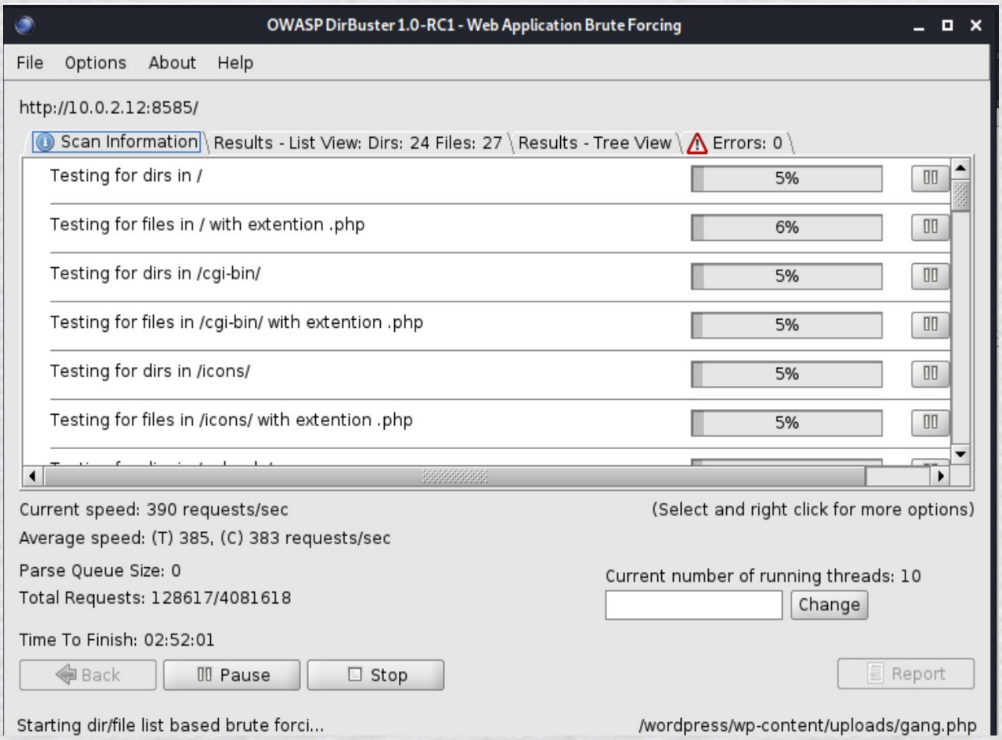
Name : Ahmed Alzahrani || **Email** : You-187@hotmail.com

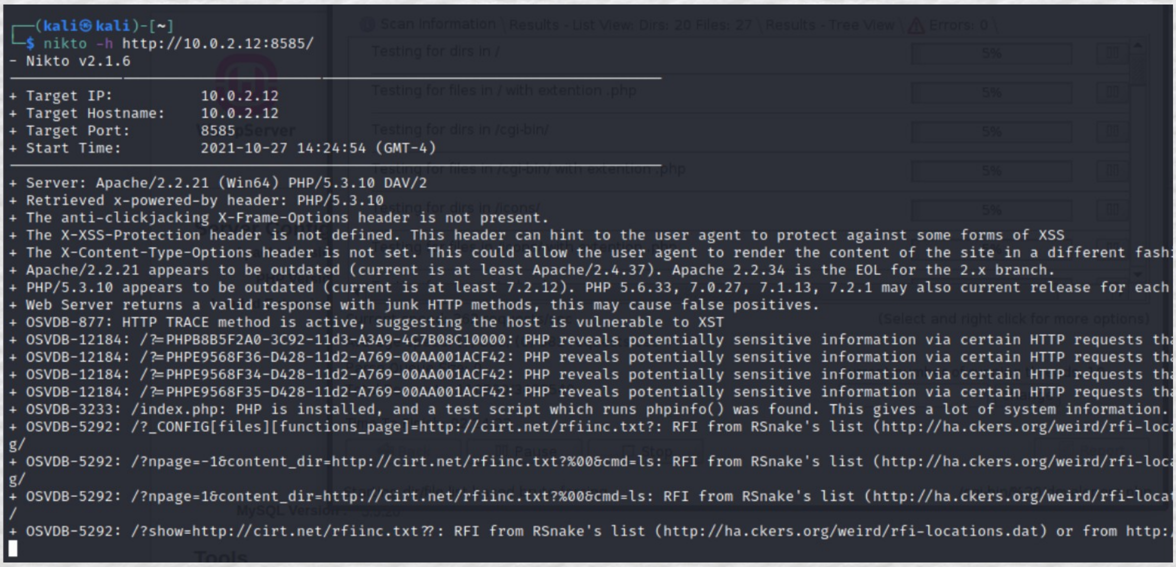
Specialized Scanners

For port 8585, use dirbuster or gobuster to find as much information about the directory structure as possible
:


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 24 Files: 27
Results - Tree View
Errors: 0
Back
Pause
Stop
Change
Report

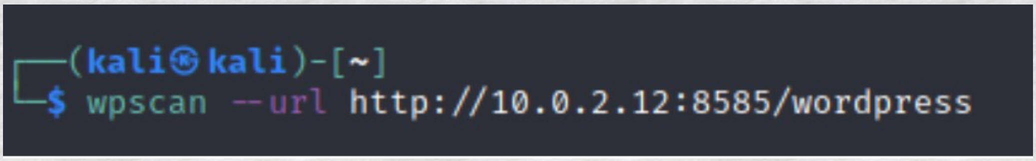
```
http://10.0.2.12:8585/

Testing for dirs in /                                   5%
Testing for files in / with extention .php              6%
Testing for dirs in /cgi-bin/                           5%
Testing for files in /cgi-bin/ with extention .php      5%
Testing for dirs in /icons/                             5%
Testing for files in /icons/ with extention .php        5%

Current speed: 390 requests/sec                 (Select and right click for more options)
Average speed: (T) 385, (C) 383 requests/sec
Parse Queue Size: 0                             Current number of running threads: 10
Total Requests: 128617/4081618
Time To Finish: 02:52:01

Starting dir/file list based brute forci...     /wordpress/wp-content/uploads/gang.php
```

For port 8585, use nikto to gather additional information about the host
Locate a specialized scanner for this web app :

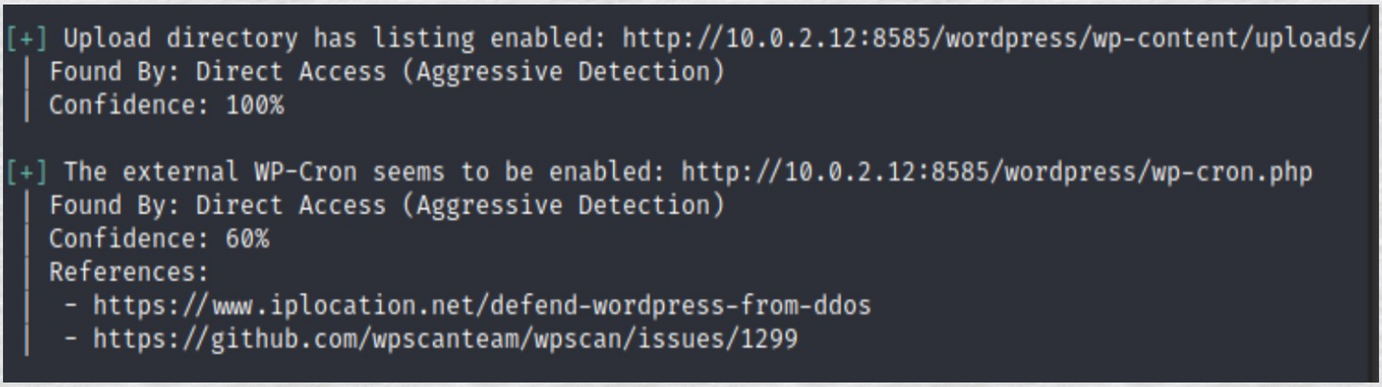


```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://10.0.2.12:8585/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.12
+ Target Hostname:    10.0.2.12
+ Target Port:        8585
+ Start Time:         2021-10-27 14:24:54 (GMT-4)
---------------------------------------------------------------------------
+ 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.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fash
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.3.10 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests tha
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests tha
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests tha
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests tha
+ OSVDB-3233: /index.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-5292: /?_CONFIG[files][functions_page]=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-loca
g/
+ OSVDB-5292: /?npage=-1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-loca
g/
+ OSVDB-5292: /?npage=1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locat
/
+ OSVDB-5292: /?show=http://cirt.net/rfiinc.txt??: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http:
```

Use the specialized scanner to enumerate the application as much as possible

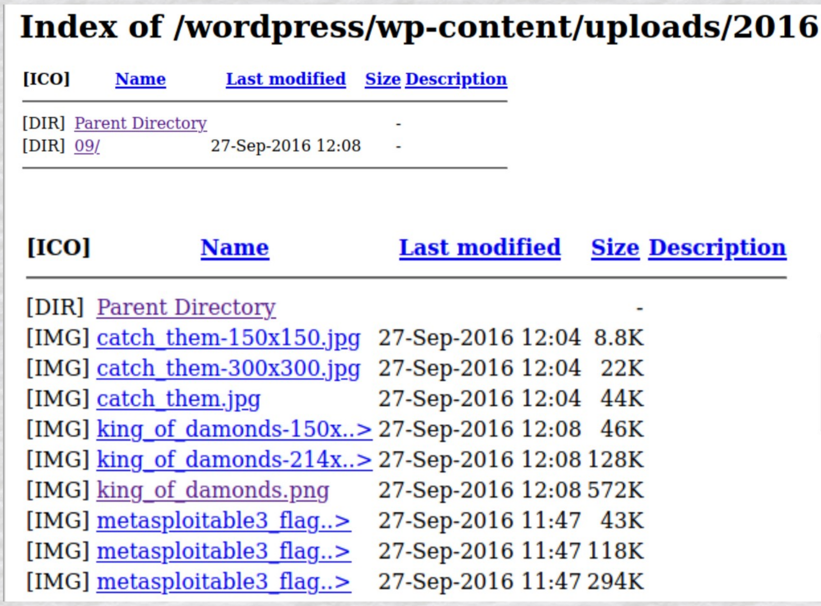


```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://10.0.2.12:8585/wordpress
```



```
[+] Upload directory has listing enabled: http://10.0.2.12:8585/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.0.2.12:8585/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
```

Find the flag



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

```
[ICO]      Name          Last modified     Size Description
[DIR]  Parent Directory                     -
[DIR]  09/             27-Sep-2016 12:08    -
```

```
[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
```