Fristileaks

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-06 12:10 EST
Stats: 0:06:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.94% done; ETC: 12:20 (0:03:22 remaining)
Nmap scan report for 192.168.103.146
Host is up (0.0018s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 416.38 seconds
```

Enum

```
80/tcp open  http    Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
```

Dirb

```
---- Scanning URL: http://192.168.103.146/ ----
+ http://192.168.103.146/cgi-bin/ (CODE:403|SIZE:-
210)
==> DIRECTORY: http://192.168.103.146/images/

+ http://192.168.103.146/index.html (CODE:200|SIZE:-
703)
+ http://192.168.103.146/robots.txt (CODE:200|SIZE:62)
```

dirbuster

```
ERROR: http://192.168.103.146:80/icons/lcd/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/cgi-bin/355/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/invest.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/icons/int.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/images/open-source/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/icons/small/play.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
```

```
ERROR: http://192.168.103.146:80/icons/tickets.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/ww.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/images/symantec.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/cgi-bin/350.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/soa.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/error/2005.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/geo/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/images/grants/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/error/en/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/625.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/1438.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/tg.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/125x800.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/images/charter/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/icons/branding.php - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
ERROR: http://192.168.103.146:80/hotlog/ - ConnectTimeoutException The host did not accept the connection within timeout of 30000 ms
```

gobuster

Nikto

```
└─$ nikto -h 'http://192.168.103.146'
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.103.146
+ Target Hostname:    192.168.103.146
+ Target Port:        80
+ Start Time:         2021-03-06 12:38:59 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
+ Server may leak inodes via ETags, header found with file /, inode: 12722, size: 703, mtime: Tue Nov 17 13:45:47 2015
+ 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
+ Entry '/cola/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/sisi/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/beer/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 3 entries which should be manually viewed.
☐ + PHP/5.3.3 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.
☐ + Apache/2.2.15 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, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
☐ + OSVDB-3233: /icons/README: Apache default file found.
+ 8729 requests: 1 error(s) and 15 item(s) reported on remote host
+ End Time:           2021-03-06 12:39:51 (GMT-5) (52 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Exploit

Apache 2.2.15