Bla Bla Car

Web Security

Let’s continue to hack!

Alain Tiemblo

Web Security Lead Engineer @ BlaBlaCar

ninsuo

Bla Bla Car

Symfony Live
PARIS 2017
30-31 MARS

What’s up?

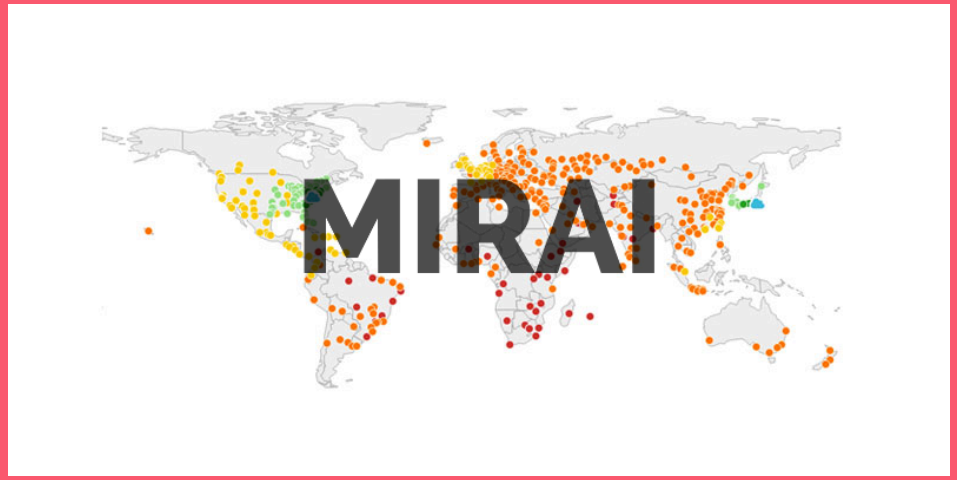
$81 million

cyber heist in Bangladesh Bank

02 2016

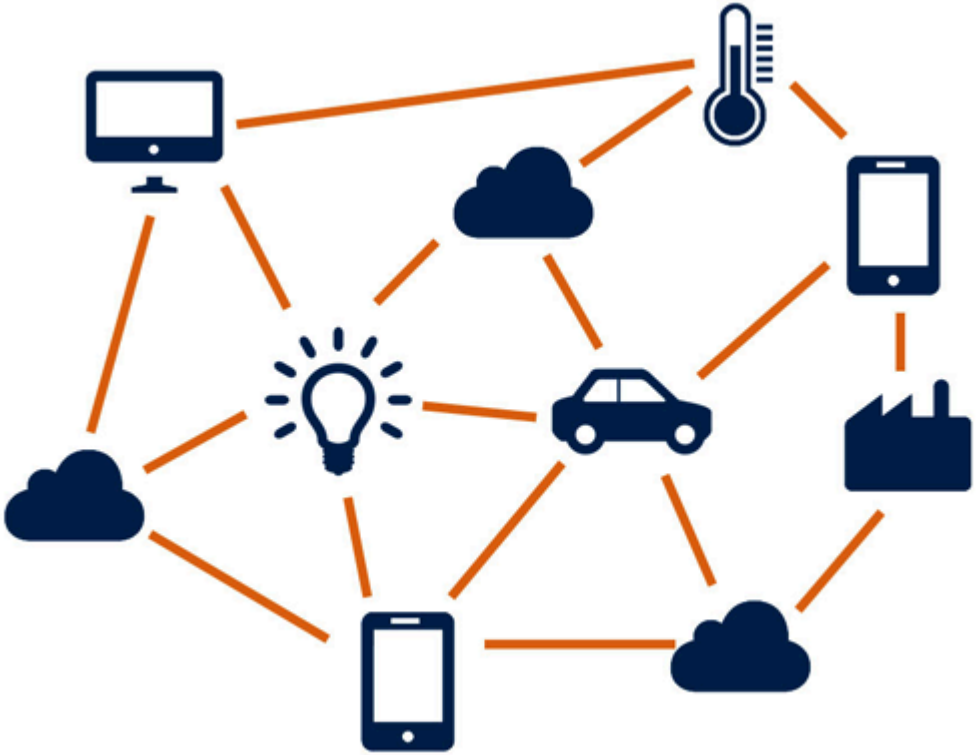
Heist record is $69.8M

08 2005

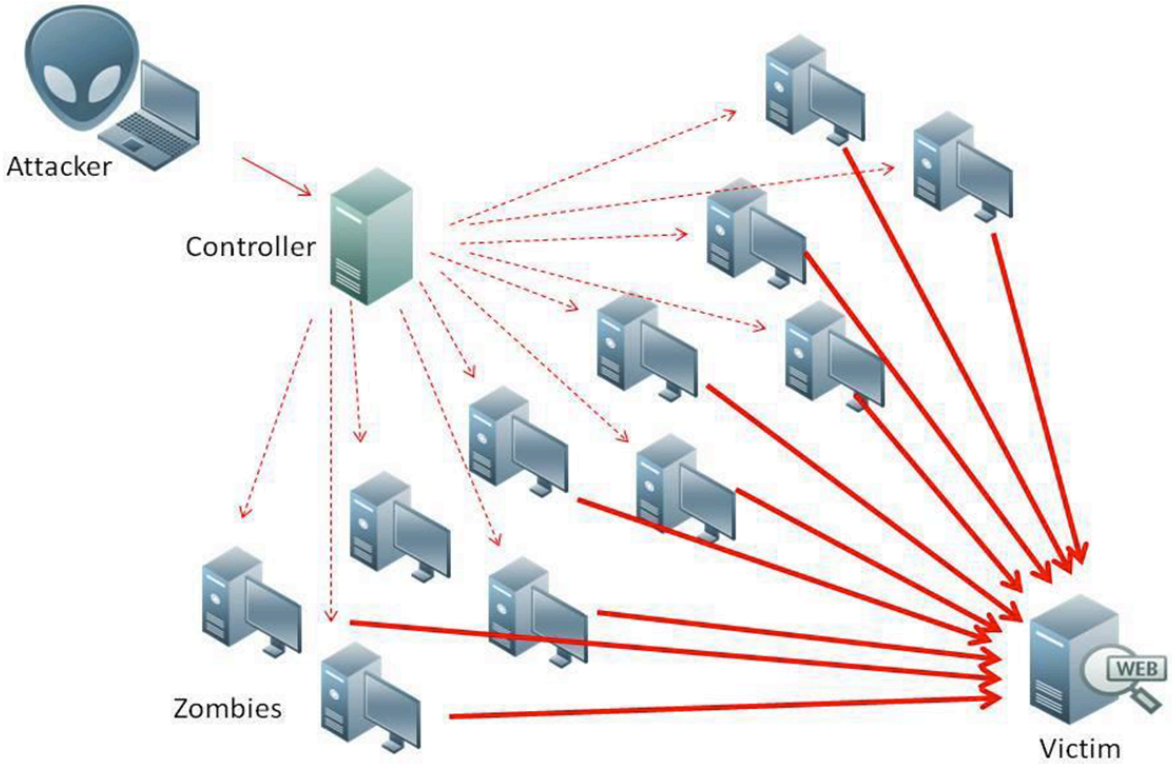


Mirai Botnet

09 2016



Default passwords on 145K connected devices



DDOS attacks at a 1TB/s rate

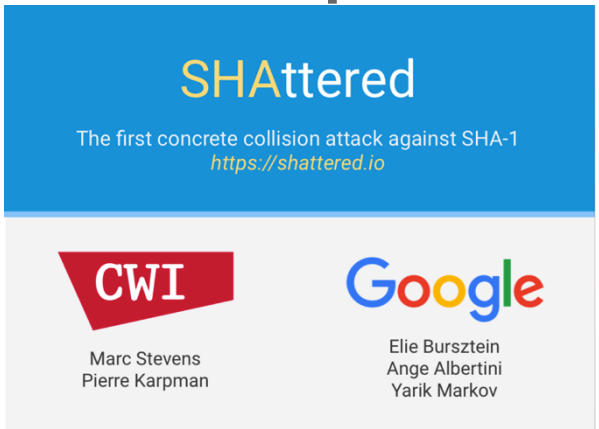
DDOS prevention checklist

1. **Set traffic thresholds** based on the average number of visits you get
2. **Create an IP blacklist and whitelist** to be able to quickly respond to attacks over your applications
3. **Automate communication with users** with a service status application to avoid support 💩storm
4. **Hire an ops** because as a backend developer, I can't help you further here 😅

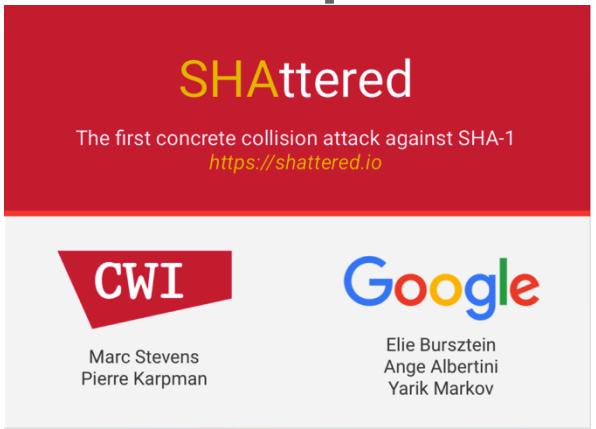
SHA-1 is proven broken

02 2017

file1.pdf



file2.pdf



sha1 = 38762cf7f55934b34d179ae6a4c80cadccbb7f0a

SHA-1 Checklist

1. **Do not hash passwords using SHA-1,** and if you did, bcrypt those hashes for more security
2. **Do not use SHA-1 certificates**, that's no standard anymore since 2015
3. **Do not use SHA-1 to check for data integrity**, collisions are still hard to get but that's doable
4. **Use SHA-256 anywhere**: in PHP, `hash("sha256", $input)`

Note that Google sunsetted SHA-1 on September, 2014

Major Data Leaks revealed!

2016

93 338 602 accounts

Plain text passwords ❤

Leaked in 2012

112 005 531 accounts

MD5 passwords without salt

Leaked in 2016

164 611 595 accounts

SHA-1 passwords without salt

Leaked in 2012

234 842 089 accounts

Plain text passwords ❤

Leaked in 2015

359 420 698 accounts

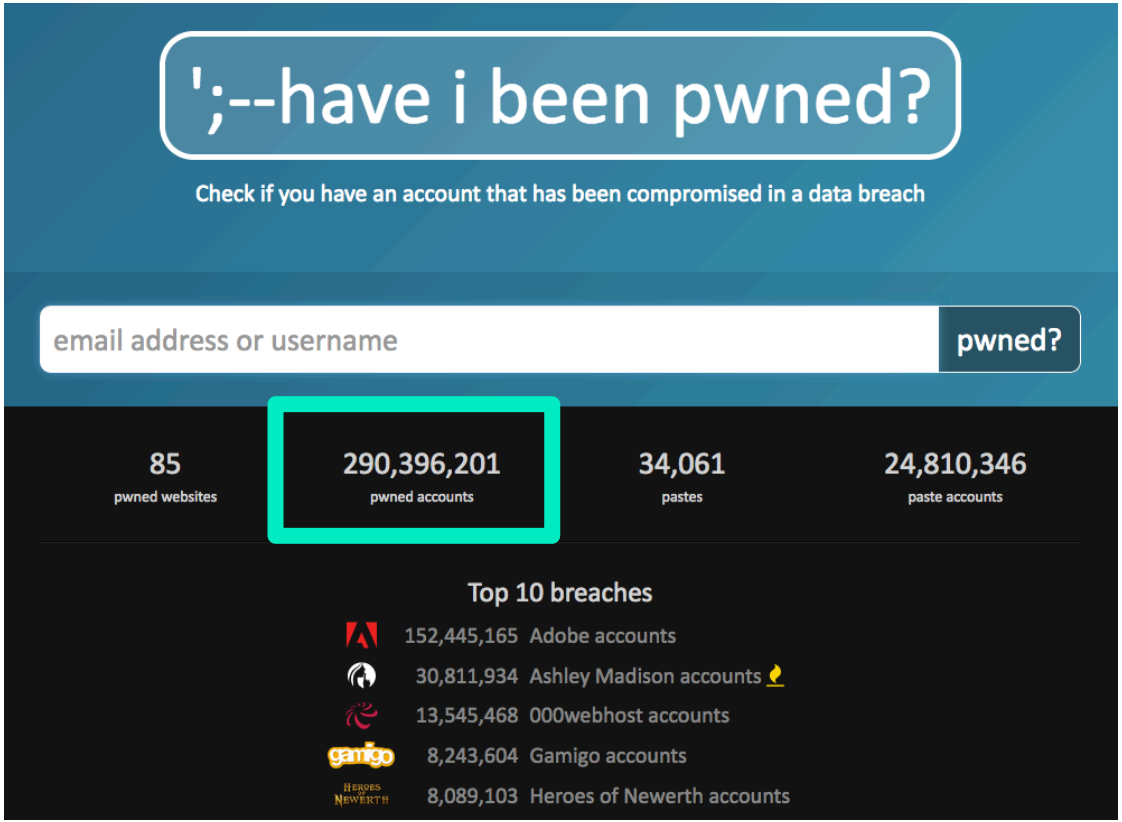
SHA-1 passwords without salt

Leaked in 2008

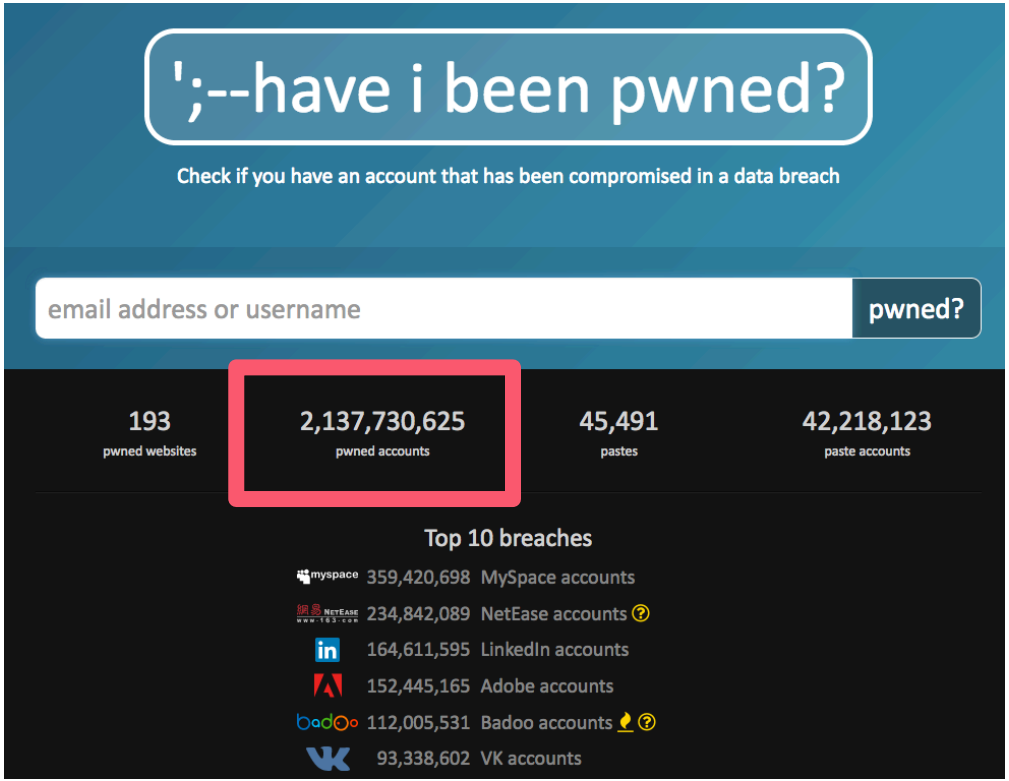
Use bcrypt to hash passwords!

Why the hell companies don’t use it!


Créateur de
Symfony


';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address or username
pwned?
85
pwned websites
290,396,201
pwned accounts
34,061
pastes
24,810,346
paste accounts
Top 10 breaches
152,445,165 Adobe accounts
30,811,934 Ashley Madison accounts
13,545,468 000webhost accounts
8,243,604 Gamigo accounts
8,089,103 Heroes of Newerth accounts

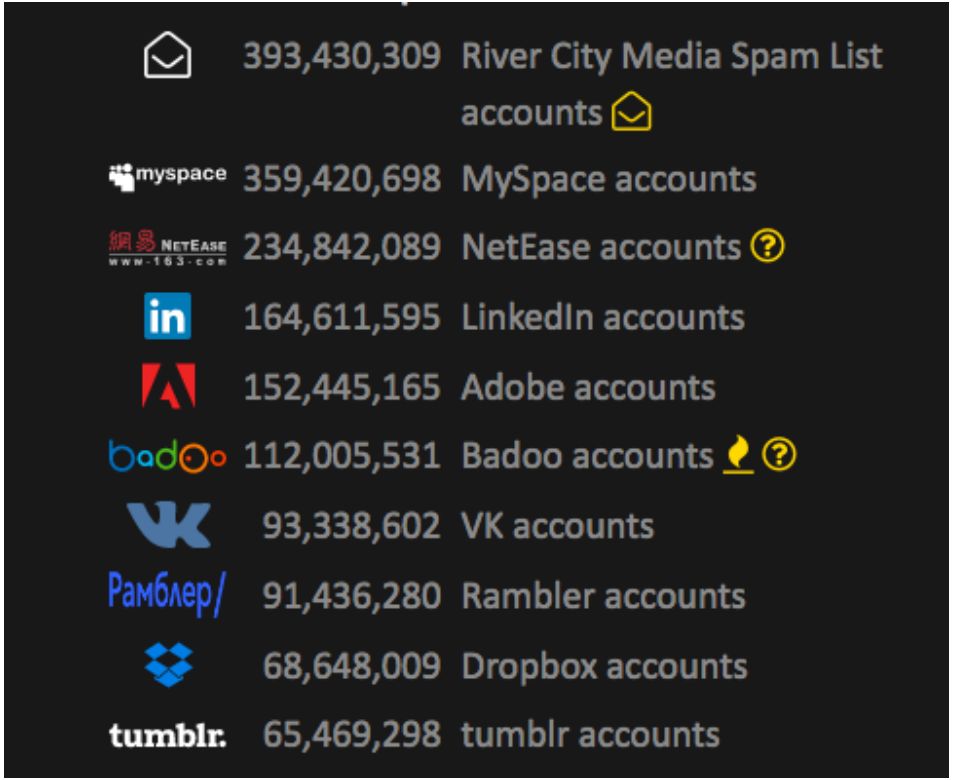
Last year…


';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address or username
pwned?
193
pwned websites
2,137,730,625
pwned accounts
45,491
pastes
42,218,123
paste accounts
Top 10 breaches
359,420,698 MySpace accounts
234,842,089 NetEase accounts
164,611,595 LinkedIn accounts
152,445,165 Adobe accounts
112,005,531 Badoo accounts
93,338,602 VK accounts

Now!

Password Reuse Attack

Most users use the same password everywhere



Companies databases get compromised

LinkedIn Data Dump

This breach dates back to 2012, but was only release in May 2016 as a sale on a "dark net" market. Allegedly it contains email addresses and passwords, which were stored as a SHA1 hash without salting. As always, use and enjoy responsibly as I make no claims over the data.

Update 1: For those who have asked how they can help with server costs, see https://www.thecthulhu.com/donate/ thanks!

Download

SHA1: 8F17 1B24 EE31 8155 4C7A 2C3A 35B7 5BD4 979A BD93
SHA256: 3D45 C7DA BEBE CC32 39BD 1263 71C8 B77E D288 90B6 14C1 7157 3C85 4E56 D746 83D8

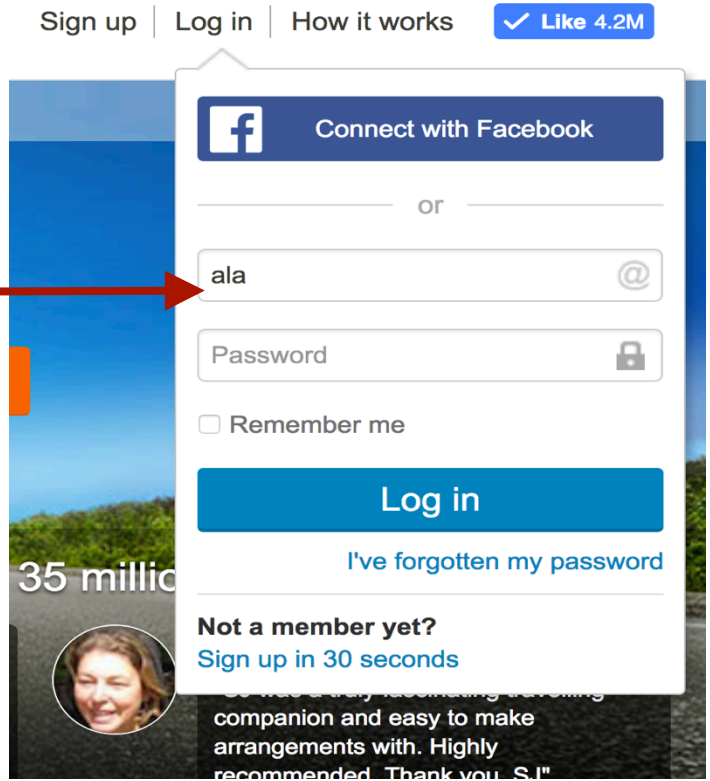
Torrent: Download LinkedIn.rar.torrent file
Magnet: Download the LinkedIn.rar file by magnet

Contact Form: https://www.thecthulhu.com/contact-me/

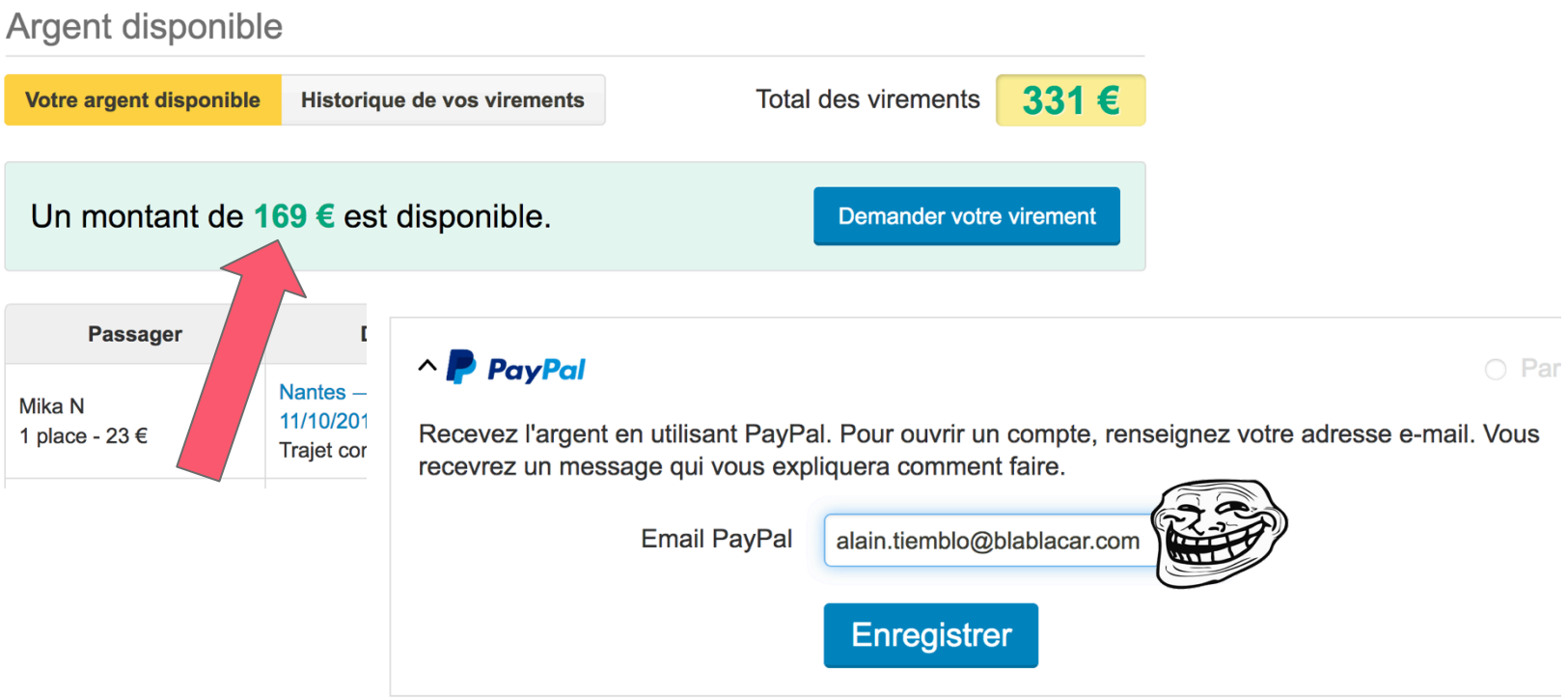
-Cthulhu (@CthulhuSec)

They can be downloaded by anyone

	A	B
1	**EMAIL**	**PASSWORD**
2	foo@example.com	password
3	bar@example.com	12345678
4	foobar@example.com	baseball
5	foo.bar@example.com	football
6	bar.foo@example.com	superman
7	foo_bar@example.com	trustno1
8	bar_foo@example.com	sunshine
9	fbar@example.com	123456789
10	barf@example.com	starwars
11	foo@gmail.com	computer
12	bar@gmail.com	corvette
13	foobar@gmail.com	princess
14	foo.bar@gmail.com	iloveyou
15	bar.foo@gmail.com	maverick
16	foo_bar@gmail.com	samantha
17	bar_foo@gmail.com	steelers
18	fbar@gmail.com	whatever
19	barf@gmail.com	hardcore
20	foo@yahoo.com	internet
21	bar@yahoo.com	mercedes
22	foobar@yahoo.com	bigdaddy
23	foo.bar@yahoo.com	midnight

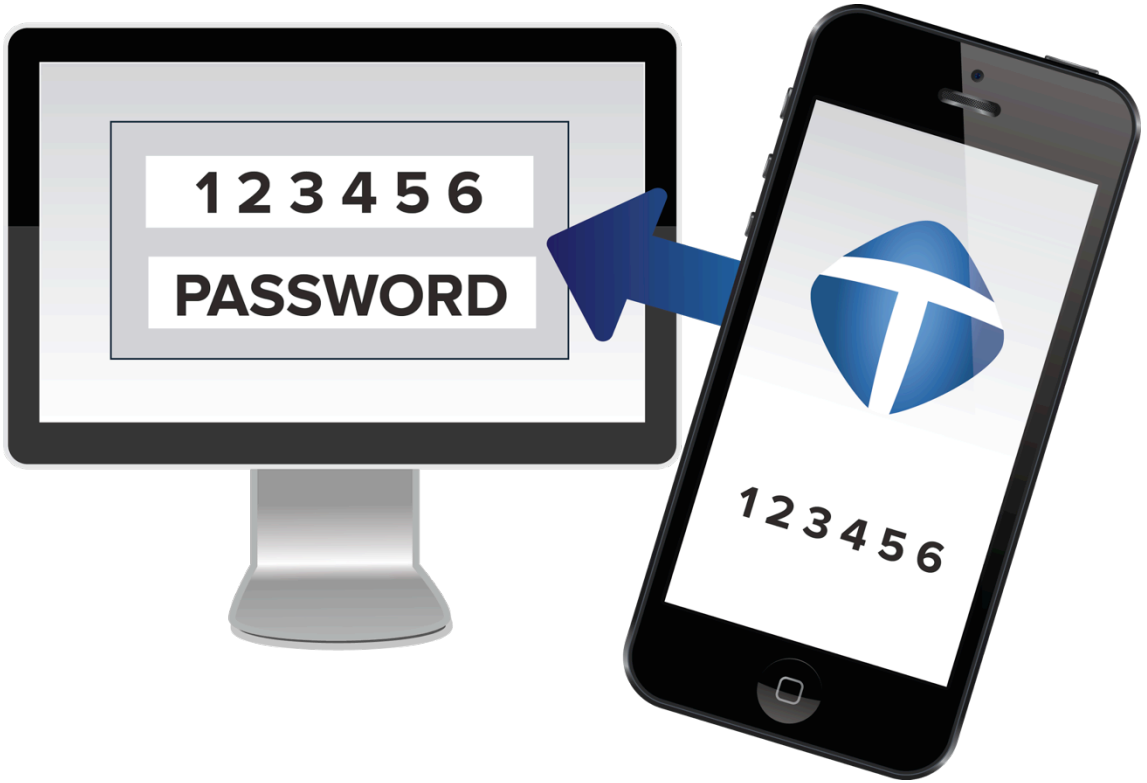


Passwords can be reused!

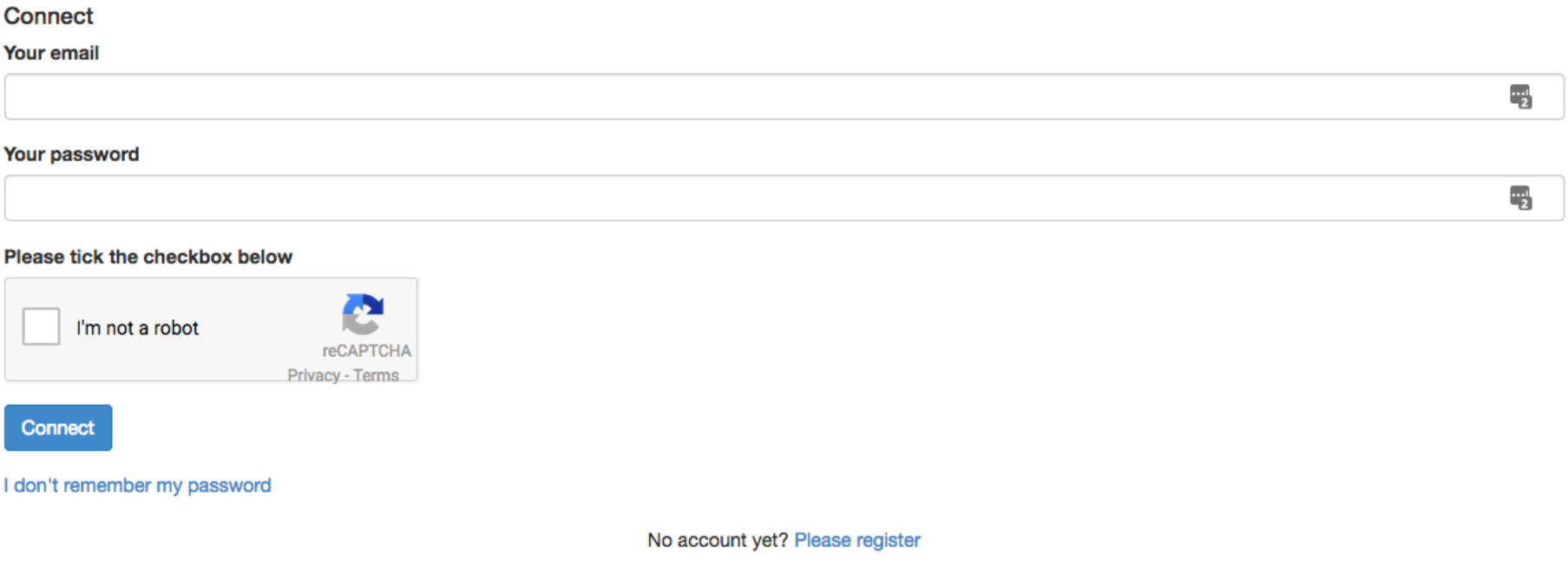


And when they succeed...

How to protect our applications?



Multi-factor authentication


Connect
Your email
Your password
Please tick the checkbox below
I'm not a robot
reCAPTCHA
Privacy - Terms
Connect
I don't remember my password
No account yet? Please register

Captcha

Enforce password change in a regular basis

Login using any of the following services

SensioLabsConnect

Click here to login using SensioLabs Connect

Login using Google

Login using GitHub

Login using Facebook

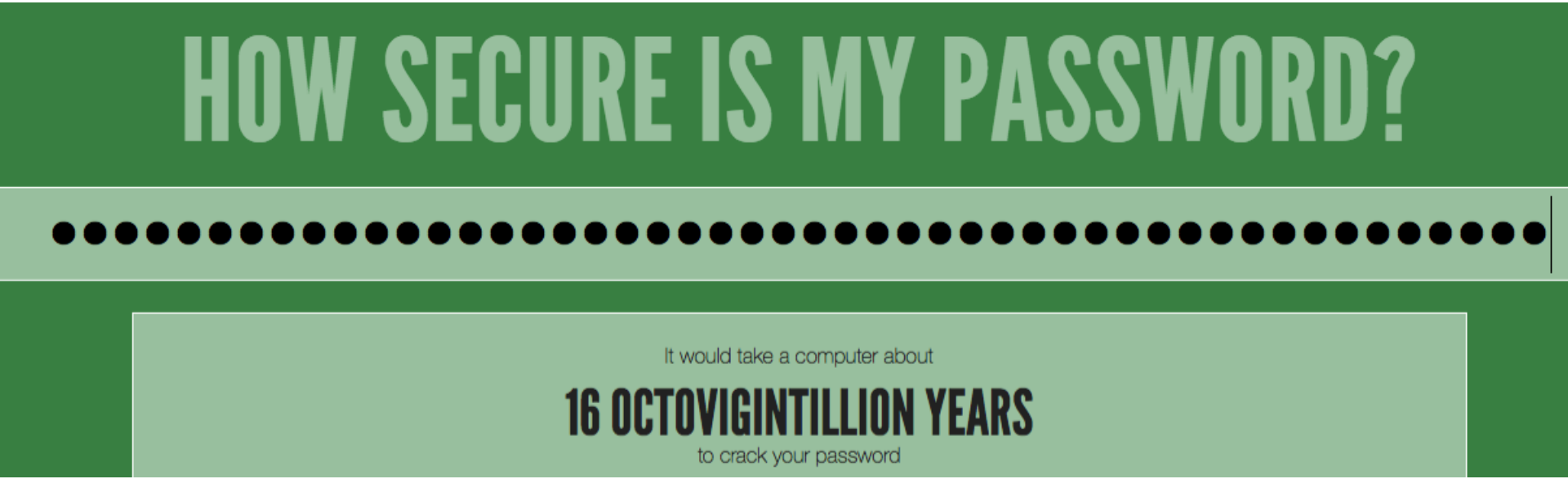
Login using Twitter

Delegate sign-in to others ❤

How to protect our family & friends?

Spread the word!

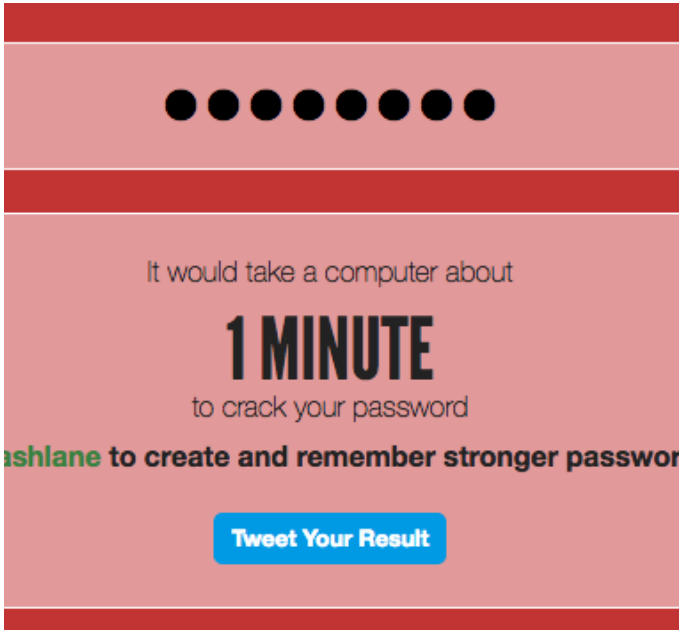
Don’t use guessable passwords



https://HowSecureIsMyPassword.net

Check your password strength

banana75



I love fruit.

Prefer a passphrase

banana75 + twitter = tbanana75r

banana75 + facebook = fbanana75k

banana75 + Bla Bla Car = bbanana75r

One unique password per website

I love fruit. + twitter = I love twitter's fruit.

I love fruit. + facebook = I love facebook's fruit.

I love fruit. + Bla Bla Car = I love blablacar's fruit.

LastPass •••|

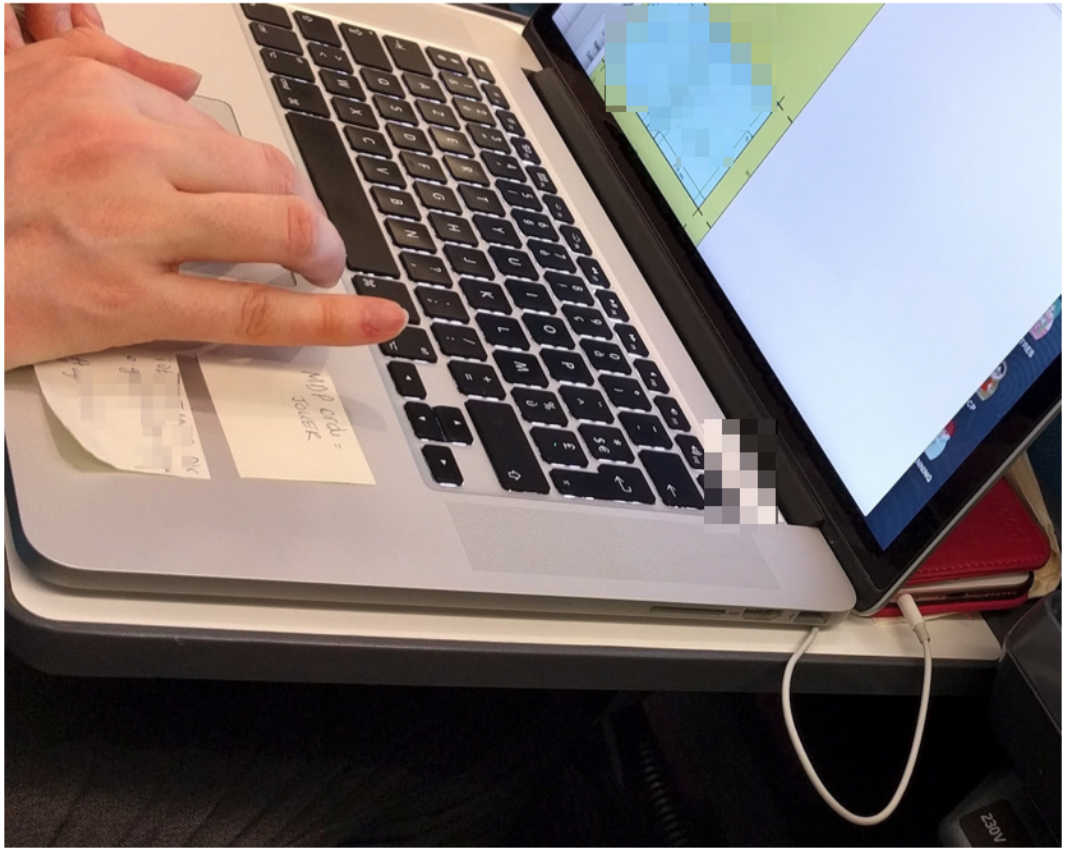
StickyPassword
securing your personal data

keeper®

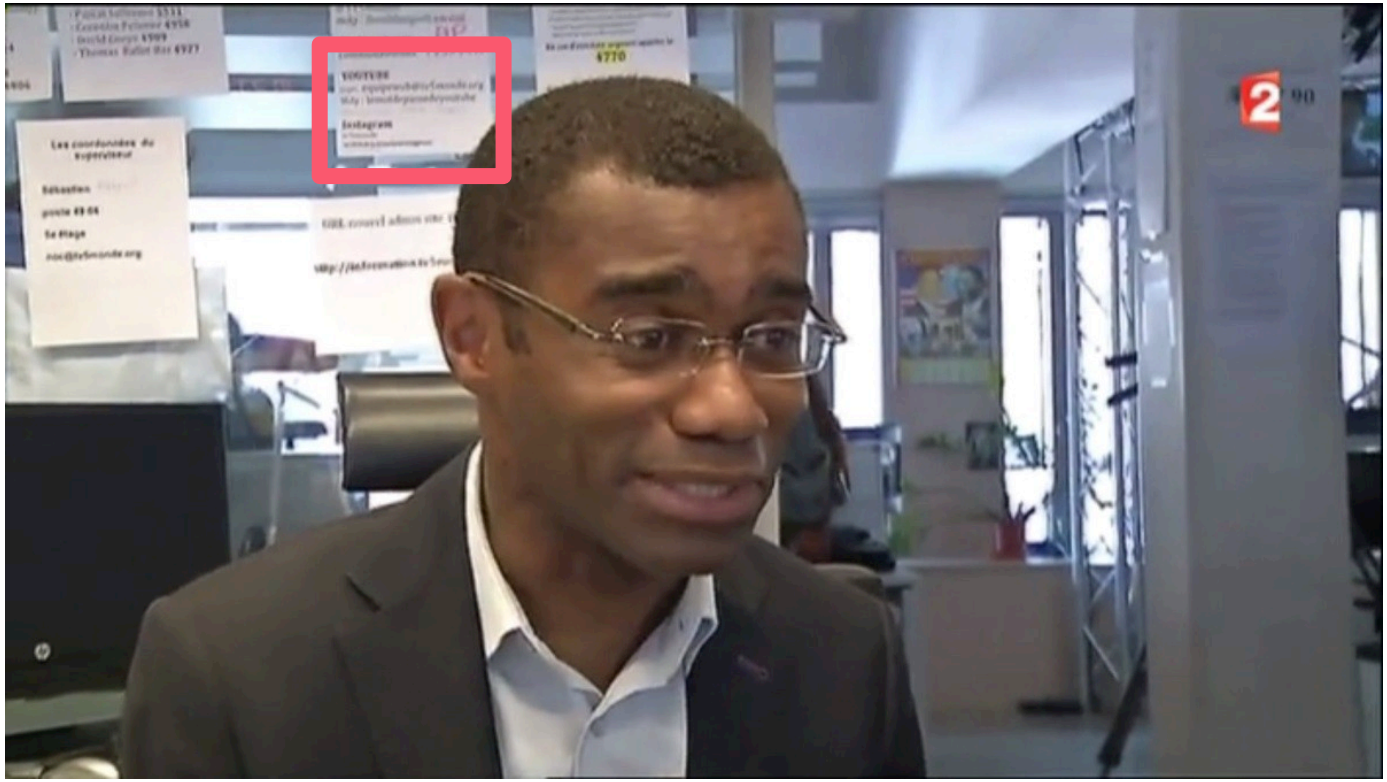
PASSWORD BOSS

Use a password manager

Other password reuse attack factors

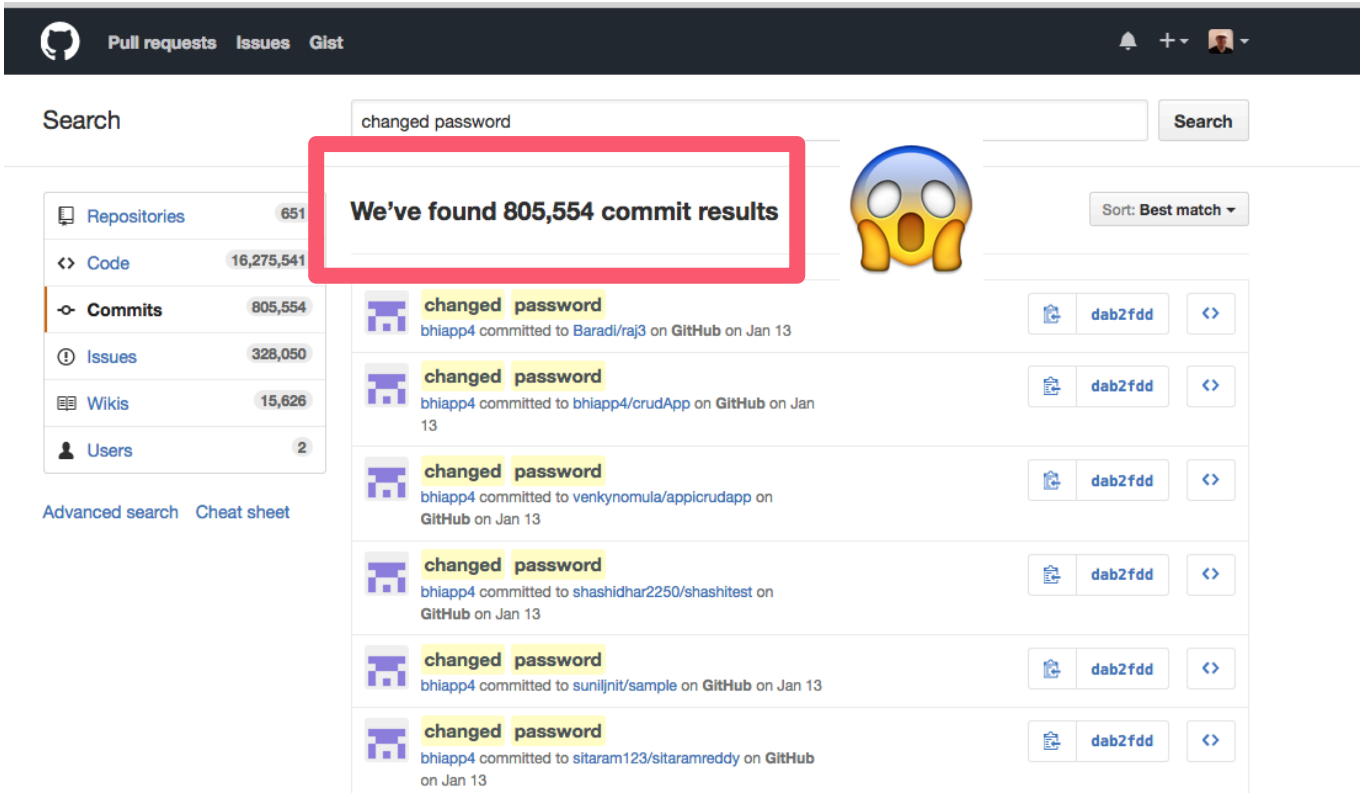


Passwords on a post-it ❤



Passwords on walls

WiFi passwords on walls



Production passwords on GitHub

This repository Search Pull requests Issues Gist

ninsuo / irc-scrabble

Unwatch 1 Star 0 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Wiki Pulse Graphs Settings

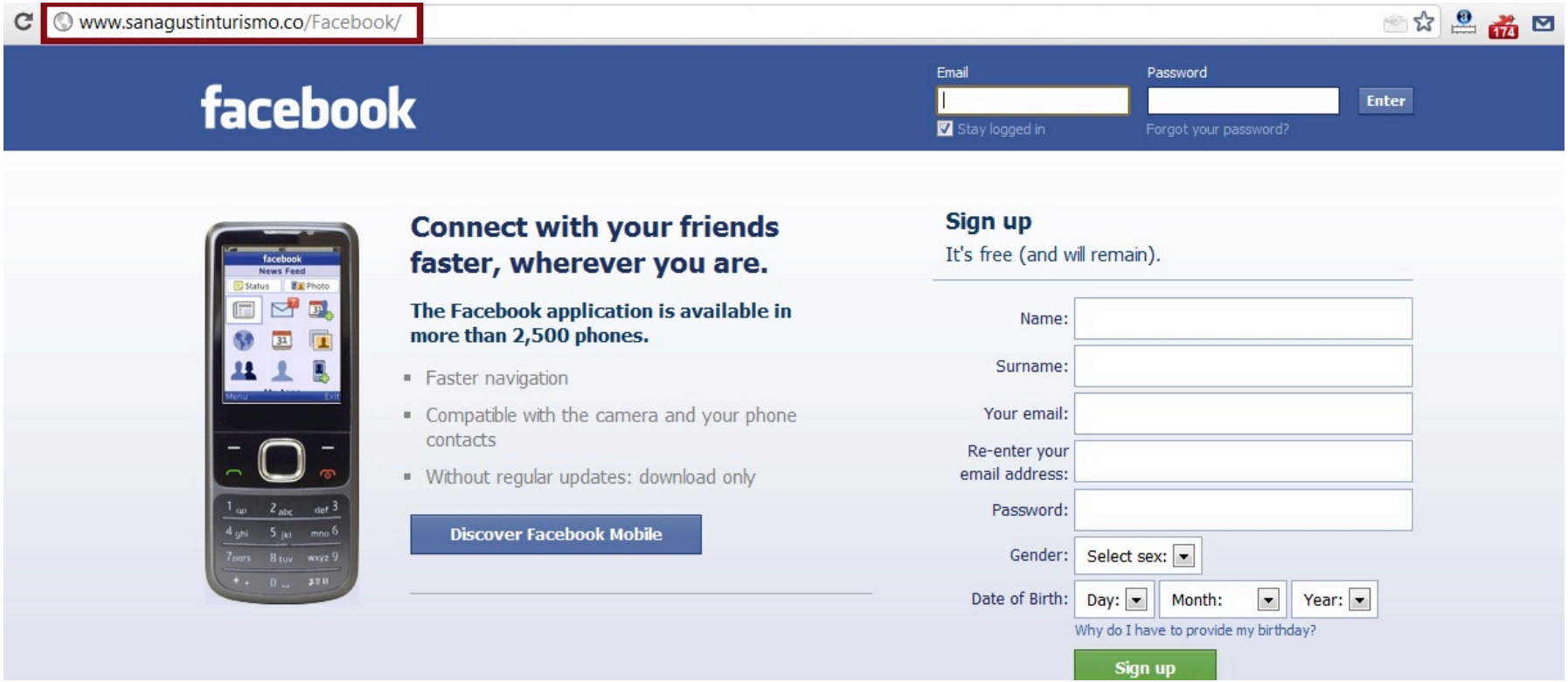
Branch: master irc-scrabble / Scrabble / robot.ini Find file Copy path

ninsuo initial commit e404705 on Jan 2

1 contributor

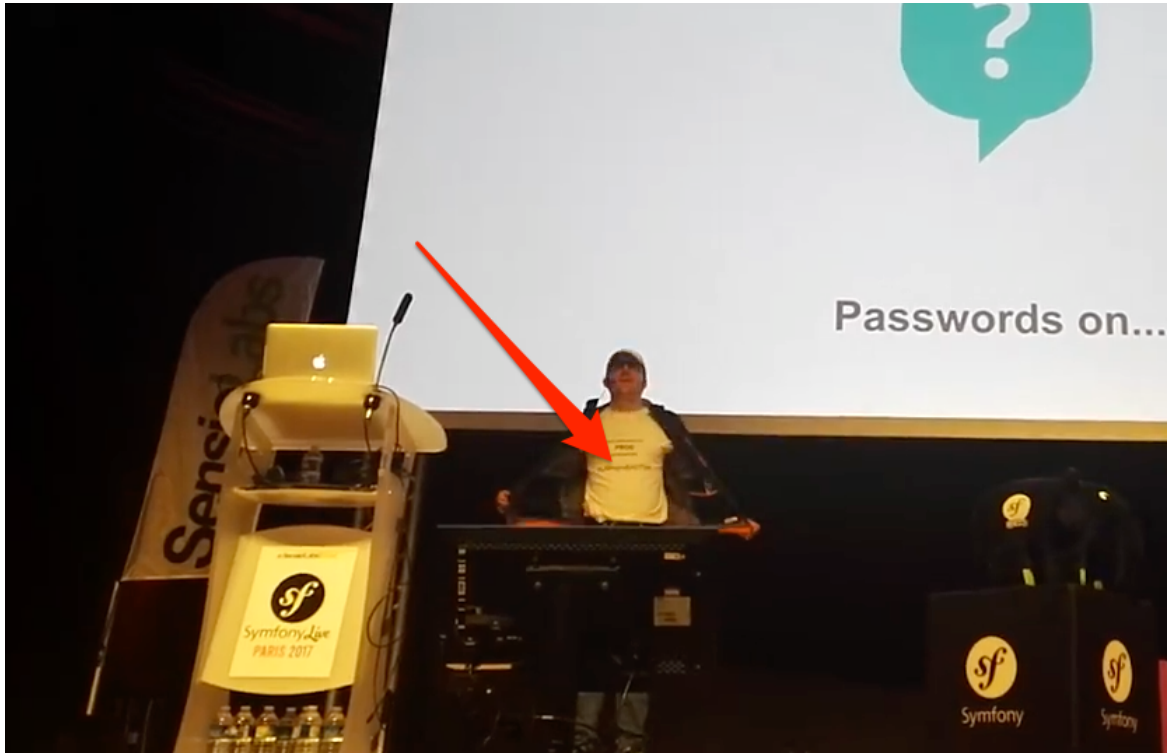
24 lines (23 sloc) 322 Bytes Raw Blame History

```
1  [AUTOJOIN]
2  1=#test
3  [IRCOP]
4  login=Krix
5  password=J35u15Kr1xL35up3rb3R0b0tD3L4M0rtQu1Tu3!!!!!
6  [OPTIONS]
7  autojoin=yes
8  ircop=yes
9  log=yes
10 output=yes
11 register=yes
12 [REGISTER]
13 nickname=NickServ
14 password=toto42
```


www.sanagustinturismo.co/Facebook/
facebook
Email
Password
Enter
Stay logged in
Forgot your password?
Connect with your friends faster, wherever you are.
The Facebook application is available in more than 2,500 phones.
Faster navigation
Compatible with the camera and your phone contacts
Without regular updates: download only
Discover Facebook Mobile
Sign up
It's free (and will remain).
Name:
Surname:
Your email:
Re-enter your email address:
Password:
Gender:
Select sex:
Date of Birth:
Day:
Month:
Year:
Why do I have to provide my birthday?
Sign up

Phishing

Passwords on...



Passwords on...


FAIR
DES
IGN


SymfonyLive
PARIS 2017
Symfony

Captcha Cracking

Completely Automated Public Turing test to tell Computers and Humans Apart

Method #1

The Geeky way

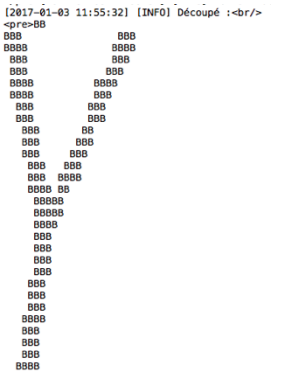
Capcha is made black & white

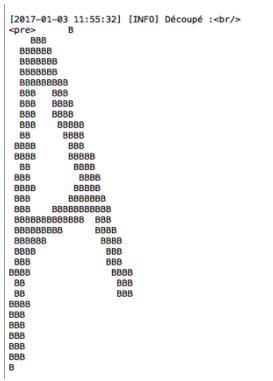
<pre>[2017-01-03 11:55:32] [INFO] Forme binaire :

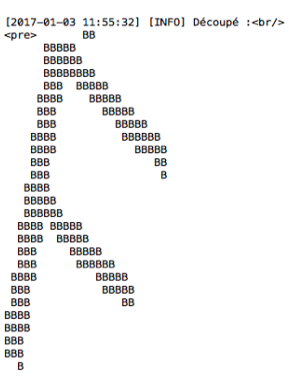
No need to work on large images, reduce it enough

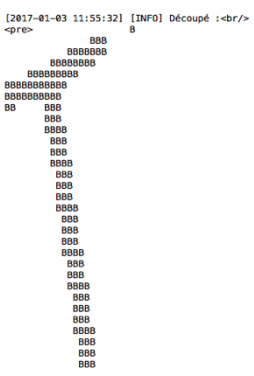
</pre>[2017-01-03 11:55:32] [INFO] Recherche verticcale des lettres...
<pre>[2017-01-03 11:55:32] [INFO] Forme binaire :

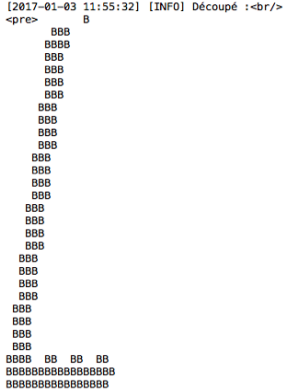
Look for spaces between letters

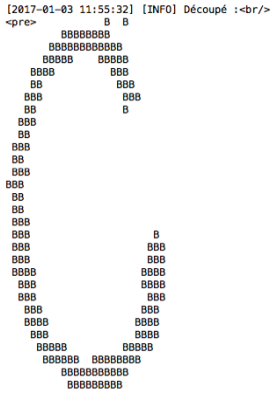

[2017-01-03 11:55:32] [INFO] Découpé :
<pre>BB
BBB BBB
BBBB BBBB
BBB BBB
BBB BBB
BBBB BBBB
BBBB BBB
BBB BBB
BBB BBB
BBB BB
BBB BBB
BBB BBB
BBB BBBB
BBBB BB
BBBBB
BBBBB
BBBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBBB
BBB
BBB
BBB
BBBB
B


[2017-01-03 11:55:32] [INFO] Découpé :
<pre> B
BBB
BBBBBB
BBBBBBB
BBBBBBB
BBBBBBBBB
BBB BBB
BBB BBBB
BBB BBBB
BBB BBBBB
BB BBBB
BBBB BBB
BBBB BBBBB
BB BBBB
BBB BBBB
BBBB BBBBB
BBB BBBBBBB
BBB BBBBBBBBBB
BBBBBBBBBBBBB BBB
BBBBBBBBB BBBB
BBBBBB BBB
BBBB BBB
BBB BBB
BBBB BBBB
BB BBB
BB BBB
BBBB
BBB
BBB
BBB
BBB
BBB
B

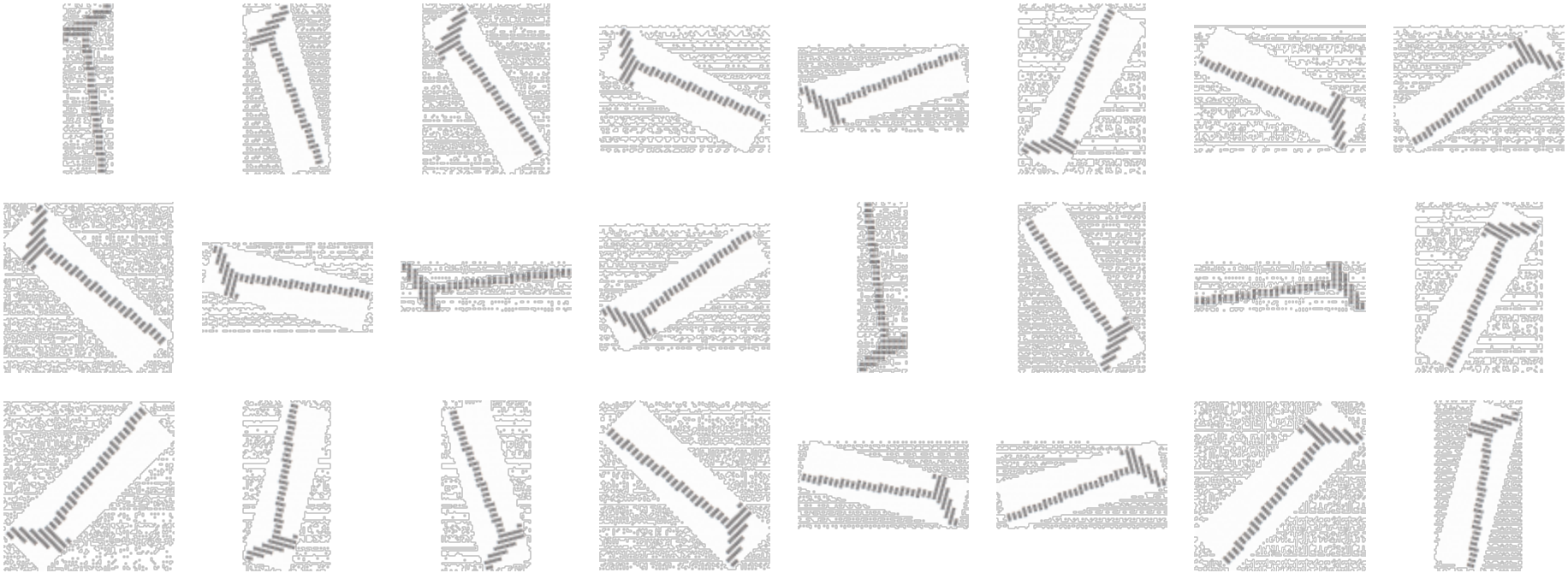

[2017-01-03 11:55:32] [INFO] Découpé :
<pre> BB
BBBBB
BBBBBB
BBBBBBBB
BBB BBBBB
BBBB BBBBB
BBB BBBBB
BBB BBBBB
BBBB BBBBBB
BBBB BBBBBB
BBB BB
BBB B
BBBB
BBBBB
BBBBBB
BBBB BBBBB
BBBB BBBBB
BBB BBBBB
BBB BBBBBB
BBBB BBBBB
BBB BBBBB
BBB BB
BBBB
BBBB
BBB
BBB
B


[2017-01-03 11:55:32] [INFO] Découpé :
<pre> B
BBB
BBBBBBB
BBBBBBBB
BBBBBBBBB
BBBBBBBBBB
BB BBB
BBB
BBB
BBBB
BBB
BBB
BBBB
BBB
BBB
BBBB
BBB
BBB
BBBB
BBB
BBB
BBBB
BBB
BBB
BBB
BBB
BBB

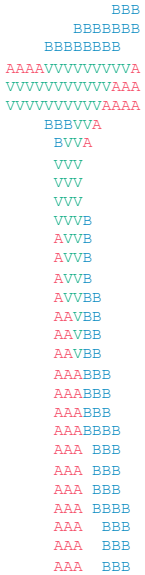

[2017-01-03 11:55:32] [INFO] Découpé :
<pre> B
BBB
BBBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBB
BBBB BB BB BB
BBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBB


[2017-01-03 11:55:32] [INFO] Découpé :
<pre> B B
BBBBBBBB
BBBBBBBBBBB
BBBBB BBBBB
BBBB BBB
BB BBB
BBB BBB
BB B
BBB
BB
BBB
BB
BBB
BB
BBB
BBB B
BBB BBB
BBB BBB
BBBB BBBB
BBB BBBB
BBB BBB
BBB BBB
BBBB BBBB
BBB BBBB
BBBBB BBBBB
BBBBBB BBBBBBBB
BBBBBBBBBB
BBBBBBBB

Cut



Get each letter rotated from 0” to 359”



A = known dictionary

B = character to test

V = common part

Compare each rotated char with known dictionary

A = known dictionary

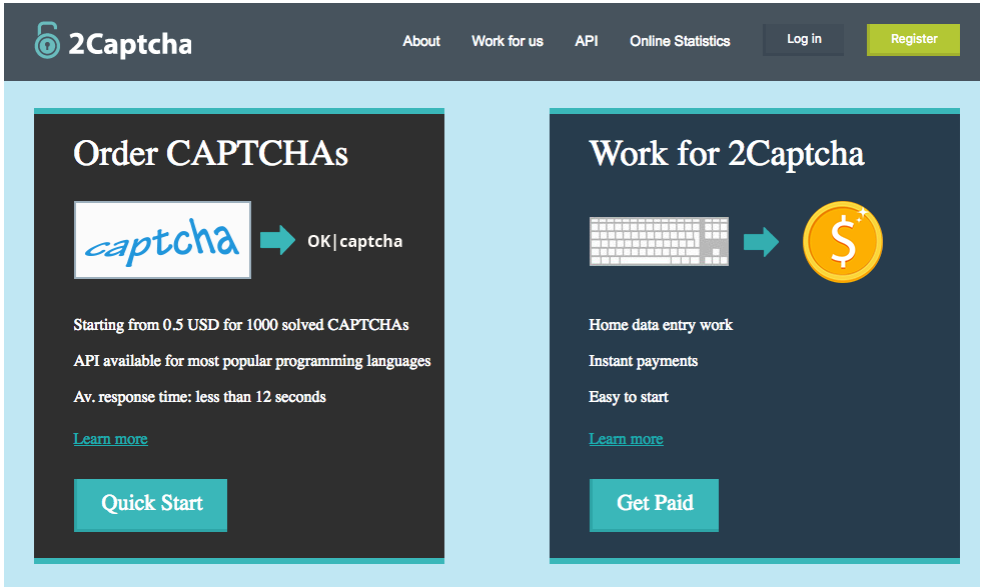
B = character to test

V = common part

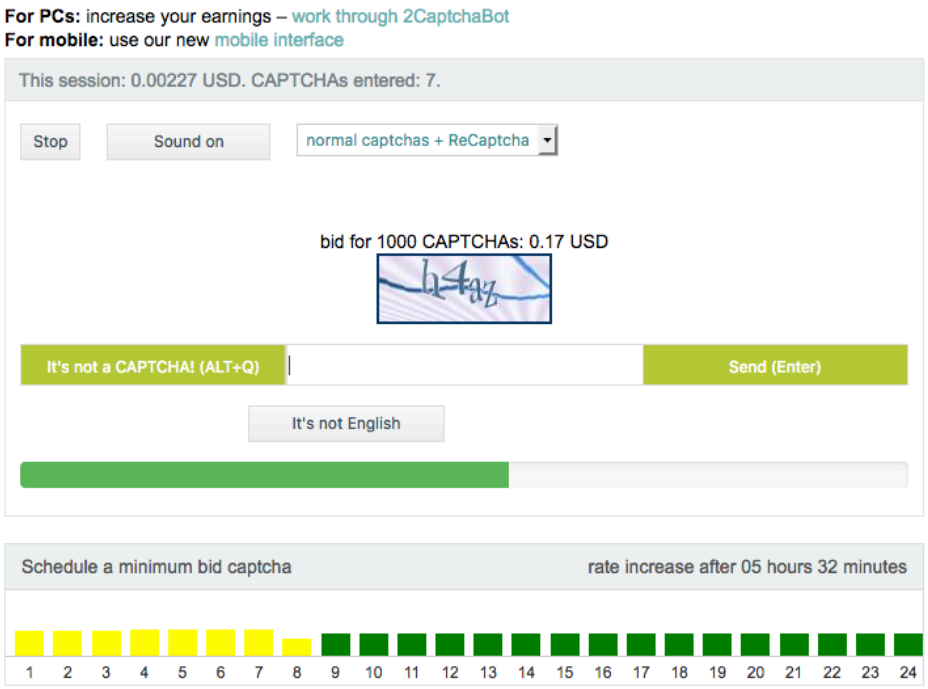
Matching character is the one having higher common part

Method #2

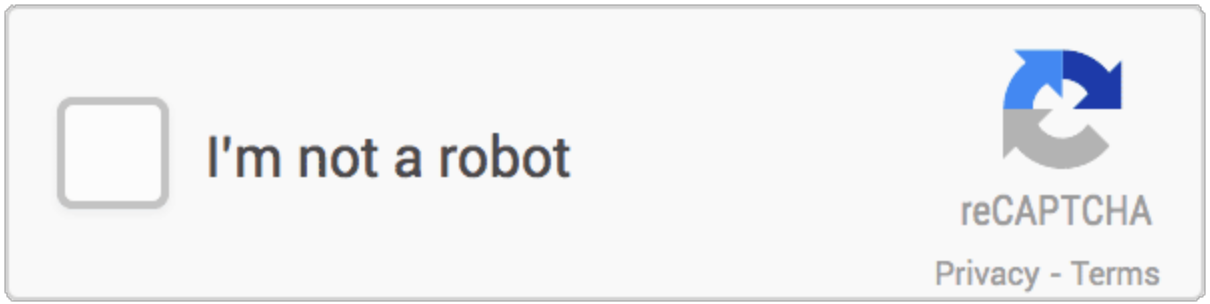
The Lazy way



Pay people to fill your captcha 🤔

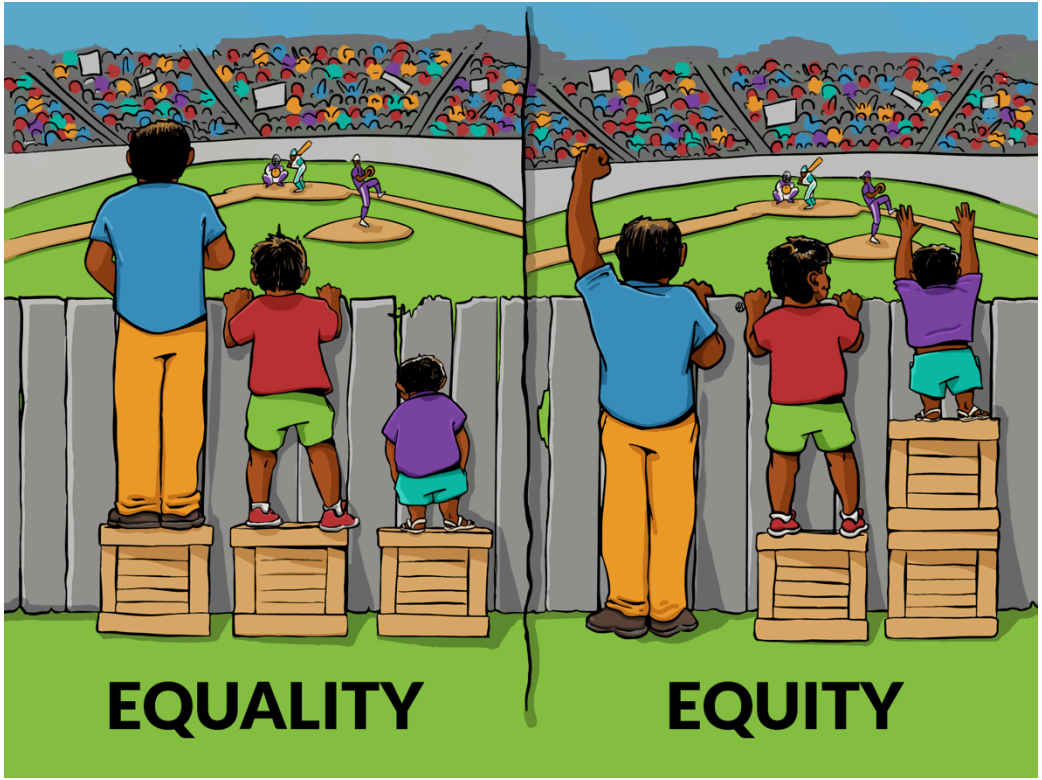


I've earned 0.00227 USD for 7 captchas 😅



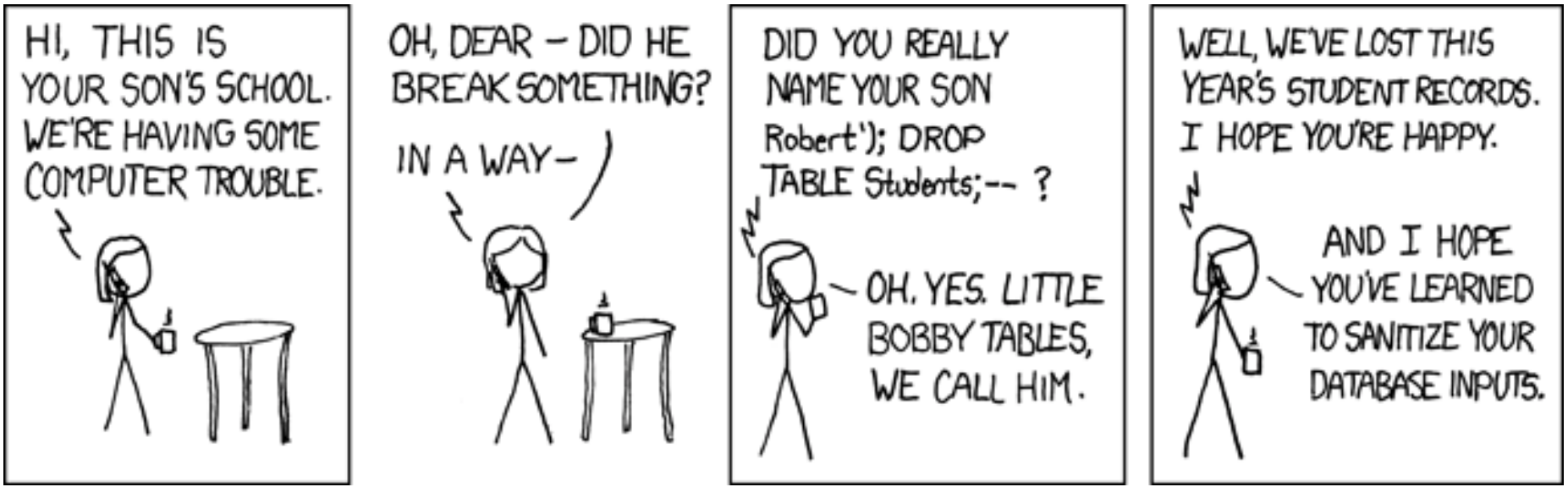
Also works for reCaptcha

But paid application



And questionable equity

MySQL injections



Everyone knows Bobby!

and this is the query

```
:tBundle:ProjectUser pu WHERE u.id = pu.user AND p.id=pu.project AN  p.name='$projectName'");
```

ajax twig symfony

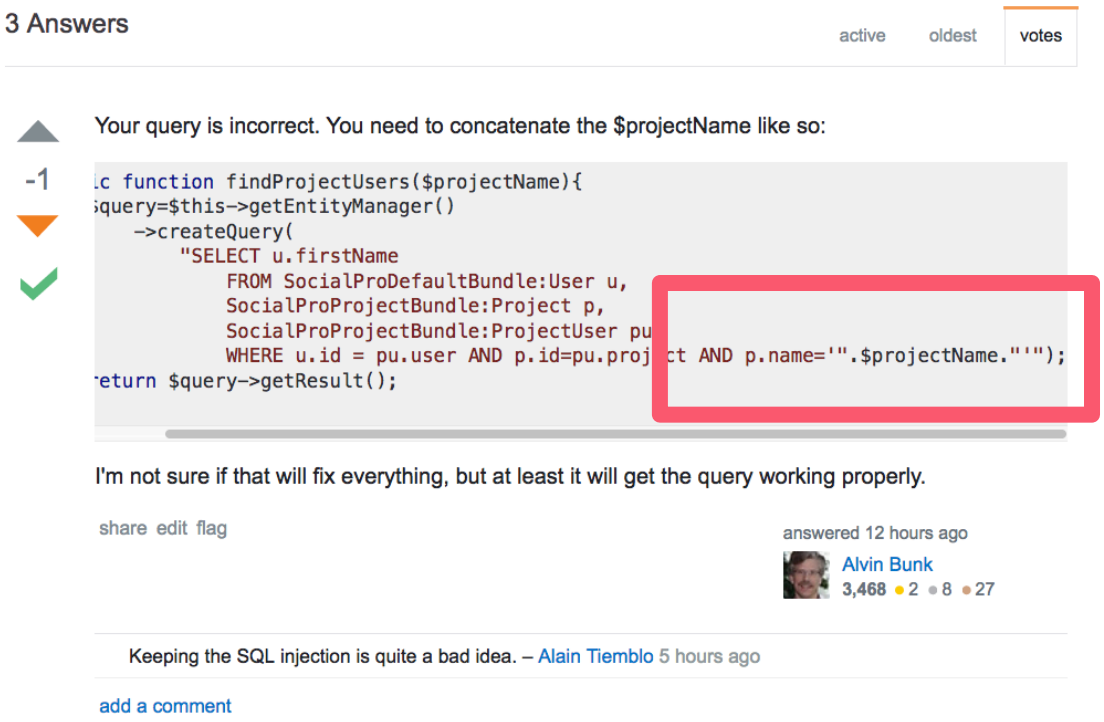
share edit close flag protect

asked Feb 12 at 18:48

Rym Haouachi

7 • 3

… or not



An associated answer to this recent question

```
$connection->fetchAssoc('
SELECT * FROM user WHERE username = "$username" AND password = "$password"
');
```

With `$username = 'admin"-- '`

```
SELECT * FROM user WHERE username = "admin"-- " AND password = ""
```

Let’s be admin

```
$connection->fetchAll('
SELECT * FROM product WHERE shop_id = "{$_GET['shop_id']}"
');
```

Getting to `/products.php?shop_id=42 OR 1=1`

```
SELECT * FROM product WHERE shop_id = 42 OR 1=1
```

Let’s access everything

```
$connection->execute('
DELETE FROM product WHERE id = "{$_GET[‘id’]}"
');
```

Getting to `/delete_product.php?id=42 OR 1=1`

```
DELETE FROM product WHERE id = 42 OR 1=1
```

Let’s delete everything

With `$username = 'admin"--/**/'`

```
SELECT * FROM user WHERE username = "admin"--/**/" AND password = ""
```

If spaces are sanitized, use //**

With `$username = '" UNION SELECT * FROM admin-- '`

```
SELECT * FROM user WHERE username = ""
UNION
SELECT * FROM admin-- " AND password=""
```

Use UNION to take over other tables

With `$username = '" UNION SELECT table_name as id FROM information_schema.tables-- '`

```
SELECT id FROM users WHERE username = ""
UNION
SELECT table_name as id FROM information_schema.tables-- " AND password=""
```

… and discover the schema

```
$connection->fetchAssoc('
SELECT * FROM user WHERE username = :username AND password = :password
', [
            'username' => $username,
            'password' => $password,
]);
```

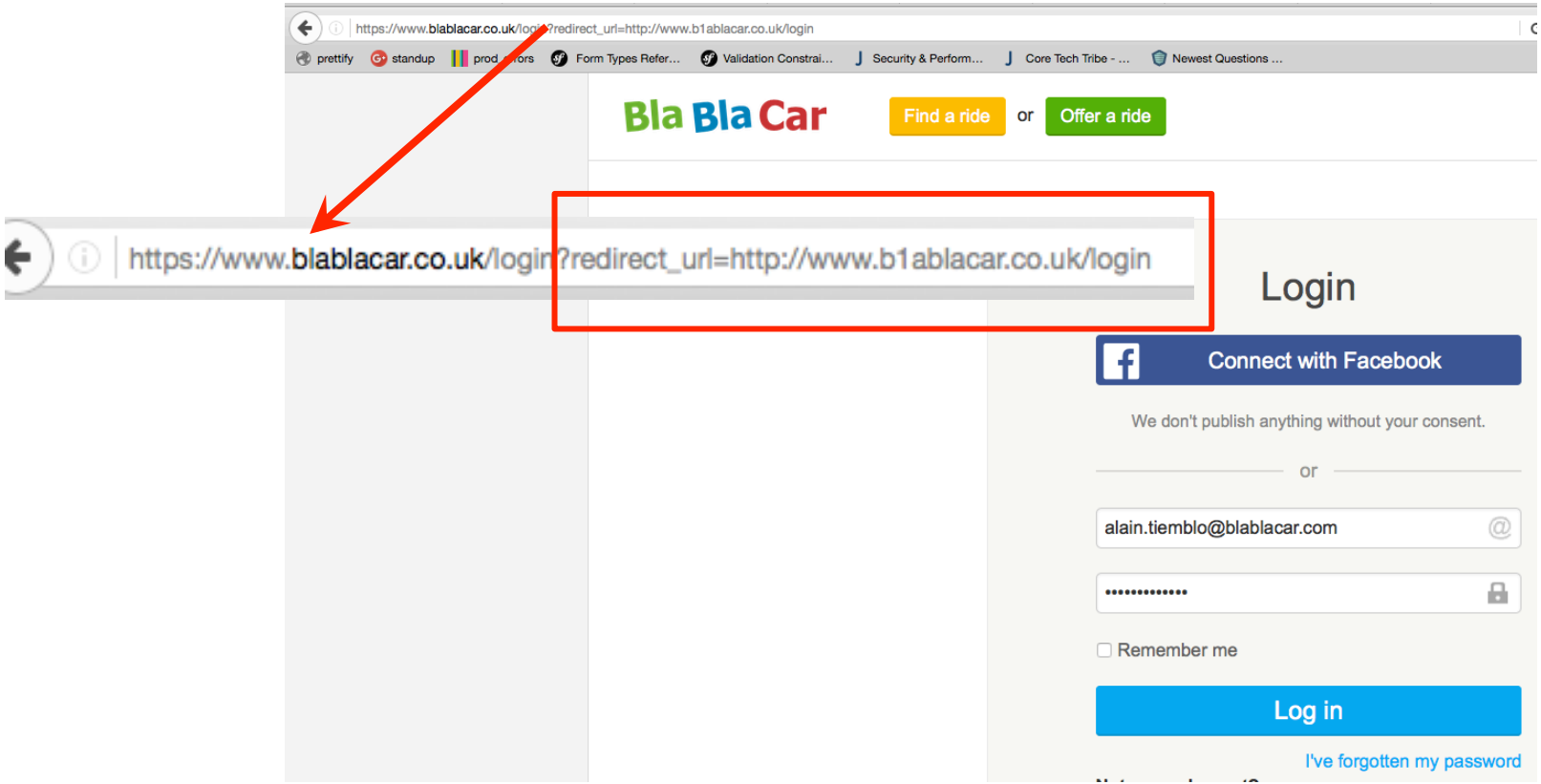
In any way, use prepared statements

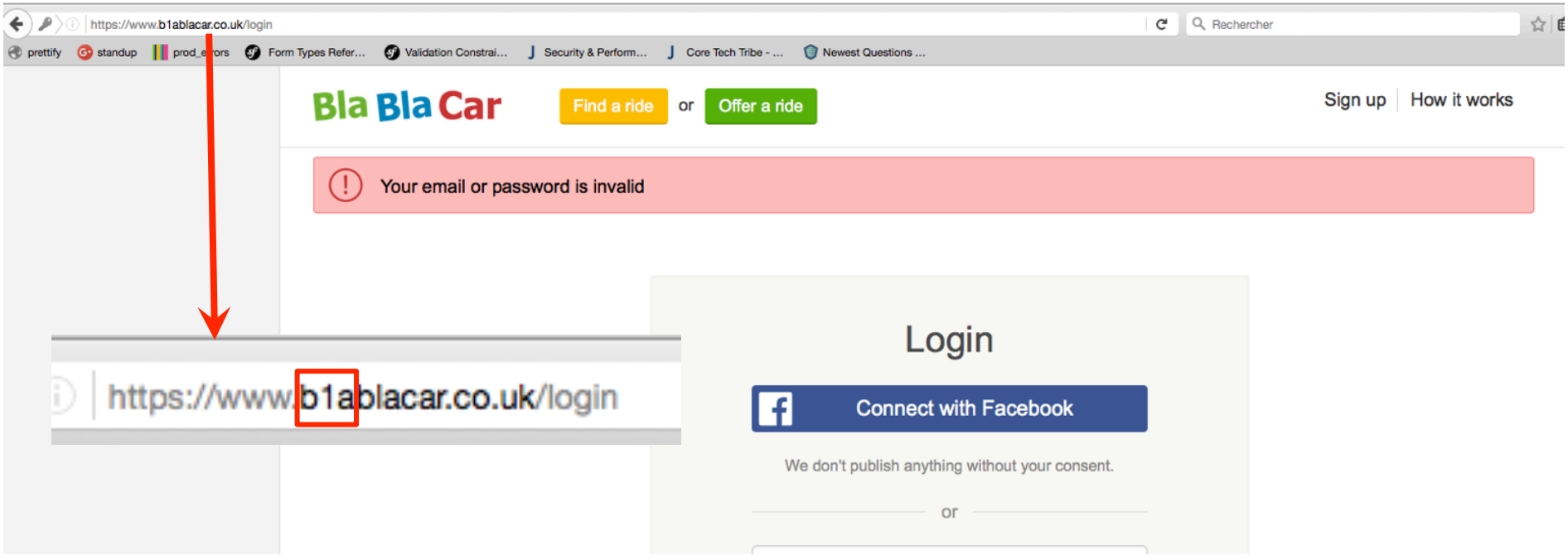
Redirect Attacks

Redirect attack principle

1. You need to redirect your member to a specific page after he successfully logs in.

2. Attacker will use your redirection strategy with malicious URL to gather personal information (credentials, …) using a phishing website.


https://www.blablacar.co.uk/login?redirect_url=http://www.b1ablacar.co.uk/login
prettify
standup
Form Types Refer...
Validation Constrai...
Security & Perform...
Core Tech Tribe - ...
Newest Questions ...
Bla Bla Car
Find a ride
or
Offer a ride
https://www.blablacar.co.uk/login?redirect_url=http://www.b1ablacar.co.uk/login
Login
Connect with Facebook
We don't publish anything without your consent.
or
alain.tiemblo@blablacar.com
Remember me
Log in
I've forgotten my password


https://www.b1ablacar.co.uk/login
Rechercher
prettify
standup
prod_errors
Form Types Refer...
Validation Constrai...
Security & Perform...
Core Tech Tribe - ...
Newest Questions ...
Bla Bla Car
Find a ride
or
Offer a ride
Sign up
How it works
Your email or password is invalid
https://www.b1ablacar.co.uk/login
Login
Connect with Facebook
We don't publish anything without your consent.
or

alain.tiemblo@blablacar.com

••••••••••••

Remember me

Log in

I've forgotte

Not a member yet?

Sign up in 30 seconds

Bla Bla Car Find a ride or Offer a ride Alain

Dashboard Rides offered Bookings Messages Ride alerts Ratings Profile Money

Hello Alain
→ Edit my profile
→ See my public profile

Your current level
→ Find out more about Experience Levels
Newcomer Intermediate Experienced Expert Ambassador

Rideshare preferences

→ Edit my preferences

Profile verification

- Phone number verified
- Email address verified
- 72 Facebook friends
- Agreement accepted

Notifications (0)

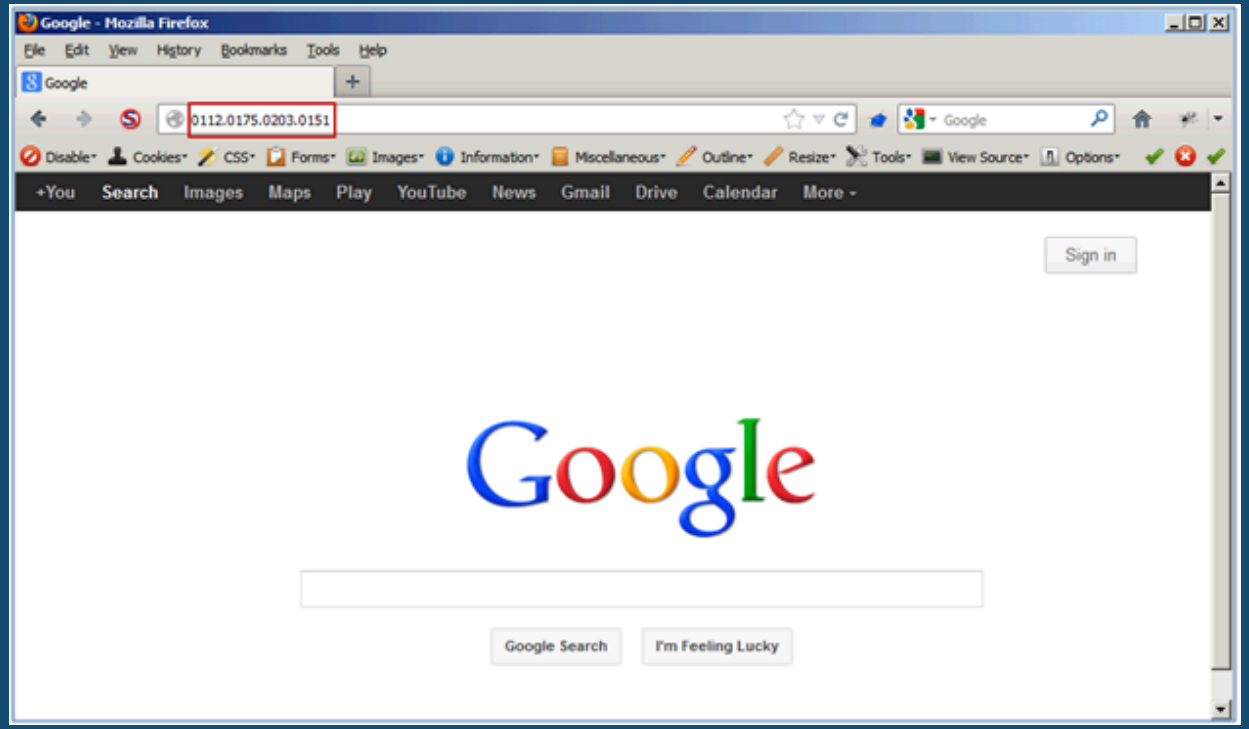
New messages (0)

See all my messages

Solution:

Put redirection URLs in a white list.

URL obfuscation

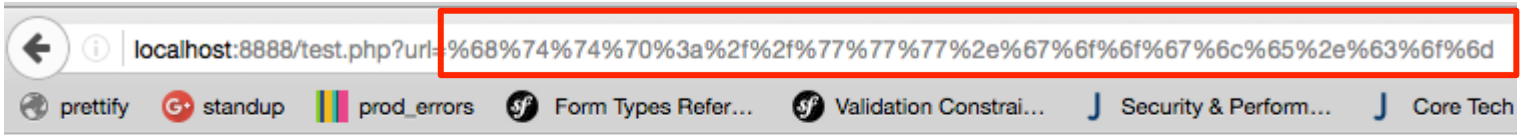


URL obfuscation principle

1. Attacker wants to bypass spam filters or put an URL somewhere without drawing attention

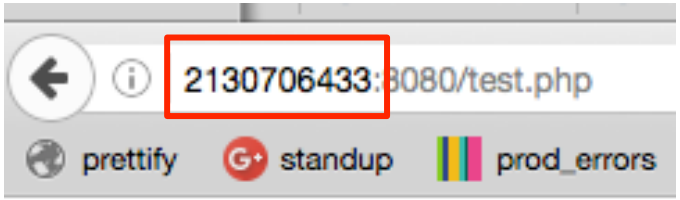
2. He will encode the URL’s host, or convert the target ip to something more discreet (an integer, a hexadecimal number…)

URL encoding:




```
array(1) {
  ["url"]=>
  string(21) "http://www.google.com"
}
```

IP conversion

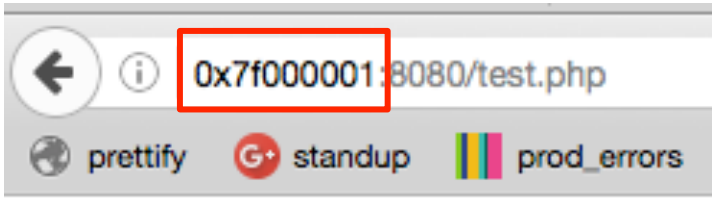


You're on 127.0.0.1 :)

Decimal

You're on 127.0.0.1 :)

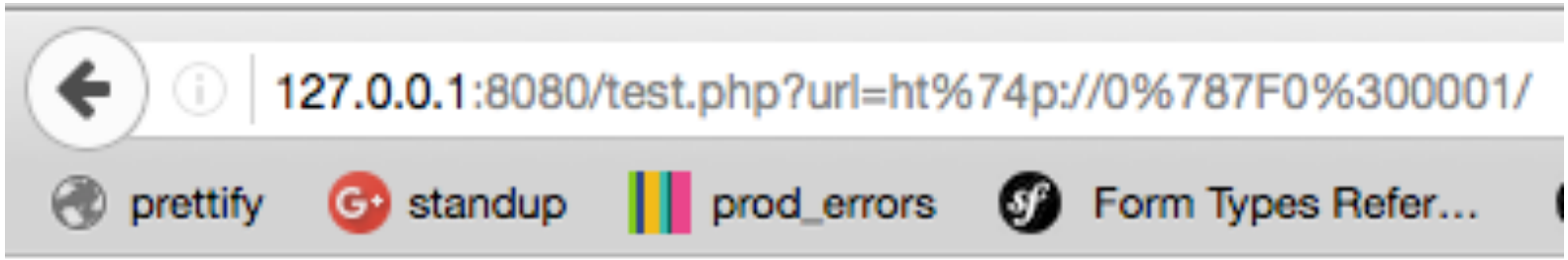
Octal



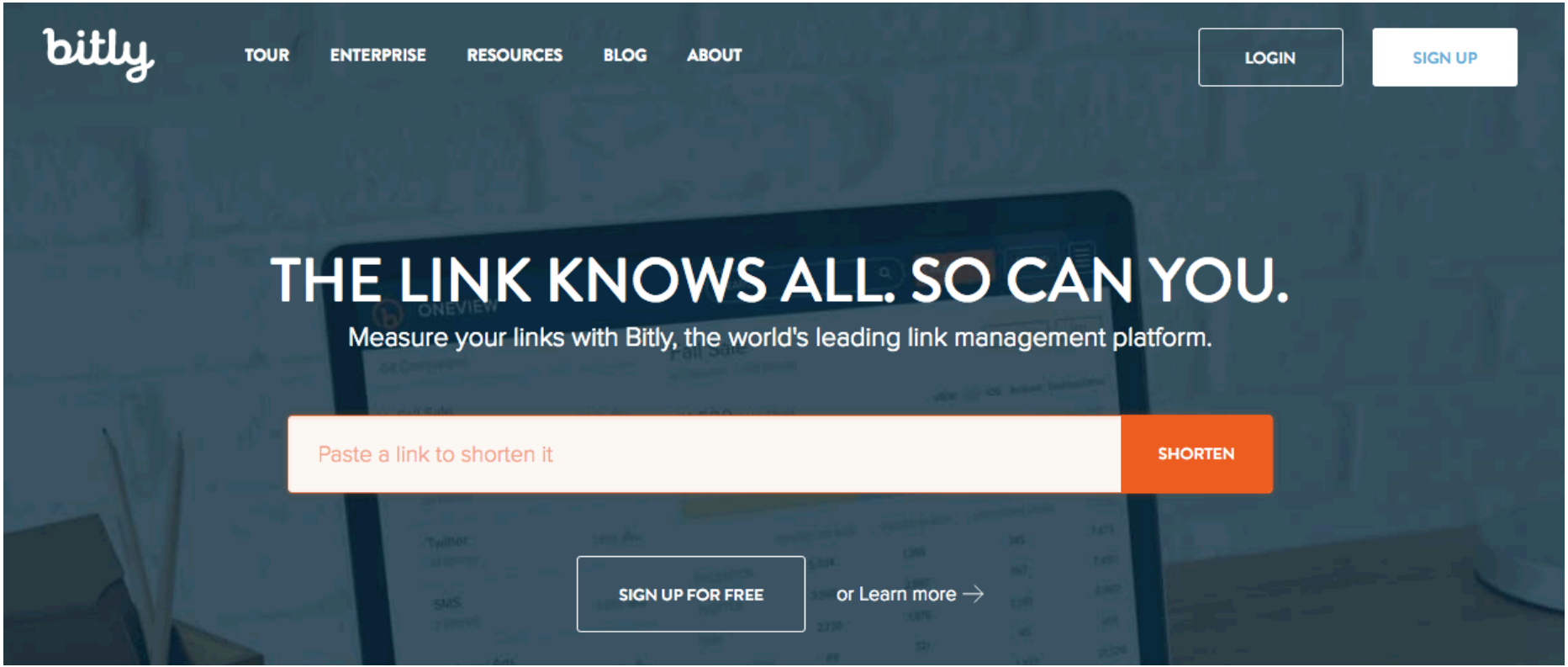
You're on 127.0.0.1 :)

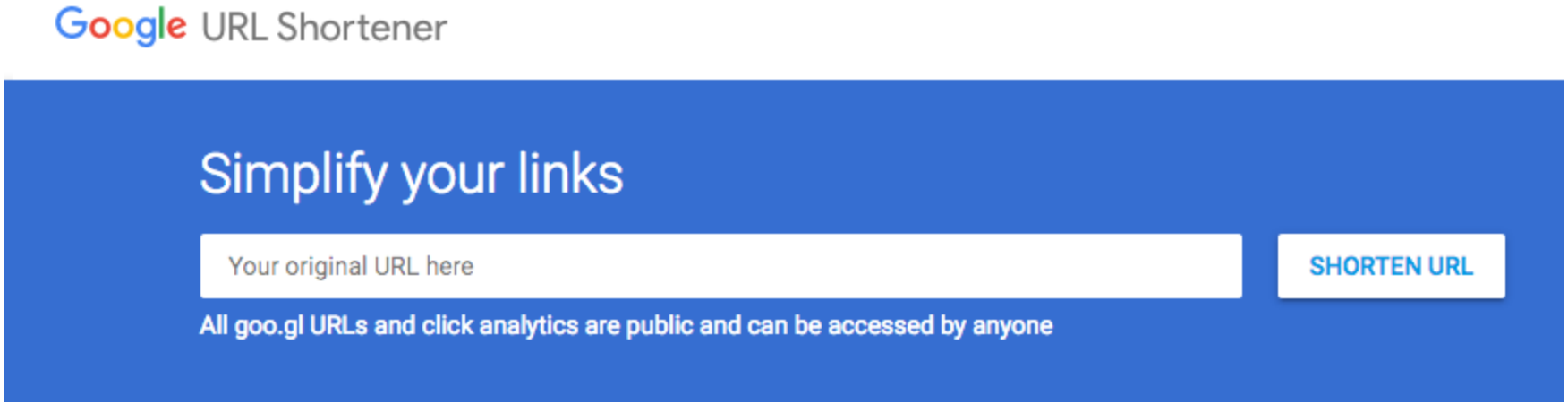
Hexadecimal

Altogether...




```
array(1) {
  ["url"]=>
  string(18) "http://0x7F000001/"
}
```


bitly
TOUR
ENTERPRISE
RESOURCES
BLOG
ABOUT
LOGIN
SIGN UP
THE LINK KNOWS ALL. SO CAN YOU.
Measure your links with Bitly, the world's leading link management platform.
Paste a link to shorten it
SHORTEN
SIGN UP FOR FREE
or Learn more


Google URL Shortener
Simplify your links
Your original URL here
SHORTEN URL
All goo.gl URLs and click analytics are public and can be accessed by anyone

Do not use public URL shorteners

1. **That’s easy to fake**, nobody will see the difference between bit.ly/xZahhGfk and bit.ly/BJzENdJq
2. **That’s easy to bruteforce**, many private documents were accessed by crawling possible combinations
3. **In any way, think twice** before opening shortened links

Use your own URL shortener

At BlaBlaCar, we use blbl.cr, for example:

- http://blbl.cr/symfony

This one is easy to fake by using typosquatting attacks though.

Man-in-the-Middle Attacks

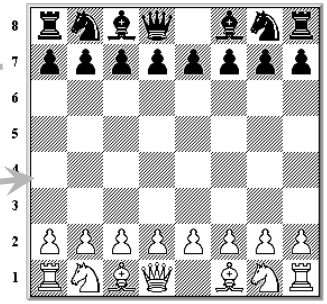
The Chess game analogy: how to win against Grand Masters?

a) GM1 plays X

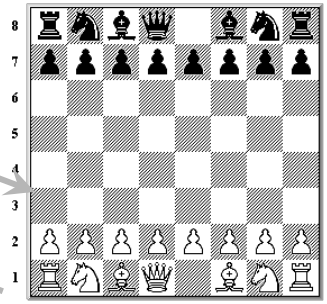
d) MITM plays Y

b) MITM plays X

c) GM2 plays Y



...



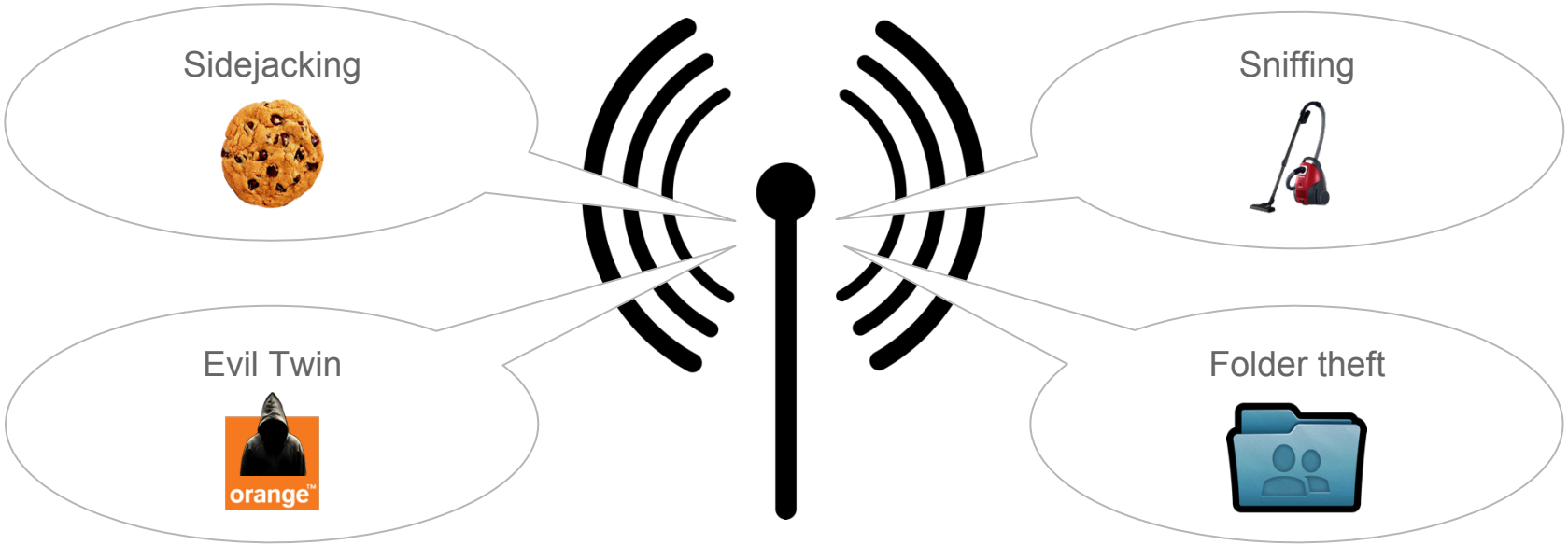
Grand Master 1

Grand Master 2

MITM goals

1. Gather data from users (eavesdropping)
2. Alter delivery by adding, removing or updating data
3. Debug (for development purposes)

A public, unsecured hotspot



DNS spoofing

google.com
216.58.208.206

Attacker

1) What is google.com's ip?

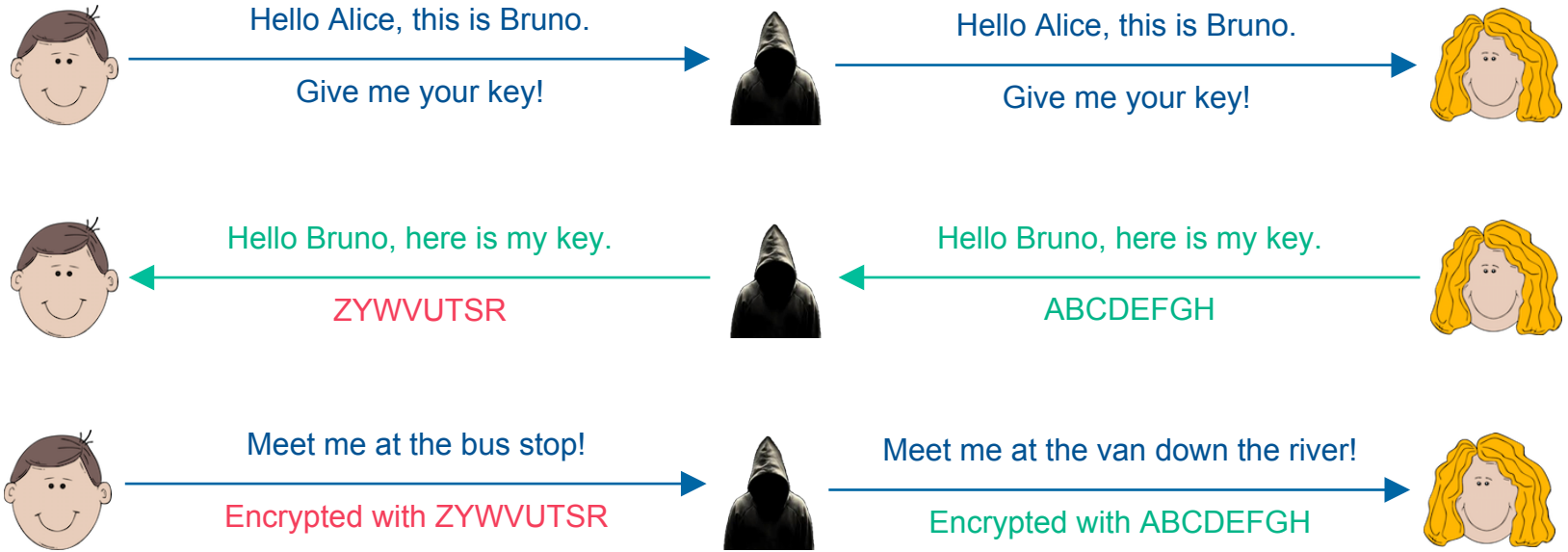
Victim

2) It's 123.123.123.123 😅

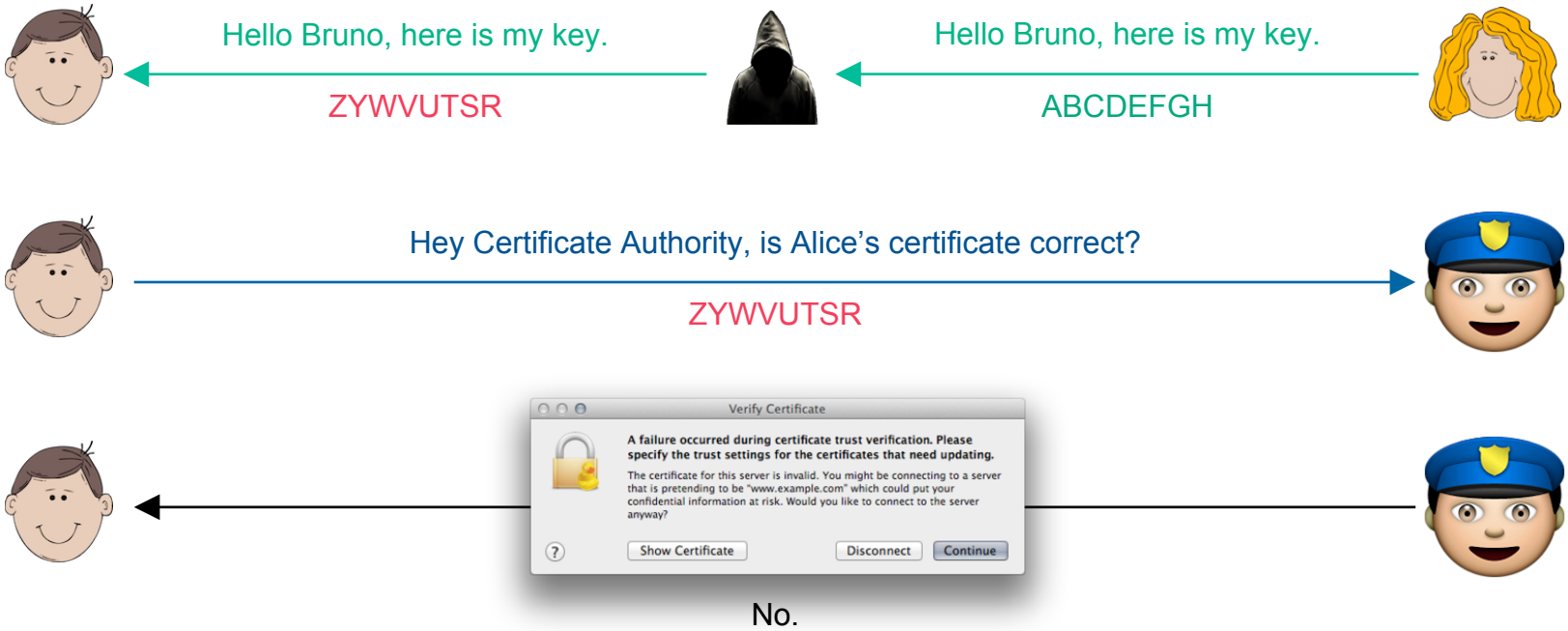
my-porn-website.com
123.123.123.123

3) Thanks 😘😑

MITM through HTTPS



MITM through HTTPS : protection



XSS strikes back

```twig
{# file.html.twig #}
<div>{{ content }}</div>
```

=

```twig
{# file.html.twig #}
<div>{{ content | e }}</div>
```

=

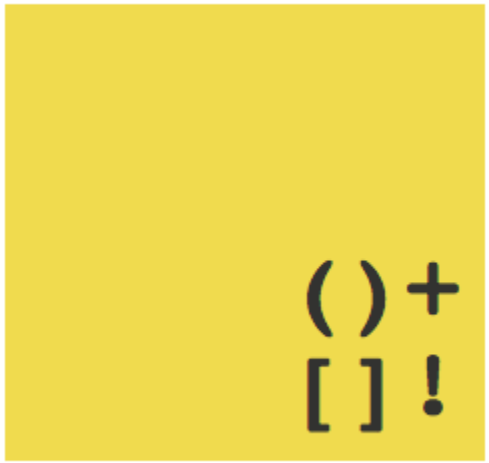
```twig
{# file.html.twig #}
<div>{{ content | e('html') }}</div>
```

js

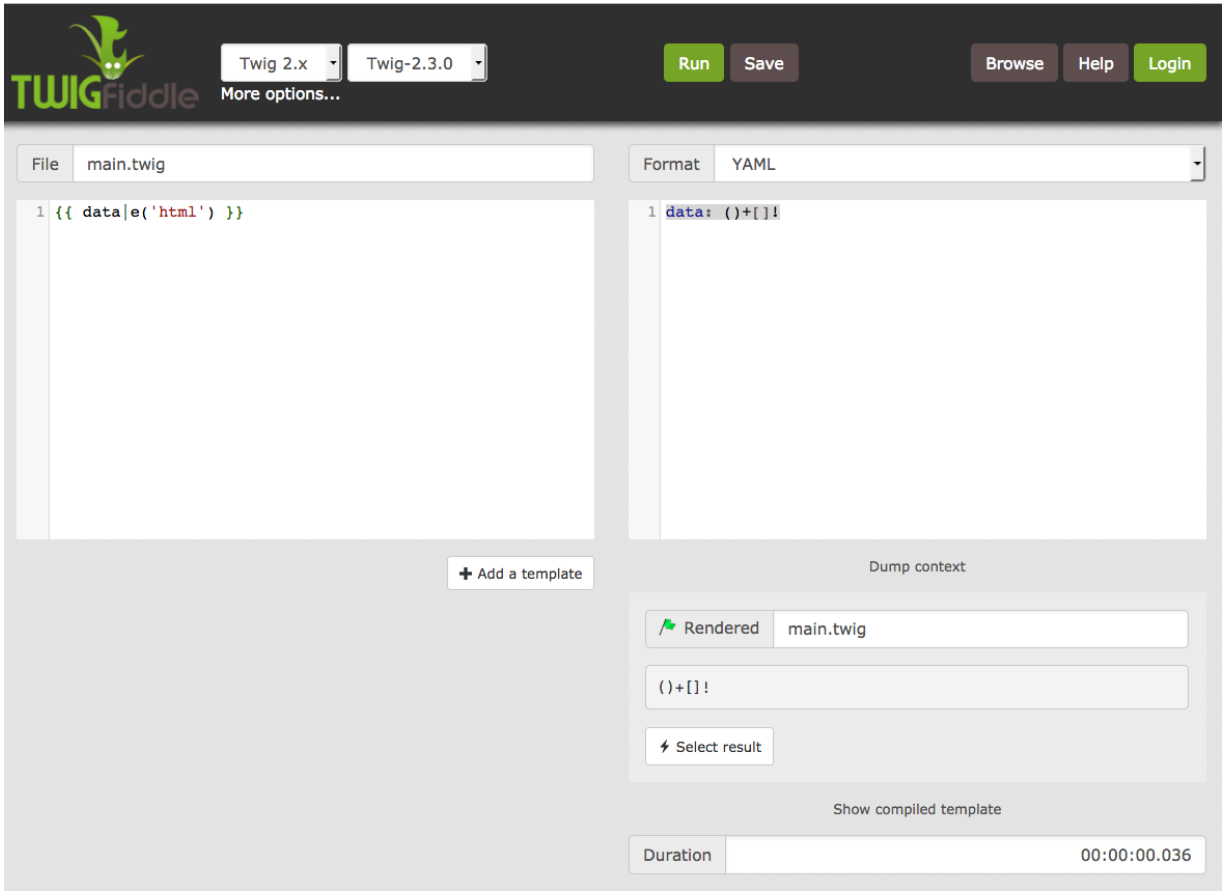
`alert(document.cookie);` in `regex`?

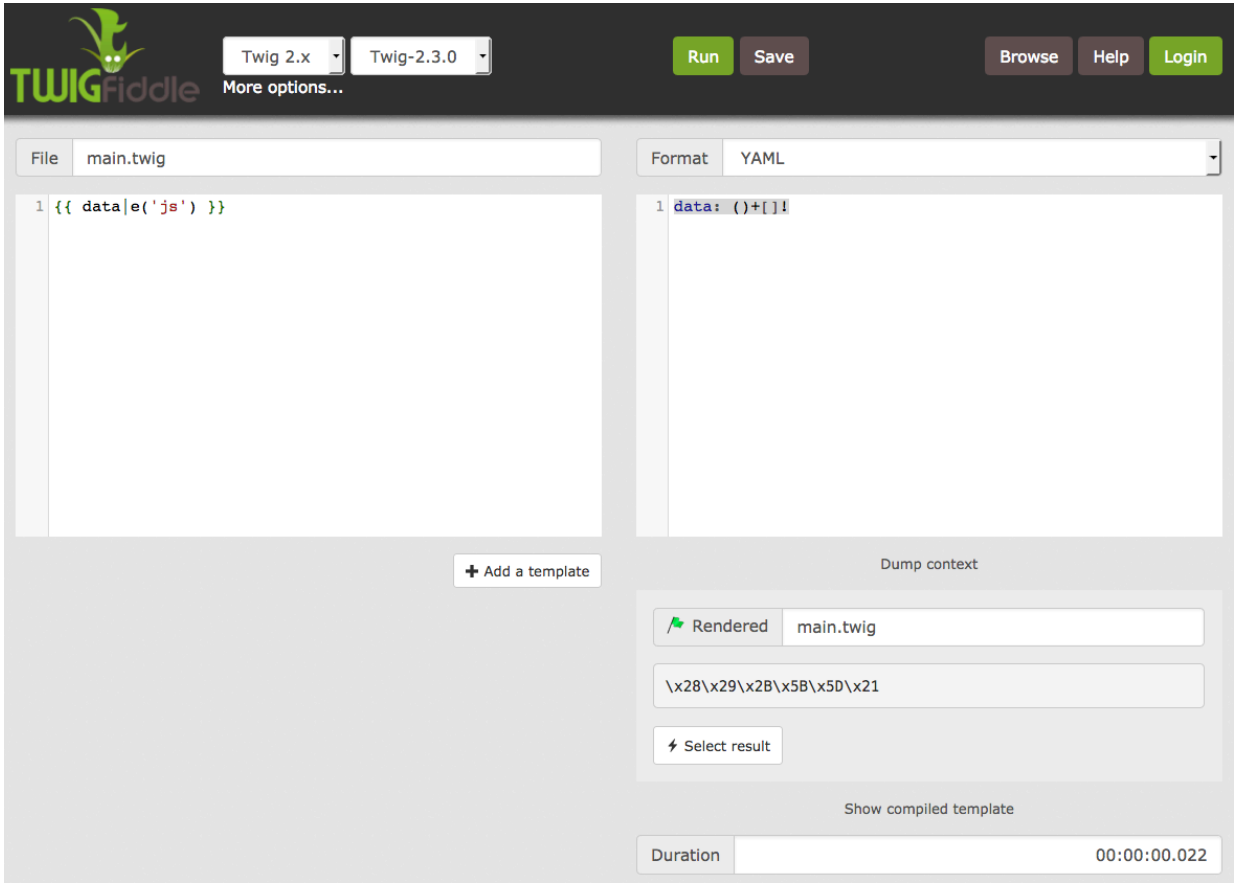
```
{# file.html.twig #}
<script>
    var regex = {{ regex }};
    // ...
</script>

{# will output #}
<script>
    var regex = alert(document.cookie);
    // ...
</script>
```

```
{# file.html.twig #}
<script>
    var regex = {{ regex|e('js') }};
    // ...
</script>

{# will output #}
<script>
    var regex = alert\x28document.cookie\x29;
    // ...
</script>
```



JSFuck


TWIGFiddle
Twig 2.x
Twig-2.3.0
More options...
Run
Save
Browse
Help
Login
File
main.twig
1 {{ data|e('html') }}
+ Add a template
Format
YAML
1 data: ()+[]!
Dump context
Rendered
main.twig
()+[]!
Select result
Show compiled template
Duration
00:00:00.036


TWIGFiddle
Twig 2.x
Twig-2.3.0
More options...
Run
Save
Browse
Help
Login
File
main.twig
{{ data|e('js') }}
Format
YAML
data: ()+[]!
Add a template
Dump context
Rendered
main.twig
\x28\x29\x2B\x5B\x5D\x21
Select result
Show compiled template
Duration
00:00:00.022

Never use |raw filter

- sanitize data using HTMLPurifier (http://htmlpurifier.org/)
- use HTMLPuriferBundle and `|purify` filter in Symfony

Questions?

Please leave your feedback!
https://joind.in/talk/04748

Thanks!

Slides soon available at:
https://github.com/ninsuo/slides