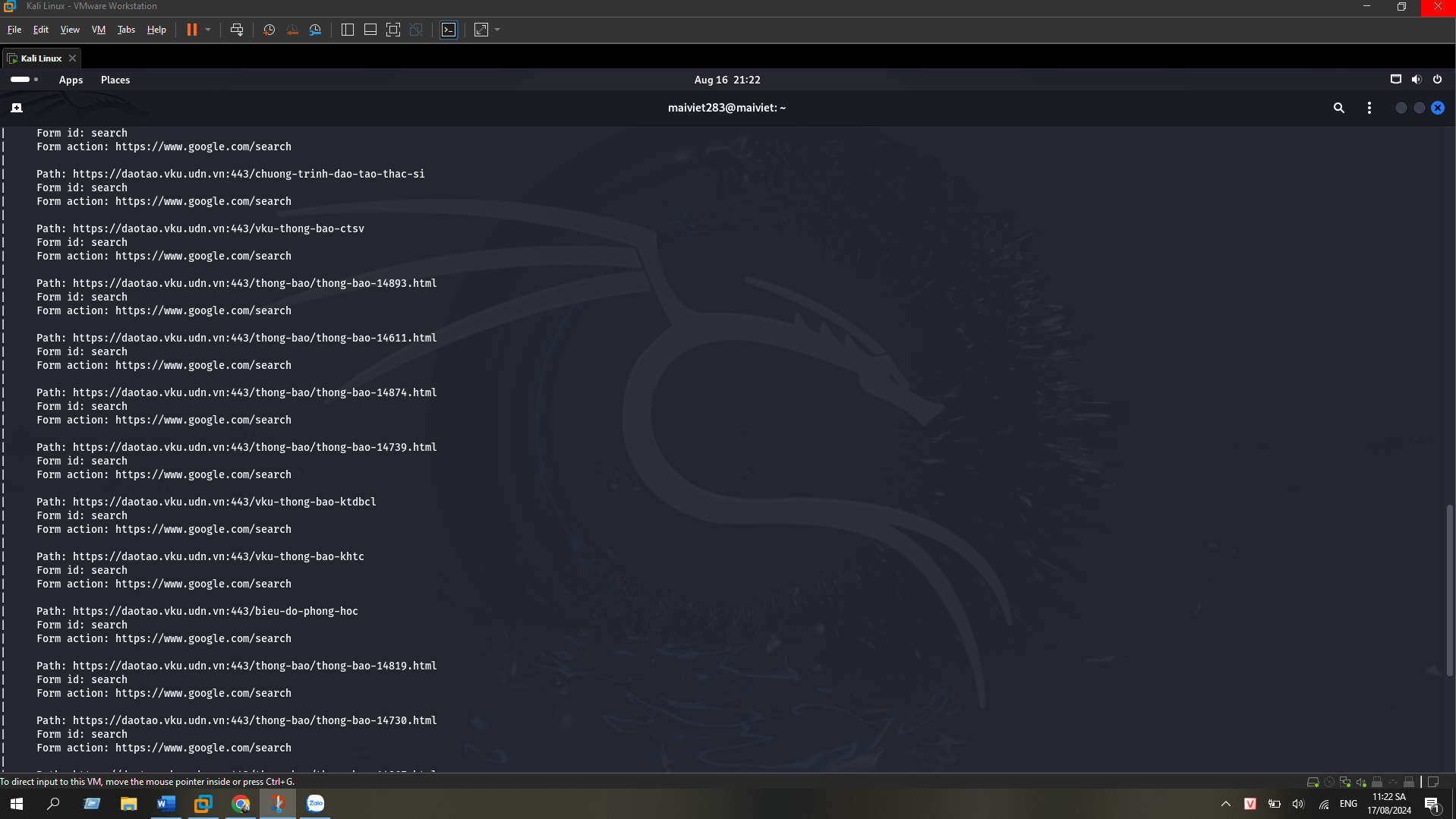
Bảng danh sách các công nghệ trong trang web



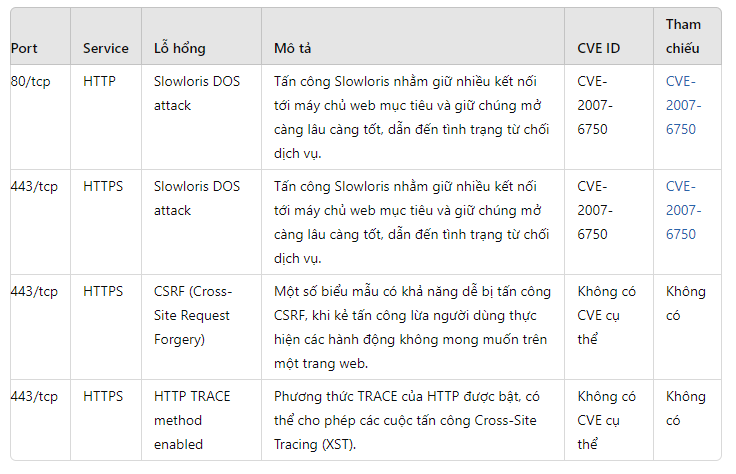


**Câu 6 : Tồn tại trong CVE nào ?**

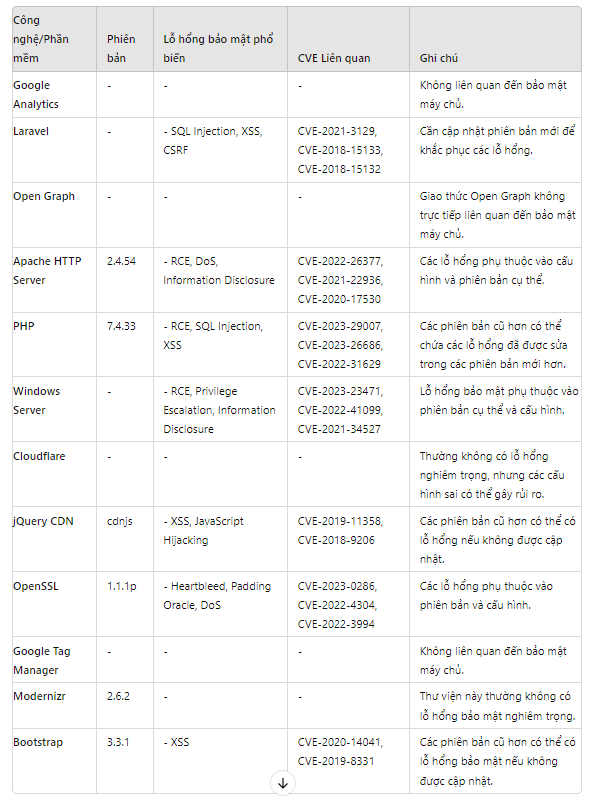




Dưới đây là bảng liệt kê các lỗ hổng bảo mật được tìm thấy từ kết quả quét Nmap trên tên miền https://daotao.vku.udn.vn/



Dưới đây là bảng các lỗ hổng bảo mật phổ biến và liên quan đến từng công nghệ/phần mềm mà bạn liệt kê, cùng với các CVE (Common Vulnerabilities and Exposures) liên quan:

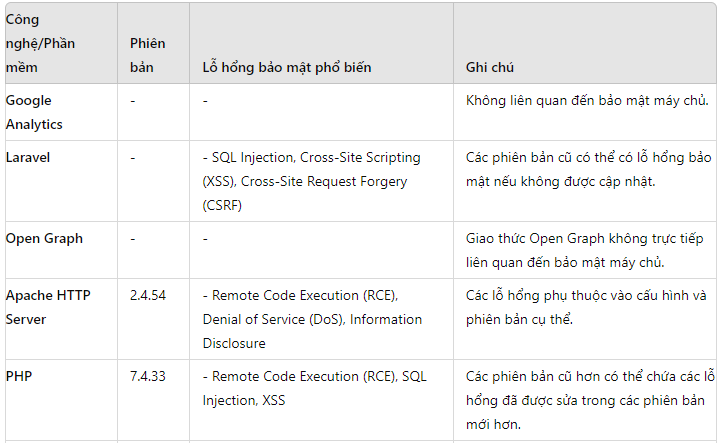


**Câu 7 : Đường dẫn lộ lọt thông tin user thông tin qua CMS ?**



**Câu 8 : Danh sách lỗ hổng tồn tại của CMS ?**

Dưới đây là bảng tóm tắt về các lỗ hổng bảo mật thường gặp trong các công nghệ và phần mềm được liệt kê



## 