

A vertical decorative image on the left side of the slide showing a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

HTML5 Web Security

Thomas Röthlisberger – IT Security Analyst
thomas.roethlisberger@csnc.ch

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

A vertical decorative image on the left side of the slide shows a magnifying glass with a wooden handle and a metal rim. The lens is focused on a yellow sticky note placed on a computer keyboard. The keyboard keys are light blue and white. A solid blue vertical bar is on the far left edge of the image.

What is this talk about?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

What is HTML5?

**Vulnerabilities, Threats
& Countermeasures**

Conclusion

Demo CORS

Demo Web Workers

Quiz and Q&A





The Voting Device

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

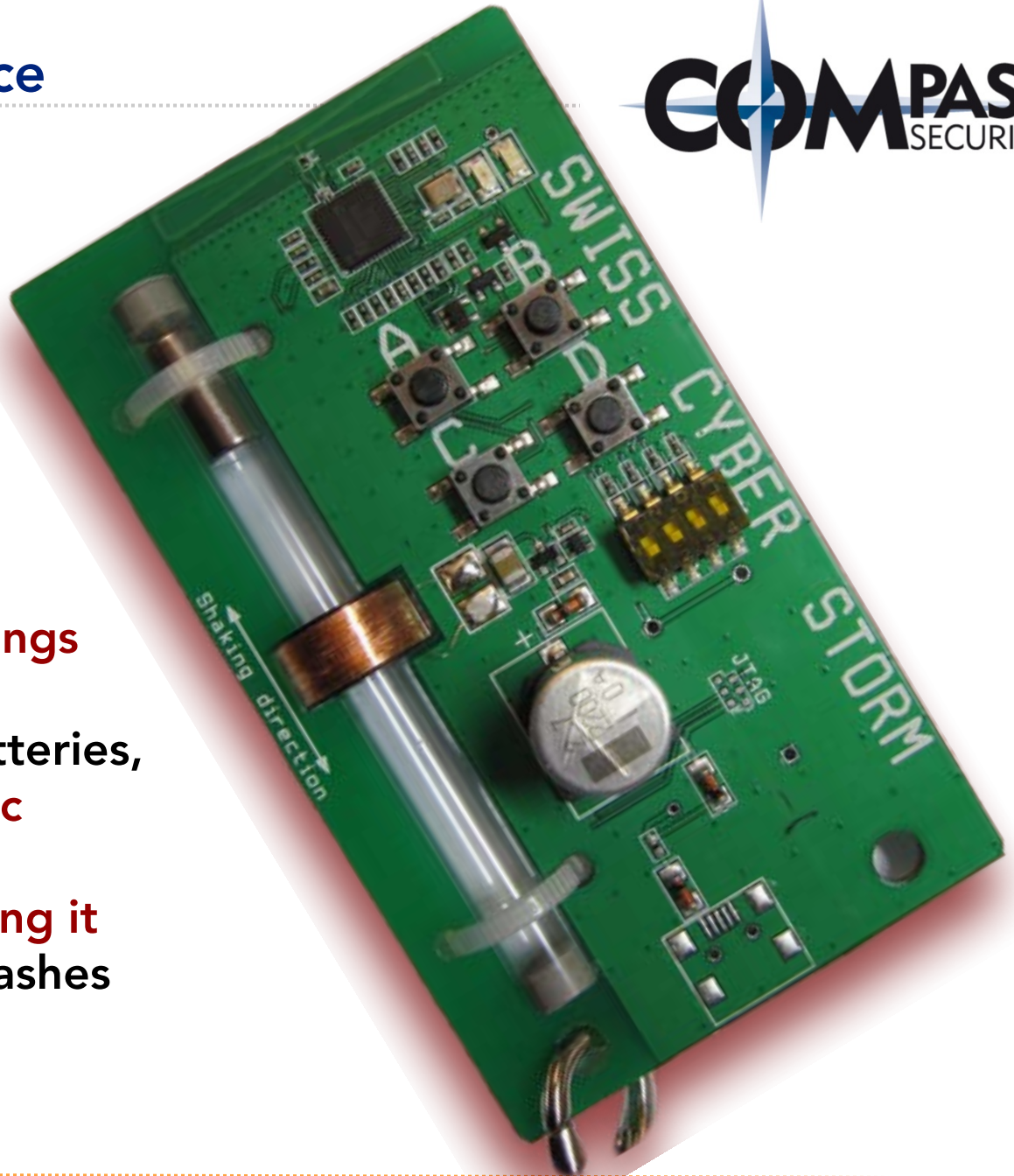
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

The Voting Device

It enables you to participate on **votings**

The device has no batteries, so it works **autarkic**

You power it by **shaking it** until green light flashes



The Voting



Let's give it a try...

An interactive voting interface on a black background. At the top left is a green PCB labeled "SWISS CYBER STORM" with a silver probe. In the center is the COMPASS SECURITY logo and the text "shake and test". At the top right is a white box with "HTML" in black, an orange stylized "G" logo, and a silver padlock. Below these is a large red arrow pointing right labeled "Question". Underneath are two rows of answer options, each consisting of a red arrow pointing left and a red arrow pointing right. The first row contains "Answer A" (left) and "Answer B" (right), with a small "A" and "B" between them. The second row contains "Answer C" (left) and "Answer D" (right), with a small "C" and "D" between them.

A vertical decorative image on the left side of the slide shows a close-up of a computer keyboard with a magnifying glass resting on it. A solid blue vertical bar is positioned to the left of the keyboard image.

What is HTML5?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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



HTML 4.01
XHTML 1.0
XHTML 1.1

 WHATWG



~~XHTML 2.0~~

~~Web Applications 1.0~~

HTML5

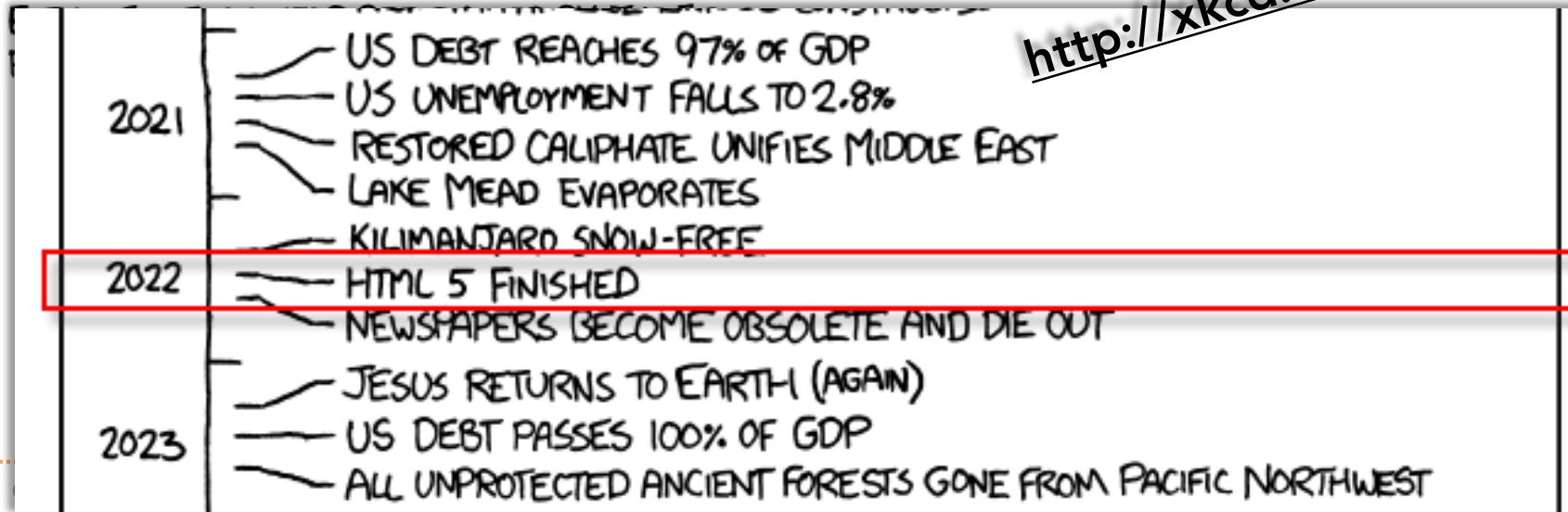


HTML5 is not finished!

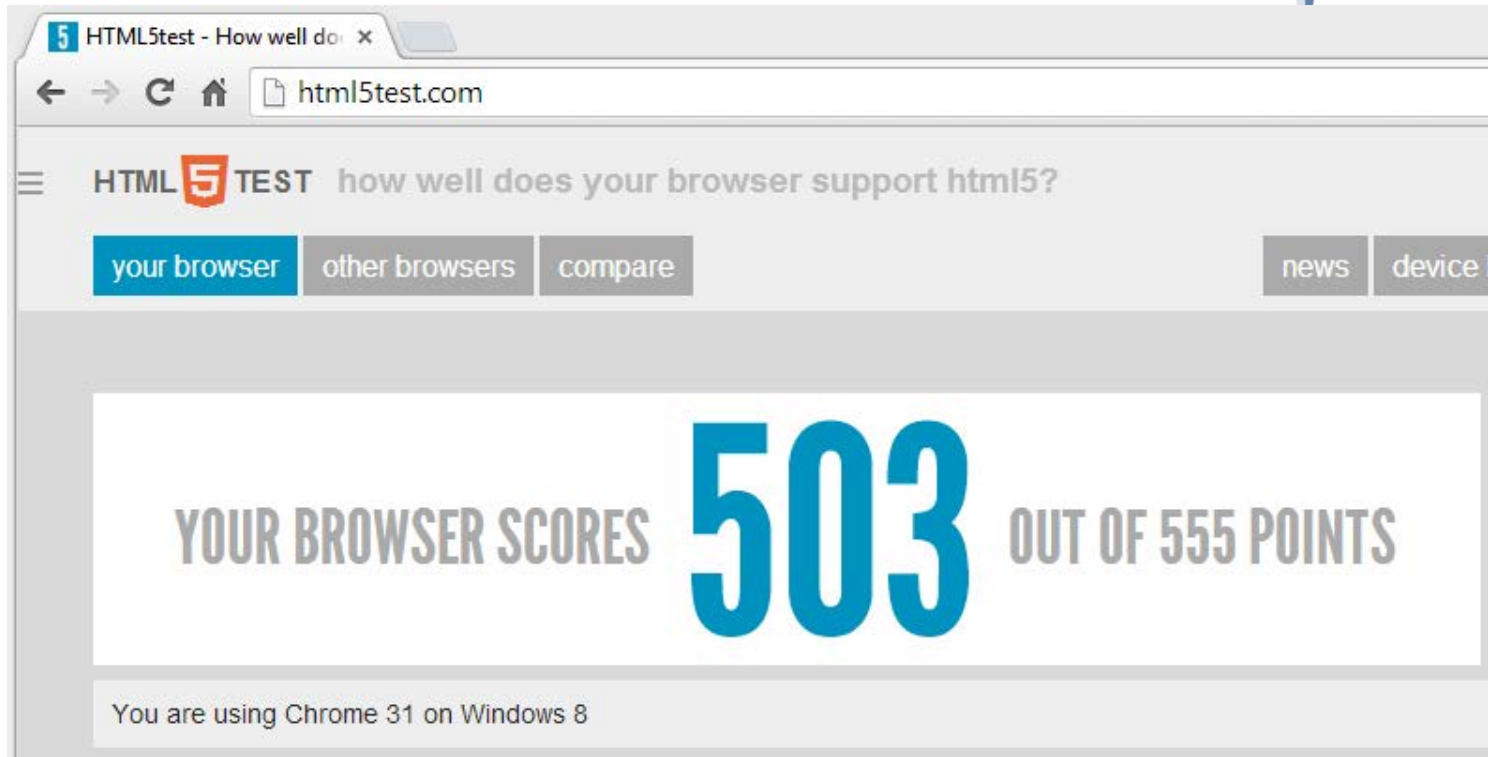
The specification achieved CANDIDATE RECOMMENDATION status on 17 December 2012. Newest version is from 6 August 2013.

However, it is still a draft version and may be updated.

THE FUTURE ACCORDING TO GOOGLE SEARCH RESULTS

A hand-drawn timeline titled "THE FUTURE ACCORDING TO GOOGLE SEARCH RESULTS". The timeline is a vertical line with horizontal branches pointing to the right, indicating events for the years 2021, 2022, and 2023. The year 2022 is highlighted with a red rectangular box. A URL "http://xkcd.com/887/" is written diagonally across the right side of the timeline.

2021	US DEBT REACHES 97% OF GDP
	US UNEMPLOYMENT FALLS TO 2.8%
	RESTORED CALIPHATE UNIFIES MIDDLE EAST
	LAKE MEAD EVAPORATES
	KILIMANJARO SNOW-FREE
2022	HTML 5 FINISHED
	NEWSPAPERS BECOME OBSOLETE AND DIE OUT
	JESUS RETURNS TO EARTH (AGAIN)
2023	US DEBT PASSES 100% OF GDP
	ALL UNPROTECTED ANCIENT FORESTS GONE FROM PACIFIC NORTHWEST

A screenshot of a web browser displaying the HTML5 Test website. The browser's address bar shows "html5test.com". The page title is "HTML5 TEST how well does your browser support html5?". Below the title are navigation buttons: "your browser" (highlighted in blue), "other browsers", "compare", "news", and "device". The main content area displays "YOUR BROWSER SCORES 503 OUT OF 555 POINTS" in large blue and grey text. At the bottom of the screenshot, it says "You are using Chrome 31 on Windows 8".

Browser	Score
Chrome 31	503
Firefox 25	447
Internet Explorer 11	377
Android 4.4	424
iOS 7.0	415

503

Chrome 31

447

Firefox 25

377

Internet Explorer 11

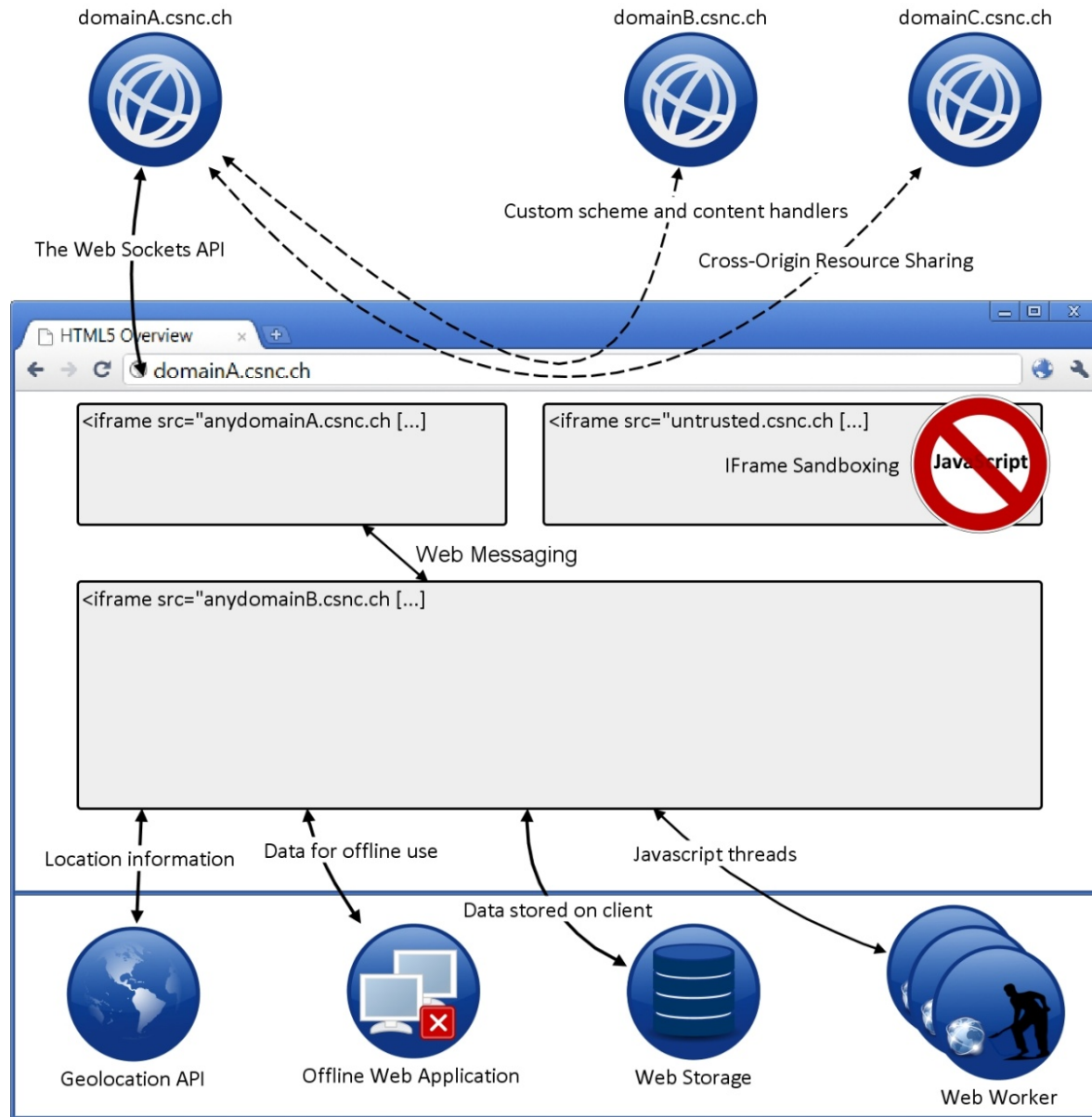
424

Android 4.4

415

iOS 7.0

Overview



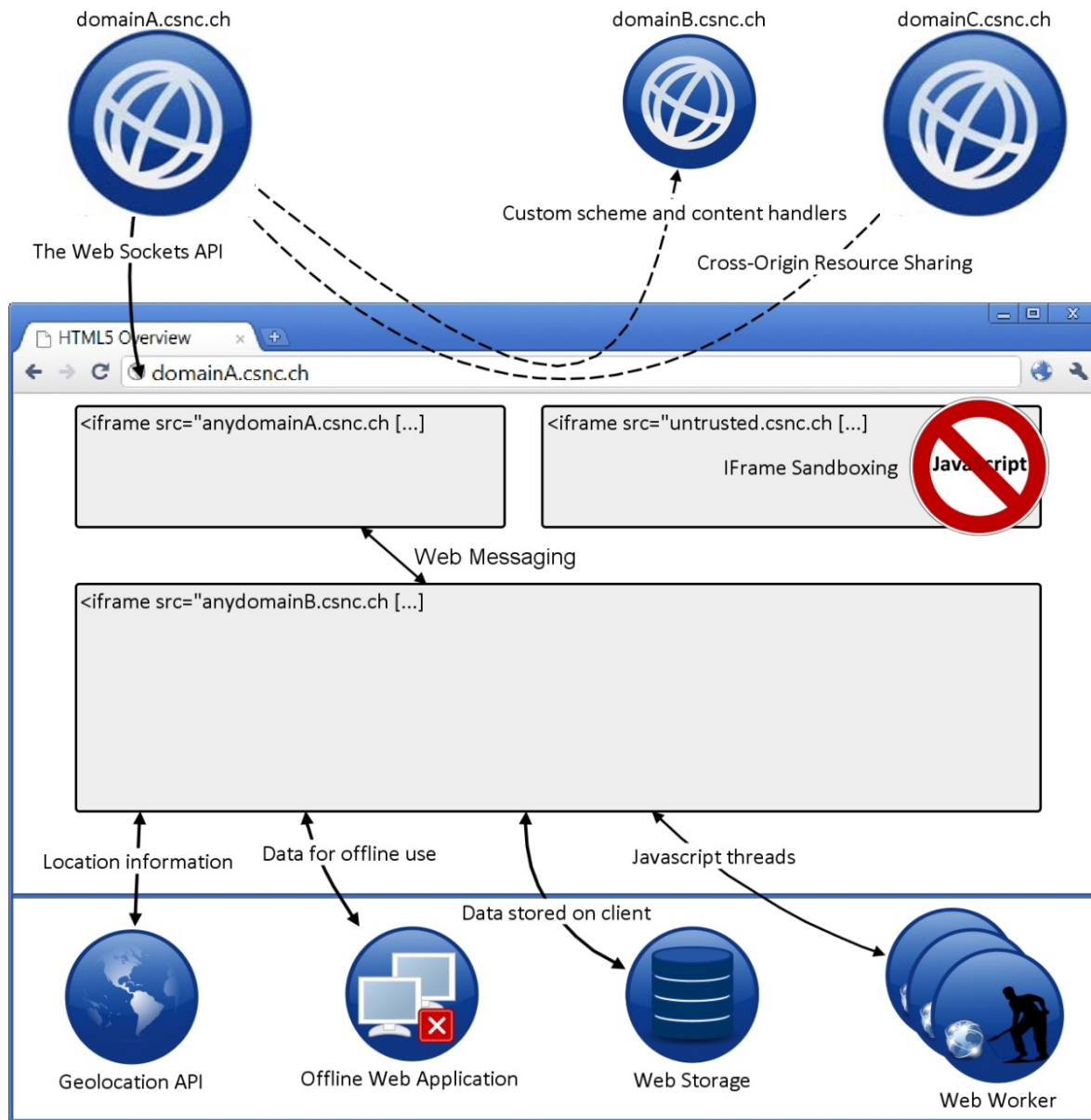
A vertical decorative image on the left side of the slide shows a close-up of a computer keyboard with a magnifying glass resting on it. A solid blue vertical bar is positioned to the left of the keyboard image.

Vulnerabilities, Threats and Countermeasures *(if any)*

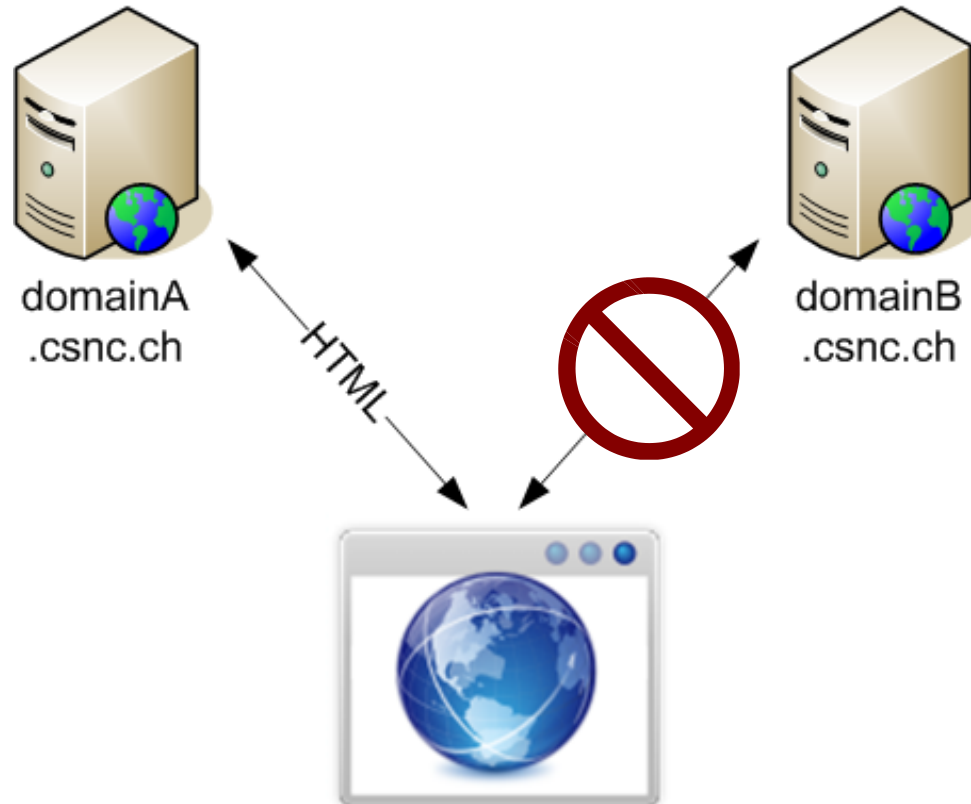
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Cross-Origin Resource Sharing



Cross-Origin Resource Sharing I



Cross-Origin Resource Sharing II



GET / HTTP/1.1

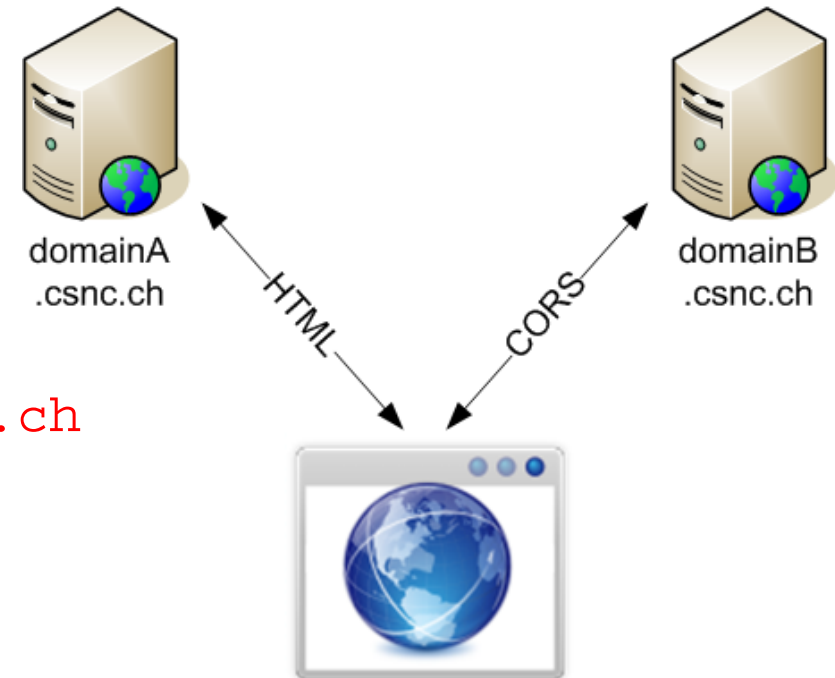
Host: **domainB.csnc.ch**

Origin: **http://domainA.csnc.ch**

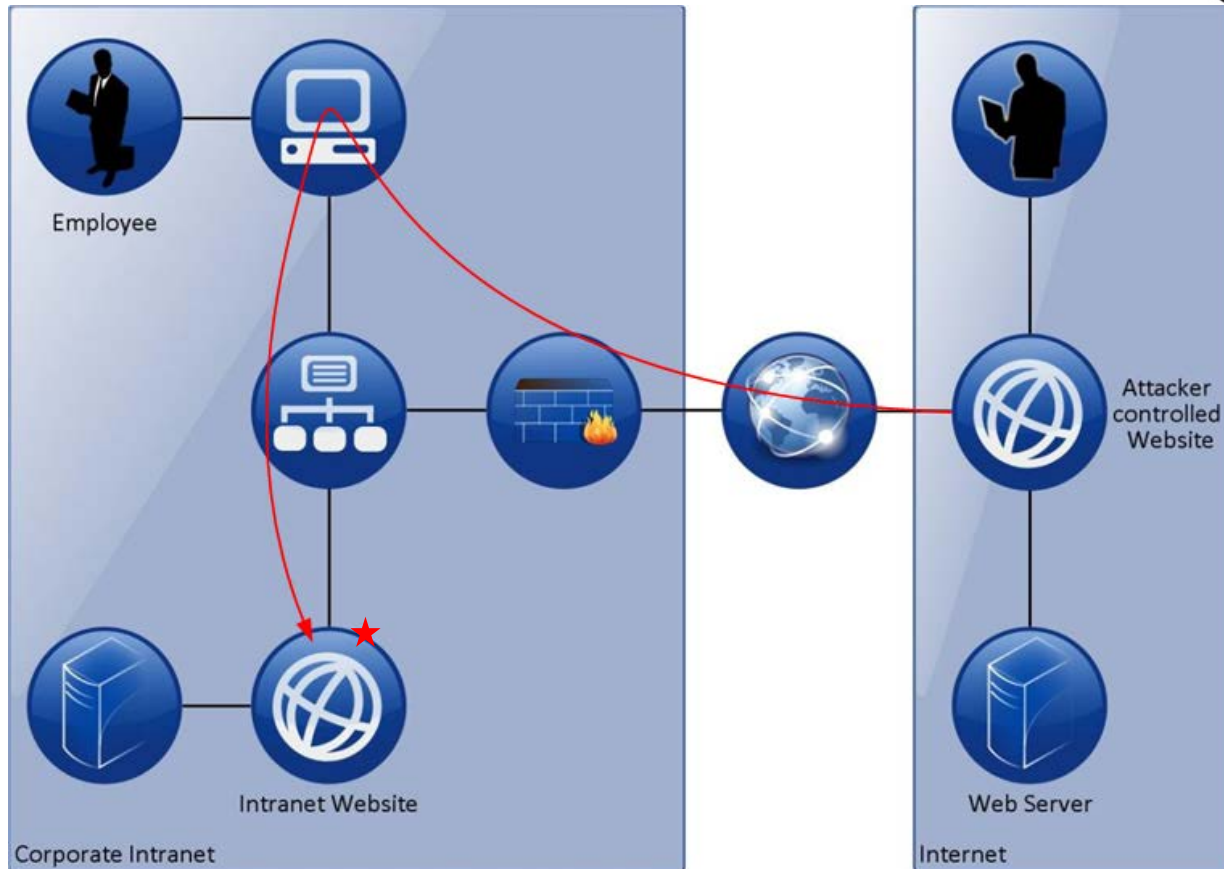
HTTP/1.1 200 OK

Content-Type: text/html

Access-Control-Allow-Origin: **http://domainA.csnc.ch**



CORS – Vulnerabilities & Threats I



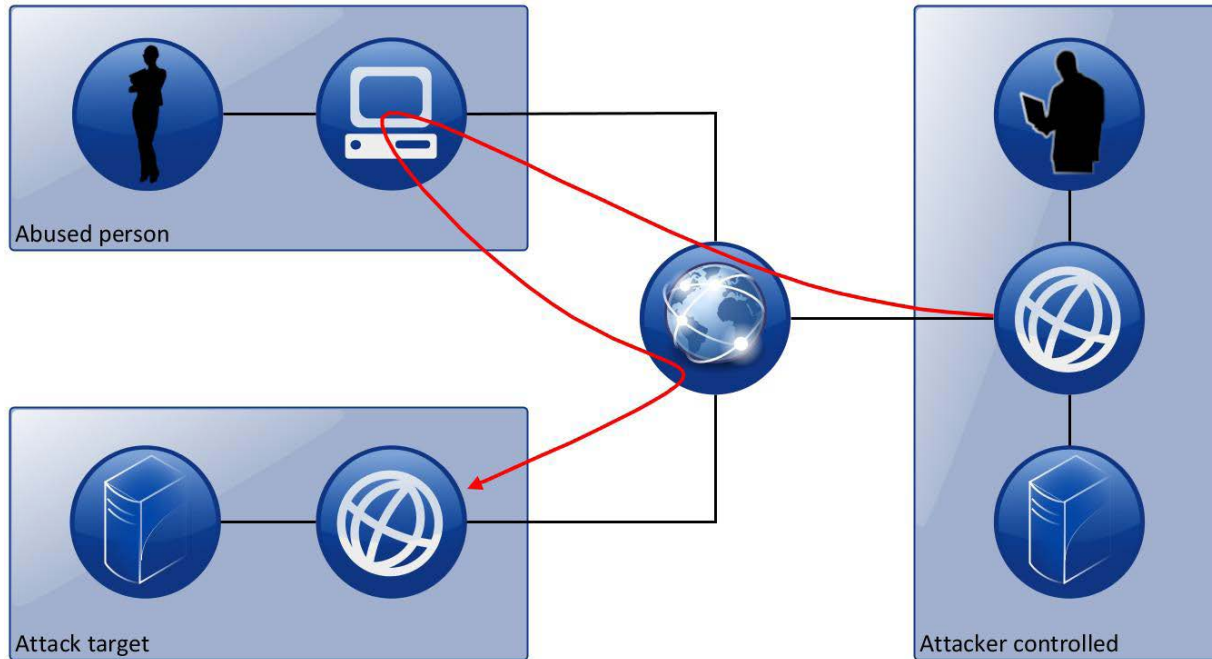
Accessing internal websites



Scanning the internal network



CORS – Vulnerabilities & Threats II



Remote attacking a web server



Easier exploiting of Cross-Site Request Forgery (XSRF)



Establishing a remote shell (*DEMO*)



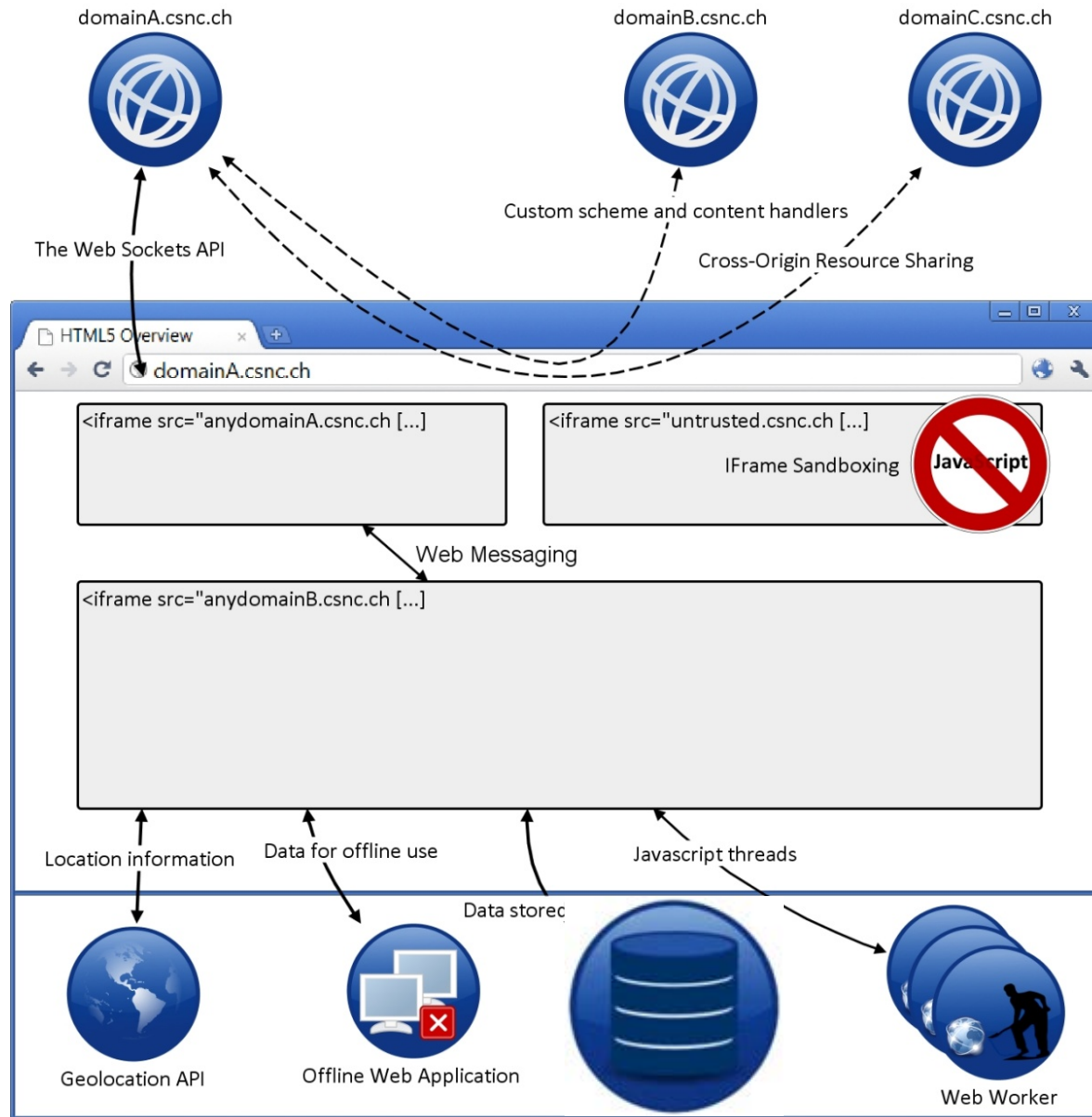
Use the `Access-Control-Allow-Origin` header to restrict the allowed domains.

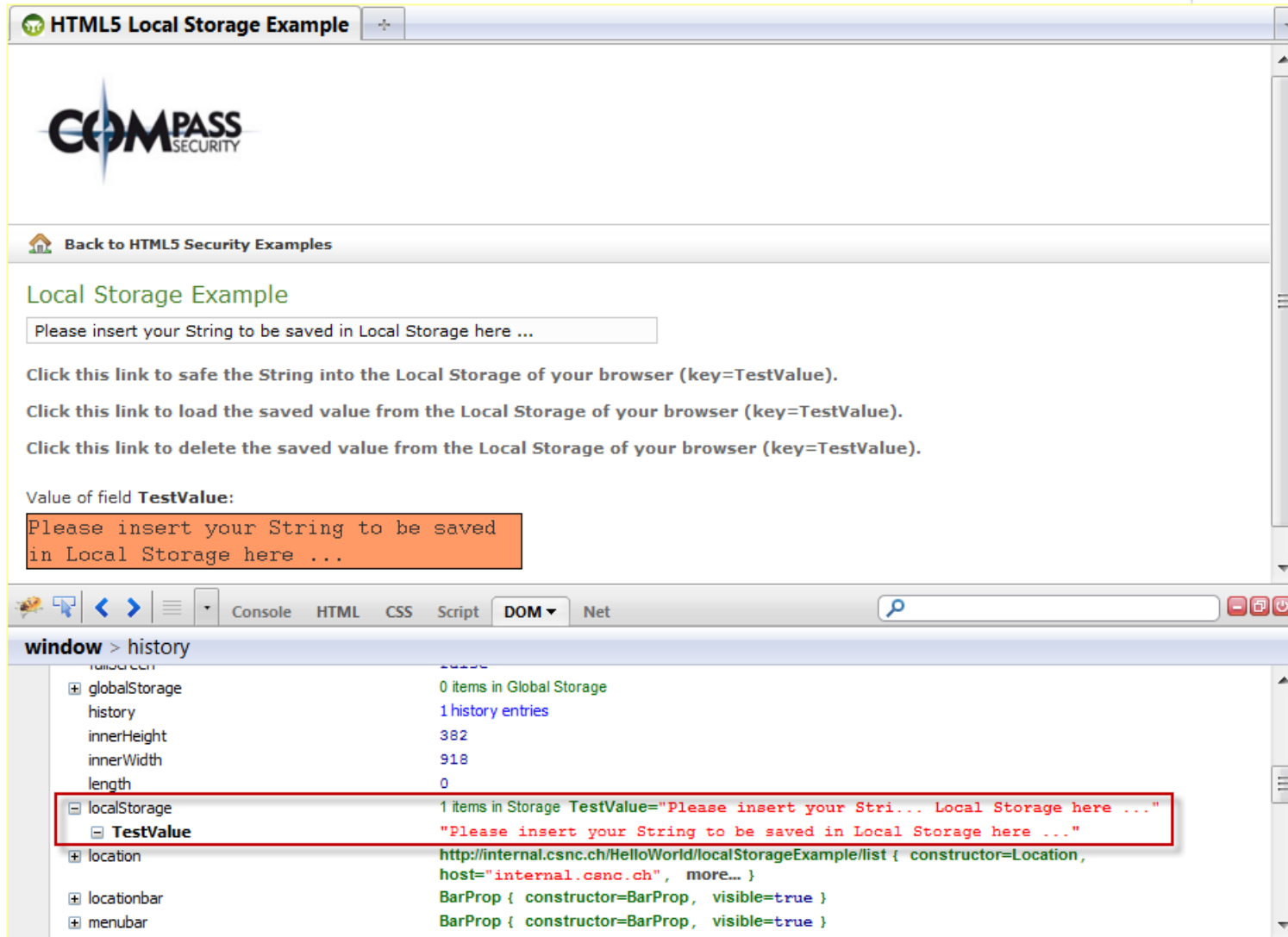
Never set the header to `*`.

Do not base access control on the origin header.

To mitigate DDoS attacks the Web Application Firewall (WAF) needs to block CORS requests if they arrive in a high frequency.

Web Storage





The screenshot shows a web browser window titled "HTML5 Local Storage Example". The page content includes the COMPASS SECURITY logo, a "Back to HTML5 Security Examples" link, and a section titled "Local Storage Example". This section contains a text input field with the placeholder text "Please insert your String to be saved in Local Storage here ...". Below the input field are three instructions: "Click this link to save the String into the Local Storage of your browser (key=TestValue).", "Click this link to load the saved value from the Local Storage of your browser (key=TestValue).", and "Click this link to delete the saved value from the Local Storage of your browser (key=TestValue).".

Below the instructions, the text "Value of field TestValue:" is followed by a highlighted orange box containing the text: "Please insert your String to be saved in Local Storage here ...".

The browser's developer console is open, showing the "DOM" tab. The "window" object is expanded to show the "localStorage" property, which contains one item: "TestValue". The value of "TestValue" is highlighted in a red box and matches the text in the orange box above: "Please insert your String to be saved in Local Storage here ...".



Session Hijacking



- ✦ If session identifier is stored in local storage, it can be stolen with JavaScript.
- ✦ No *HTTPOnly* flag.

Disclosure of Confidential Data



- ✦ If sensitive data is stored in the local storage, it can be stolen with JavaScript.

User Tracking



- ✦ Additional possibility to identify a user.

Persistent attack vectors



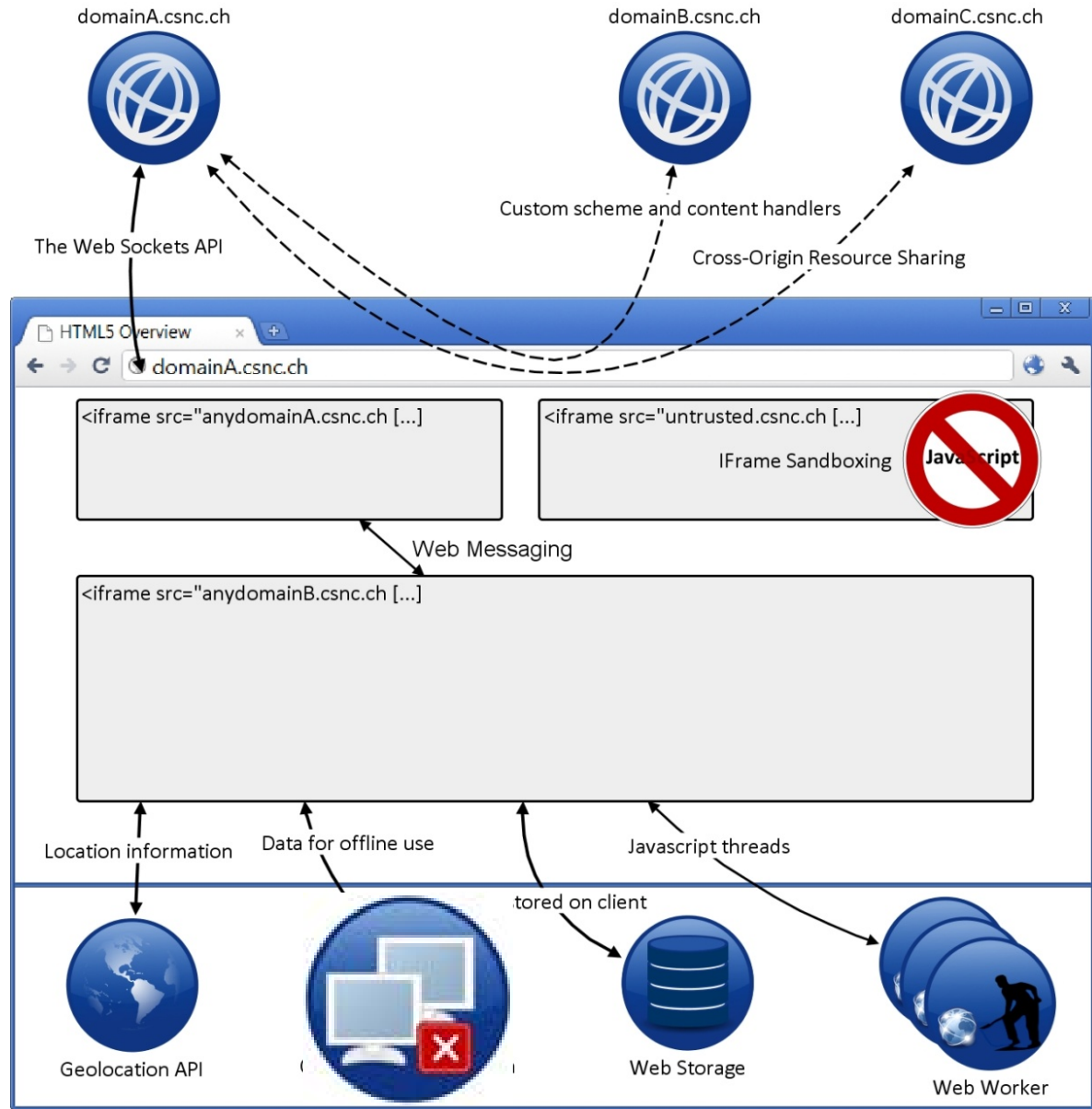
- ✦ Attack vectors can be stored persistently in the victim's browser.



Use cookies instead of Local Storage for session handling.

Do not store sensitive data in Local Storage.

Offline Web Application



```
<!DOCTYPE HTML>  
<html manifest="/cache.manifest">  
<body>  
...
```

Example **cache.manifest**

```
CACHE MANIFEST  
/style.css  
/helper.js  
/csnc-logo.jpg  
NETWORK:  
/visitor_counter.jsp  
FALLBACK:  
/ /offline_Error_Message.html
```



Cache Poisoning



- ✦ Caching of the root directory possible.
- ✦ HTTP and HTTPS caching possible.

Persistent attack vectors



- ✦ Attack vectors can be stored persistently in the victim's browser.

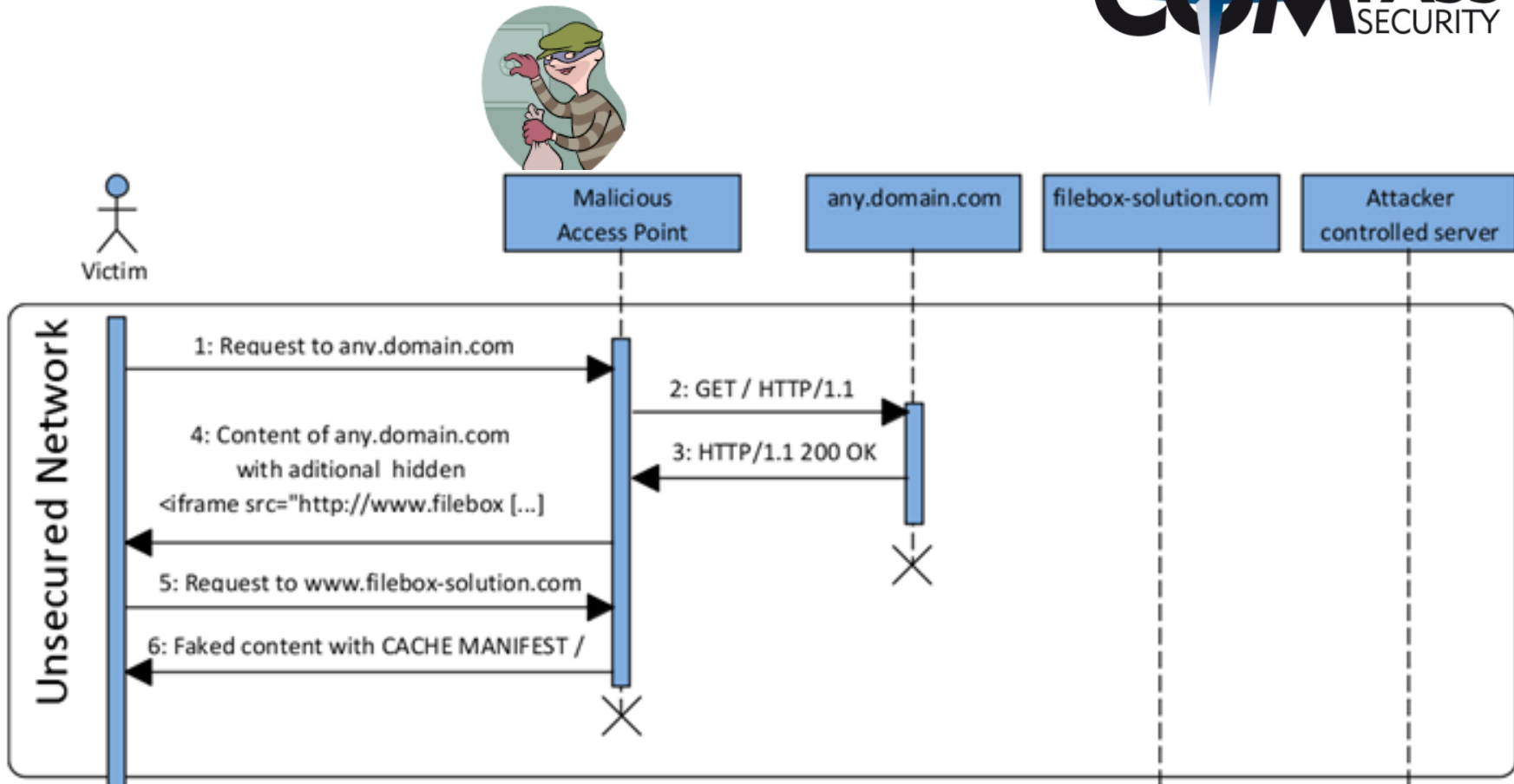
User Tracking



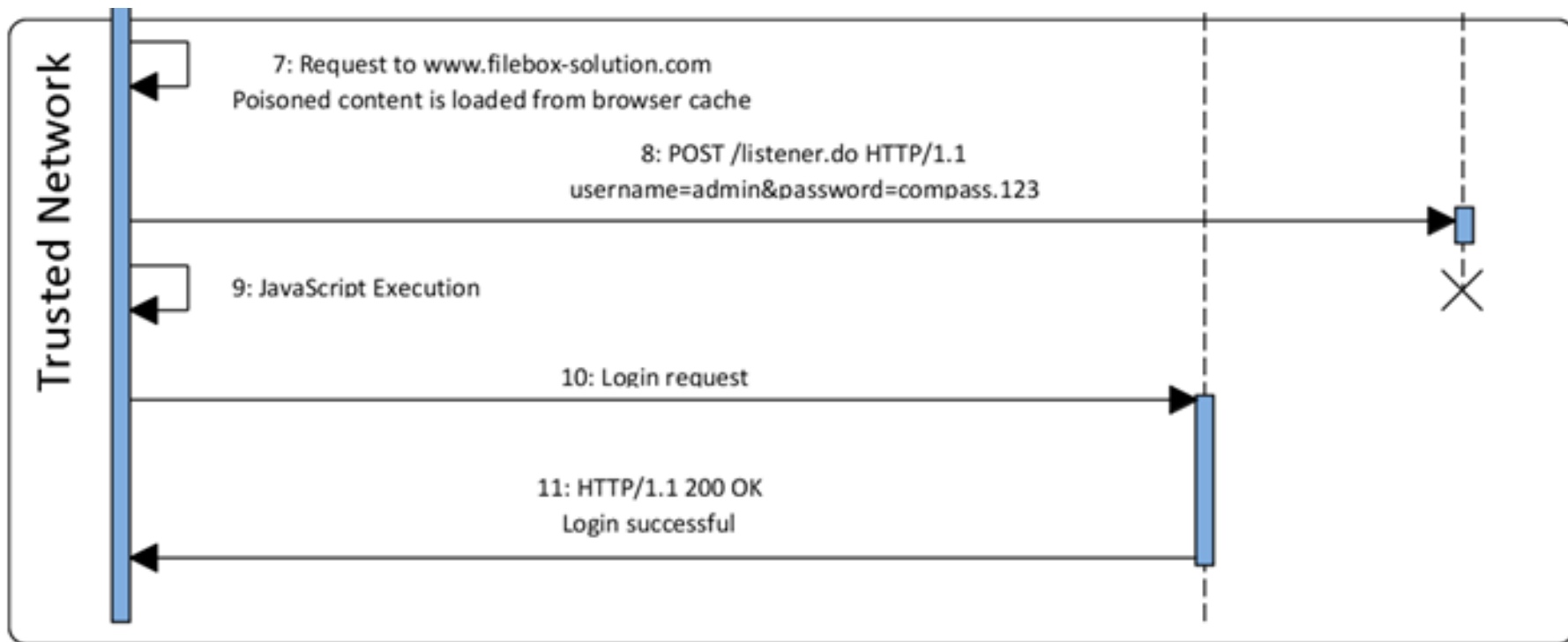
- ✦ Additional possibility to identify a user.
- ✦ Unique identifiers could be stored along with the cached files.



Offline Web Application – Attack 1/2



Offline Web Application – Attack 2/2

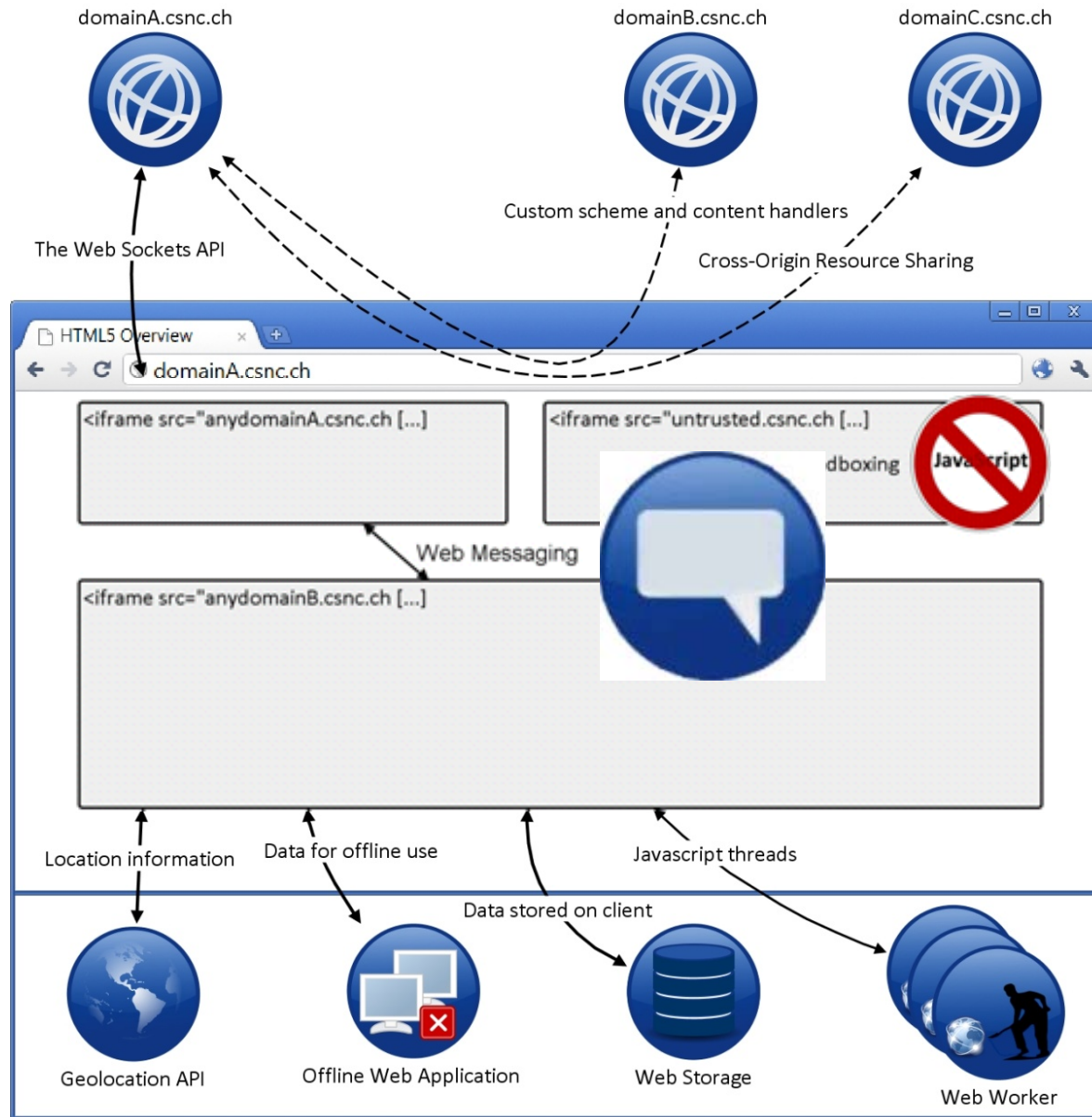


User Training

=> Do not accept caching of web applications!

=> Clear the cache including Local Storage and Offline Web Applications!

Web Messaging



Embedding HTML Page
html5demos.com

`postMessage()`



`<IFrame src="jsbin.com" [...]`

Send Message:

```
var win =  
document.getElementById("iframe").contentWindow;  
win.postMessage(  
    document.getElementById("message").value,  
    "http://jsbin.com"  
);
```



Embedding HTML Page
html5demos.com

postMessage()



<IFrame src="jsbin.com" [...]

Receive Message:

```
window.onmessage = function(e){  
    if ( e.origin !== "http://html5demos.com" ) {  
        return;  
    }  
    document.getElementById("test").innerHTML =  
    e.origin + " said: " + e.data;  
};
```



Embedding HTML Page
html5demos.com

postMessage()



<IFrame src="jsbin.com" [...]

Stealing confidential data



- ★ Sensitive data may be sent accidentally to a malicious IFrame.

Expands attack surface to the client



- ★ IFrames can send malicious content to other IFrames.
- ★ Input validation on the server is not longer sufficient.



Web Messaging - DEMO



Embedding HTML Page
html5demos.com

postMessage()



```
<IFrame src="jsbin.com" [...]
```

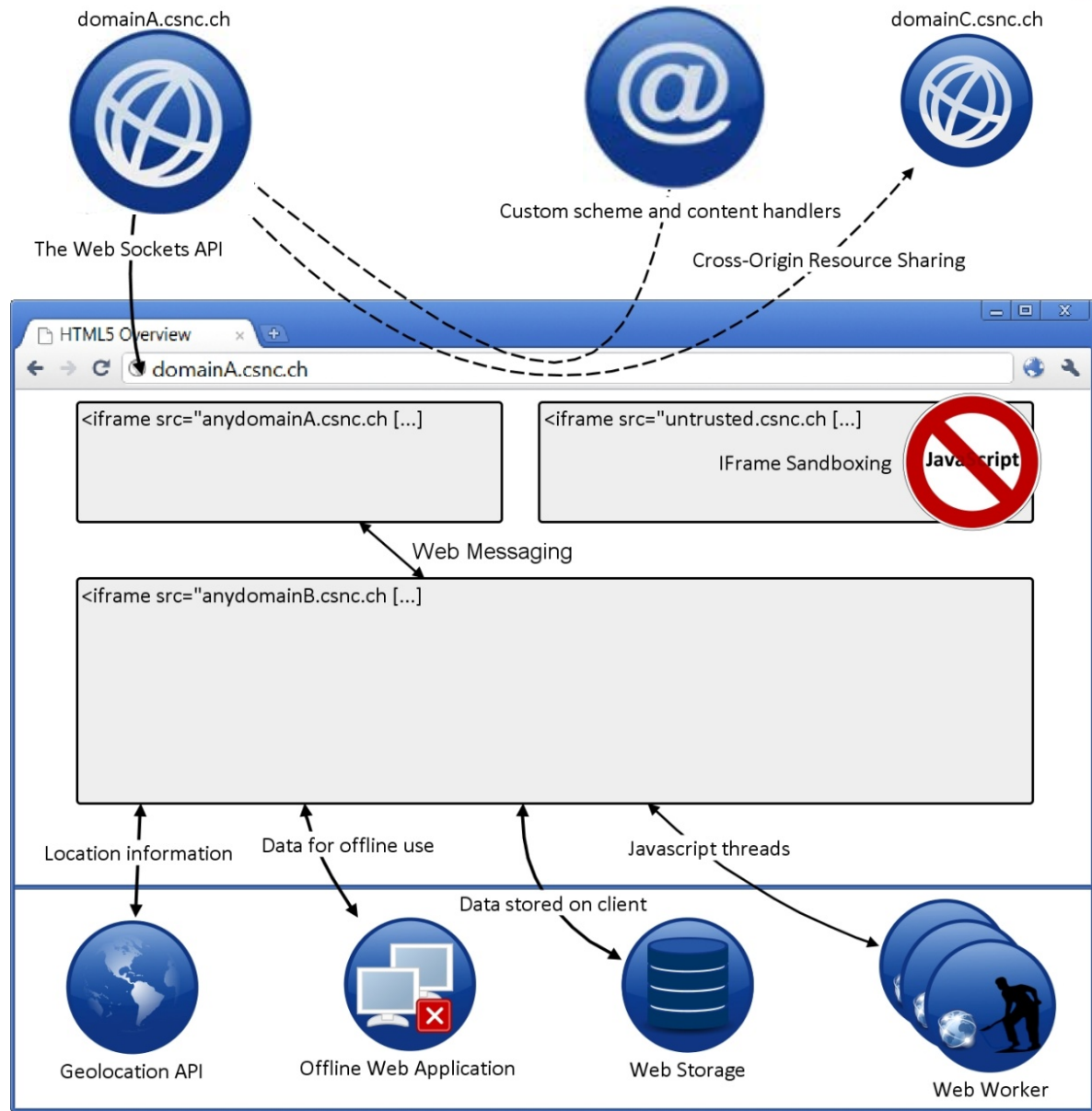


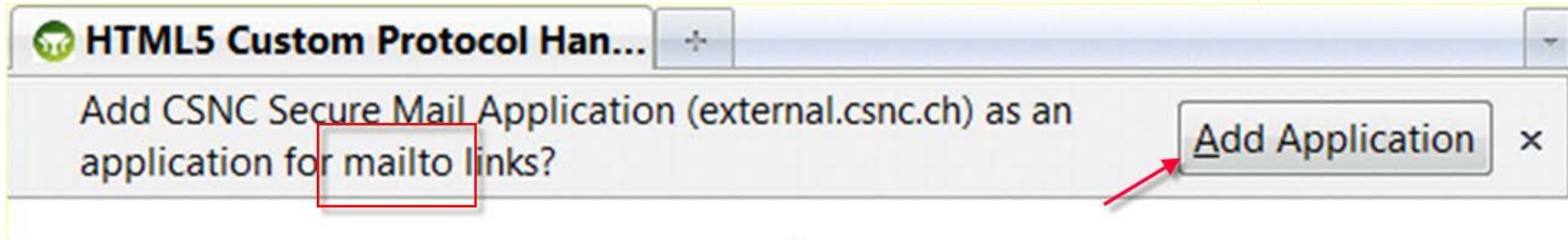
The target in `postMessage()` should be defined explicitly and not set to `*`.

The receiving `IFrame` should not accept messages from any domain. E.g. `e.origin == "http://internal.csnc.ch"`

The received message needs to be validated on the client to avoid malicious content being executed.

Custom scheme and content handlers





Stealing confidential data



- ★ An attacker tricks the user to register a malicious website as the e-mail protocol handler.
- ★ Sending e-mails through this web application gives the attacker access to the content of the e-mail.

User Tracking



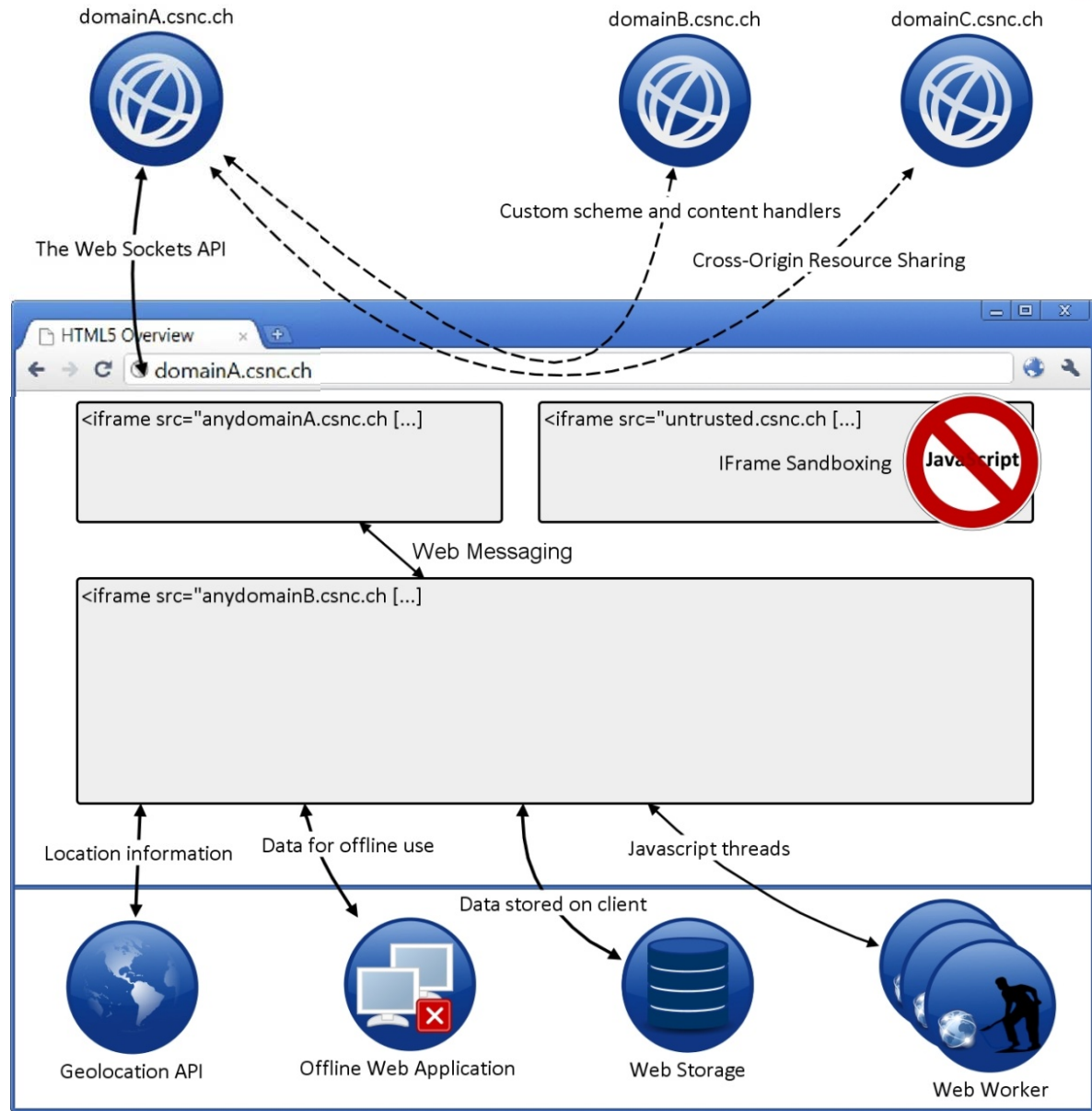
- ★ Additional possibility to identify a user.
- ★ Unique identifiers could be stored along with the protocol handler.



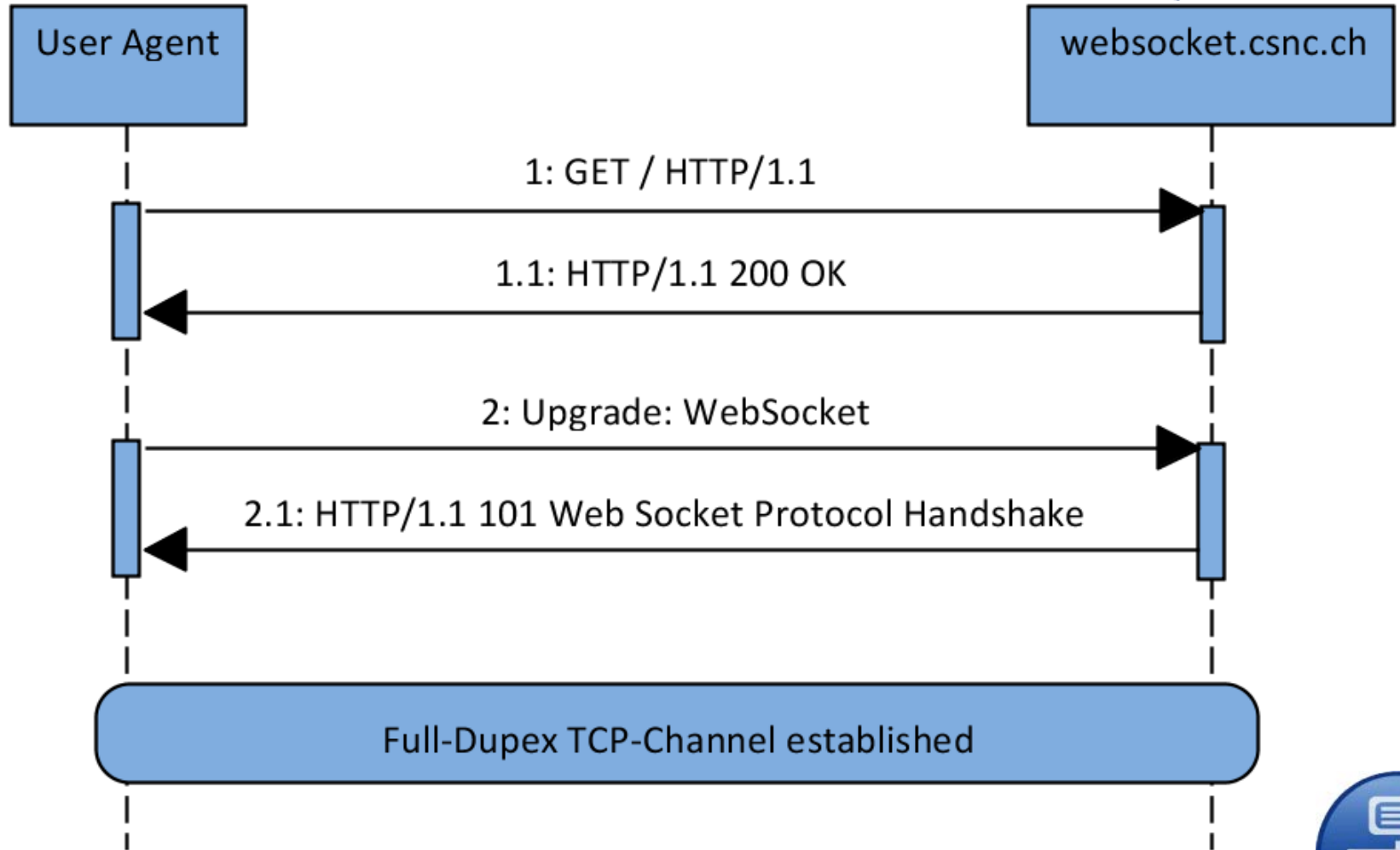
User Training

=> Do not accept registration of protocol handlers!

Web Sockets API



Web Sockets API



Cache Poisoning



- ★ A misunderstanding proxy could lead to a cache poisoning vulnerability.
- Fixed by introducing masking of the web socket data frames.

Scanning the internal network



- ★ The browser of a victim can be used for port scanning of internal networks.

Establishing a remote shell



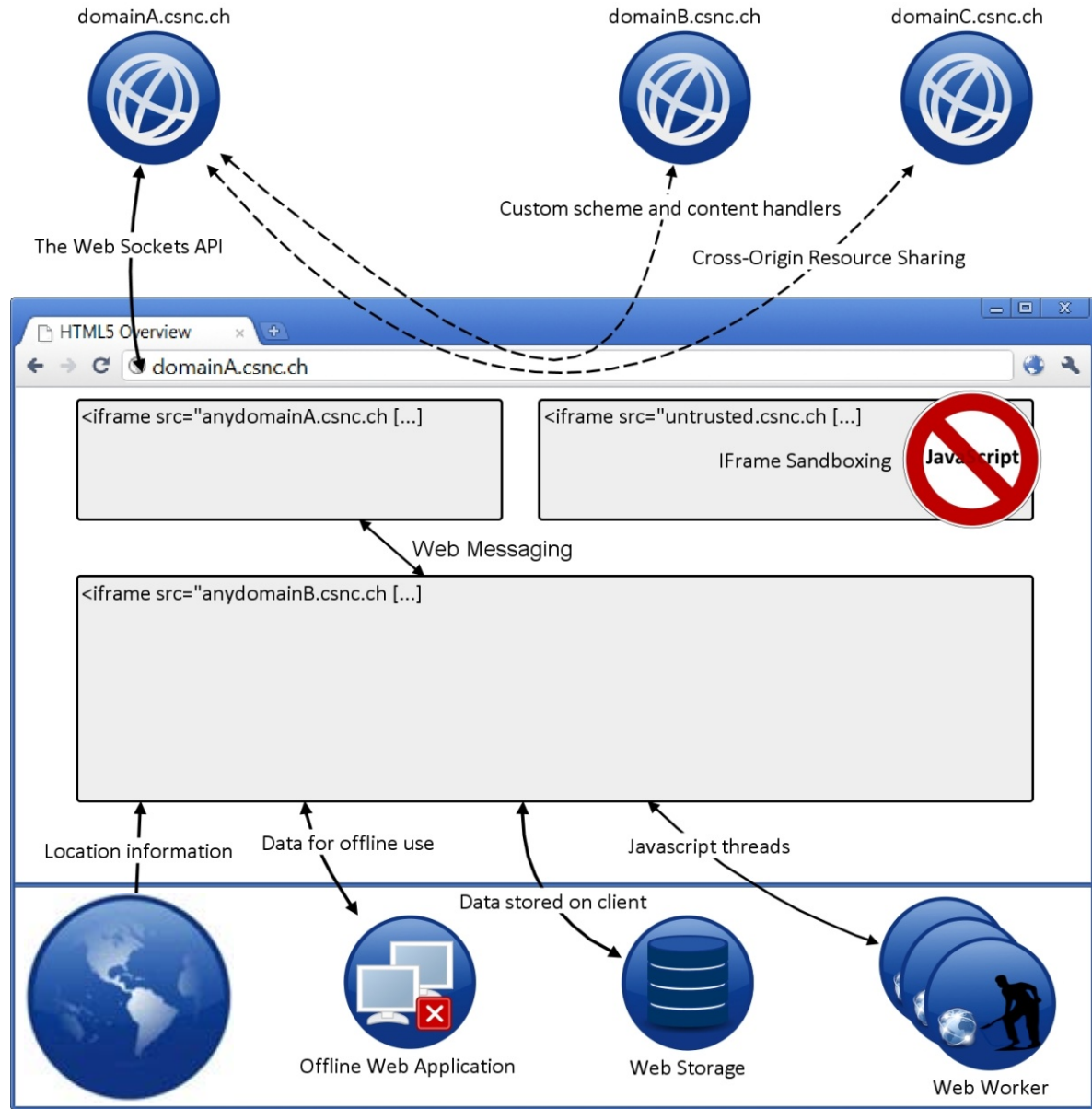
- ★ Web Sockets can be used to establish a remote shell to a victim's browser.



The risks of the Web Sockets API needs to be accepted.

The user could disable it in the browser.

Geolocation API



Geolocation API



Finding your location: **found you!**



User Tracking



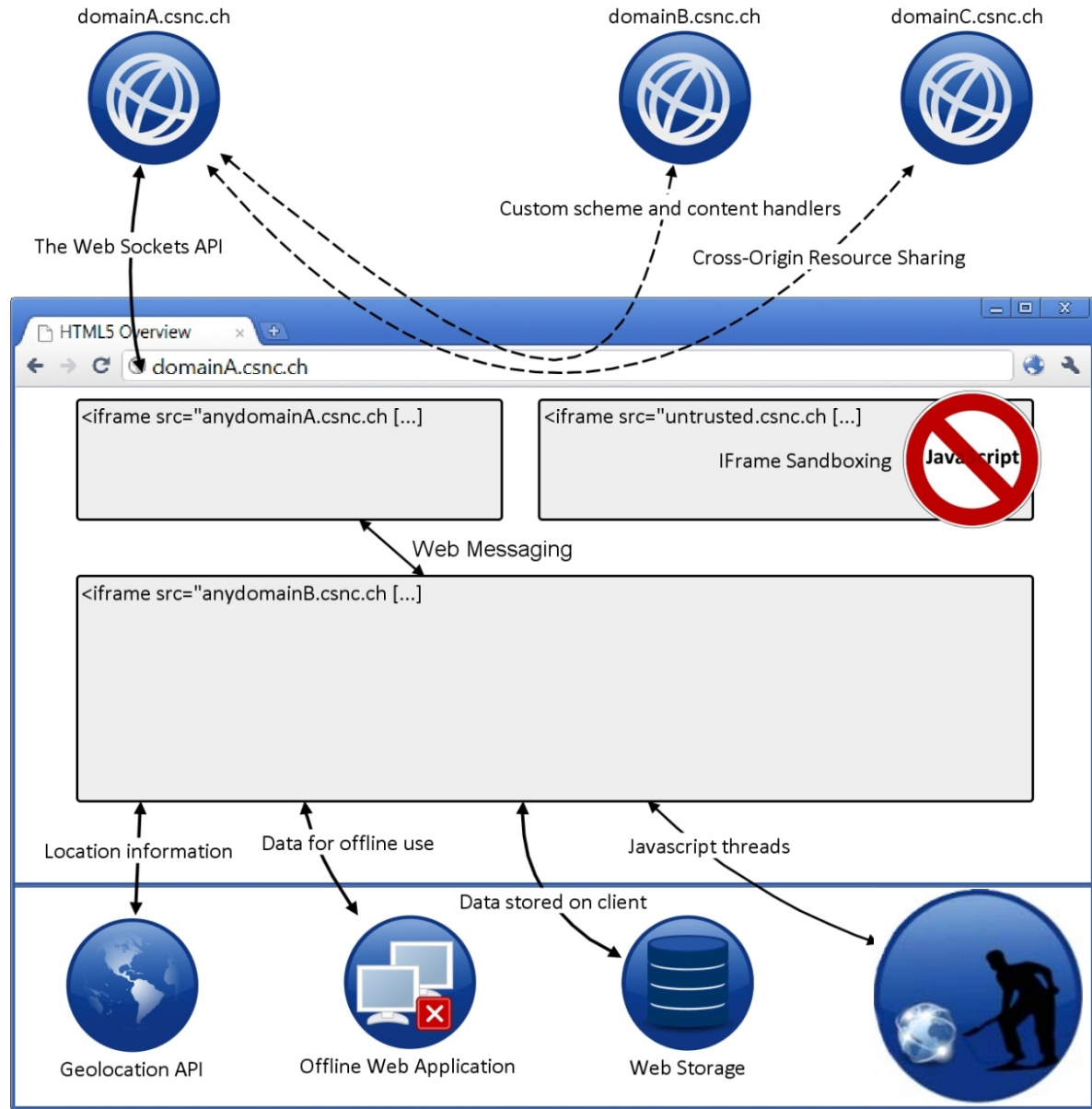
- ◆ User tracking based on the location of a user.
- ◆ If users are registered, their physical movement profile could be tracked.
- ◆ The anonymity of users could be broken.



User Training

=> Do not accept to share location information!

Web Workers



Web Workers provide the possibility for JavaScript to run in the background

Prior to Web Workers using JavaScript for long processing jobs was not feasible because

- ✦ it is slower than native code and
- ✦ the browsers freezes till the processing is completed

Web Workers alone are not a security issue.

But they can be used indirectly for launching work intensive attacks without the user noticing it.

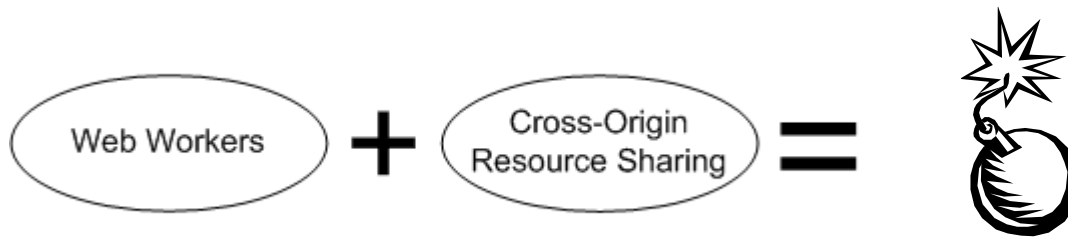


Worst Case Scenarios

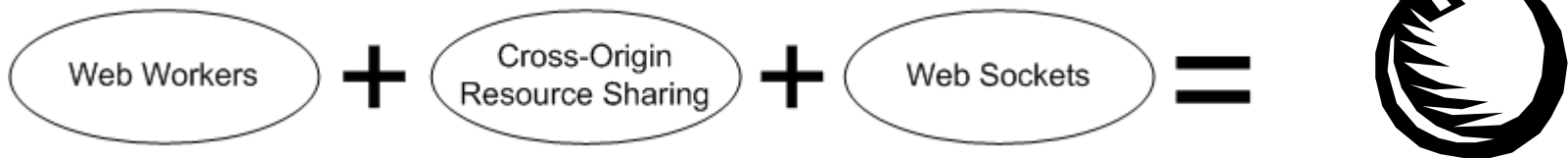


Web Workers = *Feature!*

Cracking Hashes in JS Cloud (*DEMO*).



Powerful DDoS attacks.



Web-based Botnet.

A vertical decorative image on the left side of the page shows a close-up of a computer keyboard with a magnifying glass resting on it. A solid blue vertical bar is positioned to the left of the keyboard image.

Conclusion

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona


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

A vertical decorative image on the left side of the slide. It shows a close-up of a computer keyboard with a magnifying glass resting on it. The magnifying glass is focused on a yellow sticky note placed on a key. The background is a soft-focus view of the keyboard keys.

Some HTML5 features are the vulnerabilities themselves.

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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



**Not all issues can be mitigated through
secure server-side implementation.**

Cross-Site Scripting (XSS) becomes even worse.

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

USE IE 6



Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

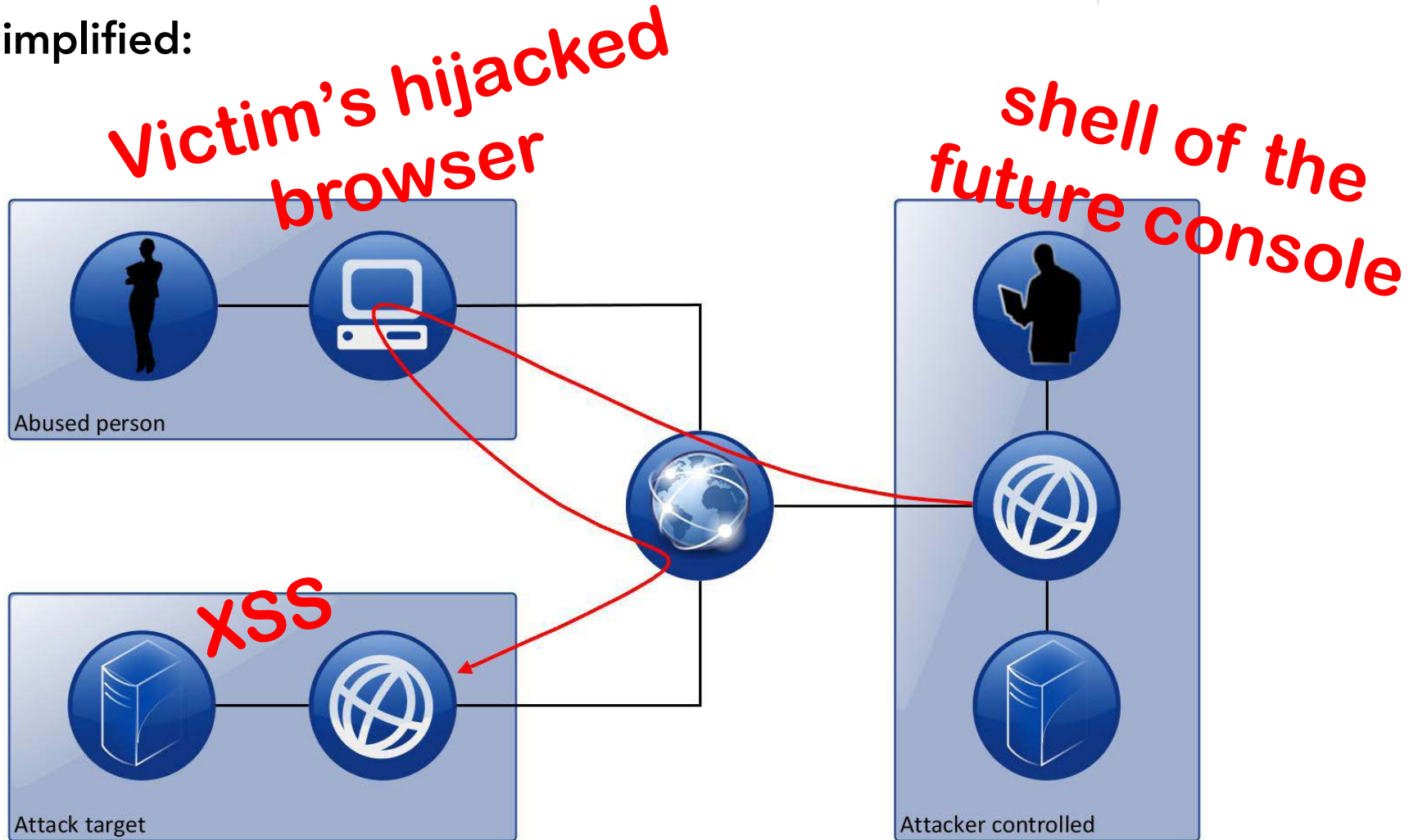
DEMO – Exploiting Cross-Origin Resource Sharing

Shell of the Future

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Simplified:



DEMO – Exploiting Web Workers

Ravan

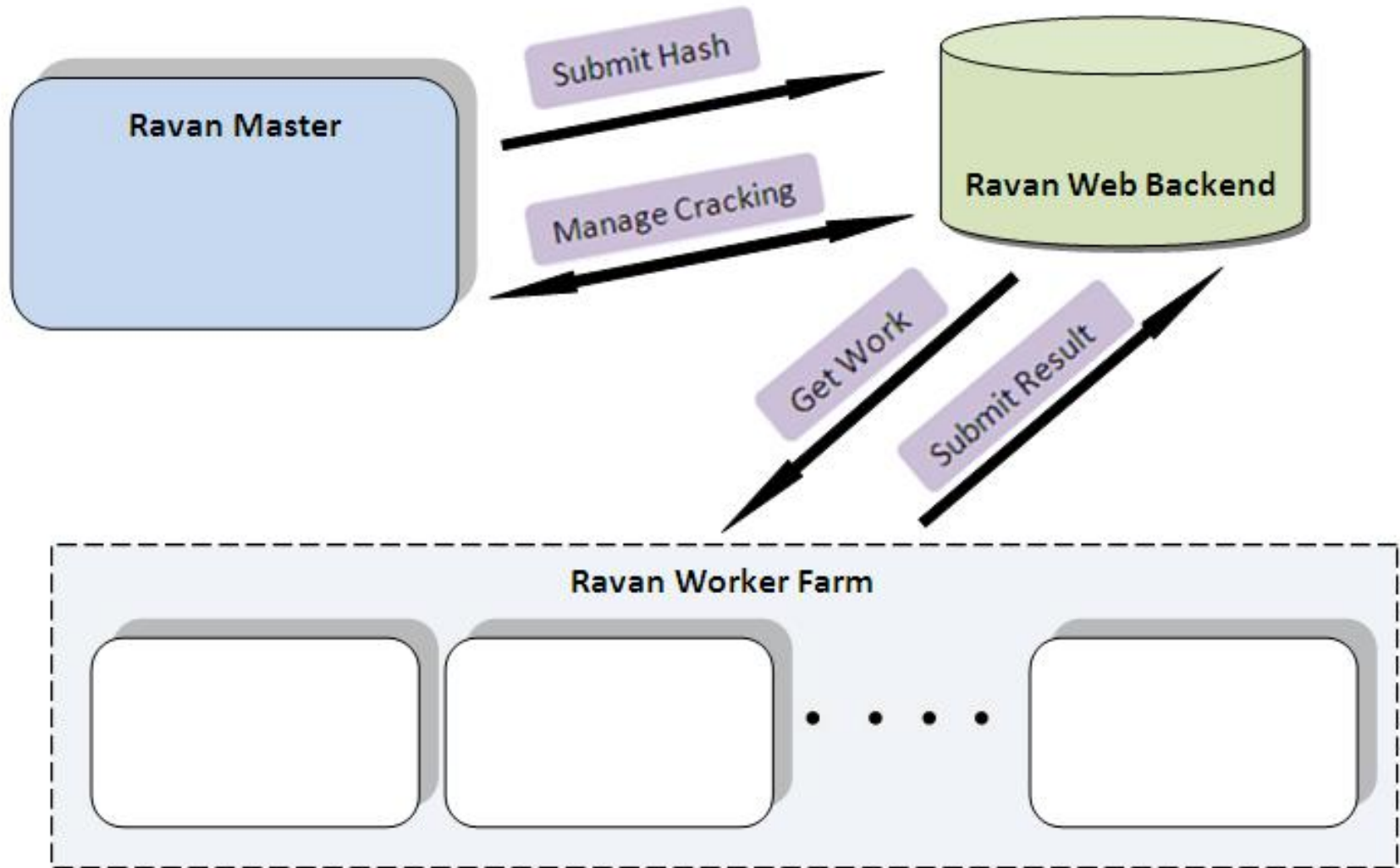
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

DEMO – Web Workers – Ravan



<http://www.andlabs.org/tools/ravan.html>



DEMO – Web Workers – Ravan

<http://www.andlabs.org/tools/ravan.html>



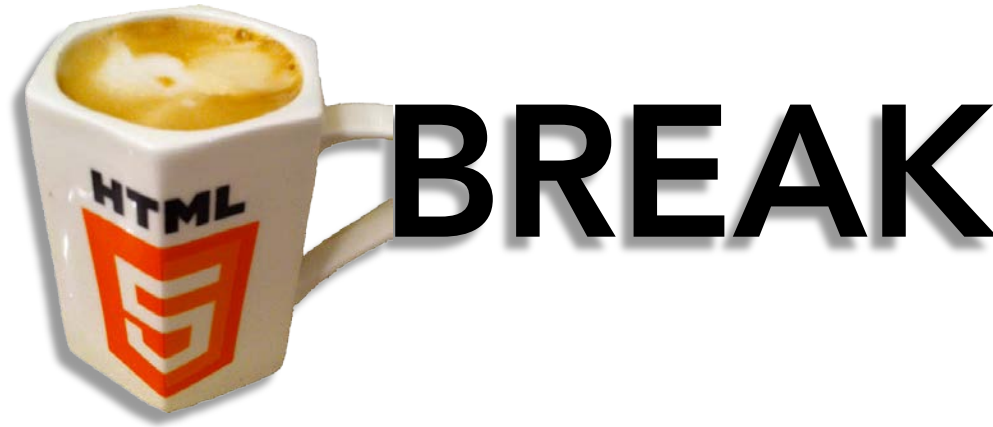
14d6a3e0201f58bfe7c01e775973e80e

Quiz and Q&A



DEMO – Web Workers – Ravan

<http://www.andlabs.org/tools/ravan.html>



HTML5 Web Security Video (May 2011):

<http://www.youtube.com/watch?v=Eju4e5mhEN0>

Test HTML5 security yourself:

<https://www.hacking-lab.com/sh/Gb5VF4q>



References



- ✦ **Master Thesis „HTML 5 web security“**
Michael Schmidt
31 March 2011
- ✦ **Article „HTML5 web security“** (*extract of master thesis*)
Michael Schmidt, Thomas Röthlisberger
6 December 2011
http://media.hacking-lab.com/hlnews/HTML5_Web_Security_v1.0.pdf
- ✦ **Attack and Defense Labs**
Lavakumar Kuppan
<http://www.andlabs.org>
- ✦ **HTML 5 Demos and Examples**
Remy Sharp (<https://twitter.com/rem>)
<http://html5demos.com/>
- ✦ **A vocabulary and associated APIs for HTML and XHTML**
W3C, HTML5 specification
6 August 2013
<http://www.w3.org/TR/html5/>