



Oops! I forgot my password

www.eleven-labs.com

Thierry Thuon
github.com/lepiaf

Who am I



Thierry Thuon

Web Developer @ Eleven-Labs

Github: @lepiat



An awesome feature

A screenshot of a Trello card titled "As a user, I want to reset my password". The card is part of a "Backlog" list. It includes labels "Ready" and "User story", a description of the feature, acceptance tests, and a sidebar with options to add members, labels, checklist, due date, and attachments. The card is displayed in a modal window over a Trello interface.

As a user, I want to reset my password

Dans la liste [Backlog](#)

Étiquettes

Ready User story +

Description [Éditer](#)

A user can forget his password. Create a page where user can enter his email address. Then, he receive an email with a link to reset his password. On the reset password page, display two field for new password.

Acceptance tests:

- I reset password of know user, I should receive an email and reset password.
- I reset password of unknown user, I should see an error.


[Ajouter un commentaire](#)

Ajouter

- Membres
- Étiquettes
- ☒ Checklist
- Échéance
- Pièce jointe

Actions

- Déplacer

- 
- A faint, light-colored line drawing of a rocket ship is visible in the background on the left side of the slide. The rocket is oriented vertically, with a large cylindrical body and a pointed nose cone. It has several windows or portholes along its side and a small, rounded base. The drawing is done in a sketchy, hand-drawn style.
- create a controller to generate link
 - create a form
 - create a service to generate link with token
 - send link to user by email
 - create controller to check that the token is valid and display form to change password

How do you generate a token?



Let me Google that for you



php generate random string



Tous

Actualités

Images

Vidéos

Shopping

Plus

Paramètres

Outils

Environ 177 000 résultats (0,36 secondes)

PHP random string generator - Stack Overflow

<https://stackoverflow.com/questions/.../php-random-string-generat...> ▼ Traduire cette page

4 déc. 2010 - **Generate a random string**, using a cryptographically secure * pseudorandom number generator (random_int) * * For PHP 7, random_int is a ...

More than a thousand vote



To answer this question specifically, two problems:

1008

1. `$randstring` is not in scope when you echo it.
2. The characters are not getting concatenated together in the loop.



Here's a code snippet with the corrections:

```
function generateRandomString($length = 10) {  
    $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';  
    $charactersLength = strlen($characters);  
    $randomString = '';  
    for ($i = 0; $i < $length; $i++) {  
        $randomString .= $characters[rand(0, $charactersLength - 1)];  
    }  
    return $randomString;  
}
```


Let's implement it



A few days later...



A customer comes and says:
"It is slow, could you check it?"



Check on grafana



Check access log



```
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET / HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET / HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET / HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET / HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET / HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET / HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /forgot-password HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "POST /forgot-password HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /forgot-password HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "POST /forgot-password HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /reset-password/eEadfgP HTTP/1.1" 404 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /reset-password/zrgnbvr HTTP/1.1" 404 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /reset-password/prfhfdr HTTP/1.1" 404 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /reset-password/tghfdhy HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /reset-password/mZExcty HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "GET /admin/users HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
95.31.18.119 - [08/Nov/2017:10:58:05 +0100] "POST /admin/users HTTP/1.1" 200 4286 "-" "Mozilla/5.0"
```

What's wrong?

The IT team asks the customer:

- *Is doge administrator's here? He tries to access the platform.*
- *No, he is in the Bahamas*




What is this IP?


A faint, light gray line drawing of a rocket ship is visible in the background on the left side of the slide. The drawing shows the side profile of the rocket, including a large circular porthole, a smaller circular hatch, and a series of small circles along the side, possibly representing rivets or sensors. The rocket is positioned vertically, with its nose pointing upwards.

95.31.18.119

Let me GeoIP it


 **Geo IP Tool**

[View my IP information](#) [Forum](#) [More info about IPs](#) [Language ▾](#)



Hostname: 95.31.18.119

IP Address: 95.31.18.119

Country:  Russian Federation

Country Code: RU (RUS)

Region: Moscow City

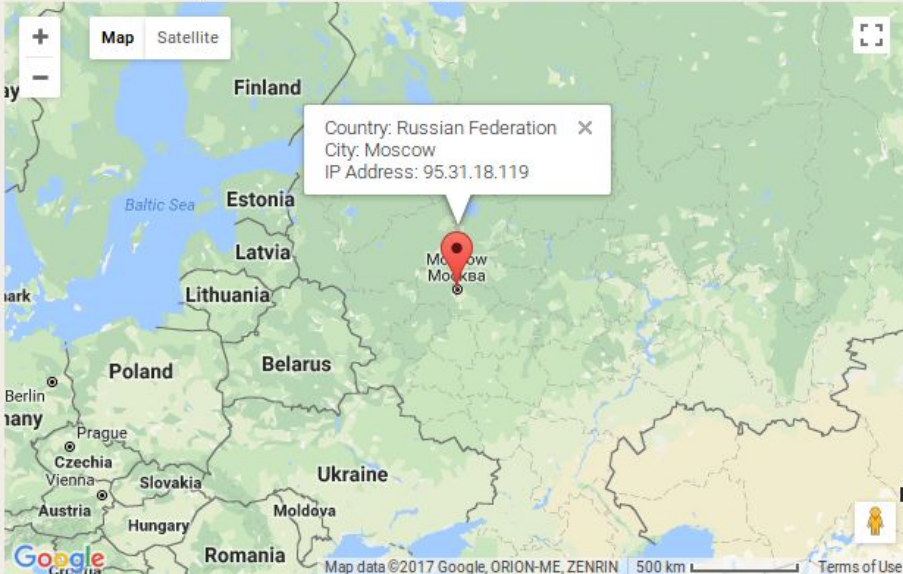
City: Moscow

Local time: 09 Nov 11:51 (MSK+0300)

Postal Code: 101194

Latitude: 55.7485

Longitude: 37.6184



Country: Russian Federation ✕
City: Moscow
IP Address: 95.31.18.119

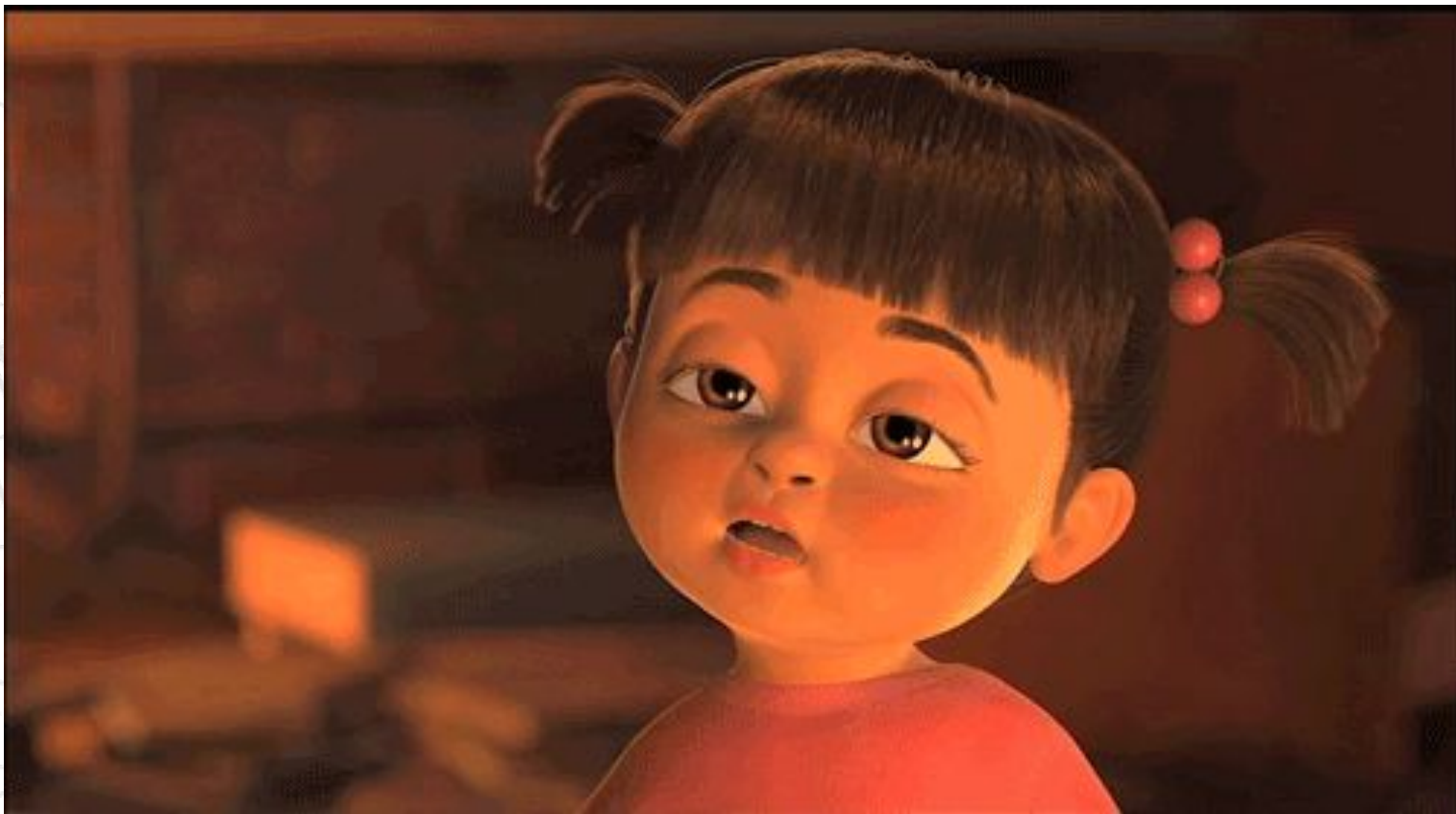
Map data ©2017 Google, ORION-ME, ZENRIN 500 km [Terms of Use](#)



What could go wrong?



I don't see it



Then, an expert arrives



Found it!



```
<?php
// src/AppBundle/Service/TokenService.php

private function generateRandomString($length = 10) {
    $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = '';
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[mt_rand(0, $charactersLength - 1)];
    }
    return $randomString;
}
```

mt_rand(int \$min, int \$max)

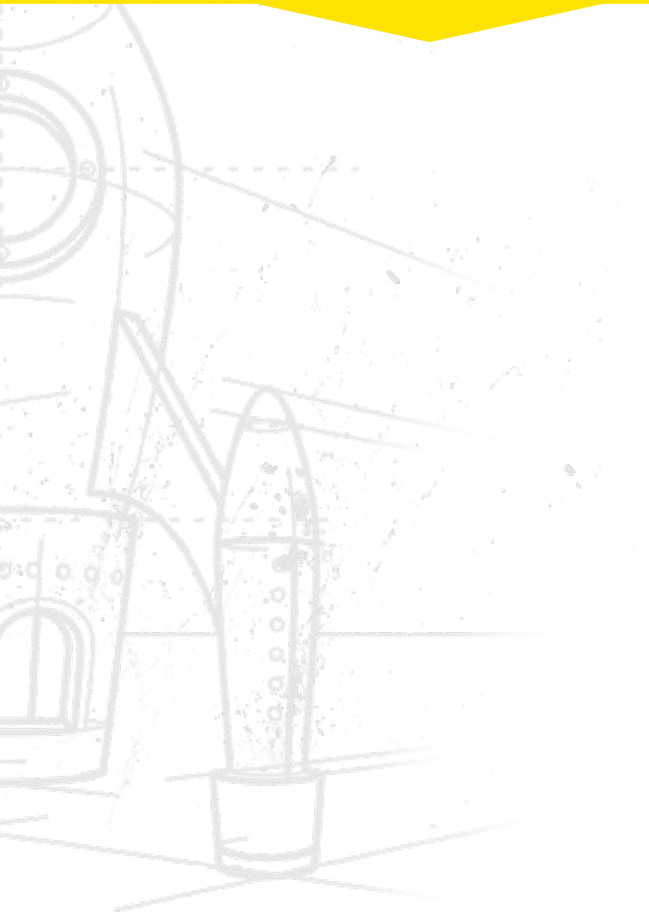


```
int mt_rand ( int $min , int $max )
```

use Mersenne Twister algorithm

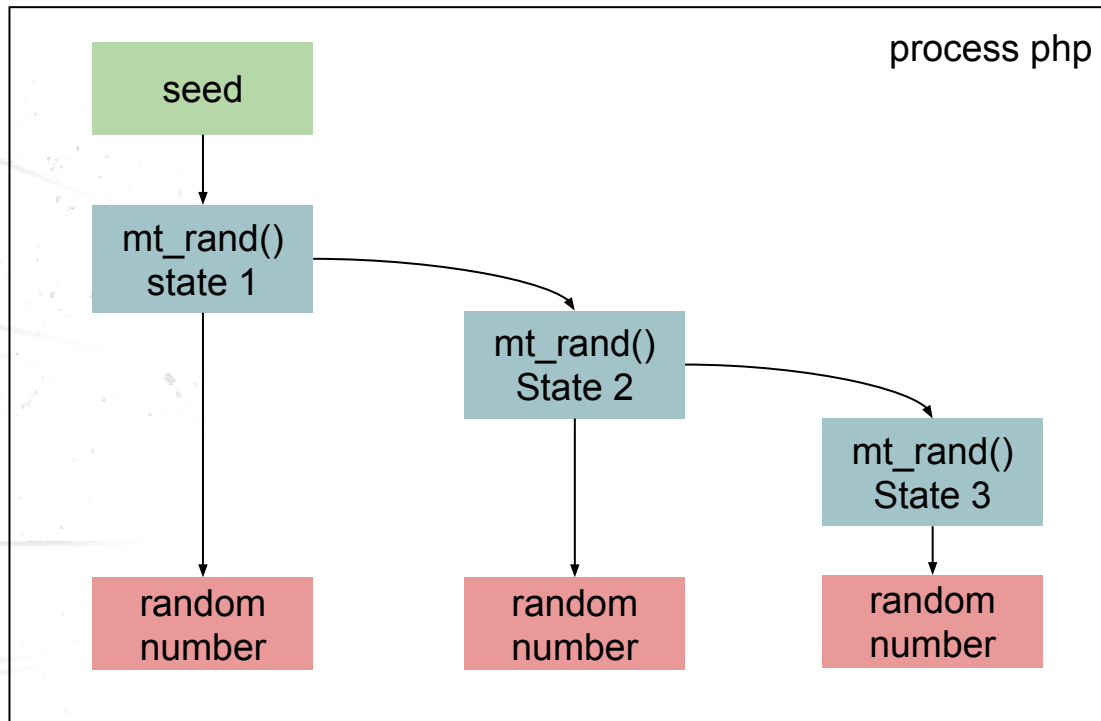
Return Values

A random integer value between **min** (or 0) and **max** (or [mt_getrandmax\(\)](#), inclusive), or **FALSE** if **max** is less than **min**.




**Not random enough
and predictable**

Weak in state



Break down into steps

A faint, light-colored illustration of a rocket launch is visible in the background on the left side of the slide. It shows a rocket being launched from a launch pad, with smoke and fire at the base.

mt_rand() call number	seed
1 st	initial seed value
2 nd	get state 1 as seed
3 rd	get state 2 as seed
n th	get state n-1 as seed

A faint, light gray line drawing of a rocket ship is visible in the background on the left side of the slide.

`seed max 232-1`
`[0, 2 147 483 647]`



Attack by seed

WANT DO WE WANT?



SEED



**WHEN DO WE
WE WANT IT?**



imgflip.com

NOW!!!



Made by openwall (known for John the ripper)

Re-implement `mt_rand()` in fast way

Scan 32 bit space of seed

How it works




```
token = m4QT2
```

```
characters =  
'0123456789abcdefghijklmnopqrstuvwxyzABCDE  
FGHIJKLMNOPQRSTUVWXYZ';
```

```
→ mt_rand(0, 60)
```

Break down the token

A faint, sketchy illustration of a rocket launch is visible on the left side of the slide. It shows a rocket being launched from a launch pad, with smoke and fire at the base, and a large structure in the background.

character	index
m	22
4	4
Q	52
T	55
2	2

Usage php_mt_seed



```
./php_mt_seed VALUE_OR_MATCH_MIN [MATCH_MAX [RANGE_MIN RANGE_MAX]]
```

```
./php_mt_seed 22 22 0 60 // m
                4 4 0 60 // 4
                52 52 0 60 // Q
                55 55 0 60 // T
                2 2 0 60 // 2
```

```
Found 0, trying 637534208 - 671088639, speed 89667258 seeds per
second
seed = 658126103
```


How fast can I break it?



2 minute on 16 vCores @ 3,1 GHz



- Website with admin panel
- Attacker has an user account

GOAL
**Take control of the
admin account**

Make some assumptions



- Server Apache with PHP mod
- Flood server to get fresh apache process



Make some assumptions



- How many calls of `mt_rand()` before generating token?
 - We don't know
- We need to take it into account when using `php_mt_seed`

Let's try it



lulzcat


HOEM

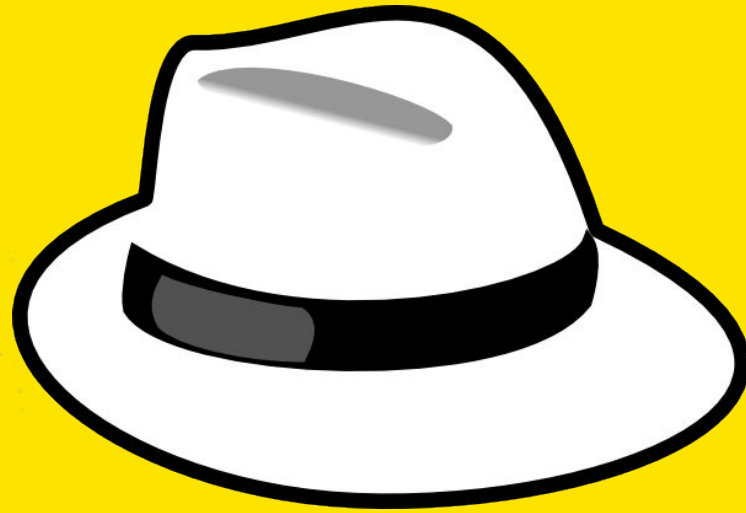
LOGIN

WOW SO MUTCH BEAUTIFUL!



lulzcat© 2017

- 
- A faint, light-colored line drawing in the background on the left side of the slide. It depicts a rocket or space lander on a launch pad, with a large plume of smoke or fire coming out of its engines, suggesting a launch or explosion. The drawing is composed of simple lines and dots, giving it a sketchy, technical appearance.
- use CSPRNG function
 - in PHP 7:
 - use `random_bytes()`
 - use `sodium_randombytes_buf()`
 - include in PHP 7.2



Thank you

- <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final218.pdf>
- <https://www.insomniasec.com/downloads/publications/Not%20So%20Random%20-%20Exploiting%20Unsafe%20Random%20Number%20Generator%20Use.pdf>
- <https://sockpuppet.org/blog/2014/02/25/safely-generate-random-numbers/>
- https://media.blackhat.com/bh-us-12/Briefings/Argyros/BH_US_12_Argyros_PRNG_WP.pdf
- <http://github.com/lepiaf/weak-app>
- <https://github.com/lepiaf/exploit-weak-app>