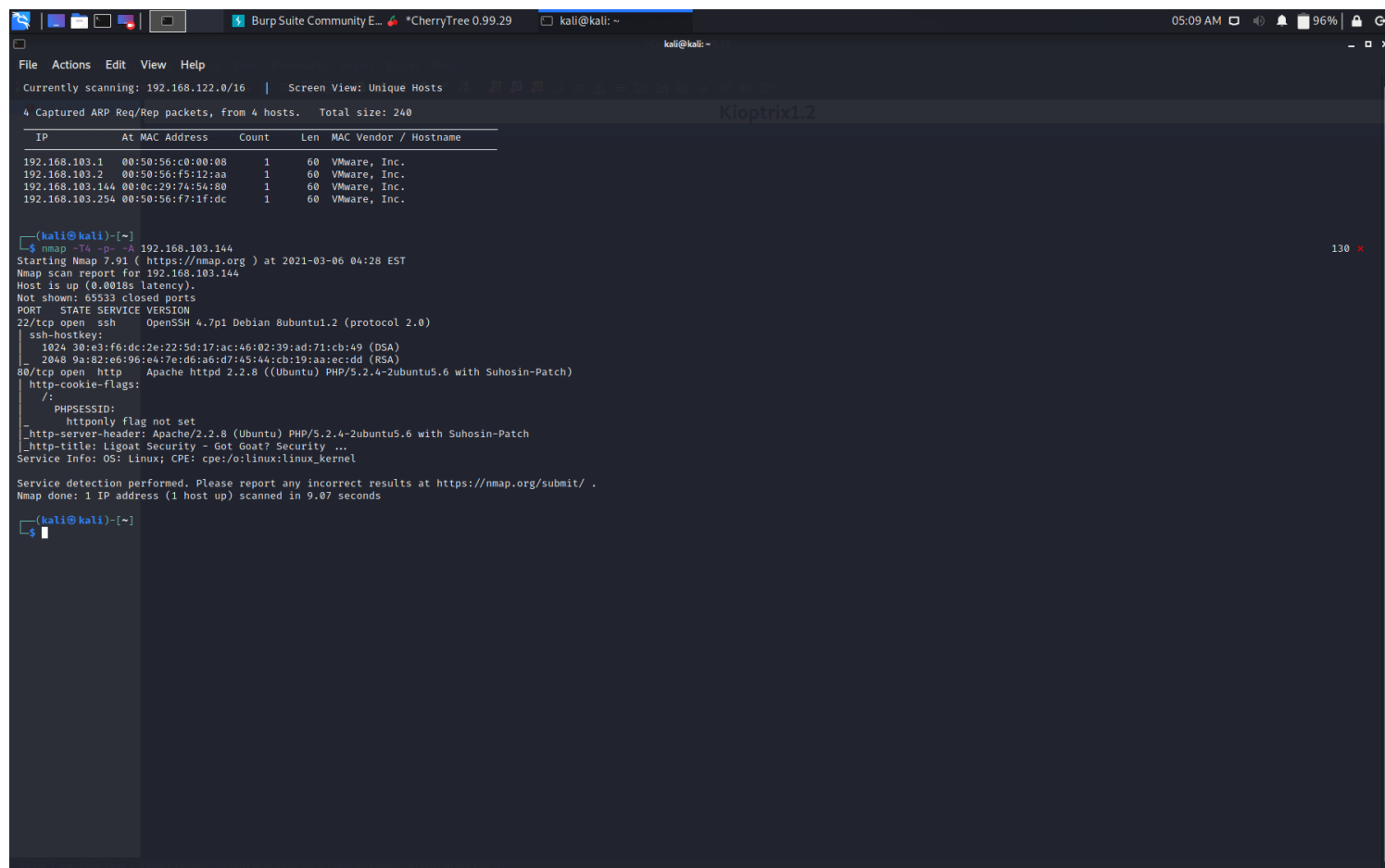


# Kioptrix1.2



```
File Actions Edit View Help
Currently scanning: 192.168.122.0/16 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP      At MAC Address  Count  Len  MAC Vendor / Hostname
192.168.103.1  00:50:56:c0:00:08  1      60  VMware, Inc.
192.168.103.2  00:50:56:f5:12:aa  1      60  VMware, Inc.
192.168.103.144 00:0c:29:74:54:80  1      60  VMware, Inc.
192.168.103.254 00:50:56:f7:1f:dc  1      60  VMware, Inc.

(kali@kali)-[~]
$ nmap -T4 -p- -A 192.168.103.144
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 04:28 EST
Nmap scan report for 192.168.103.144
Host is up (0.0018s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_ 2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_ http-title: Ligoat Security - Got Goat? Security ...
Service Info: OS: linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.07 seconds

(kali@kali)-[~]
$
```

## 22/tcp

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)  
| ssh-hostkey:  
| 1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)  
|\_ 2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)

## 80/tcp

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)  
| http-cookie-flags:  
| /:  
| PHPSESSID:  
|\_ httponly flag not set  
|\_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch  
|\_ http-title: Ligoat Security - Got Goat? Security ...  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

	Name	Link
1	Apache httpd 2.2.8	
2	PHP/- 5.2.4-2ubuntu5.6 with Suhosin-Patch	<a href="https://www.exploit-db.com/exploits/-29290">https://www.exploit-db.com/exploits/-29290</a>
3	Lotus CMS	<a href="https://www.exploit-db.com/exploits/-15964">https://www.exploit-db.com/exploits/-15964</a>

## Enum

## Nikto

- Nikto v2.1.6

```
-----
+ Target IP:      192.168.103.144
+ Target Hostname: 192.168.103.144
+ Target Port:    80
+ Start Time:     2021-03-06 05:23:54 (GMT-5)
-----
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ 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 fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
☒ + Apache/2.2.8 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/5.2.4-2ubuntu5.6 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 branch.
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126,
mtime: Fri Jun 5 15:22:00 2009
+ 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 that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and
should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
```

+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.  
+ 7914 requests: 0 error(s) and 19 item(s) reported on remote host  
+ End Time: 2021-03-06 05:24:40 (GMT-5) (46 seconds)

-----

## dirbuster

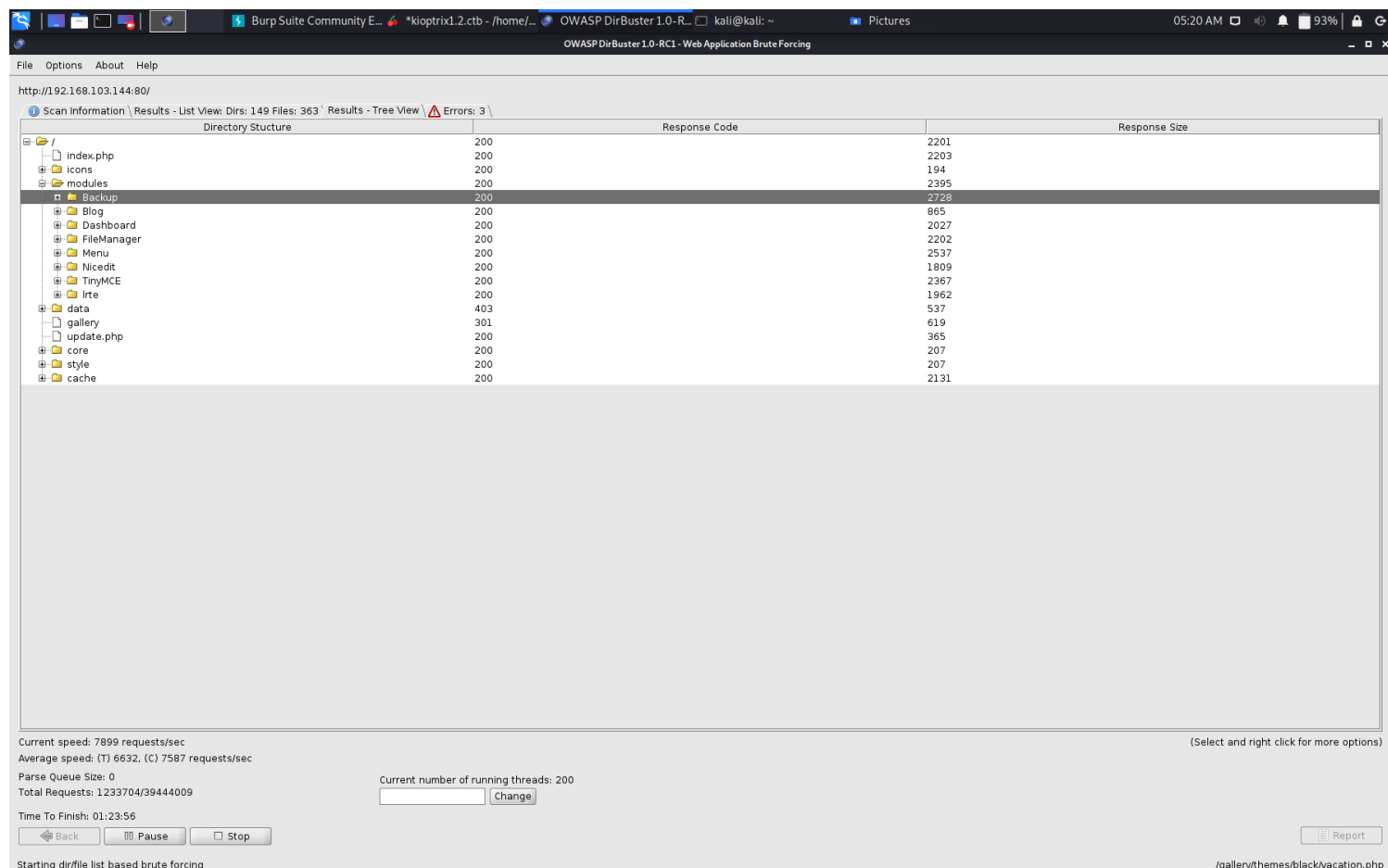
File Options About Help

http://192.168.103.144:80/

Scan Information \ Results - List View: Dirs: 148 Files: 358 \ Results - Tree View \ Errors: 3 \

Directory Structure	Response Code	Response Size
/	200	2201
index.php	200	2203
icons	200	194
small	200	194
README.html	200	37149
modules	200	2395
Backup	200	2728
BackupModuleAdmin.php	200	357
BackupModuleInfo.php	200	355
BackupModuleInstall.php	200	361
Browse.plb	200	5093
noDisableStatus.dat	200	307
pclzip.lib.php	200	207
readme.txt	200	377
zips	200	977
Blog	200	865
news.php	200	207
index.php	200	865
rss.php	200	1836
display	200	1156
basic	200	2529
template	200	1162
default	200	3506
Dashboard	200	2027
FileManager	200	2202
Menu	200	2537
Nicedit	200	1809
TinyMCE	200	2367
Irte	200	1962
EditorViewPlugin.php	200	357
code	200	2336
images	200	1612
jquery.ocupload-1.1.4.js	200	2633
jquery.rte.css	200	6213
jquery.rte.js	200	8916
jquery.rte.tb.js	200	11957
styles.php	200	207
uploader.php	200	422
IrteModuleAdmin.php	200	353
IrteModuleInfo.php	200	351
IrteModuleInstall.php	200	357
data	403	537
nallerv	301	619

Current speed: 7845 requests/sec  
Average speed: (T) 5822, (C) 7717 requests/sec  
Parse Queue Size: 0  
Total Requests: 465782/39181051  
Time To Finish: 01:23:36  
Back Pause Stop  
Starting dirfile list based brute forcing  
Report  
(Select and right click for more options)  
/modules/TinyMCE/tiny\_mce/plugins/paste/dl.php



## Exploit

## Lotus CMS

```
(kali㉿kali)-[~/Desktop/exe]
└─$ python exploit.py -l -t 192.168.103.144:80 -
d /
```

1 x

```
| ----- |
| Lotus CMS v3.0 Remote Code Execution Exploit |
| by mr_me - net-ninja.net ----- |
```

(+) Exploiting target @: 192.168.103.144:80/

(+) Testing the file inclusion vulnerability.. file inclusion failed..

(-) Exiting..