

moz://a

Web Security in 2017

Johann Hofmann



Me.

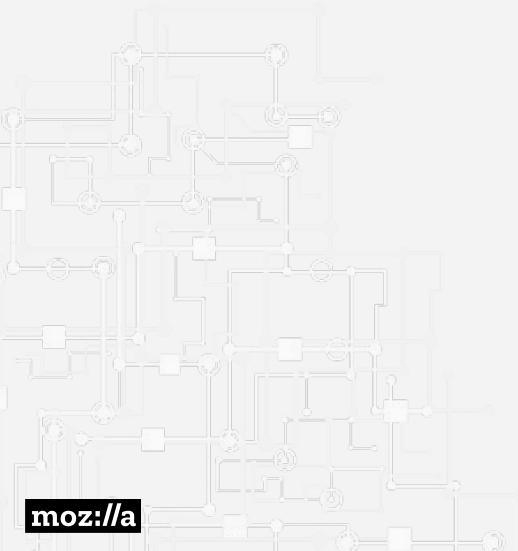
I am Johann Hofmann

I work on Firefox (Security & Privacy)

Twitter [@johannh](https://twitter.com/johannh)

GitHub [@johannhof](https://github.com/johannhof)

Secure websites



Secure Connections



Secure Web Content



Secure Access to Device Capabilities

moz://a

Secure Connections



A laptop screen displaying code in Komodo IDE. The code is in PHP and appears to be part of a registration form. It includes logic for handling file uploads, validating fields like email and unique names, and rendering templates. The interface shows a sidebar with project files and a main editor window with syntax-highlighted code.

```
public_html >
    > .cent
    > cgi-bin
    > config
    > wp-admin
    > wp-content
        > themes
            > astrapaper
                > acf-accordion
                > advanced-custom-fields-pro
                > advanced-image-any-widget
                > charitable
                > charitable-ambassadors
                > charitable-awards
                > charitable-license-tester
                > charitable-user-avatar
                > contact-form-7
                > custom-registration-form-database-extension
                > custom-registration-form-builder-with-submission
                > disable-comments
                > extended-registration
                > extended-registration
                > functions.php
                > LayerSlider
                > nimbuzz-image-captcha
                > regenerate-thumbnails
                > relative-image-urls
    > projects
```

```
functions.php >
    > include($view_path . 'header.php');
    $fields = ER_Model::factory('Field')->loadTemplates();
    foreach ($fields as $field) {
        er_render_field($field);
    }
    include($view_path . 'footer.php');

    function er_handle_registration_form() {
        if (!empty($_POST['submit'])) {
            $username = null;
            $password = null;
            $username = $_POST['er_username_field'];
            $password = $_POST['er_password_field'];

            # Create new registration
            $registration = ER_Model::factory('Registration');
            $registration['title'] = date('Y-m-H-i-s');
            $fields = ER_Model::factory('Field')->loadTemplates();
            foreach ($fields as $field) {
                $field['template_id'] = $field['id'];
                $field['id'] = null;
            }

            # Assign value and validate
            switch ($field['type']) {
                case 'title':
                    case 'description':
                        continue;
                    break;
                case 'checkbox':
                    if ($field['value'] == 'true') {
                        $errors[$field['unique_name']] = 'Vous devez cocher cette case pour continuer.';
                    }
                    if ($field['required'] && !$field['value']) {
                        $errors[$field['unique_name']] = 'Vous devez entrer une valeur dans ce champs.';
```

MacBook Pro

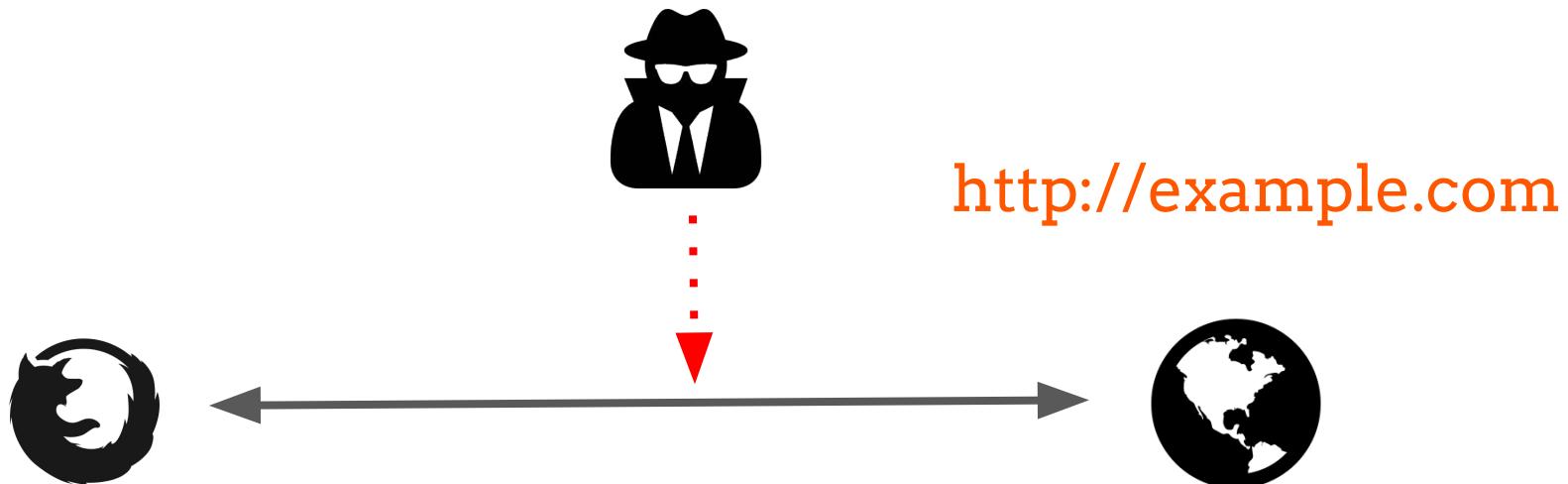
HTTP

<http://example.com>



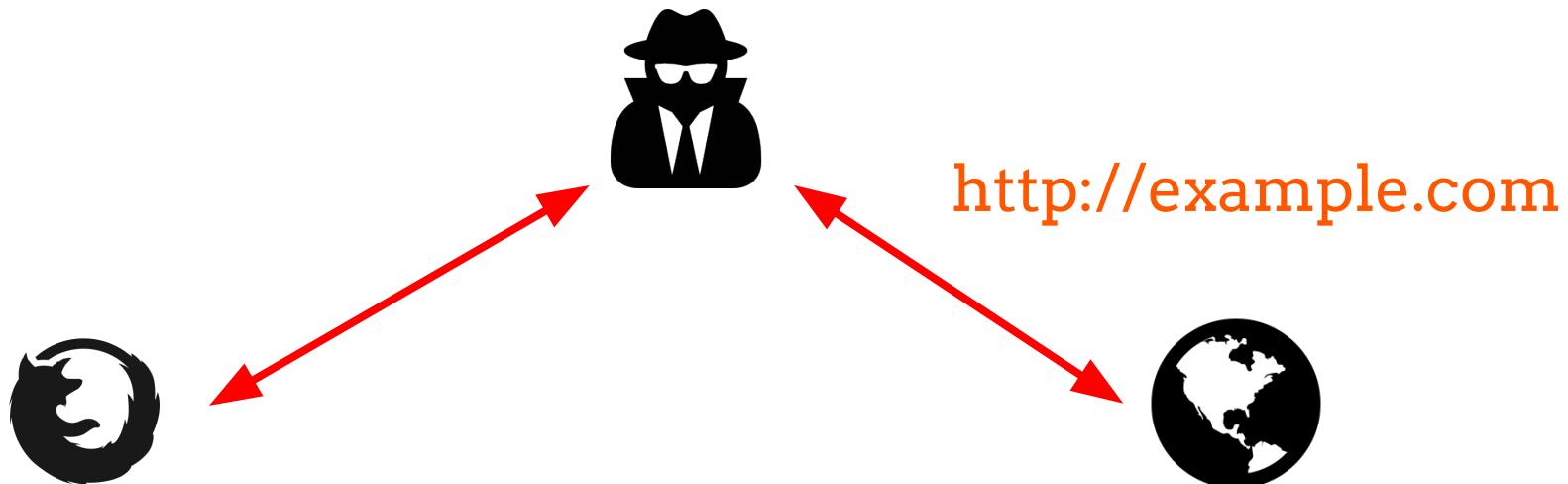
HTTP is the protocol your browser uses to load websites.

HTTP



Attackers can snoop on HTTP traffic on the same network.

HTTP



Attackers can intercept and replace
(man-in-the-middle) HTTP traffic on the same network.

HTTP



"http://example.com"

<http://example.com>



Attackers can impersonate your entire website.

Secure Connections

HTTPS protects confidentiality and integrity of your and your user's data during transmission.

(Yes it's not perfect, but that's a different story.)

Read more about how protocols on the web work: <https://hpbn.co/>

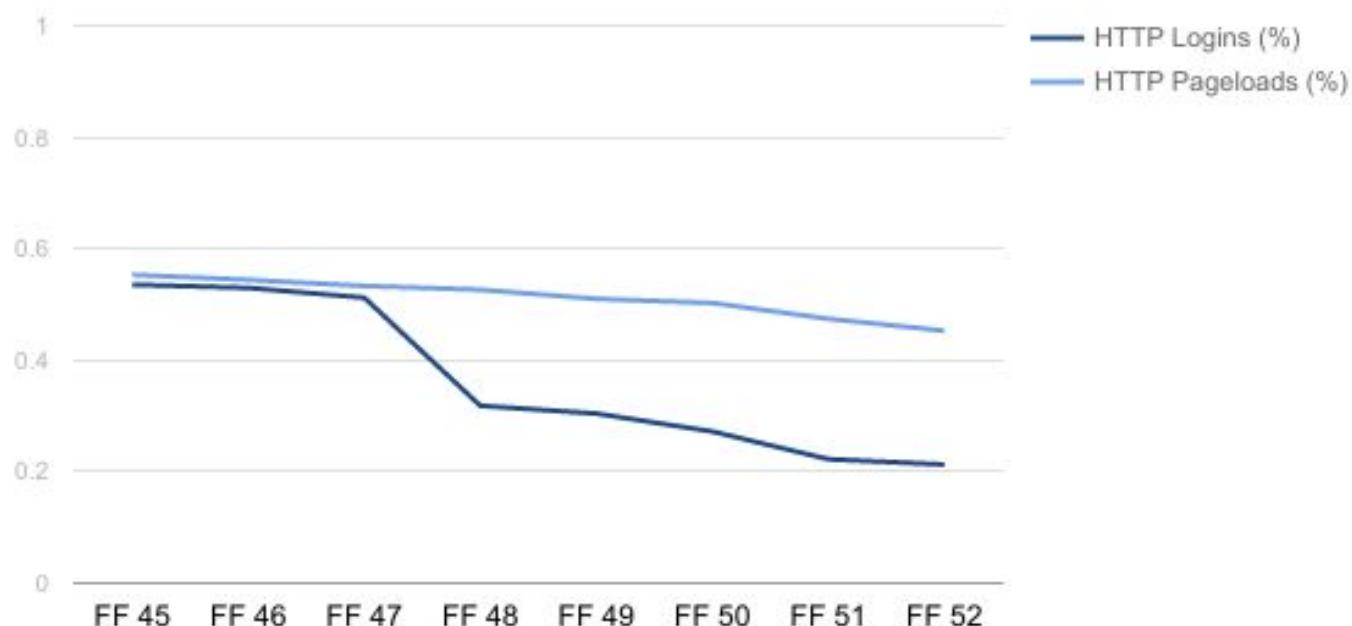
The bad news

Over 25% of user credentials are transmitted over HTTP.

https://telemetry.mozilla.org/new-pipeline/dist.html#!cumulative=0&end_date=2016-12-09&keys=__none__!__none__!__none__&max_channel_version=release%252F50&measure=PWMGR_LOGIN_PAGE_SAFETY&min_channel_version=release%252F46&processType=*&product=Firefox&sanitize=1&sort_keys=submissions&start_date=2016-11-04&table=1&trim=1&use_submission_date=0

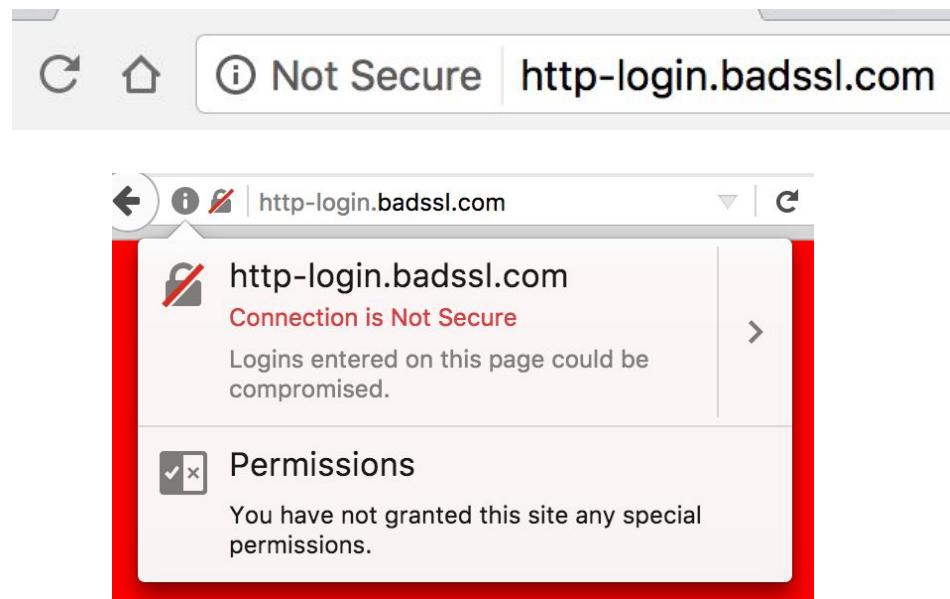
The good news

Decline of insecure connections

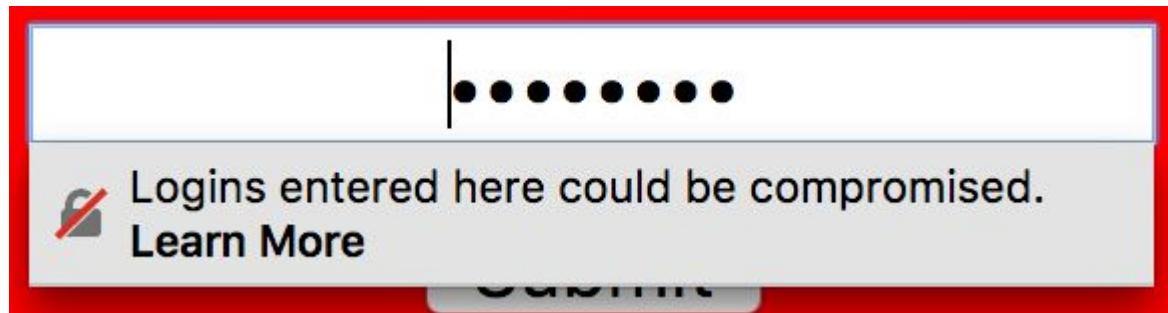


The switch to HTTPS

Browsers now aggressively flag insecure sites.



The switch to HTTPS



The switch to HTTPS

Landing Page 

source: firefox-console-errors

1. /en-US/docs/Web/Security/Mixed_content
2. /en-US/docs/Web/Security/Insecure_passwords
3. /en-US/docs/Web/Security/Weak_Signature_Algorithm
4. /en-US/docs/Web/Security/Mixed_content/How_to_fix_website_with_mixed_content
5. /en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion
6. /en-US/docs/Web/Security/Same-origin_policy

* MDN Google Analytics: Pageviews in /en-US/docs/Web/Security from utm_medium=firefox-console-errors

The switch to HTTPS

It's getting easier to obtain free certificates



<https://certbot.eff.org/>

Secure Connections

So I just need to turn on HTTPS?

Mixed Content

Landing Page 

source: firefox-console-errors

1. /en-US/docs/Web/Security/Mixed_content
2. /en-US/docs/Web/Security/Insecure_passwords
3. /en-US/docs/Web/Security/Weak_Signature_Algorithm
4. /en-US/docs/Web/Security/Mixed_content/How_to_fix_website_with_mixed_content
5. /en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion
6. /en-US/docs/Web/Security/Same-origin_policy

* MDN Google Analytics: Pageviews in /en-US/docs/Web/Security from utm_medium=firefox-console-errors

Mixed Content

Mixed **Passive** Content (The bad kind)

```

```

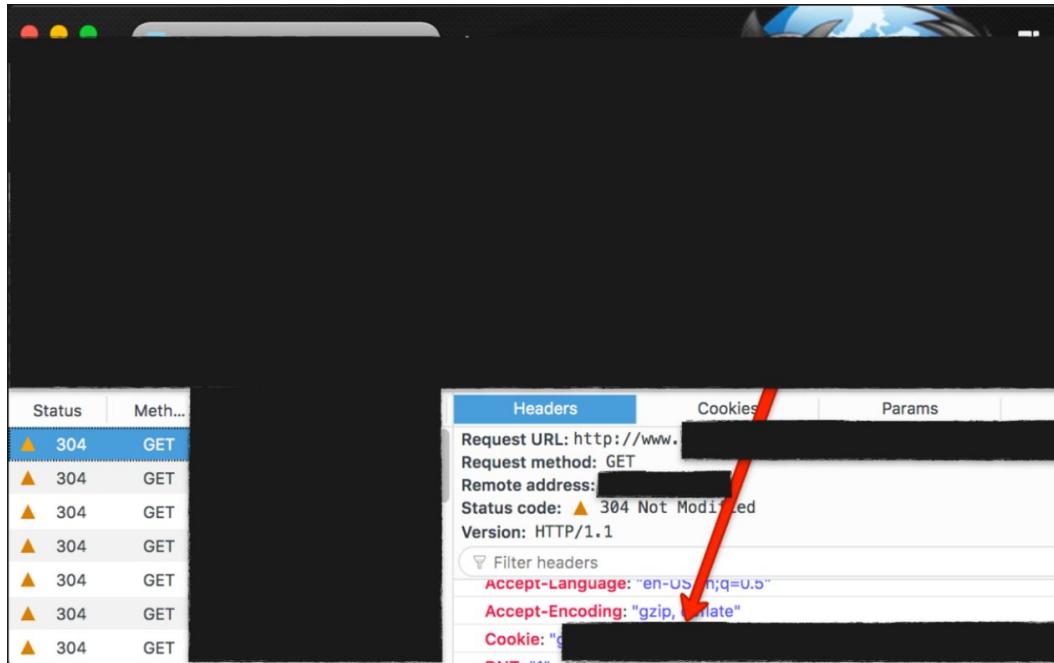
Mixed **Active** Content (The really bad kind)

```
<script src="http://example.com/script.js"></script>
```

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

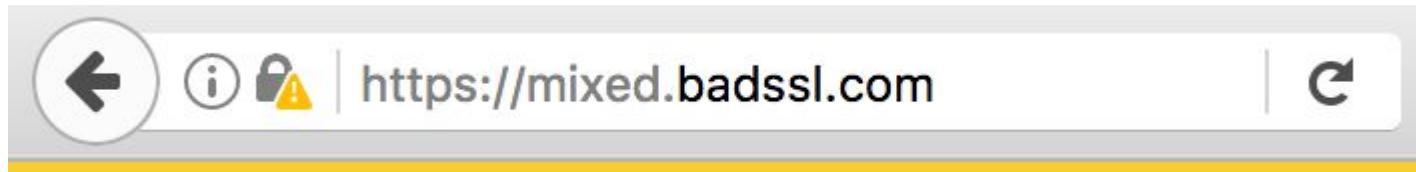
Mixed Passive Content - Session Snooping

So... mixed passive content is fine, right? Nope.



By Luke Crouch (@groovecoder)

Mixed Passive Content

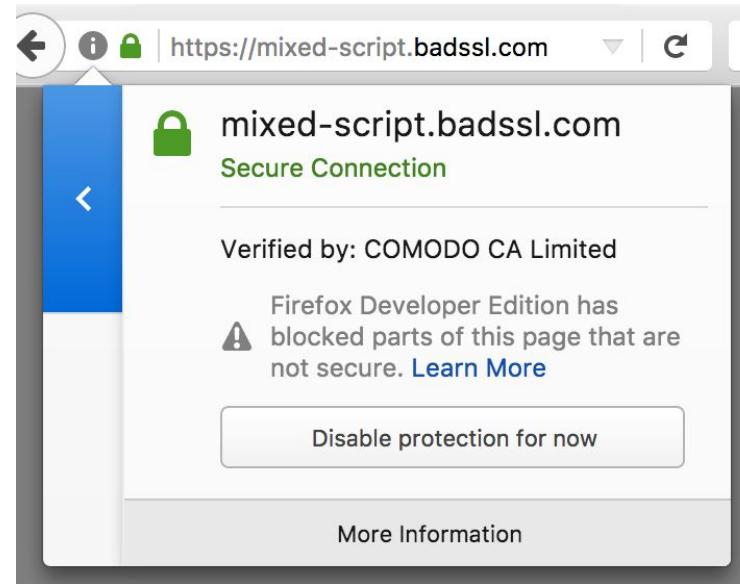


The screenshot shows the Mozilla Firefox developer tools interface. The top bar includes tabs for Inspector, Console (which is selected), Debugger, Style Editor, Performance, Memory, and Network. Below the tabs, there are buttons for zooming and closing the panel. The main area displays three error messages in a list:

- ⚠ Loading mixed (insecure) display content "http://mixed.badssl.com/image.jpg" on a secure page [\[Learn More\]](#) mixed.badssl.com
- ⚠ Loading mixed (insecure) display content "http://mixed.badssl.com/image.jpg" on a secure page [\[Learn More\]](#) mixed.badssl.com
- ⚠ Loading mixed (insecure) display content "http://mixed.badssl.com/image.jpg" on a secure page [\[Learn More\]](#) mixed.badssl.com

Mixed Active Content

Browsers block mixed active content by default



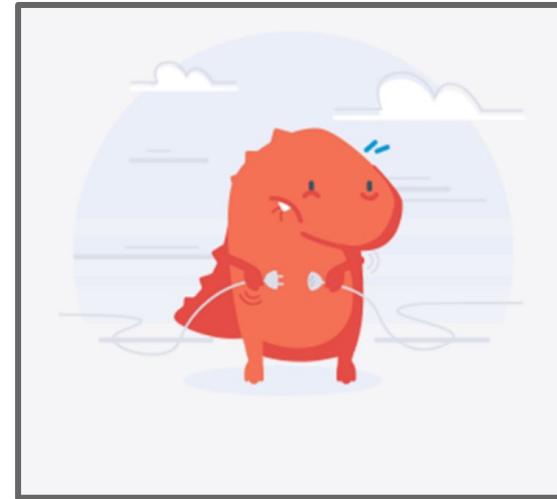
Mixed Active Content

Can it alter the DOM?

It's Mixed Active Content (The really bad kind).

Secure Connections

The web is moving to HTTPS, don't be a dinosaur!



Secure Connections

If you've moved to HTTPS (yay),
consider turning on the HSTS header

Strict-Transport-Security: max-age=31536000;
includeSubDomains

Why? <https://moxie.org/software/sslstrip/>

moz://a

Secure Web Content



A laptop screen displaying code in Komodo IDE. The code is PHP, specifically from a file named 'functions.php'. The code handles user registration, including validation and database insertion. It uses the ER_Model library to handle fields and templates. The interface shows a sidebar with project files like 'public_html' and 'extended-registration', and a bottom bar with various application icons.

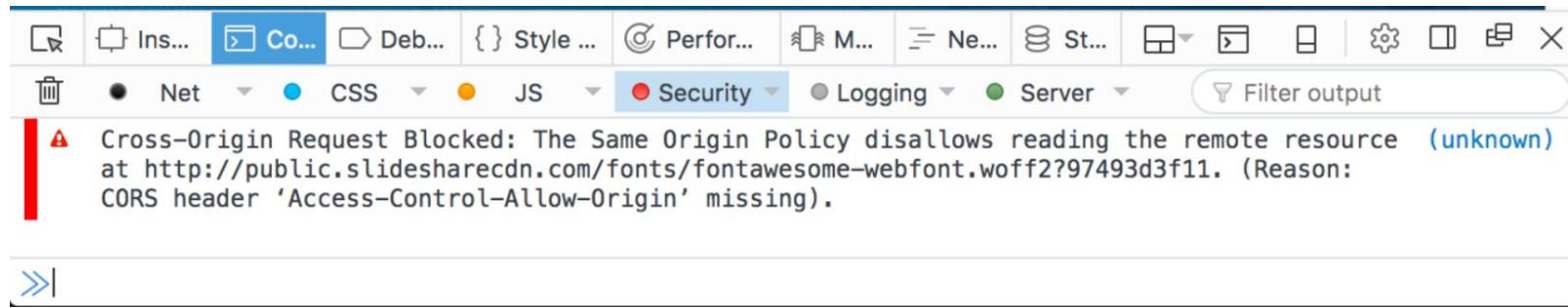
```
public_html >
  - cent
  > cgi-bin
  > config
  > wp-admin
  > wp-content
    > themes
      > astrapaper
        > acf-accordion
        > advanced-custom-fields-pro
        > advanced-image-any-widget
        > charitable
        > charitable-ambassadors
        > charitable-awards
        > charitable-license-tester
        > charitable-user-avatar
        > contact-form-7
        > contact-form-7-database-extension
        > custom-registration-form-builder-with-submissio
        > disable-comments
        > extended-registration
        > footer
        > classes
        > js
        > less
        > debug.php
        > extended-registration.php
      functions.php
    > Layer-Slider
      > images
      > example-captcha
      > regenerate-thumbnails
      > relative-image-urls
  projects >
```

```
76   include($view_path . 'header.php');
77
78   $fields = ER_Model::factory('Field')->loadTemplates();
79   foreach ($fields as $field) {
80     er_render_field($field);
81   }
82
83   include($view_path . 'footer.php');
84
85 }
86
87 function er_handle_registration_form() {
88   if (!empty($_POST['submit'])) {
89     $username = null;
90     $password = null;
91     $username = $_POST['er_username_field'];
92     $password = $_POST['er_password_field'];
93
94     # Create new registration
95     $registration = ER_Model::factory('Registration');
96     $registration['title'] = date('Y-m-H-i-s');
97
98     $fields = ER_Model::factory('Field')->loadTemplates();
99     foreach ($fields as $field) {
100       $field['template_id'] = $field['id'];
101       $field['id'] = null;
102
103       # Assign value and validate
104       switch ($field['type']) {
105         case 'title':
106           case 'description':
107             continue;
108           break;
109
110         case 'checkbox':
111           if ($field['value'] == 'on') {
112             $results['errors'][$field['unique_name']] = 'Vous devez cocher cette case pour continuer.';
113           }
114           break;
115
116         case 'email':
117           $field['value'] = safe_get($POST, $field['unique_name']);
118           if ($field['required'] && $field['value'] == '') {
119             $results['errors'][$field['unique_name']] = 'Vous devez remplir ce champs.';
120           } elseif ($filter->var($field['value']), FILTER_VALIDATE_EMAIL) == false {
121             $results['errors'][$field['unique_name']] = 'Vous devez entrer une adresse courriel valide.';
122           }
123           break;
124
125         case 'password':
126           break;
127       }
128     }
129
130     if (!empty($results['errors'])) {
131       $error = true;
132     } else {
133       $error = false;
134     }
135   }
136 }
```

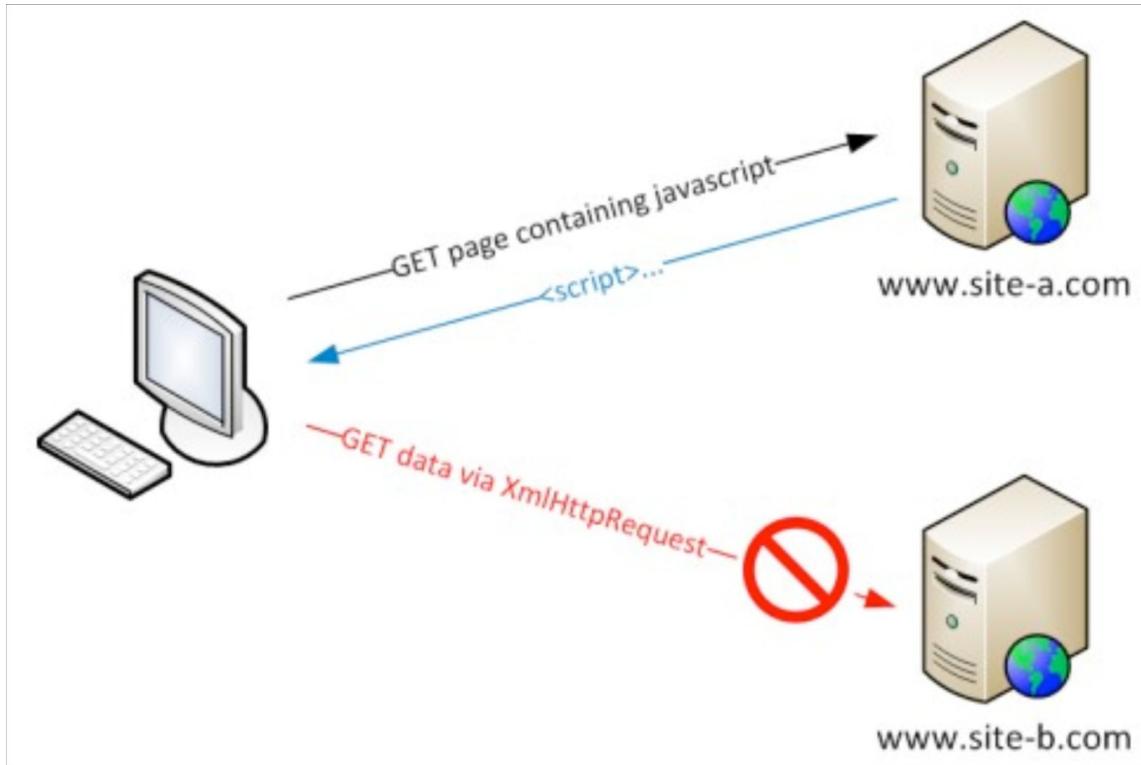
MacBook Pro

Secure Web Content

Same-Origin Policy



Same-Origin Policy



What is affected by Same-Origin Policy?

- XHR requests
- `window.opener/window.parent`, etc.
- https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

Secure Web Content

<form method="Post">?

Not protected!

Use a CSRF token. Don't rely on cookies.

Secure Web Content

It's very easy to use

`Access-Control-Allow-Origin: *`

to work around this issue. In many cases you should not have to.

Secure Web Content

How can I make sure that user generated content doesn't break my website security?

CSP (+ common sense & sanitization)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

CSP

A set of rules that define how a site may load resources.

```
<meta http-equiv="Content-Security-Policy" content="default-src 'self';  
image-src https:*; child-src 'none';">
```

You can use **Content-Security-Policy-Report-Only** to test it without breaking things

CSP features recording violations!

```
Content-Security-Policy: default-src https:;  
report-uri https://report.example.com
```

You can set up endpoints at <https://report-uri.io/>

Secure Web Content

How can I make sure that the third-party content I receive has not changed on the server?

Subresource Integrity

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Subresource Integrity

Specify an integrity attribute that is the hash digest of the referenced file.

```
<script src="https://example.com/example-framework.js"  
       integrity="sha384-oqVuAfXRK...234234234"  
       crossorigin="anonymous"></script>
```

<https://www.srihash.org/>

moz://a

Secure Device Access



A MacBook Pro displaying a code editor window for a PHP application. The code is part of a file named 'functions.php' and includes logic for handling user registration. It uses the ER Model framework and includes validation for fields like 'username', 'password', and 'email'. A sidebar shows a file tree for the project structure, including 'public_html', 'wp-content', and various plugin and theme files.

```
public_html >
  - cent
  > cog-lan
  > er-admin
  > wp-admin
  > wp-content
    > themes
      > astrapaper
        > acf-accordion
        > advanced-custom-fields-pro
        > advanced-node-any-widget
        > charitable
        > charitable-ambassadors
        > charitable-awards
        > charitable-license-tester
        > charitable-user-avatar
        > contact-form-7
        > custom-registration-extension
        > custom-registration-form-builder-with-submission
        > disable-comments
        > extended-registration
        > footer
        > classes
        > js
        > views
        > debug.php
        > extended-registration.php
      functions.php
      > LayerSlider
      > nimbuzz-image-captcha
      > regenerate-thumbnails
      > relative-image-urls
  projects >
```

```
include($view_path . "header.php");
foreach ($fields as $field) {
    er_render_field($field);
}

include($view_path . "footer.php");

function er_handle_registration_form() {
    $errors = array();
    $username = null;
    $password = null;
    $usernameField = er_field("er_username_field");
    $passwordField = er_field("er_password_field");

    # Create new registration
    $registration = ER_Model::factory("Registration");
    $registration["title"] = date("Y-m-d H-i-s");
    $fields = ER_Model::factory("Field")->loadTemplates();
    foreach ($fields as $field) {
        $field["template_id"] = $field["id"];
        $field["id"] = null;
    }

    # Assign value and validate
    switch ($field["type"]) {
        case "title":
        case "description":
            continue;
        break;
        case "checkbox":
            if ($field["value"] == true) {
                $errors[] = $field["unique_name"] . " ";
            }
            if ($field["required"] == true && $field["value"] == "") {
                $errors[] = $field["unique_name"] . " Vous devez cocher cette case pour continuer.";
            }
            break;
        case "email":
            $field["value"] = safe_get($_POST, $field["unique_name"]);
            if ($field["required"] == true && $field["value"] == "") {
                $errors[] = $field["unique_name"] . " Vous devez remplir ce champs.";
            } elseif (!filter_var($field["value"], FILTER_VALIDATE_EMAIL) == false) {
                $results["errors"][$field["unique_name"]] = "Vous devez entrer une adresse courriel valide.";
            }
            break;
        case "password":
    }
```

MacBook Pro

Secure Device Access

The web is getting more native capabilities...



Secure Device Access

... but we can't let websites access them without permission.



Secure Device Access

The web platform was not built with a permission system in mind.

"User agents must acquire permission through a user interface"

<https://dev.w3.org/geo/api/spec-source.html>

Secure Device Access

Requesting permission

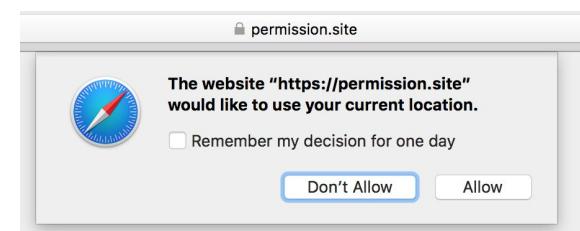
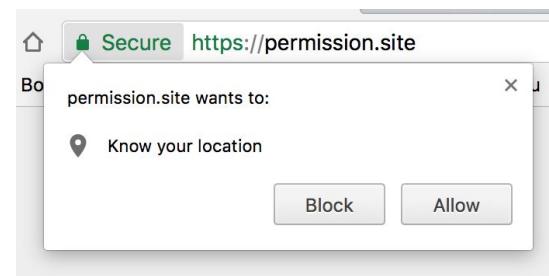
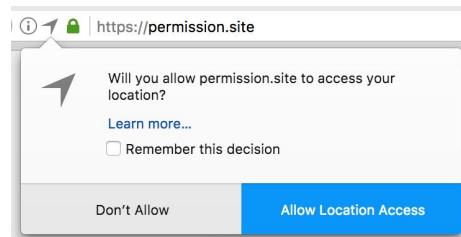
```
navigator.mediaDevices.getUserMedia({audio:  
true}).then(stream => ...);
```

```
Notification.requestPermission().then(result => ...);
```

```
navigator.geolocation.getCurrentPosition(result => ...);
```

Secure Device Access

Different prompts from browsers.



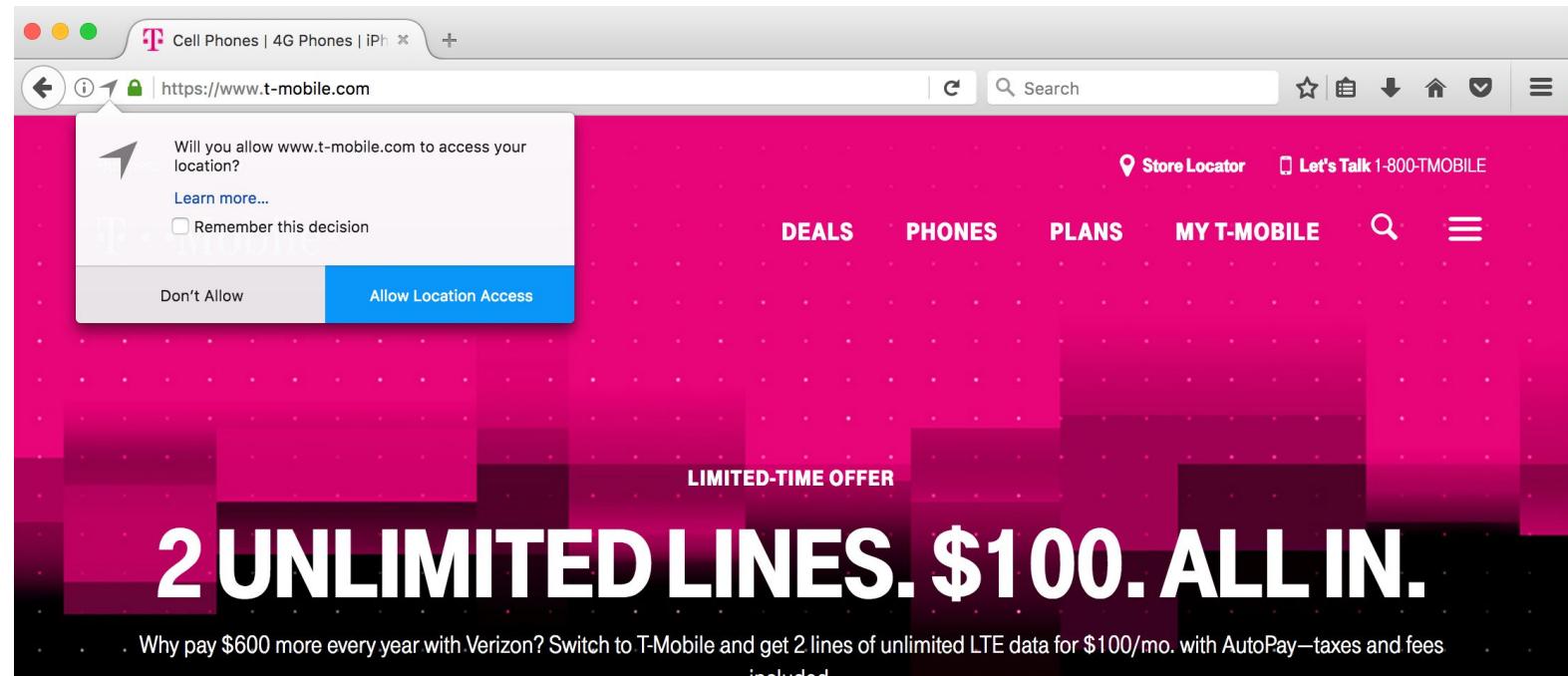
Secure Device Access

Browsers will start to penalize intrusive and surprising permission prompts.

https://bugzilla.mozilla.org/show_bug.cgi?id=1206232

<https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/fHI9GNxPPpA/VwhB6h5cDwAJ>

Secure Device Access



Secure Device Access

Pre-prompt to give the user context
and avoid the element of surprise.

(Browsers might actually force you to do that at some point)

Secure Device Access

A screenshot of a web browser displaying a Slack message from the channel '#slackbot' in the BerlinJS Slack workspace. The message is from slackbot itself, asking for permission to enable desktop notifications. It includes a link to the Help Center and a message about getting started on Slack. The browser interface shows the URL <https://berlinjs.slack.com/messages/@slackbot/> in the address bar.

slackbot | BerlinJS Slack

https://berlinjs.slack.com/messages/@slackbot/

Slack needs your permission to [enable desktop notifications](#).

BerlinJS

johannh

All Threads

CHANNELS (18)

- # admin-announcements
- # electron
- # elm
- # events
- # hi
- # javascript
- # job-search
- # kiezcoding
- # main
- # nodeschool
- # nodeschool-crowd

slackbot

active | @slackbot

You can ask me simple questions about how Slack works, or just type a few keywords. For example: [Can I edit a message I've posted?](#) Or simply: [edit message](#).

I'm only a bot, but I'll do my best to answer! If I don't understand, I'll search the [Help Center](#).

January 22nd, 2016

slackbot 2:34 PM

If you get lost and want some more help, look at our [Help Center](#) or our [guide to getting started on Slack](#). Otherwise, have a lovely day

March 2nd, 2016

Secure Device Access

Get Notified of New Messages
Turn on desktop notifications

nope

MESSAGES

Ed
✓ Nope

2/8/2016

The image shows a screenshot of the WhatsApp web browser extension. At the top, there's a blue header with a bell icon and the text "Get Notified of New Messages" followed by "Turn on desktop notifications". Below this, a message from "nope" is visible. The main area is titled "MESSAGES" and shows a conversation between "Ed" and "✓ Nope" from February 8, 2016. The "✓ Nope" message is highlighted with a large orange oval. To the right of the screenshot is a white circular graphic featuring a hand holding a smartphone with the WhatsApp logo on its screen, set against a background of white clouds and a Wi-Fi signal icon.

Secure Device Access

Soon:

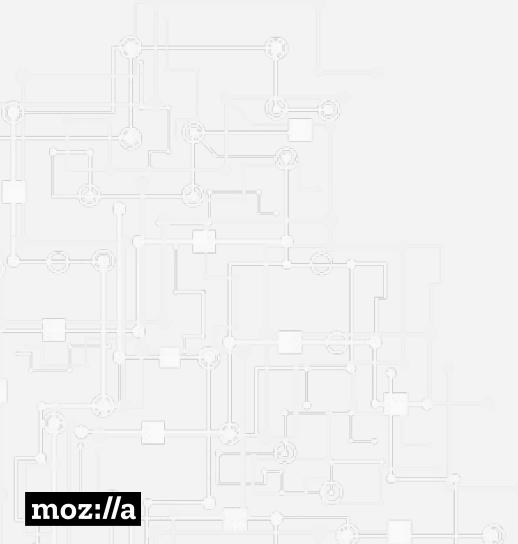
Browsers will start to restrict web permissions from iframes

https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/n37ij1E_1aY/JA-1R_pJDwAJ

Secure Device Access

With great power...

Secure websites



Secure Connections

- HTTPS All the Things!
- Take care of mixed content
- Set an HSTS header



Secure Web Content

- Embrace Cross-Origin restrictions
- Have a CSP
- Use Subresource Integrity



Secure Access to Device Capabilities

- Don't prompt from iframes or HTTP
- Pre-prompt to give the user context

Thanks!

Johann Hofmann

Twitter [@johannh](https://twitter.com/johannh)

GitHub [@johannhof](https://github.com/johannhof)

Website johannh.me

Questions

