

NAMA SEKOLAH : SMK NEGERI 2 BANDUNG

Selasa 14 Mei 2024

Ketua Tim :

Muhammad Akhtar Khawarizmi

Anggota Tim :

Harvi Muhammad Zakhir

SOAL NO 1

CTF kali ini ada di ip 192.168.10.232

Recon

Untuk recon kami menggunakan nmap dan dirsearch

```
Command Prompt
pandora@Dora: ~
pandora@Dora:~$ nmap 192.168.10.232
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-15 09:00 WIB
Nmap scan report for 192.168.10.232
Host is up (0.88s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3128/tcp   open  squid-http


Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
pandora@Dora:~$ dirsearch -u http://192.168.10.232/3128/
v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/pandora/.dirsearch/reports/192.168.10.232/-_24-05-15_09-05-06.txt
Error Log: /home/pandora/.dirsearch/logs/errors-24-05-15_09-05-06.log
Target: http://192.168.10.232/3128/
[09:05:06] Starting:
Task Completed

Command Prompt
pandora@Dora: ~
pandora@Dora:~$ dirsearch -u http://192.168.10.232
v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/pandora/.dirsearch/reports/192.168.10.232/_24-05-15_09-06-24.txt
Error Log: /home/pandora/.dirsearch/logs/errors-24-05-15_09-06-24.log
Target: http://192.168.10.232/
[09:06:24] Starting:
[09:06:25] 403 - 2930 - /_ht_wer.txt
[09:06:25] 403 - 2960 - /_htaccess.bod4
[09:06:25] 403 - 2960 - /_htaccess.orig
[09:06:25] 403 - 2960 - /_htaccess.sample
[09:06:25] 403 - 2960 - /_htaccess.extra
[09:06:25] 403 - 2978 - /_htaccess.extra
[09:06:25] 403 - 2960 - /_htaccess.BAK
[09:06:25] 403 - 2960 - /_htaccess.sc
[09:06:25] 403 - 2978 - /_htaccess.orig
[09:06:25] 403 - 2978 - /_html
[09:06:25] 403 - 2960 - /_htaccessOLD2
[09:06:25] 403 - 2960 - /_htm
[09:06:25] 403 - 2960 - /_htaccessOLD

[09:06:25] 403 - 2960 - /_htaccess.sample
[09:06:25] 403 - 2960 - /_htaccess.sample
[09:06:25] 403 - 2978 - /_htaccess.extra
[09:06:25] 403 - 2960 - /_htaccess.BAK
[09:06:25] 403 - 2960 - /_htaccess.sc
[09:06:25] 403 - 2960 - /_htaccess.orig
[09:06:25] 403 - 2978 - /_html
[09:06:25] 403 - 2960 - /_htaccessOLD2
[09:06:25] 403 - 2960 - /_htm
[09:06:25] 403 - 2960 - /_htaccessOLD
[09:06:25] 403 - 2920 - /_htpasswd
[09:06:25] 403 - 2960 - /_htpasswd.test
[09:06:25] 403 - 2930 - /_http-oauth
[09:06:25] 403 - 2960 - /_cgi-bin/
[09:06:25] 403 - 2960 - /_doc/
[09:06:25] 403 - 3815 - /_doc/en/changes.html
[09:06:25] 403 - 2960 - /_doc/api/
[09:06:25] 403 - 3815 - /_doc/html/index.html
[09:06:25] 403 - 3800 - /_doc/stable.version
[09:06:25] 200 - 210 - /_index
[09:06:25] 200 - 210 - /_index.php
[09:06:25] 200 - 210 - /_index.php/login/
[09:06:25] 200 - 400 - /_robots.txt
[09:06:25] 403 - 2960 - /_server-status/
[09:06:25] 403 - 2960 - /_server-status
Task Completed
```

Exploit

Setelah mengetahui beberapa port terbuka mari mulai dari port 80



BLEHHH!!!

Isinya hanya ini, saya penasaran dengan port http squid



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: [/](#)

Invalid URL

Some aspect of the requested URL is incorrect.

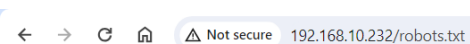
Some possible problems are:

- Missing or incorrect access protocol (should be "http://" or similar)
- Missing hostname
- Illegal double-escape in the URL-Path
- Illegal character in hostname; underscores are not allowed.

Your cache administrator is [webmaster](#).

Generated Wed, 15 May 2024 02:46:17 GMT by localhost (squid/3.1.19)

Setelah tidak ketemu apa apa, kami menelusuri robots.txt



User-agent: *
Disallow: /
Disallow: /wolfcms

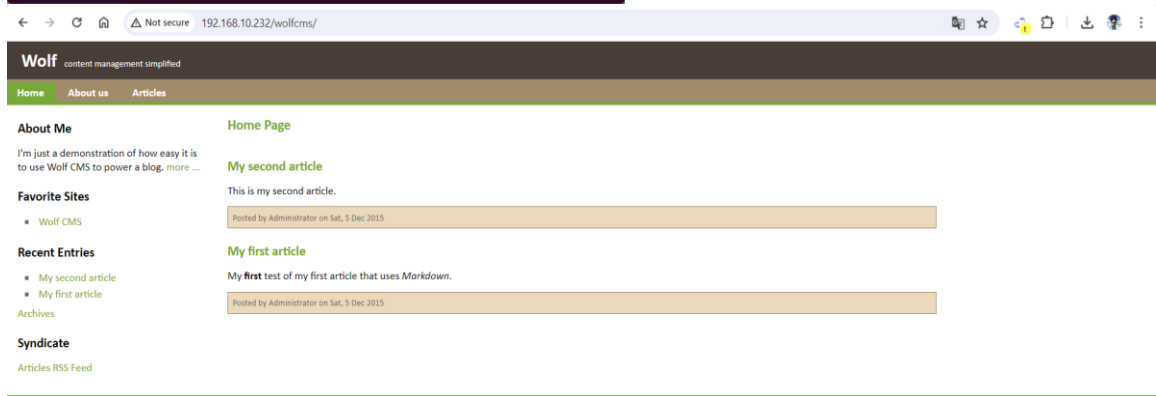
Kami menemukan /wolfcms lalu kami coba menggunakan dirsearch untuk menelusurinya

```
Command Prompt: pandora@Dora: ~
pandora@Dora:~$ dirsearch -u http://192.168.10.232/wolfcms
dirsearch v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/pandora/.dirsearch/reports/192.168.10.232-wolfcms_24-05-15_09-10-15.txt
Error Log: /home/pandora/.dirsearch/logs/errors-24-05-15_09-10-15.log
Target: http://192.168.10.232/wolfcms/

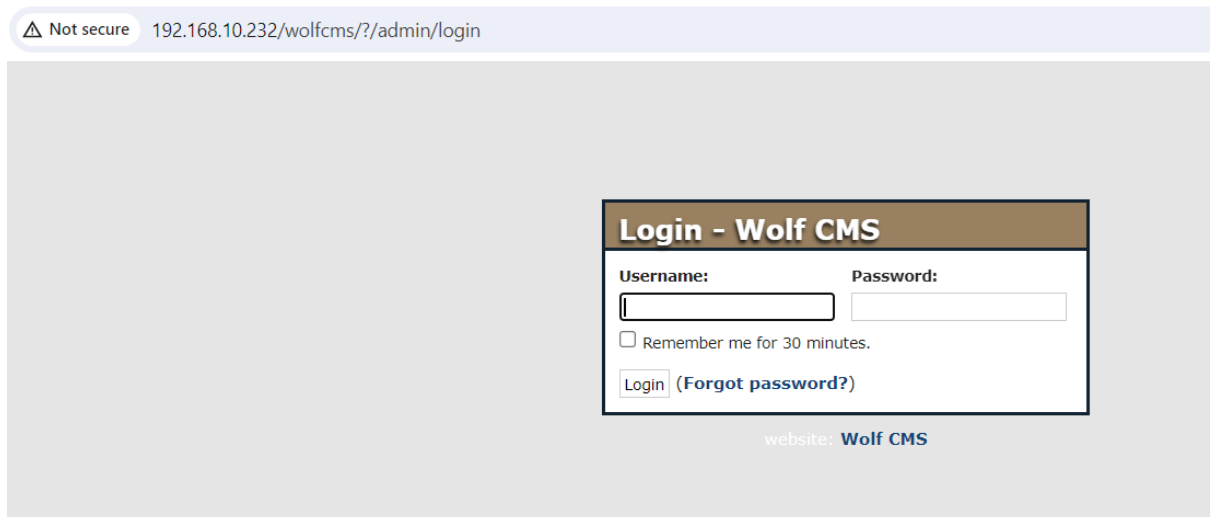
[09:10:15] Starting:
[09:10:16] 403 - 2010 - /wolfcms/.ht_wsr.txt
[09:10:16] 403 - 3000 - /wolfcms/.htaccess.backup
[09:10:16] 403 - 3000 - /wolfcms/.htaccess.sample
[09:10:16] 403 - 3000 - /wolfcms/.htaccess.save
[09:10:16] 403 - 3000 - /wolfcms/.htaccess.orig
[09:10:16] 403 - 3000 - /wolfcms/.htaccess.orig
[09:10:16] 403 - 3000 - /wolfcms/.htaccess.extra
[09:10:16] 403 - 3020 - /wolfcms/.htaccess.sc
[09:10:16] 403 - 3020 - /wolfcms/.htaccess.old
[09:10:16] 403 - 3020 - /wolfcms/.htaccess.old
[09:10:16] 403 - 3030 - /wolfcms/.htaccess.old2

[09:10:20] 200 - 00 - /wolfcms/config/initializers/secret_token.rb
[09:10:20] 200 - 00 - /wolfcms/config/master.key
[09:10:20] 200 - 00 - /wolfcms/config/monkeycheckin.ini
[09:10:20] 200 - 00 - /wolfcms/config/monkeyid.ini
[09:10:20] 200 - 00 - /wolfcms/config/routes.yml
[09:10:20] 200 - 00 - /wolfcms/config/settings.inc
[09:10:20] 200 - 00 - /wolfcms/config/settings.ini
[09:10:20] 200 - 00 - /wolfcms/config/production.yml
[09:10:20] 200 - 00 - /wolfcms/config/site.php
[09:10:20] 200 - 00 - /wolfcms/config/settings/production.yml
[09:10:20] 200 - 00 - /wolfcms/config/xml/
[09:10:20] 200 - 200 - /wolfcms/docs/
[09:10:20] 301 - 320 - /wolfcms/docs -> http://192.168.10.232/wolfcms/docs/
[09:10:20] 200 - 700 - /wolfcms/docs/updating.txt
[09:10:20] 200 - 00 - /wolfcms/favicon.ico
[09:10:20] 200 - 400 - /wolfcms/index
[09:10:20] 200 - 400 - /wolfcms/index.php
[09:10:20] 200 - 400 - /wolfcms/index.php/login/
[09:10:20] 301 - 320 - /wolfcms/public -> http://192.168.10.232/wolfcms/public/
[09:10:20] 200 - 100 - /wolfcms/public/
[09:10:20] 200 - 00 - /wolfcms/robots.txt

Task Completed
pandora@Dora:~$
```



Kami menemukan folder folder yang menarik. Setelah kami telusuri kami mencari referensi tentang wolfcms, ternyata wolf cms mempunyai halaman admin di wolfcms/?/admin



Kami mencoba login menggunakan default credential admin:admin dan ternyata bisa masuk
Setelah itu kami menemukan tempat untuk upload, kami mengupload file reverse shell, setelah itu kami listen menggunakan netcat dengan command nc -lvp 4554, namun terdapat

masalah ketika kami membuka file shellnya, sehingga kami belum bisa melanjutkan ke tahap mengakses root

