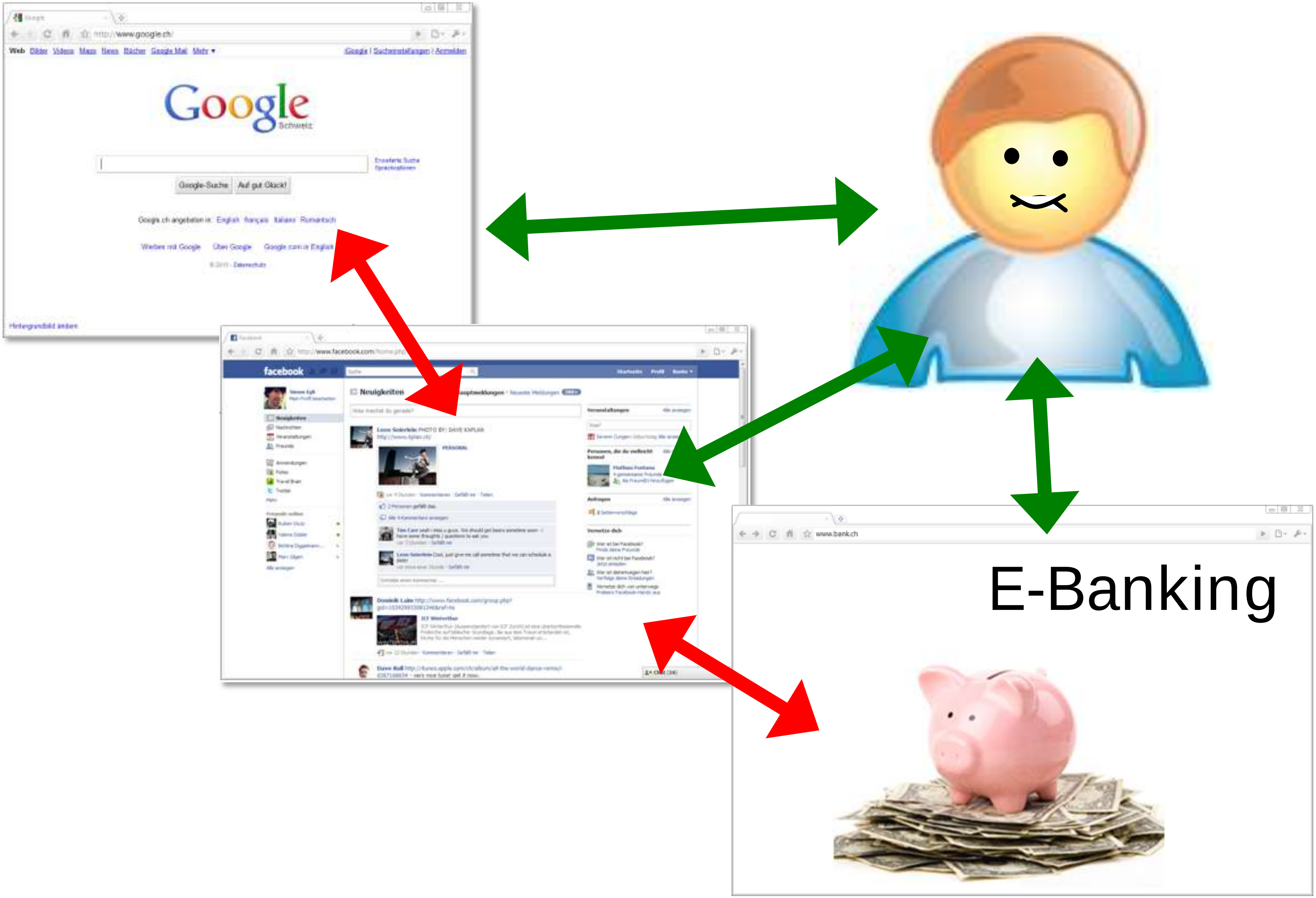
Bypassing Same Origin Policy

Simon Egli, IT Security Analyst

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch
www.csnc.ch

TU-4154
FORD
Impala

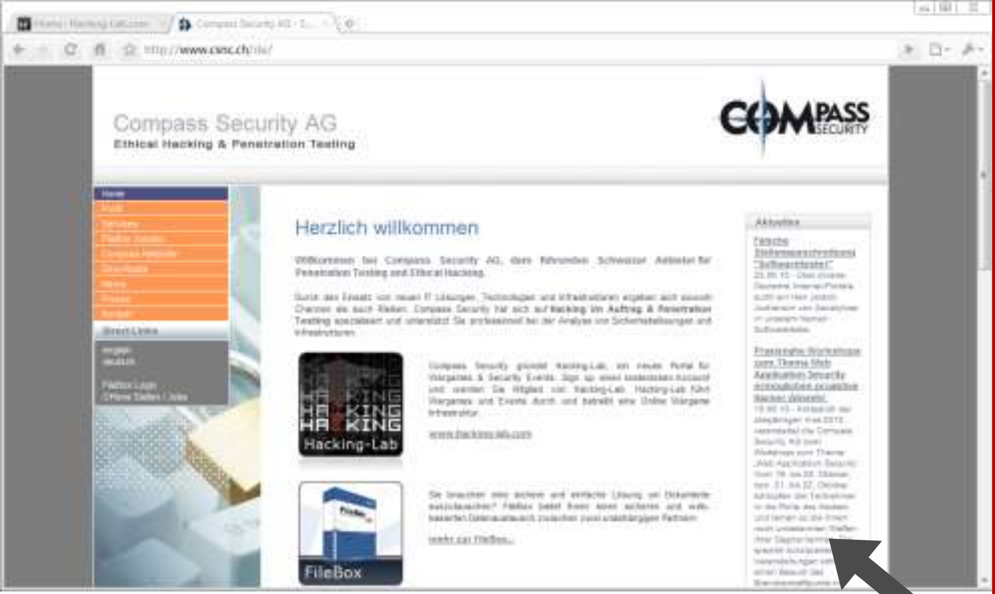

http://www.google.ch/
Google
Schweiz
Google-Suche
Auf gut Glück!
http://www.facebook.com/home.php
facebook
Neuigkeiten
www.bank.ch
E-Banking

Why?

Separated Content

Restricted DOM Access

Access to Cookies

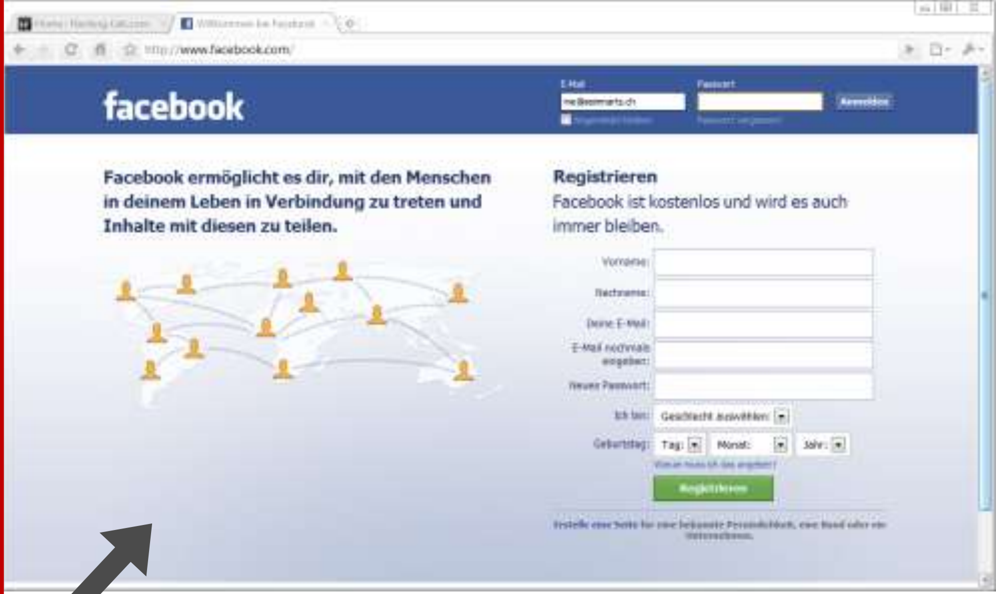

http://www.csnc.ch/de/

Compass Security AG

Ethical Hacking & Penetration Testing

Herzlich willkommen

Willkommen bei Compass Security AG, dem führenden Schweizer Anbieter für Penetration Testing und Ethical Hacking.


http://www.facebook.com/

facebook

Facebook ermöglicht es dir, mit den Menschen in deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen.

Registrieren

Facebook ist kostenlos und wird es auch immer bleiben.

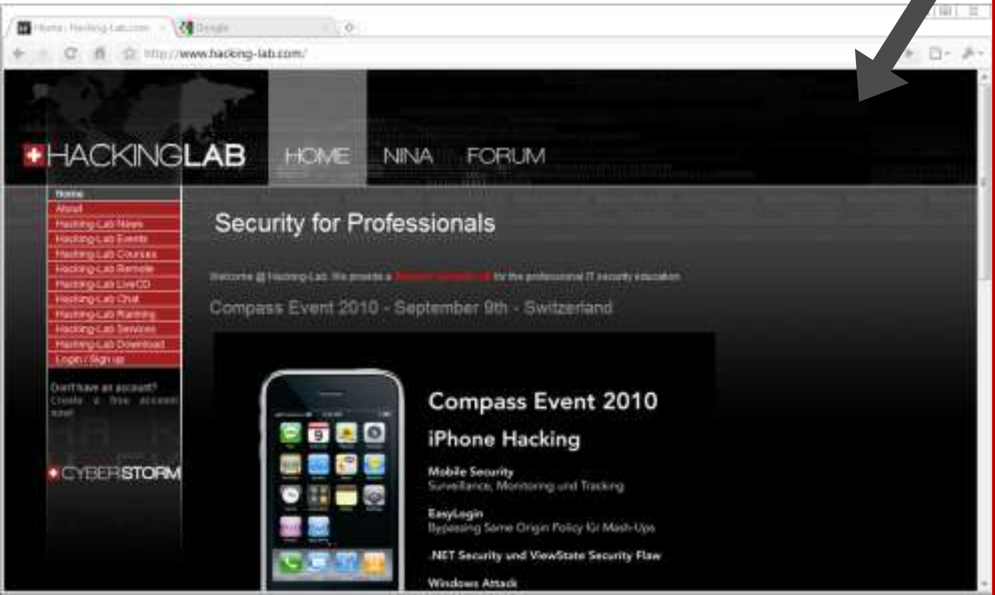
Vorname:
Nachname:
Deine E-Mail:
E-Mail nochmals eingeben:
Neues Passwort:
Ich bin: Geschlecht auswählen:
Geburtstag: Tag: Monat: Jahr:

Same Origin Policy

Same Origin Policy

Same Origin Policy

Same Origin Policy


http://www.hacking-lab.com/

Security for Professionals

Compass Event 2010 - September 9th - Switzerland

Compass Event 2010

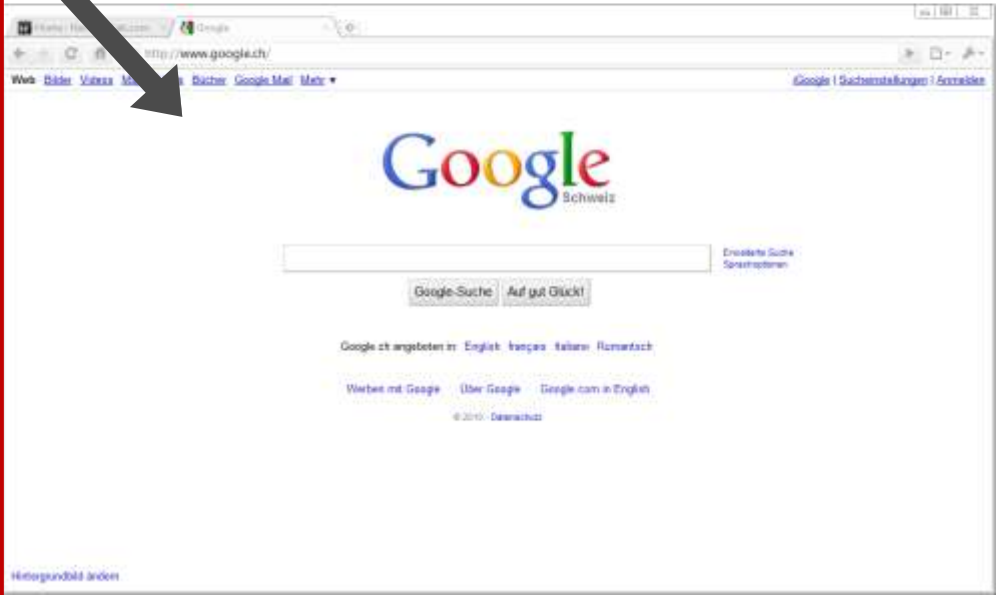
iPhone Hacking

Mobile Security
Surveillance, Monitoring und Tracking

EasyLogin
Bypassing Same Origin Policy für Mash-Ups

.NET Security und ViewState Security Flaw

Windows Attack


http://www.google.ch/

Google-Suche Auf gut Glück!

Google.ch angeboten in: English français italiano Rumantsch

Werben mit Google Über Google Google.com in English

© 2010 - Datenschutz

Hintergrundbild ändern

1990

1st Web Server

1st Web Site

1st Web Browser

PROPRIETE CERN
CERN
This machine is a ser
DO NOT POWE
DOWN!!
PROPRIETE CERN
Information Management: A Proposal
Abstract

1995

1996

JavaScript

Same Origin Policy

Netscape Navigator 2.0

100‘000 Web Servers

2003

Web 2.0

„**I** think Web 2.0 is of course a piece of jargon, nobody even knows what it means.**“** Tim Berners-Lee

Spongecell
Hula
kiko
Trumba
eskobo
mayomi
Pageflakes
vimeo
skobee
shadows
gravee
YouTube
Zimbra
LookSmart FURL Your Personal Web File
smugmug the ultimate in photo sharing
newsgator
Blogniscient The bird's eye view of the Blogosphere
TiN FiNGER
shutterfly
mefeedia
PodDater
Feedster
favoor
Planzo.com The Online Planning Community
ZAZZLE
Tailrank
TagWorld
nuvvo Learn something new
dogear
yakalike
grouper beta
ODDPOST
QOOP DIGITAL TO PRINT
iNods
Lulu
R
BR BETA
blish The easiest place to buy or sell digital content
flagr
FireAnt
simply hired
veoh BETA
theadcloud classified ads in your own way
rbloc.com
pixagogo
gather
Agatra
browsr
oyogi BETA
cafepress.com
Renkoo
standpoint
meebo
EXTRA TASTY!
last.fm
YEDDA
Jotspot
Frappr! Beta
jeteye
dabble db
Writeboard
SHOUTWIRE
iKarma
Kanoodle
AirSet
tech.memeorandum
CalendarHub
Suprglu PIECING YOUR WEB TOGETHER
pando
zigtag
Findory
backfence.com
clipmarks
wayfaring
gOFFICE
AllPeers
orb
Rallypoint
Zoozio coming soon
blogbeat
Ziggs
zooto
vSocial
Boltfolio
wink
riya
Audible Wordcast
Opinity Because your reputation matters!
reddit
measure map
gumshoo beta
bluepulse
imvu BETA
STREAMLOAD Freedom for Your Digital Lifestyle
Ta-da Lists
FeedSky
jellyBarn.INC
FeedTier
phanfare
WIKIPEDIA The Free Encyclopedia
Fruitcast
PubSub
nativetext
CONGOO BETA
PODZINGER BETA
RSS MAD
dPolls
flickr
Ning
Ookles
Strongspace
zoominfo
CASTPOST ALPHA
yubnub
AC ASSOCIATEDCONTENT
Bloop BETA
ProjectSpaces
FeedBurner
Bloglines
purevolume.com
FOTOLOG
ourmedia The Global Home for Grassroots Media
Yub.com
Spot Runner BETA
myspace a place for friends
NewsAlloy
Allmydata.com
gabbr.com a social news community
Gcast
blinkx search
openomy
riffs
ajchat alpha
jambo NETWORKS
ROLLYO
ClipShack beta
chatsum
PANDORA
looklater

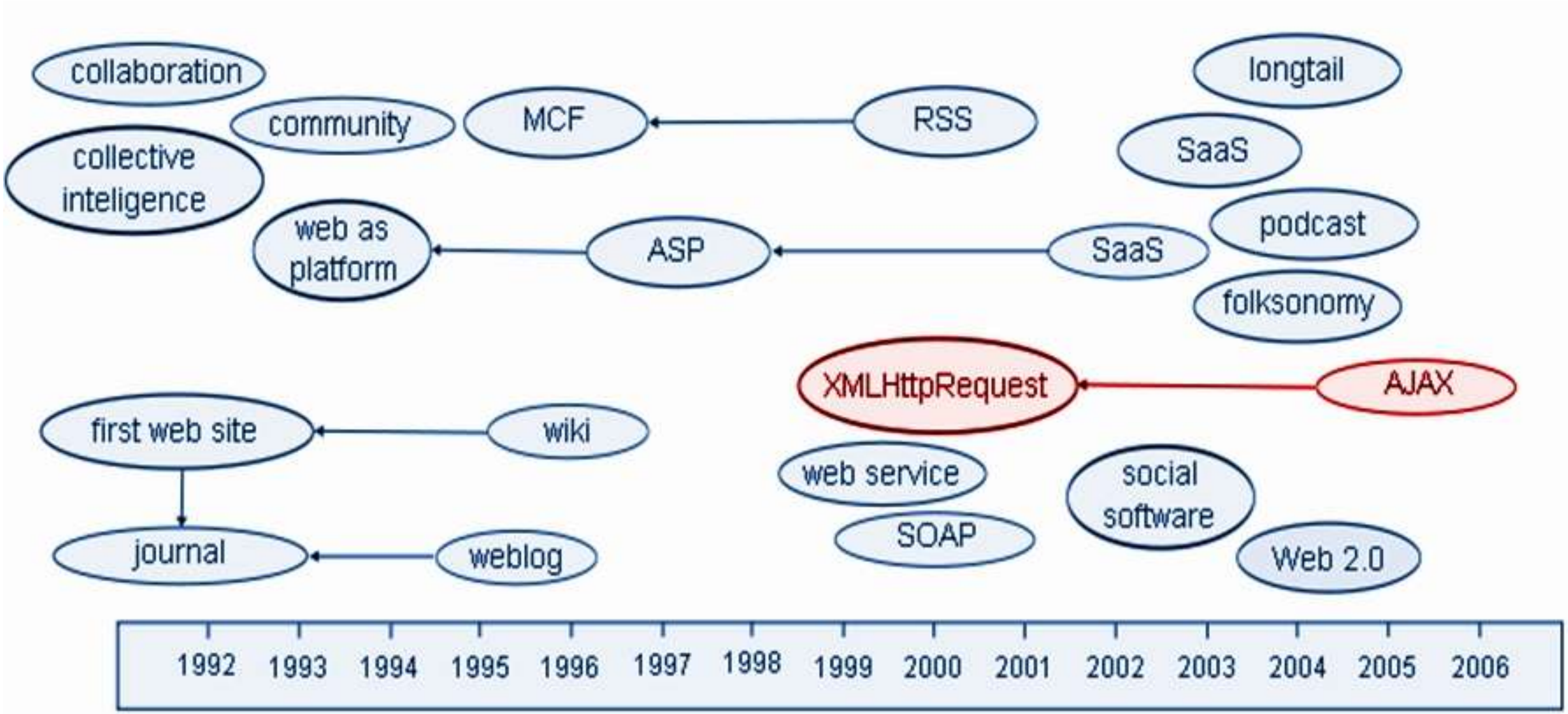
1996	hotmail™	
1998	napster™	
1999	Google! BETA	COMPASS SECURITY
2001	WIKIPEDIA The Free Encyclopedia	
2004	GMail™ by Google BETA	flickr™
2005	YouTube	
2006	facebook.	twitter

Same Origin Policy

Same Origin Followers

Restricted access to Cookies / DOM for:

- Java Script
- XMLHttpRequest (XHR)
- Adobe Flash
- Java Applet
- Microsoft Silverlight
- ActiveX
- Browser Extensions & Plugins


collaboration
community
MCF
RSS
longtail
collective inteligence
SaaS
web as platform
ASP
SaaS
podcast
folksonomy
XMLHttpRequest
AJAX
first web site
wiki
web service
social software
SOAP
journal
weblog
Web 2.0
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006

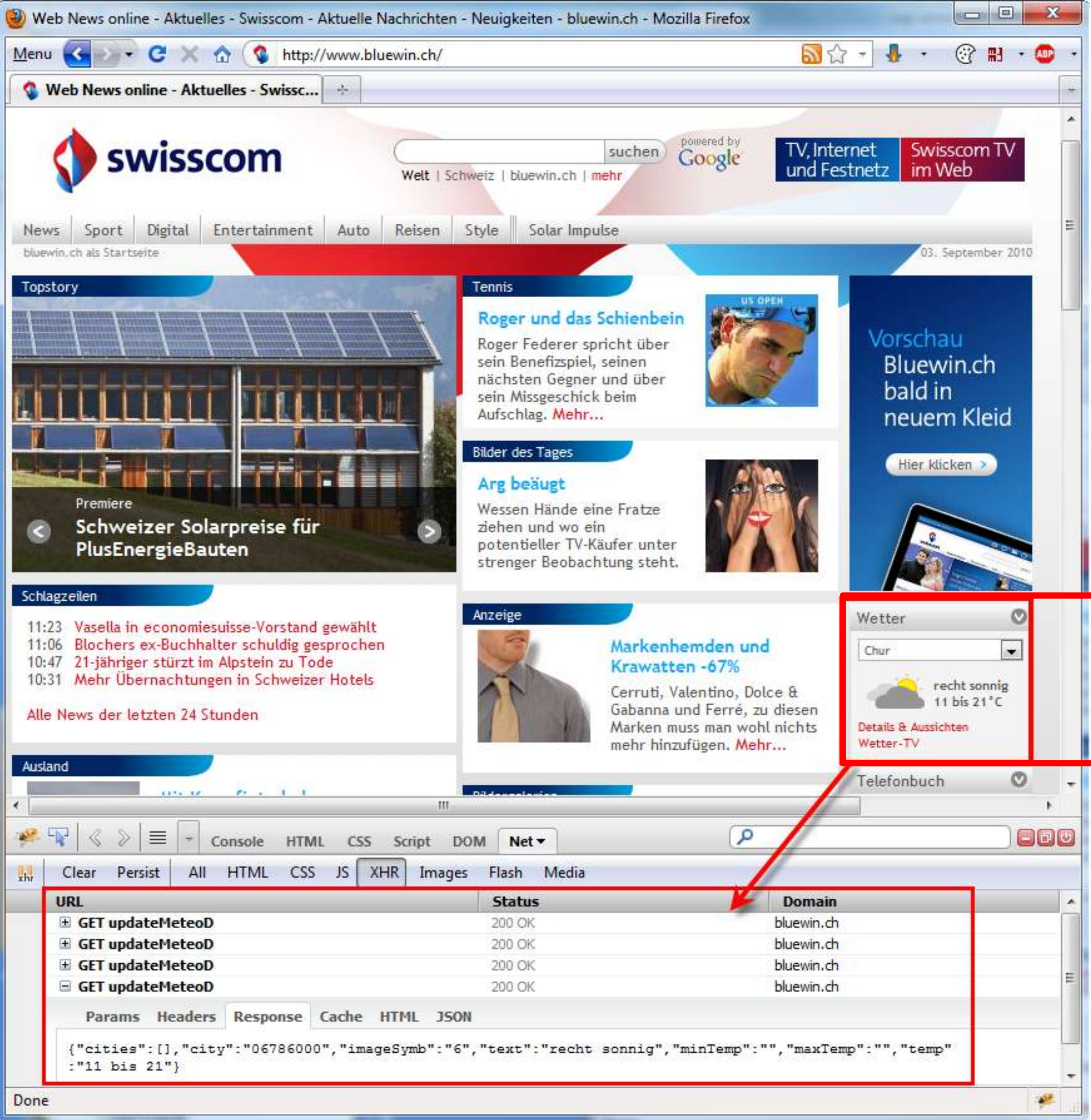
XMLHttpRequest (XHR)

Background HTTP requests from JavaScript

Invented by Microsoft in 2000 (Internet Explorer 5)

IE 5/6: COM/ActiveX object „Microsoft.XmlHttp“

IE 7, Firefox, Opera, Safari and other browsers:
Native JavaScript object „XmlHttpRequest“



Premiere

Schweizer Solarpreise für PlusEnergieBauten

Roger und das Schienbein

Roger Federer spricht über sein Benefizspiel, seinen nächsten Gegner und über sein Missgeschick beim Aufschlag. Mehr...

Arg beäugt

Wessen Hände eine Fratze ziehen und wo ein potentieller TV-Käufer unter strenger Beobachtung steht.

11:23 Vasella in economiesuisse-Vorstand gewählt
11:06 Blochers ex-Buchhalter schuldig gesprochen
10:47 21-jähriger stürzt im Alpstein zu Tode
10:31 Mehr Übernachtungen in Schweizer Hotels

Alle News der letzten 24 Stunden

Markenhemden und Krawatten -67%

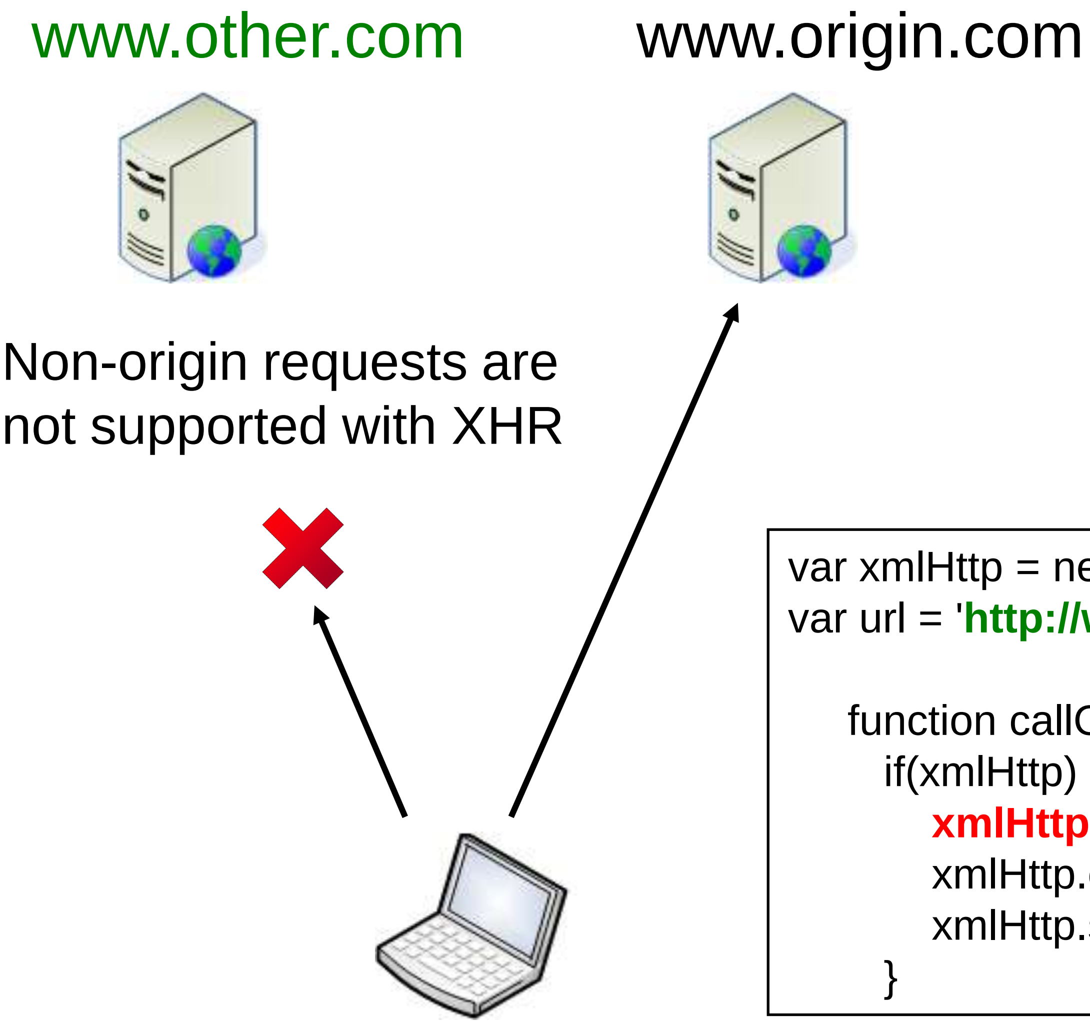
Cerruti, Valentino, Dolce & Gabanna und Ferré, zu diesen Marken muss man wohl nichts mehr hinzufügen. Mehr...

URL	Status	Domain
⊞ GET updateMeteoD	200 OK	bluewin.ch
⊞ GET updateMeteoD	200 OK	bluewin.ch
⊞ GET updateMeteoD	200 OK	bluewin.ch
⊟ GET updateMeteoD	200 OK	bluewin.ch

```
{"cities":[],"city":"06786000","imageSymb":"6","text":"recht sonnig","minTemp":"","maxTemp":"","temp"
:"11 bis 21"}
```

XMLHttp Request

And AJAX / XMLHttpRequest?



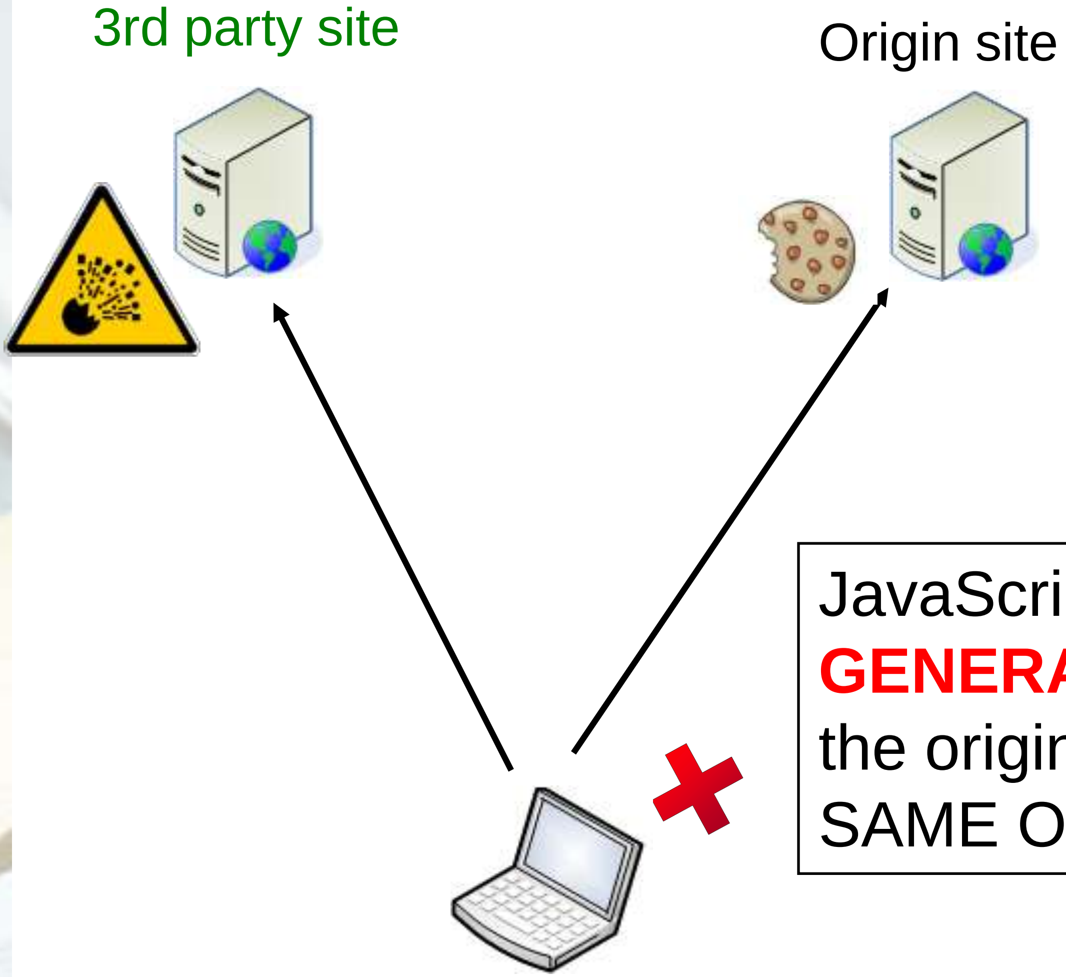
www.other.com

www.origin.com

Non-origin requests are not supported with XHR

```
var xmlHttp = new XMLHttpRequest();
var url = 'http://www.other.com/res/pub-data/';

    function callOtherDomain(){
      if(xmlHttp) {
         xmlHttp.open('GET', url, true);
         xmlHttp.onreadystatechange = handler;
         xmlHttp.send();
      }
```

Use Script from 3rd Party



JavaScript from 3rd party site **IS GENERALLY DENIED** to access the origin cookie because of the SAME ORIGIN POLICY

Origin Determination Rule

= Protokoll (http/https)

+ Host (www.csnc.ch)

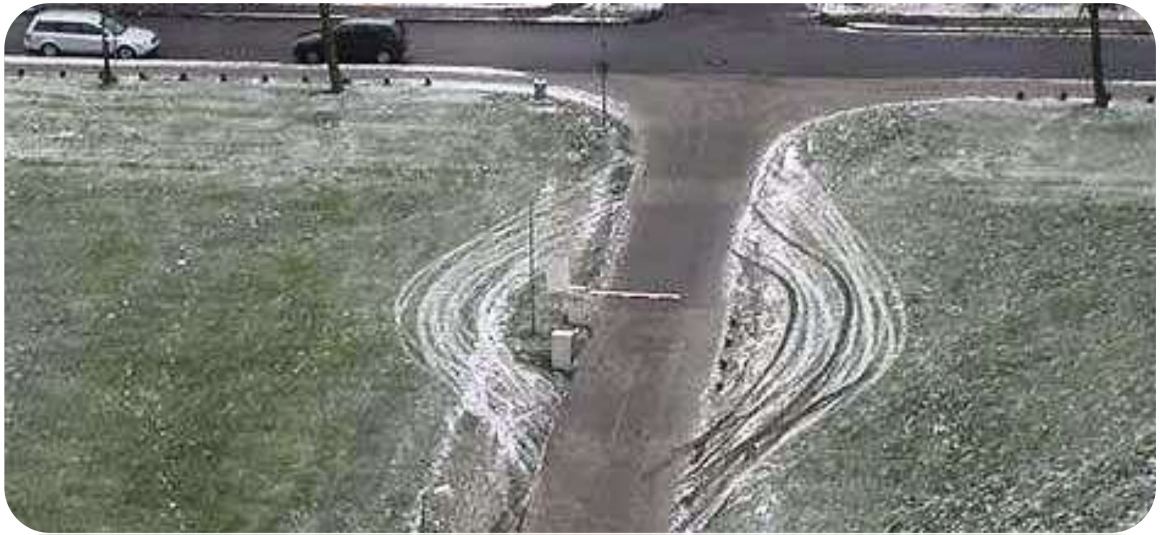
+ Port (:80)

Origin Example

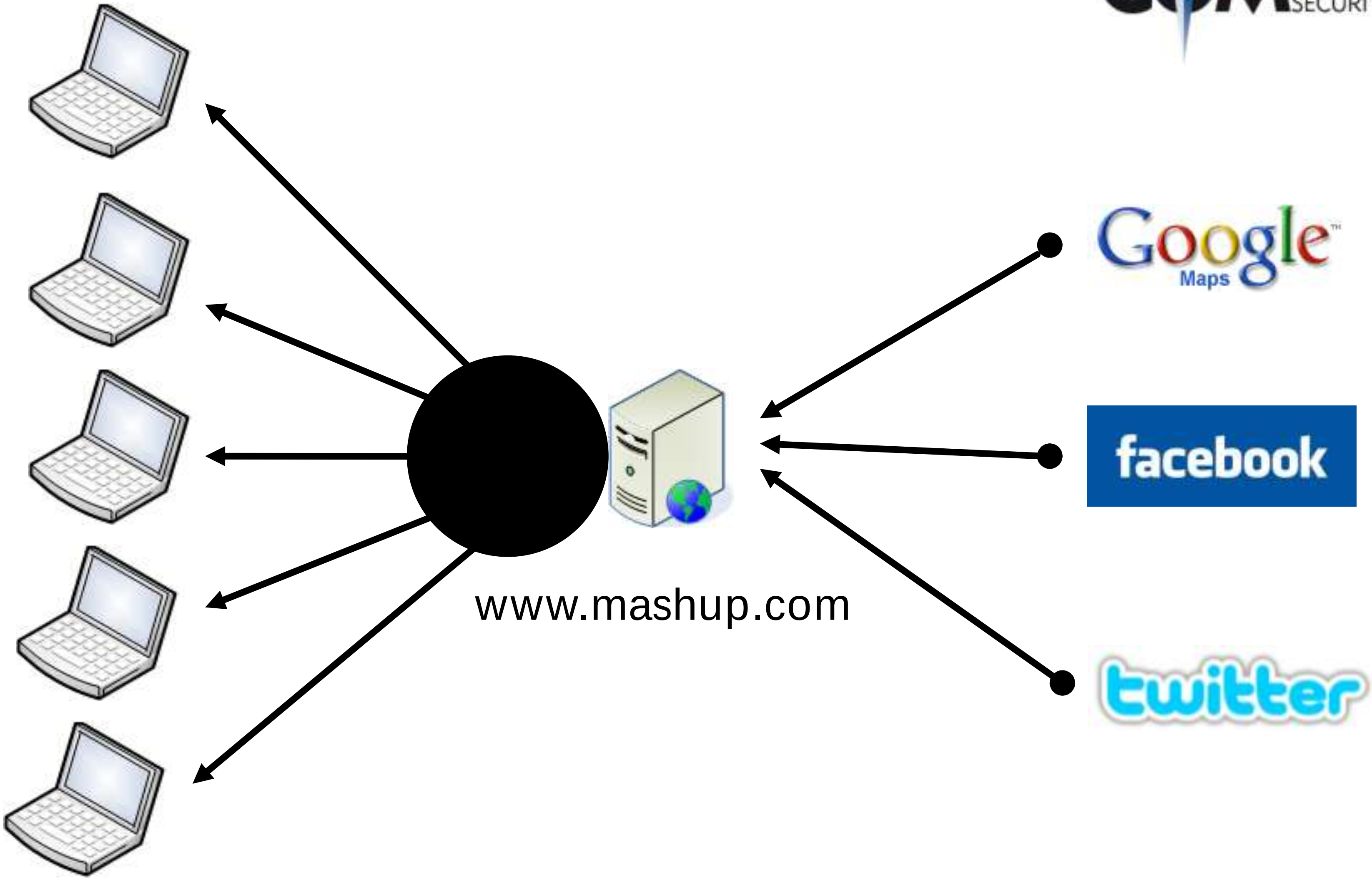
Referenz URL: *http://www.csnc.ch/de/index.html*

1. http://www.csnc.ch/en/index.html ✓
2. https://www.csnc.ch/de/index.html ✗
3. http://csnc.ch/de/index.html ✗
4. http://v1.www.csnc.ch/de/index.html ✗

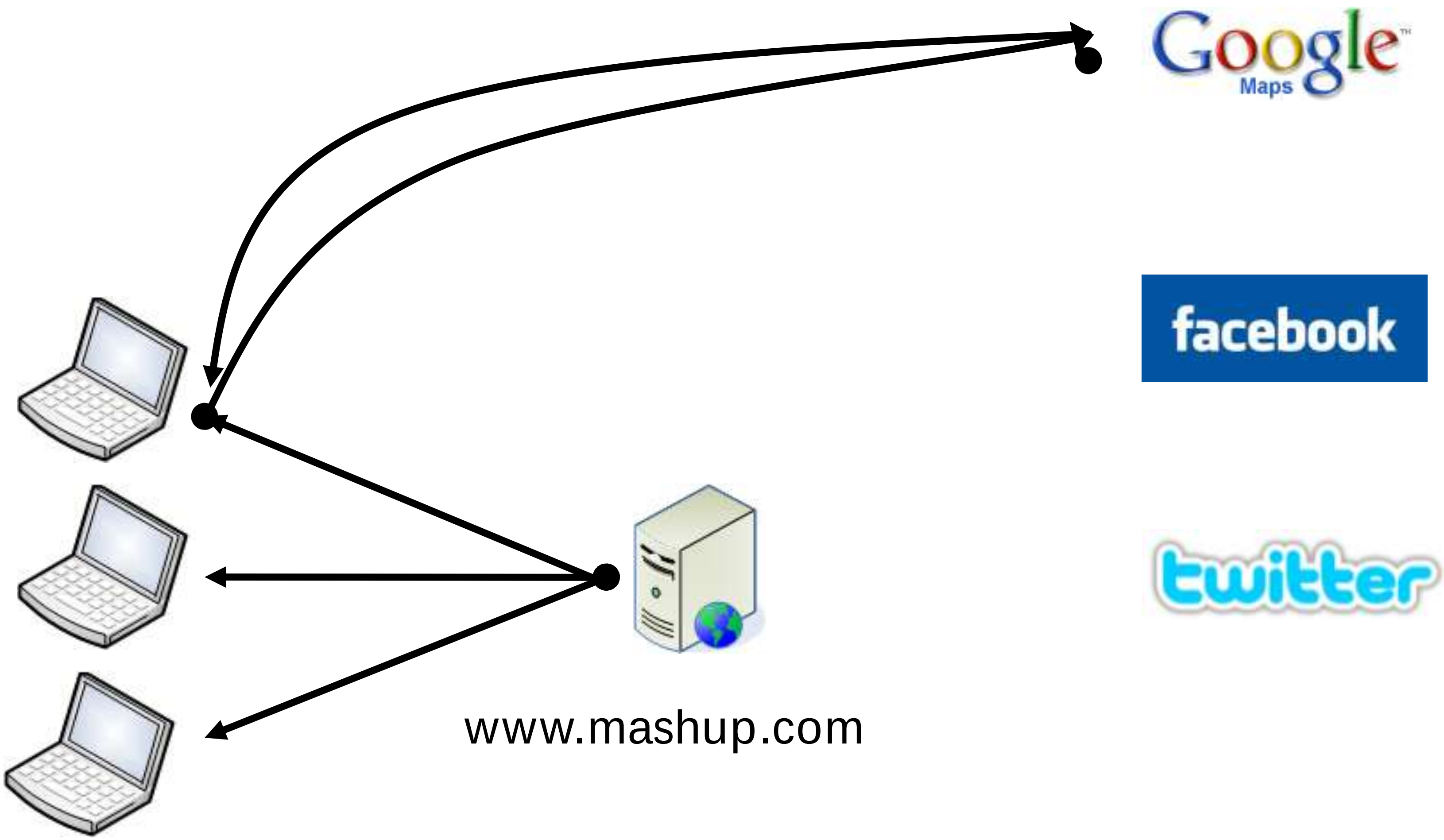
By-passing SOP?



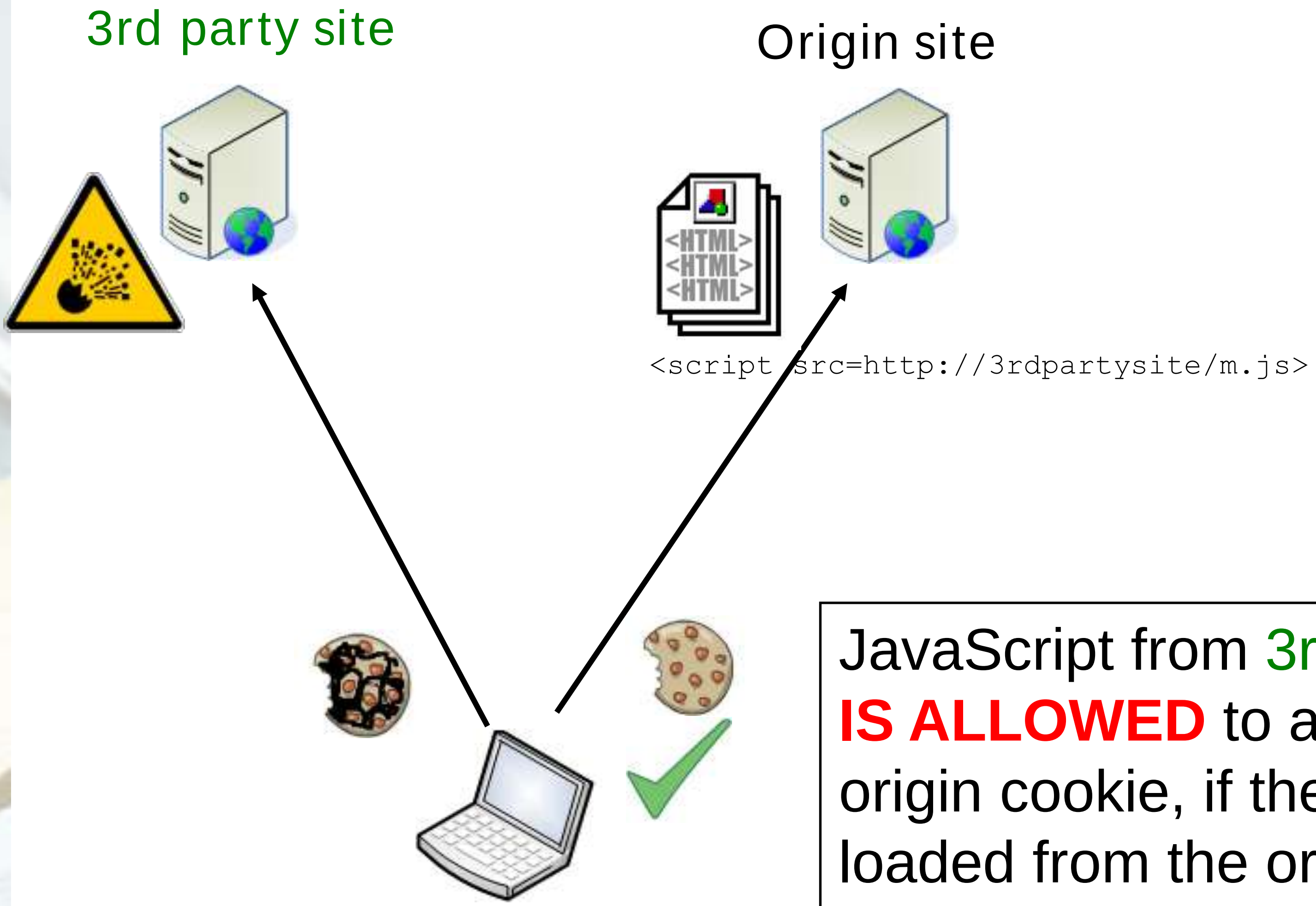
Why by-passing SOP?



Why by-passing SOP?

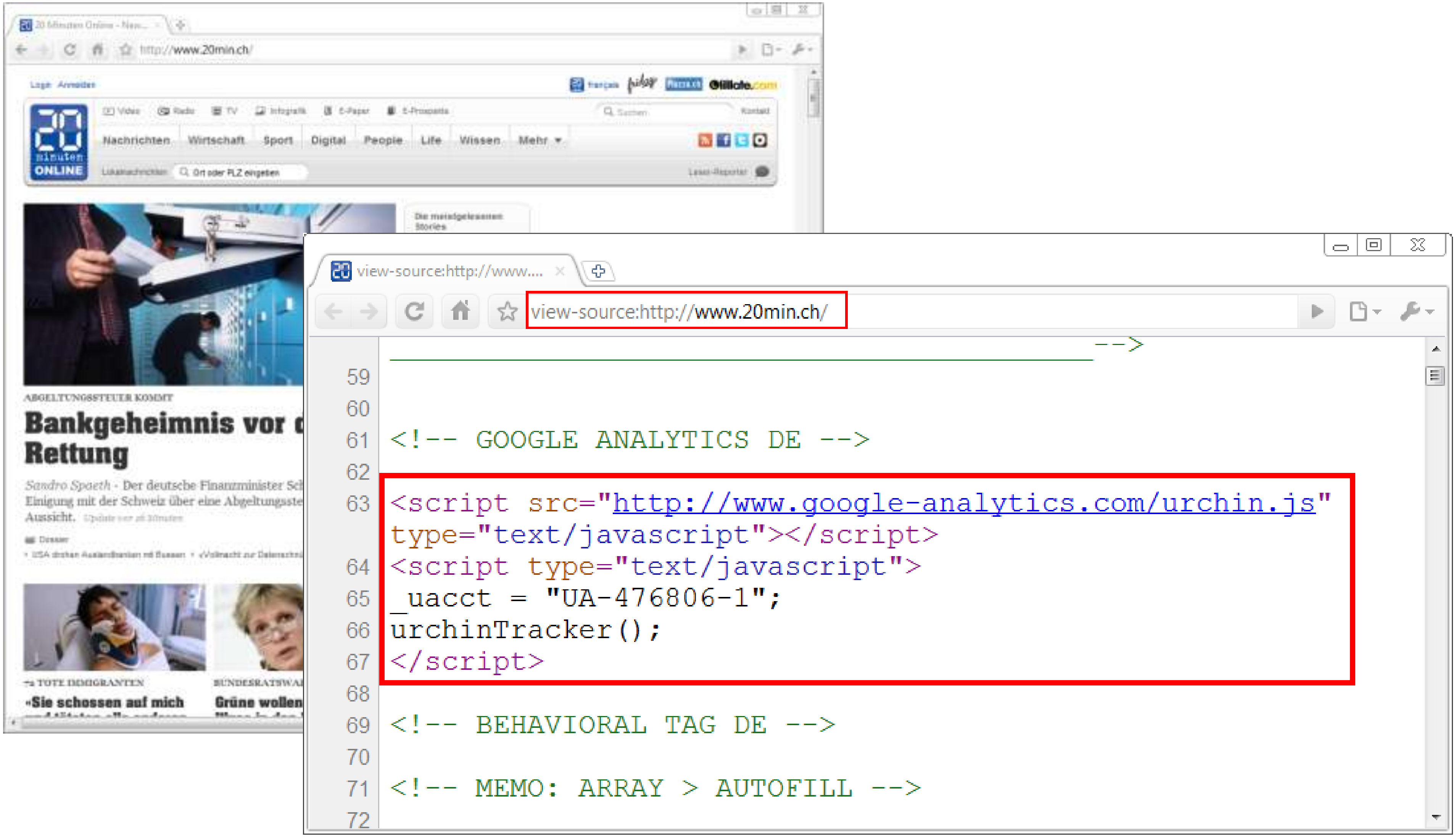


Use Script from 3rd Party



JavaScript from 3rd party site **IS ALLOWED** to access the origin cookie, if the script is loaded from the origin site with <script src=>

Google Analytics



view-source:http://www.20min.ch/

```
-->

<!-- GOOGLE ANALYTICS DE -->

<script src="http://www.google-analytics.com/urchin.js"
type="text/javascript"></script>
<script type="text/javascript">
_uacct = "UA-476806-1";
urchinTracker();
</script>

<!-- BEHAVIORAL TAG DE -->

<!-- MEMO: ARRAY > AUTOFILL -->
```

You will loose control and authority of your domain if you use <script src=“ ”> tags!

A New Solution is Required!

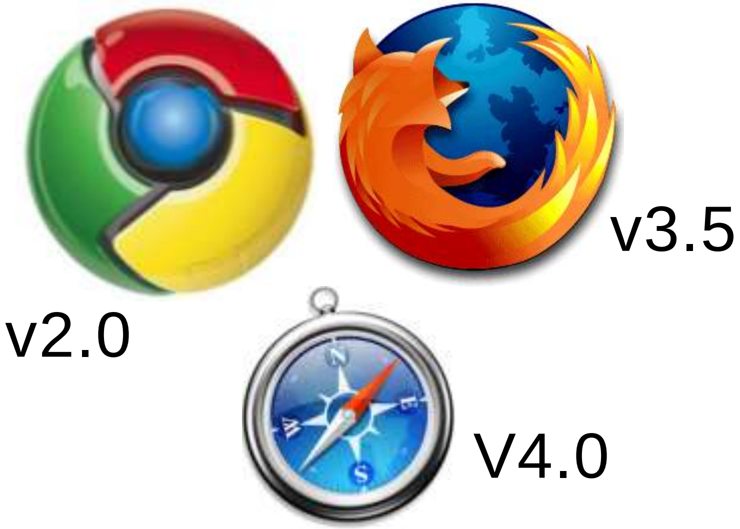
Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel +41 55-214 41 60
Fax +41 55-214 41 61
team@csnc.ch
www.csnc.ch

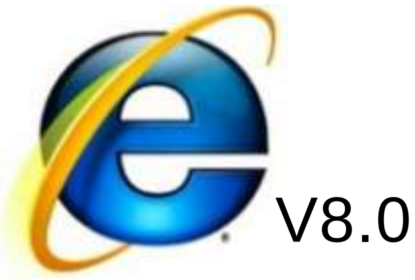
Cross-Origin Resource Sharing

CORS, a W3C Working Draft - 27 July 2010

CORS Compatibility

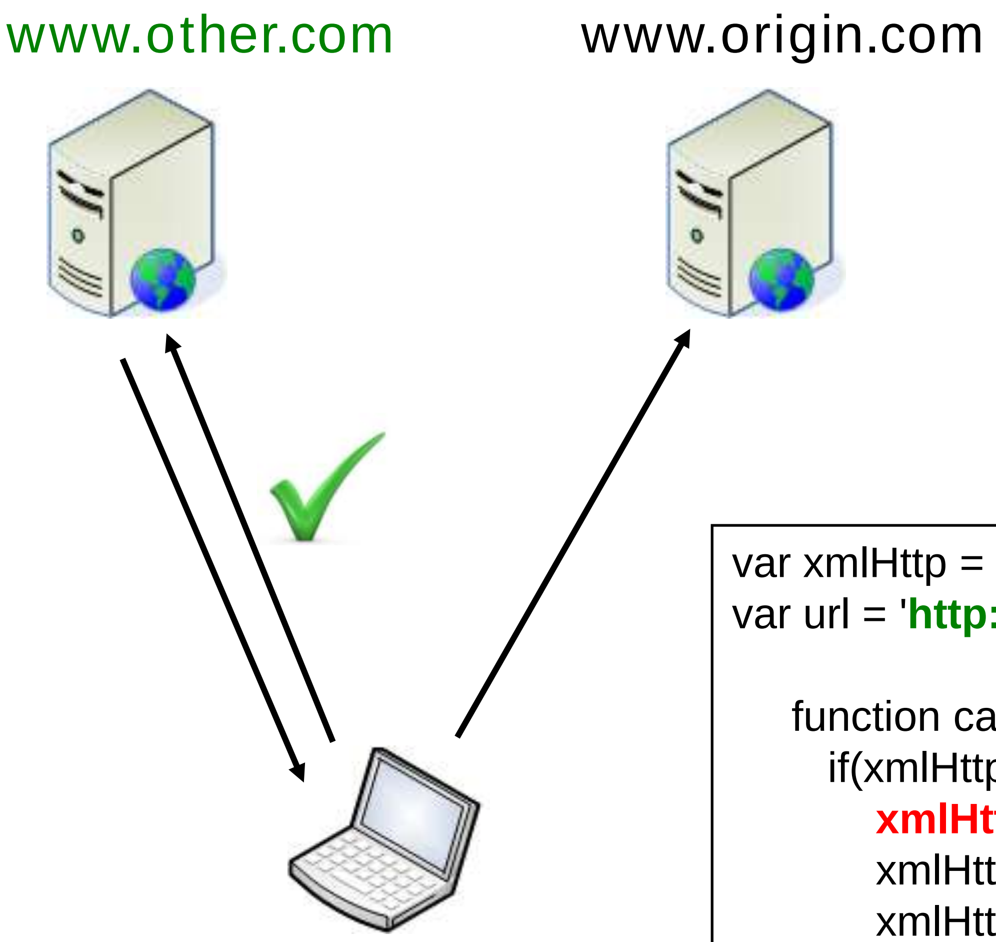


XMLHttpRequest (XHR)



XDomainRequest (XDR)

CORS Simple Request



www.other.com

www.origin.com

```
var xmlHttp = new XMLHttpRequest();
var url = 'http://www.other.com/res/pub-data/';

   function callOtherDomain(){
     if(xmlHttp) {
        xmlHttp.open('GET', url, true);
        xmlHttp.onreadystatechange = handler;
        xmlHttp.send();
     }
```

Simple Request Example

Client Request:

```
GET /resources/public-data/ HTTP/1.1
Host: bar.other
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.1b3pre)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://foo.example/examples/access-control/simpleXSInvocation.html
Origin: http://foo.example
```

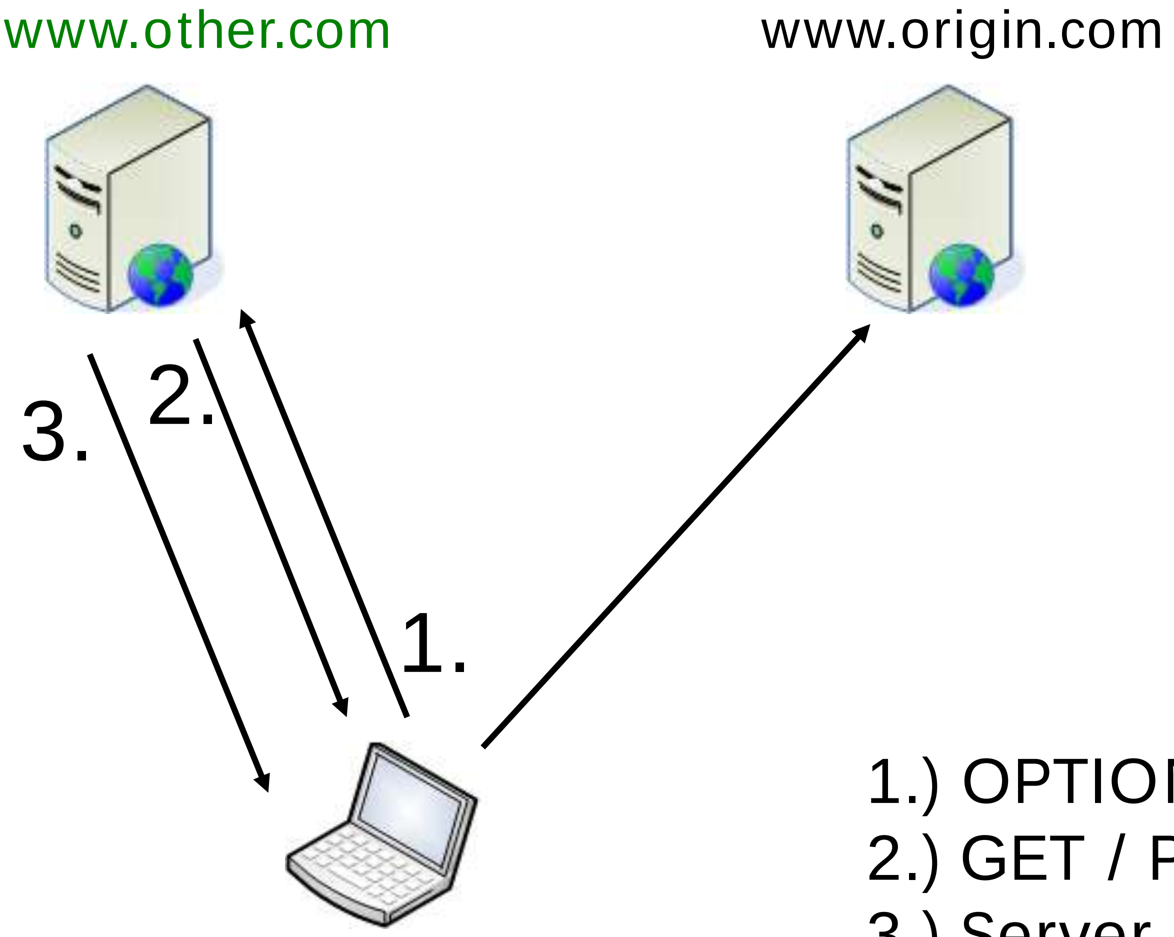
#1 Example – Server Response:

```
HTTP/1.1 200 OK
Date: Mon, 01 Dec 2008 00:23:53 GMT
Server: Apache/2.0.61
Access-Control-Allow-Origin: *
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/xml

[XML Data]
```

#2 Example – Server Response:

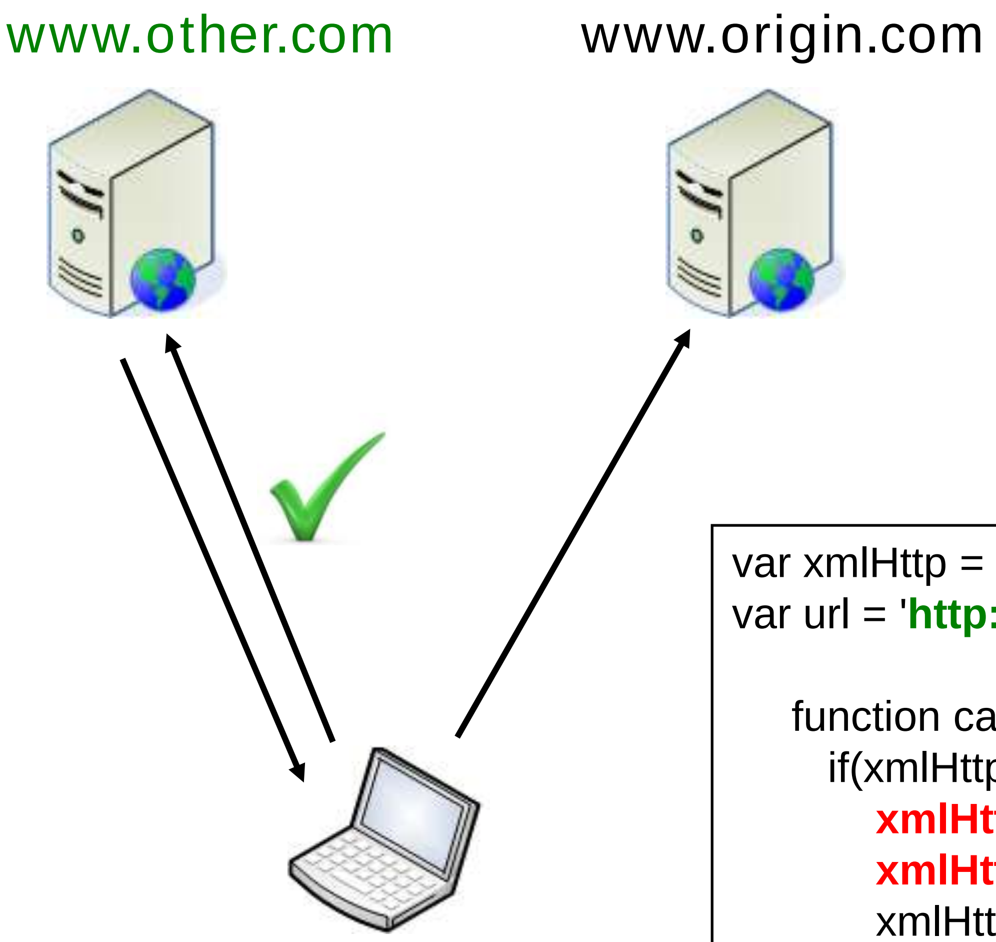
```
HTTP/1.1 200 OK
Date: Mon, 01 Dec 2008 00:23:53 GMT
Server: Apache/2.0.61
Access-Control-Allow-Origin: http://foo.example
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/xml

[XML Data]
```

CORS Preflighted Request Example



1.) OPTIONS Request
2.) GET / POST Request
3.) Server sends data

CORS Request with credentials



www.other.com

www.origin.com

```
var xmlHttp = new XMLHttpRequest();
var url = 'http://www.other.com/res/pub-data/';

    function callOtherDomain(){
      if(xmlHttp) {
         xmlHttp.open('GET', url, true);
         xmlHttp.withCredentials = "true";
         xmlHttp.onreadystatechange = handler;
         xmlHttp.send();
      }
```

Request with Credentials

Client Request:

```
GET /resources/public-data/ HTTP/1.1
Host: bar.other
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.1b3pre)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://foo.example/examples/access-control/simpleXSInvocation.html
Origin: http://foo.example
Cookie: pageAccess=2
```

Server Response:

```
HTTP/1.1 200 OK
Date: Mon, 01 Dec 2008 00:23:53 GMT
Server: Apache/2.0.61
Access-Control-Allow-Origin: http://foo.example
Access-Control-Allow-Credentials: true
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive
Content-Type: application/xml

[XML Data]
```

Mitigation

Mitigation

CORS allowes to load cross-domain data from foreign domains

Server decides which origin is allowed to access the data

Separate critical / non-critical applications into different subdomains

- E.g. http://app1.mybank.com / http://app2.mybank.com

Host third-party scripts by yourself or trust the source

Load third-party scripts via local proxy

Cross origin resource sharing (CORS)

- Fully supported (XMLHttpRequest) by Firefox 3.5, Safari 4, Google Chrome 2
- Proprietary implemented (XDomainRequest) by Internet Explorer 8

Q/A Session

References / Further Links

http://code.google.com/p/browsersec/w/list

http://www.w3.org/TR/cors/

https://developer.mozilla.org/En/HTTP_Access_Control

http://msdn.microsoft.com/en-us/library/cc709423(VS.85).aspx

http://hacks.mozilla.org/2009/07/cross-site-xmlhttprequest-with-cors/

http://www.nczonline.net/blog/2008/04/27/cross-domain-xhr-removed-from-firefox-3/