

# Bypassing Same Origin Policy

Simon Egli, IT Security Analyst

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

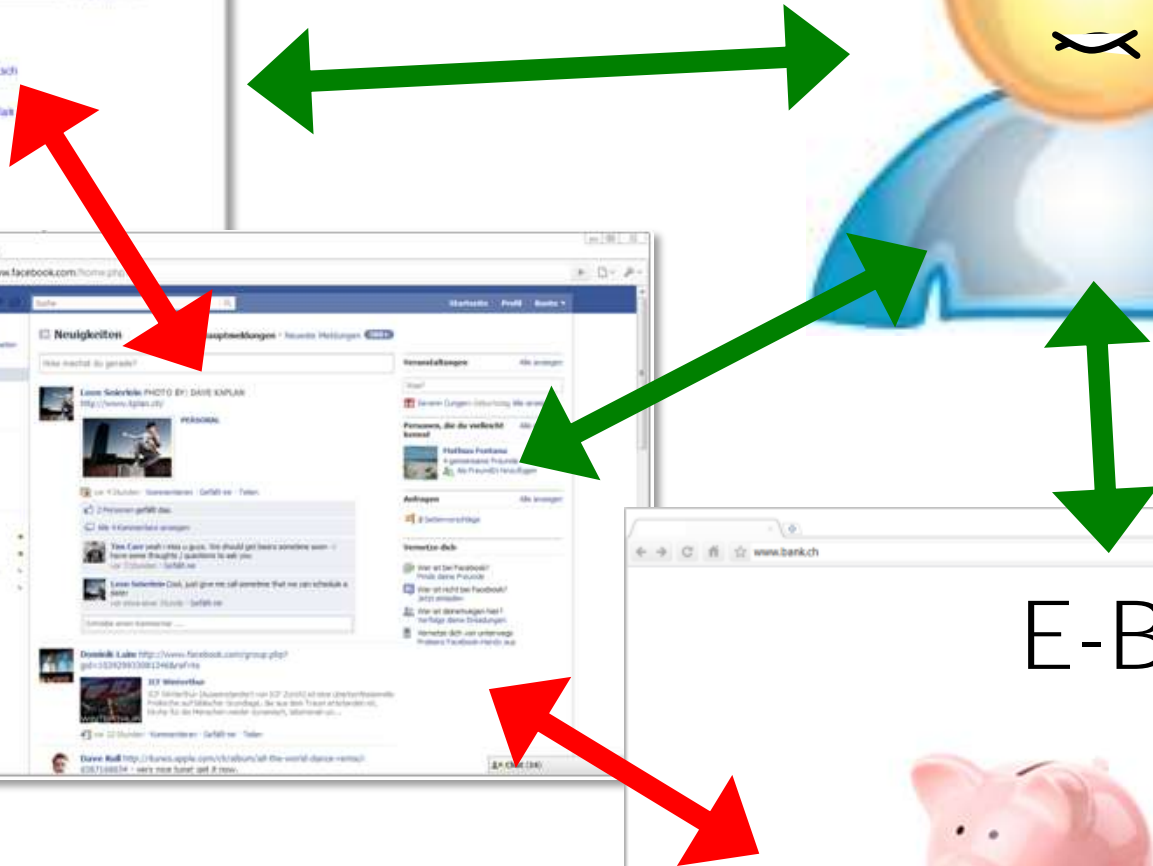
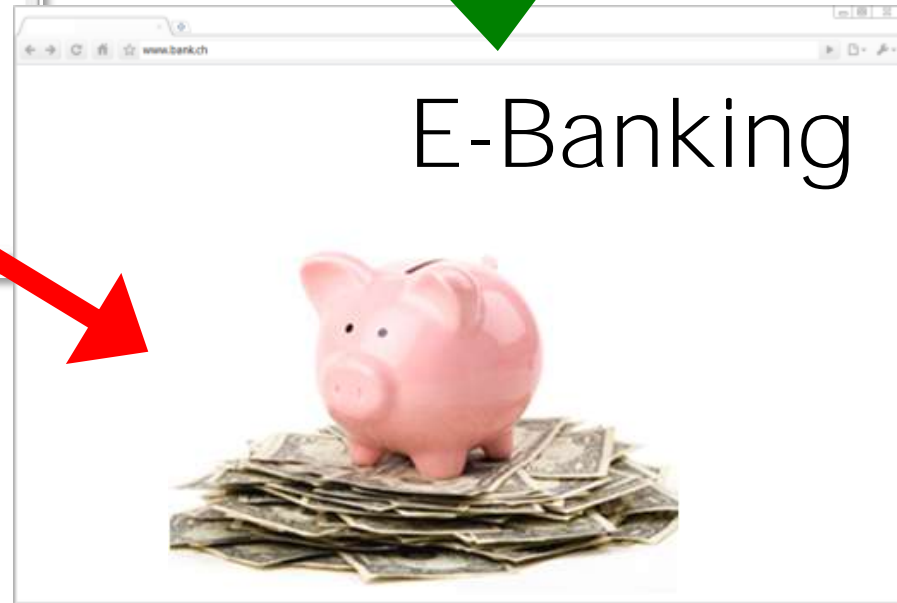
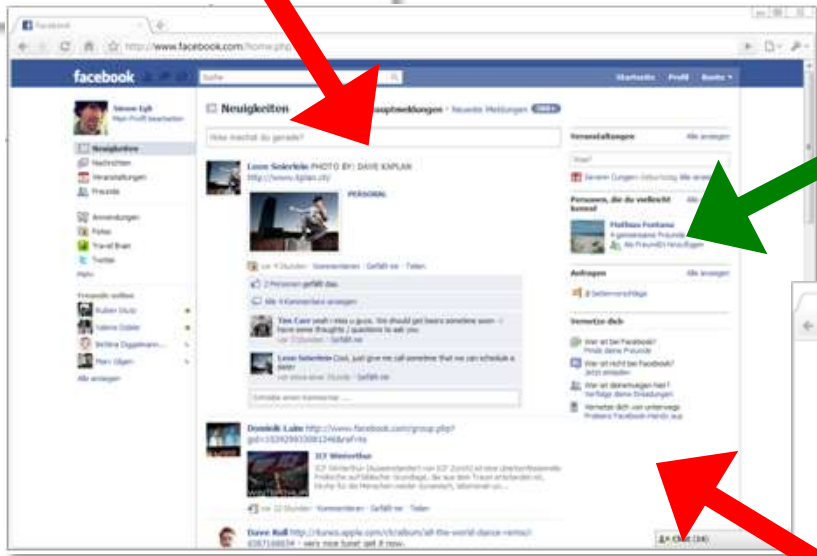
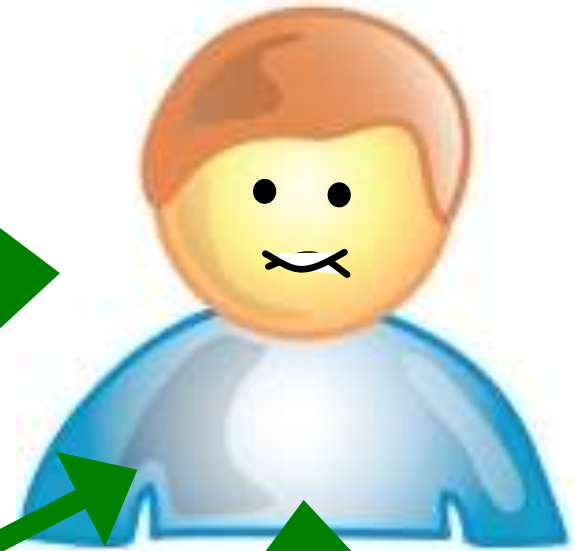
Tel +41 55-214 41 60  
Fax +41 55-214 41 61  
team@csnc.ch  
www.csnc.ch









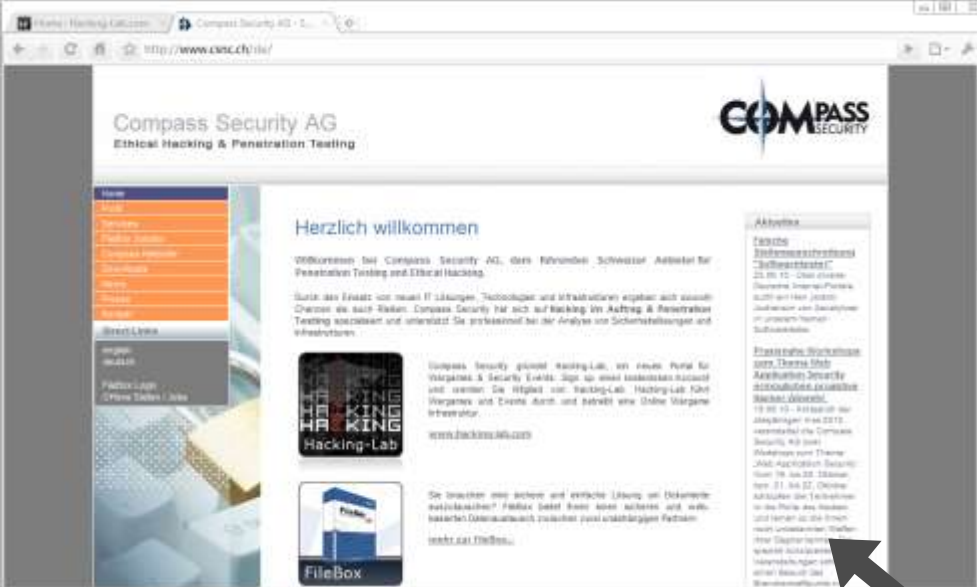


# Why?

Separated Content

Restricted DOM Access

Access to Cookies



Same Origin Policy

Same Origin Policy

Same Origin Policy



Same Origin Policy

# 1990

1st Web Server

1st Web Site

1st Web Browser



1995

YAHOO!



# 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



1996



1998



1999



2001



2004



2005



2006

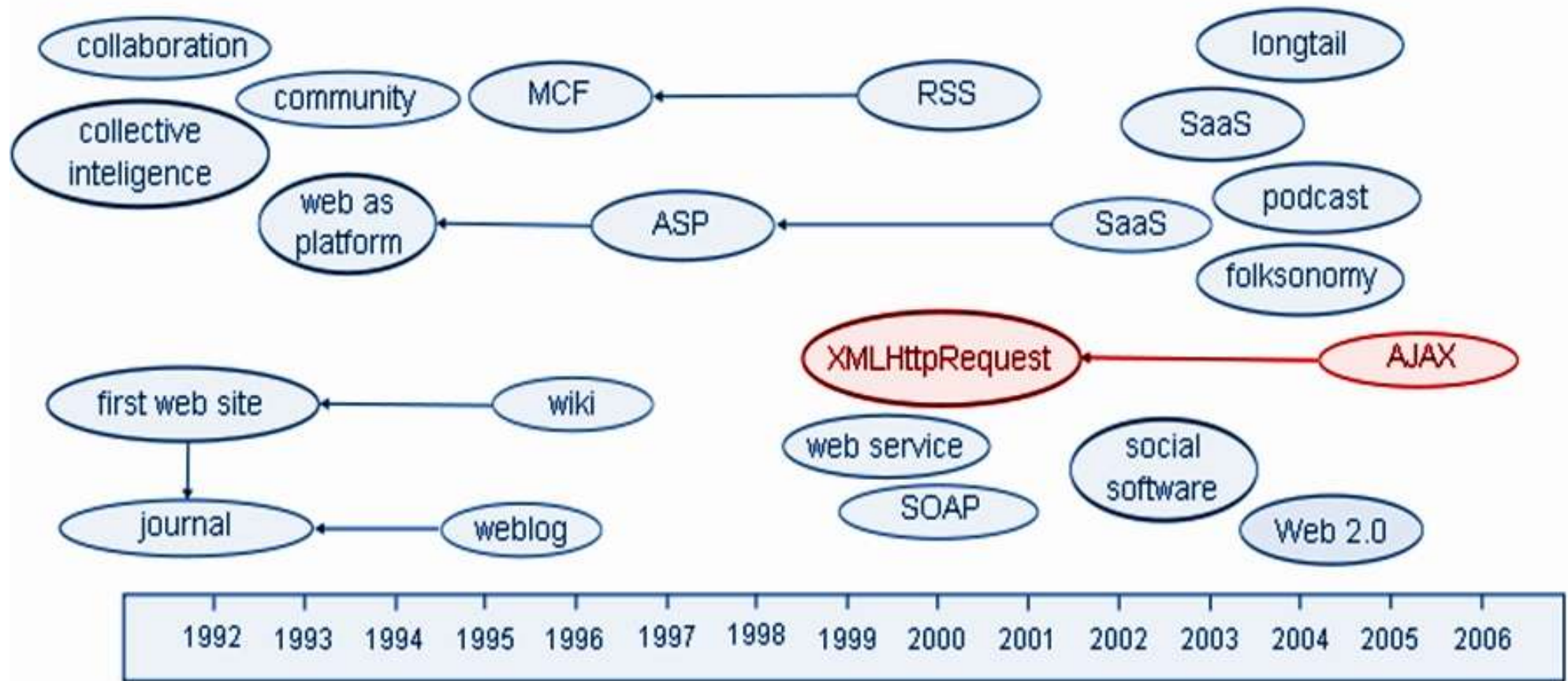


# Same Origin Policy



Restricted access to Cookies / DOM for:

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



# 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“

Web News online - Aktuelles - Swisscom - Aktuelle Nachrichten - Neuigkeiten - bluewin.ch - Mozilla Firefox

Menu [http://www.bluewin.ch/](#)

Web News online - Aktuelles - Swisscom

swisscom  suchen powered by Google

Welt | Schweiz | bluewin.ch | mehr

TV, Internet und Festnetz Swisscom TV im Web

News Sport Digital Entertainment Auto Reisen Style Solar Impulse

bluewin.ch als Startseite 03. September 2010

**Topstory**

Premiere  
Schweizer Solarpreise für PlusEnergieBauten

**Tennis**

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

**Bilder des Tages**

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

**Anzeige**

Markenhemden und Krawatten -67%  
Cerruti, Valentino, Dolce & Gabanna und Ferré, zu diesen Marken muss man wohl nichts mehr hinzufügen. Mehr...

**Wetter**

Chur  
recht sonnig  
11 bis 21°C  
Details & Aussichten  
Wetter-TV

**Schlagzeilen**

11:23 Vasella in economieuisse-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

**Ausland**

Console HTML CSS Script DOM Net

Clear Persist All HTML CSS JS XHR Images Flash Media

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

Params Headers Response Cache HTML JSON

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

XMLHttpRequest



# And AJAX / XMLHttpRequest?



www.other.com



www.origin.com



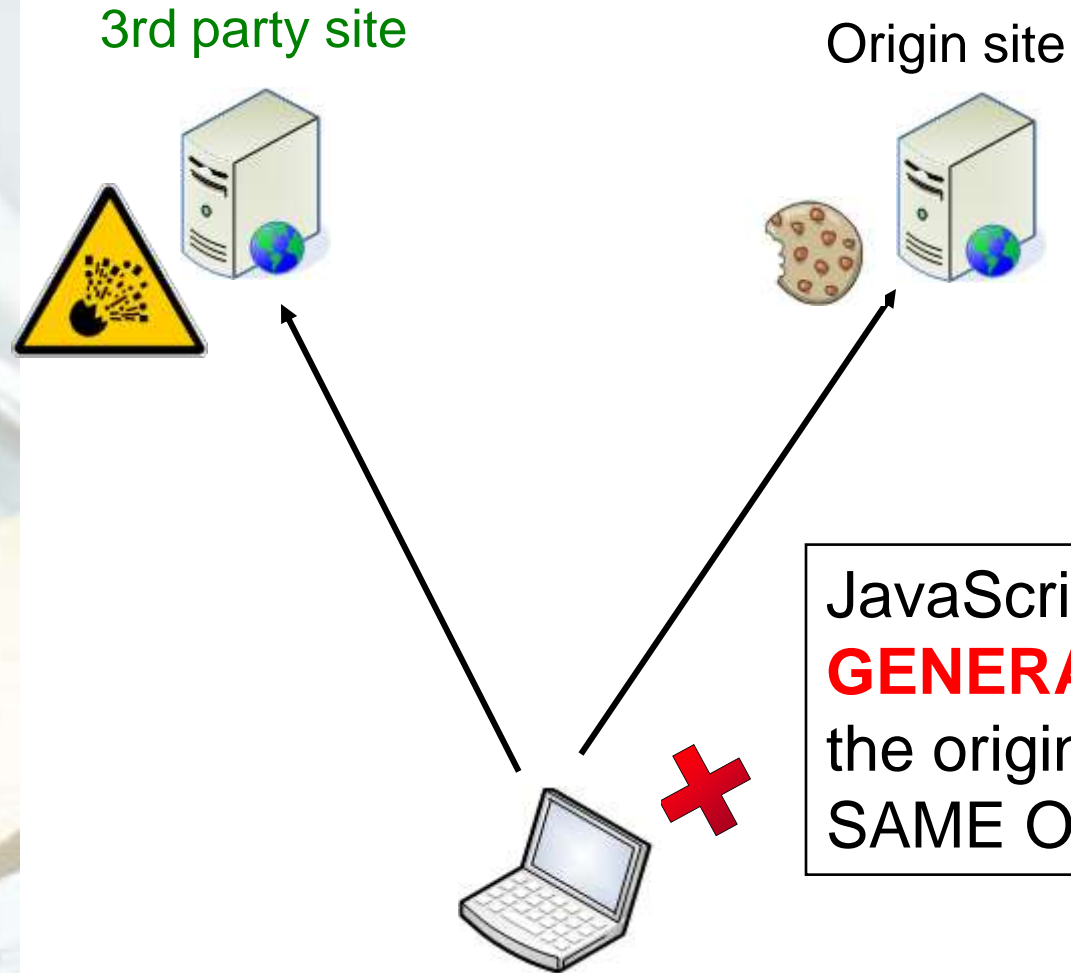
Non-origin requests are not supported with XHR



```
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**



= 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>



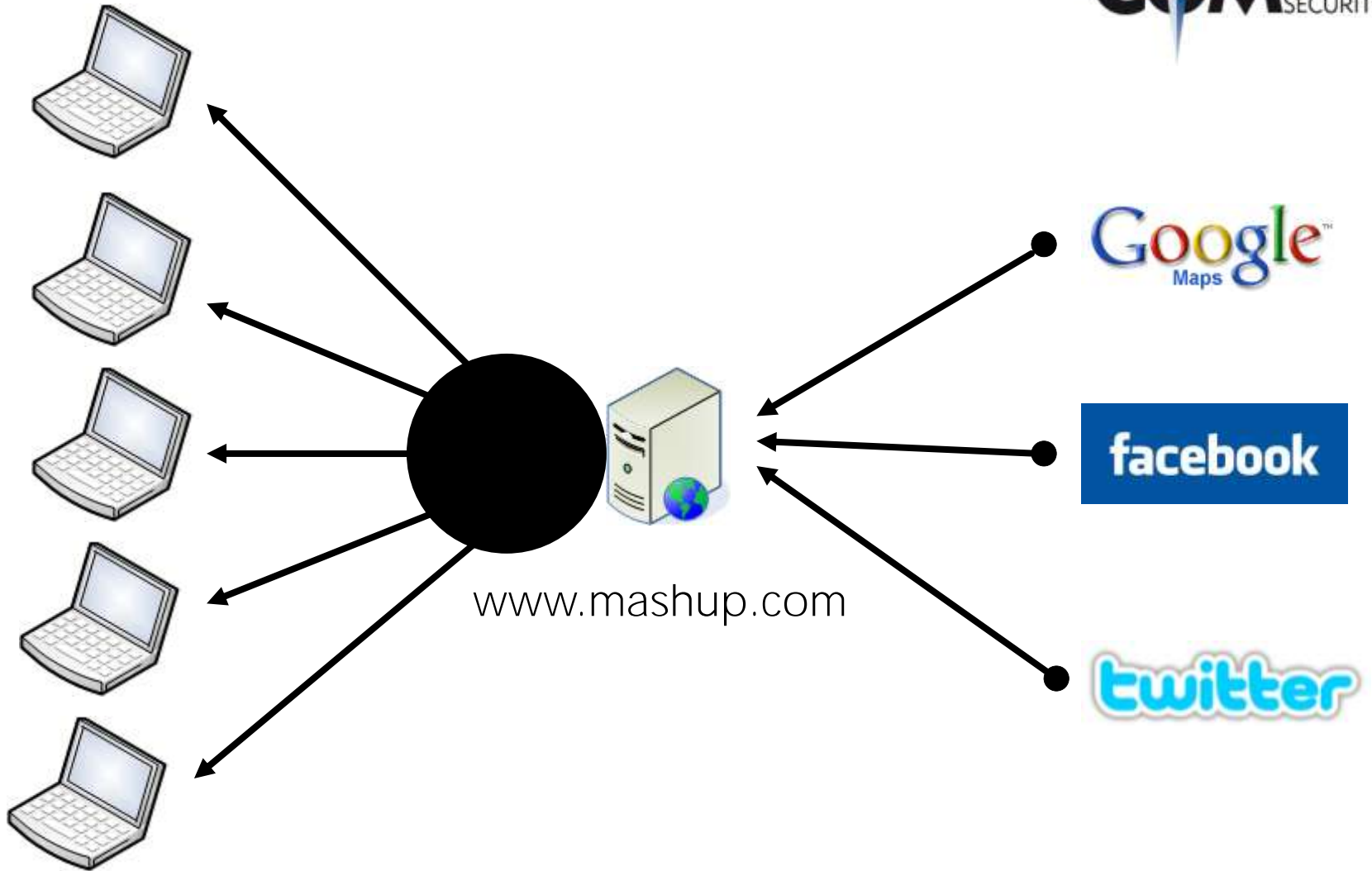
4. <http://v1.www.csnc.ch/de/index.html>



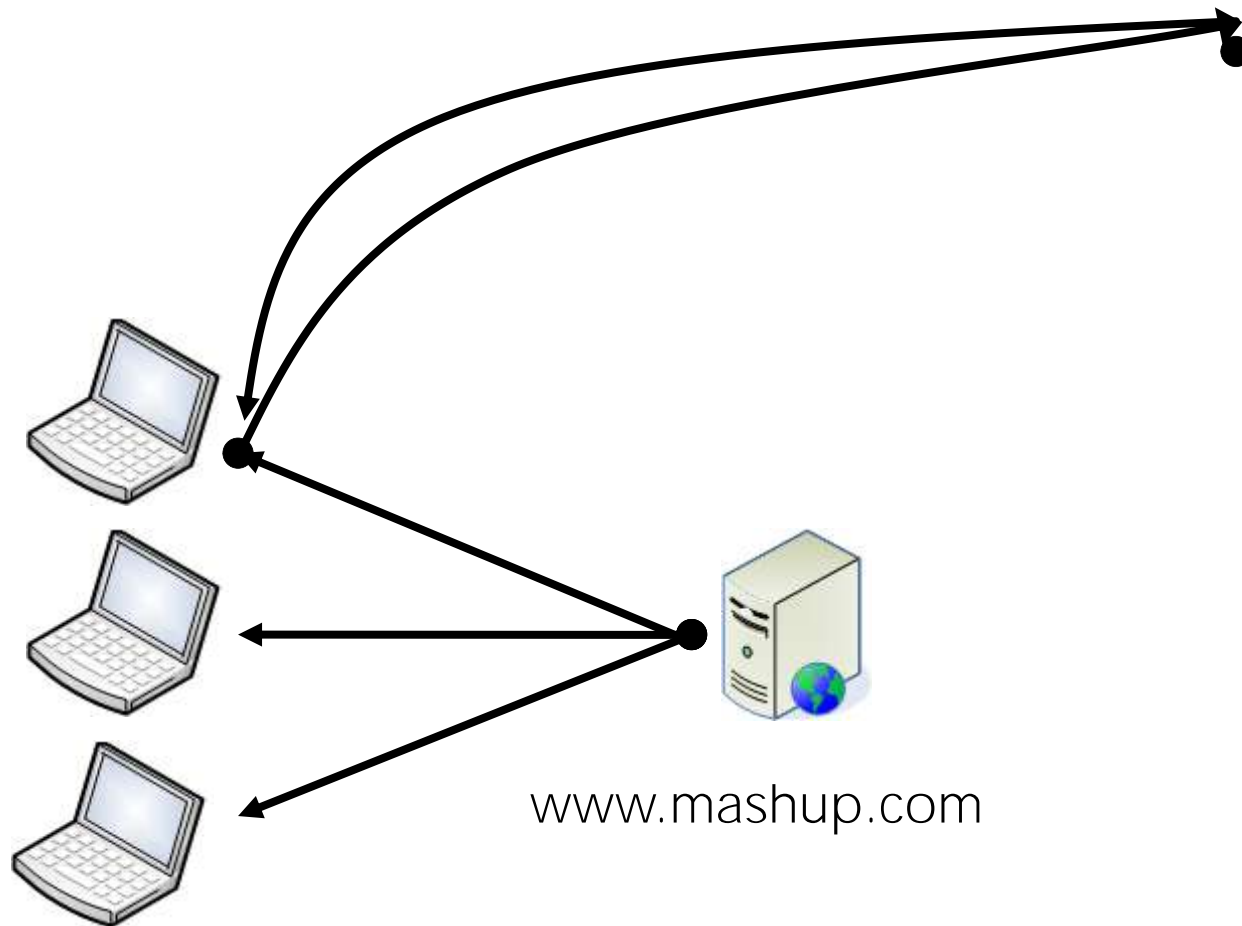
# By-passing SOP?



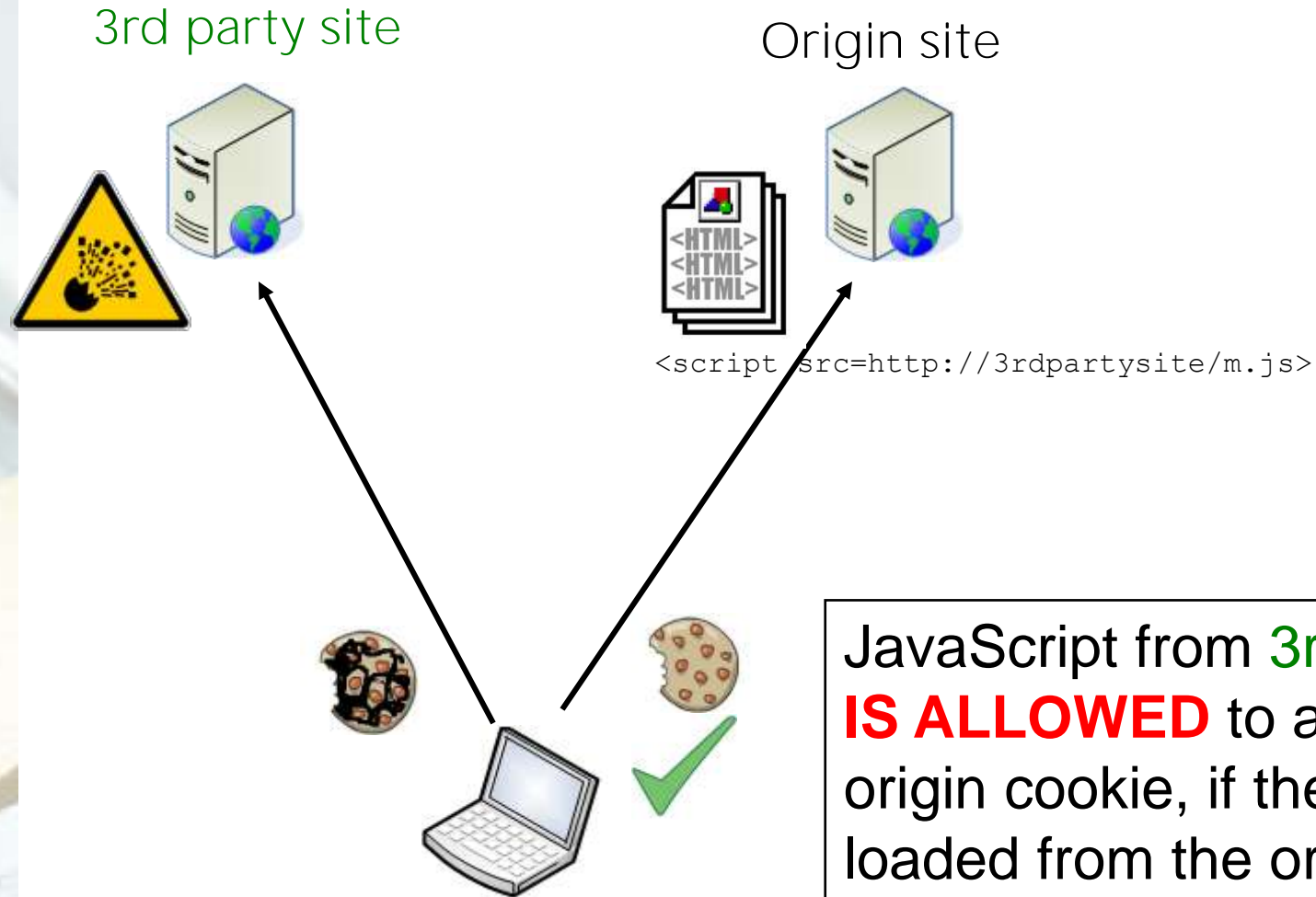
# Why by-passing SOP?



# Why by-passing SOP?

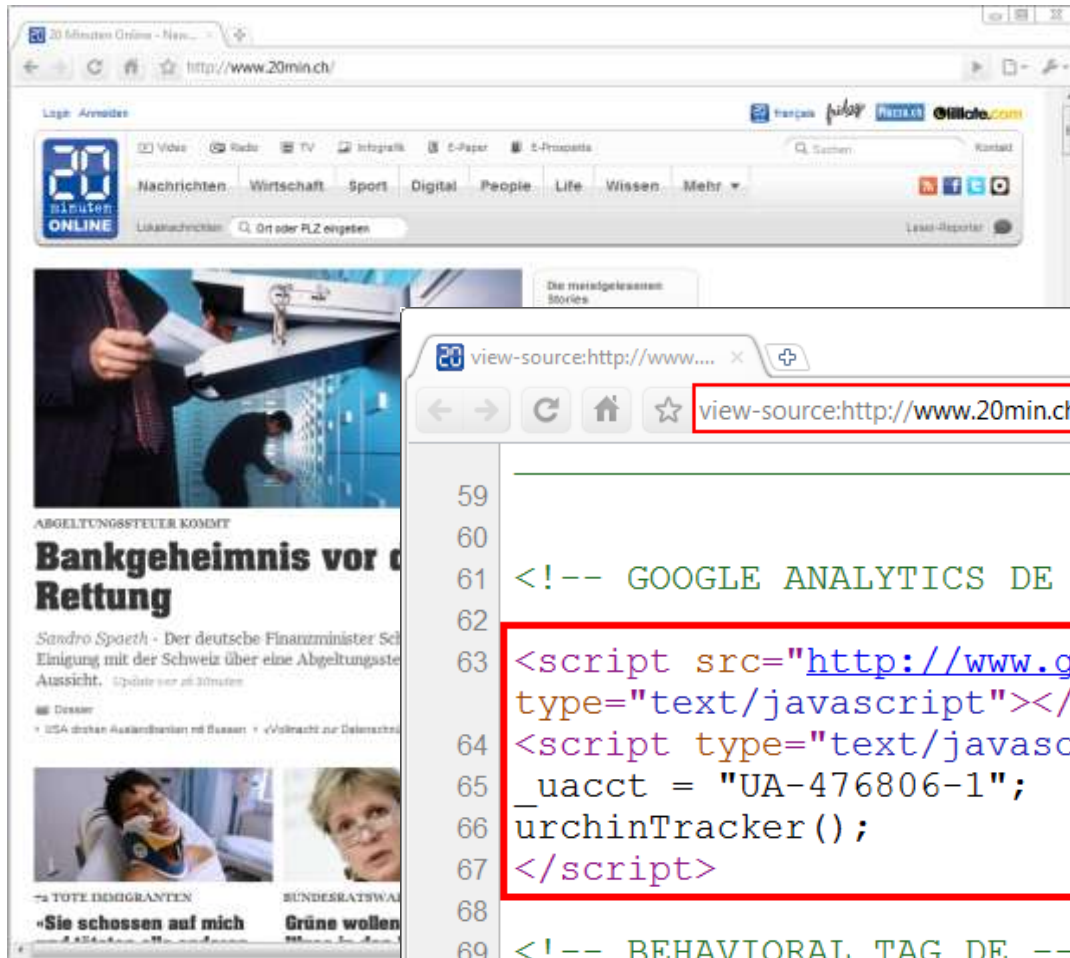


# Use Script from 3rd Party



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... x
view-source:http://www.20min.ch/
59
60
61 <!-- GOOGLE ANALYTICS DE -->
62
63 <script src="http://www.google-analytics.com/urchin.js"
64 type="text/javascript"></script>
65 <script type="text/javascript">
66 _uacct = "UA-476806-1";
67 urchinTracker();
68 </script>
69 <!-- BEHAVIORAL TAG DE -->
70
71 <!-- MEMO: ARRAY > AUTOFILL -->
72
```

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

A New Solution is Required!

# Cross-Origin Resource Sharing

CORS, a W3C Working Draft - 27 July 2010



# CORS Compatibility



XMLHttpRequest (XHR)



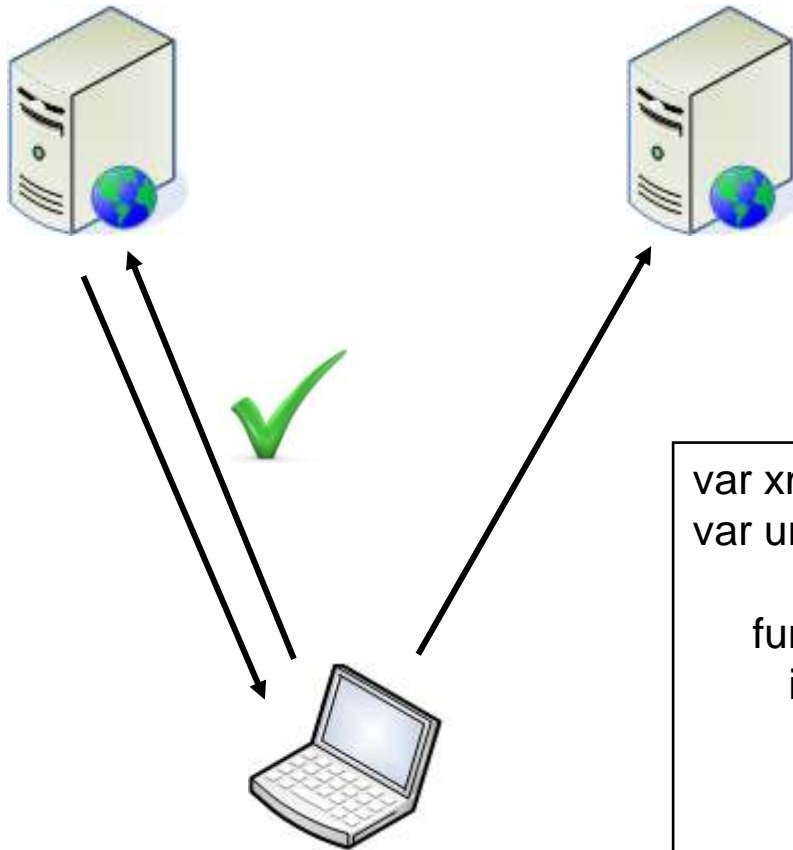
XDomainRequest (XDR)

# 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

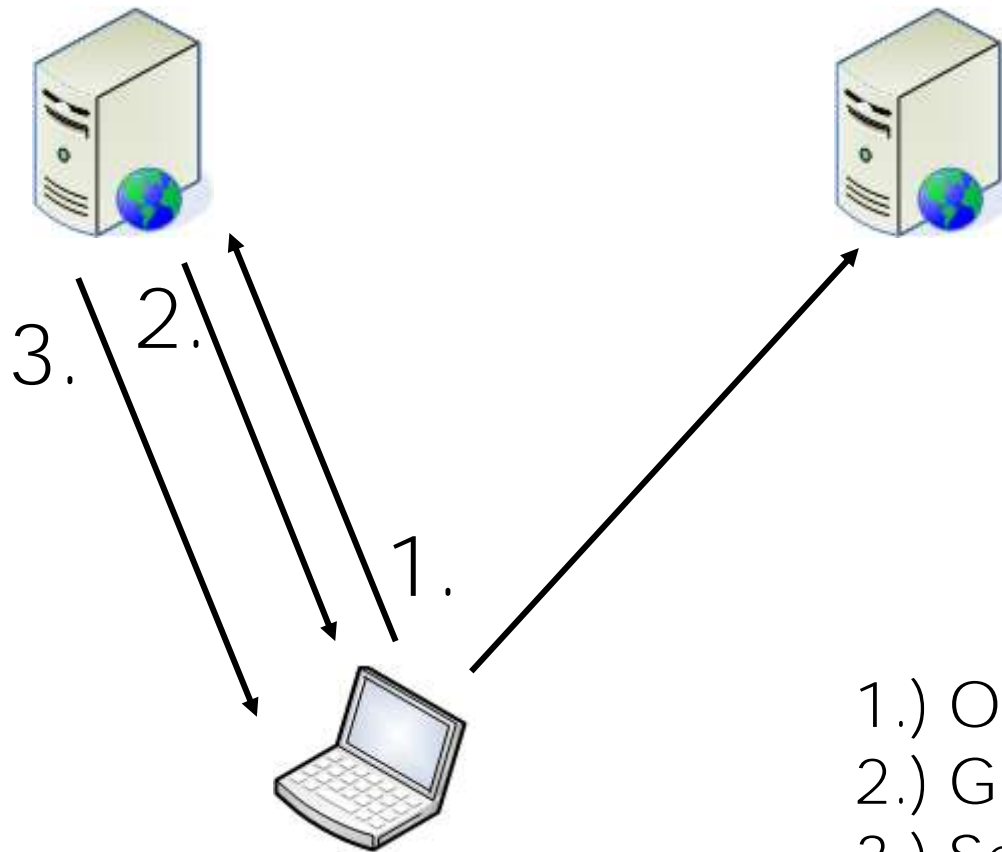
[XML Data]

# CORS Preflighted Request Example



www.other.com

www.origin.com



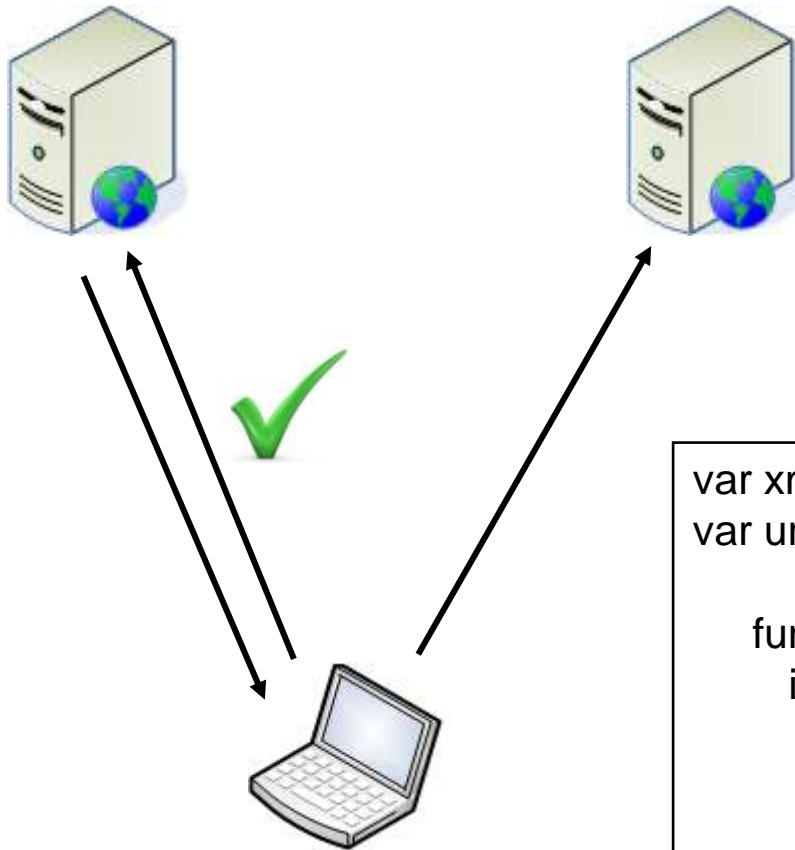
- 1.) OPTIONS Request
- 2.) GET / POST Request
- 3.) Server sends data

# 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/simpleXMLInvocation.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



CORS allows 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](https://developer.mozilla.org/En/HTTP_Access_Control)

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