On the Content Security Policy Violations due to the Same Origin Policy

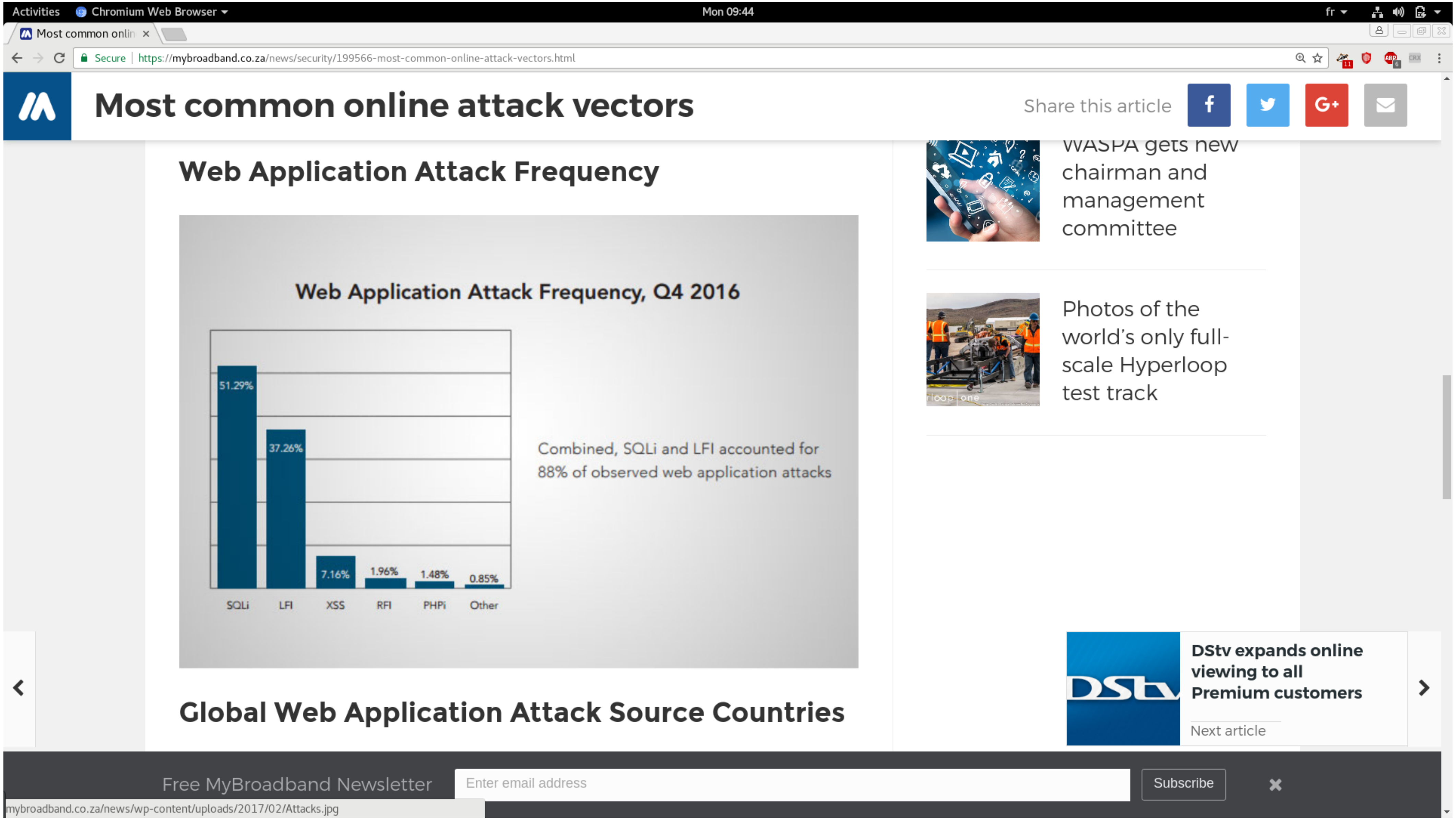
https://webstats.inria.fr

Dolière Francis Somé, Nataliia Bielova, and Tamara Rezk

AJACS Meeting (Inria Rennes)
May 09th, 2017

UNIVERSITÉ CÔTE D'AZUR

Inria
INVENTEURS DU MONDE NUMÉRIQUE


Activities
Chromium Web Browser
Mon 09:44
fr
Most common onlin
Secure
https://mybroadband.co.za/news/security/199566-most-common-online-attack-vectors.html
Share this article
Web Application Attack Frequency, Q4 2016
51.29%
37.26%
7.16%
1.96%
1.48%
0.85%
SQLi
LFI
XSS
RFI
PHPi
Other
Combined, SQLi and LFI accounted for 88% of observed web application attacks
Next article
Subscribe
Enter email address
mybroadband.co.za/news/wp-content/uploads/2017/02/Attacks.jpg

Most common online attack vectors

Web Application Attack Frequency

WASPA gets new chairman and management committee

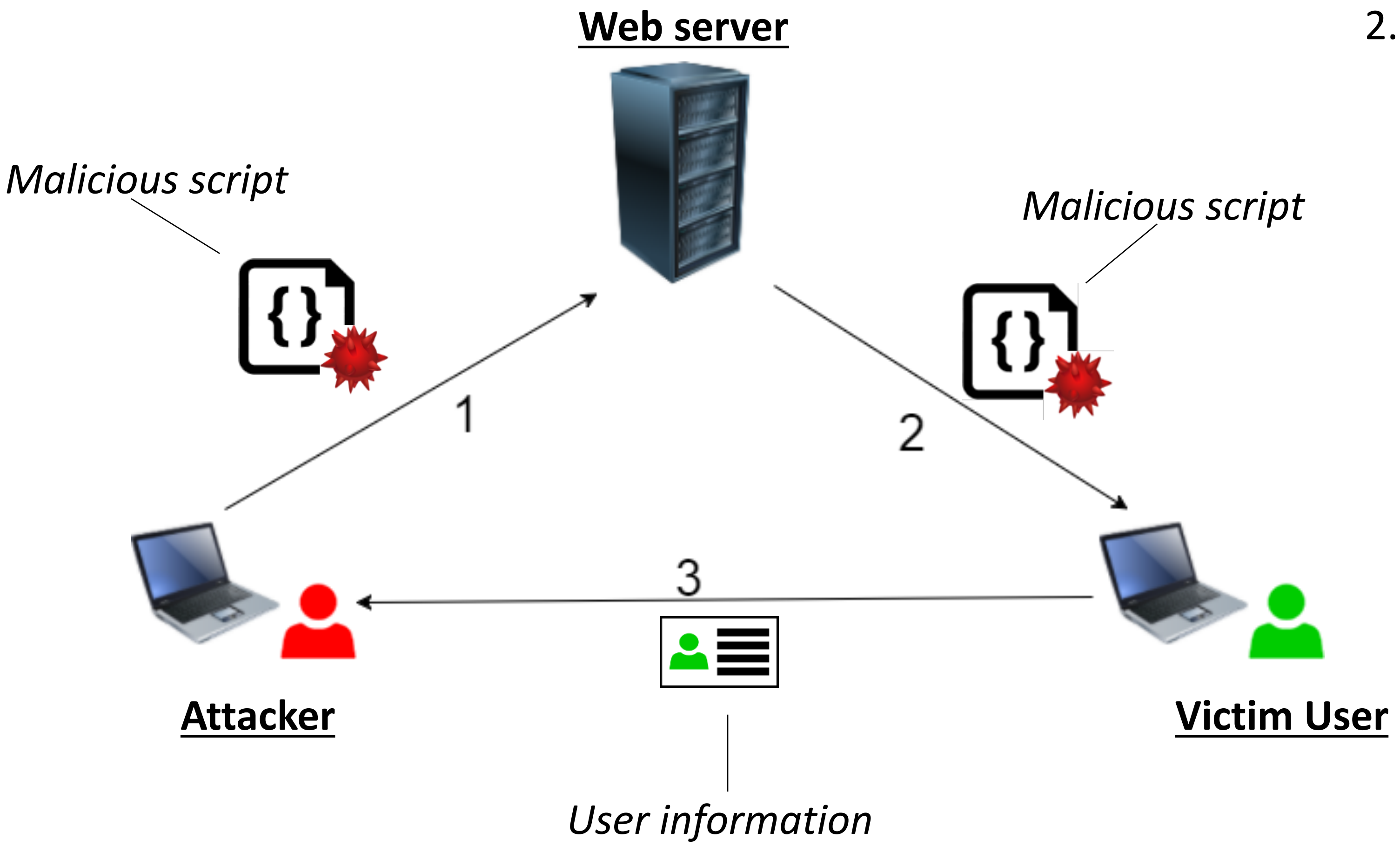
Photos of the world's only full-scale Hyperloop test track

Global Web Application Attack Source Countries

DStv expands online viewing to all Premium customers

Free MyBroadband Newsletter

Cross-Site Scripting (XSS)



1. Sanitize inputs
2. Escape outputs

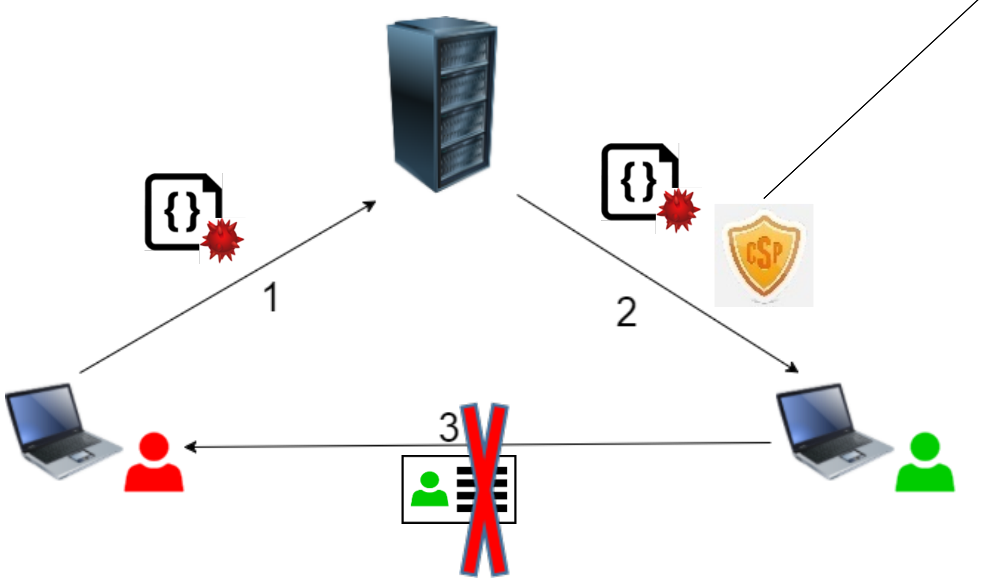
Content Security Policy (CSP)

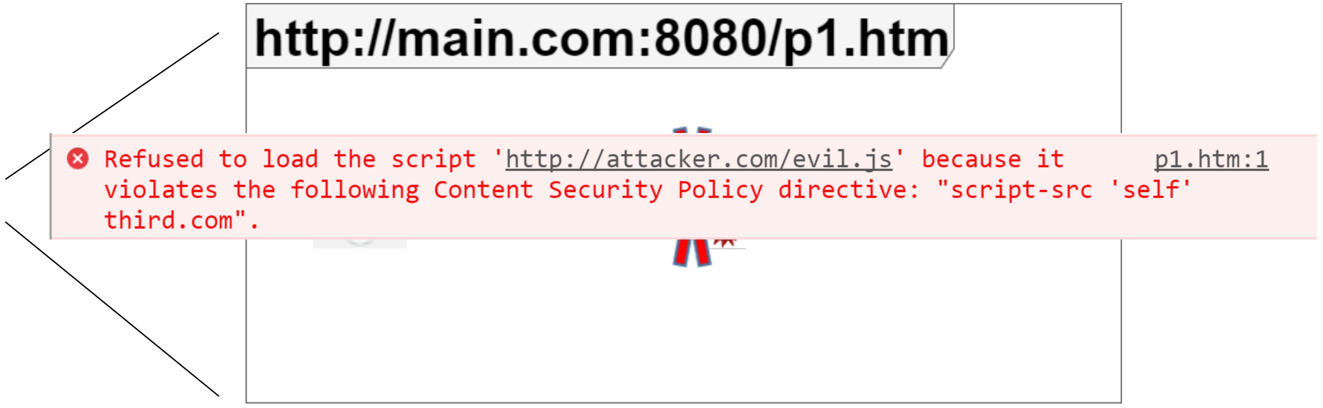
1. Declare trusted contents to the browser
2. Browser blocks unknown contents

Guarantee: unknown code will not steal user data

script-src ‘**self**’ third.com;

connect-src, child-src, style-src, object-src , img-src , media-src , font-src , frame-ancestors, default-src, …



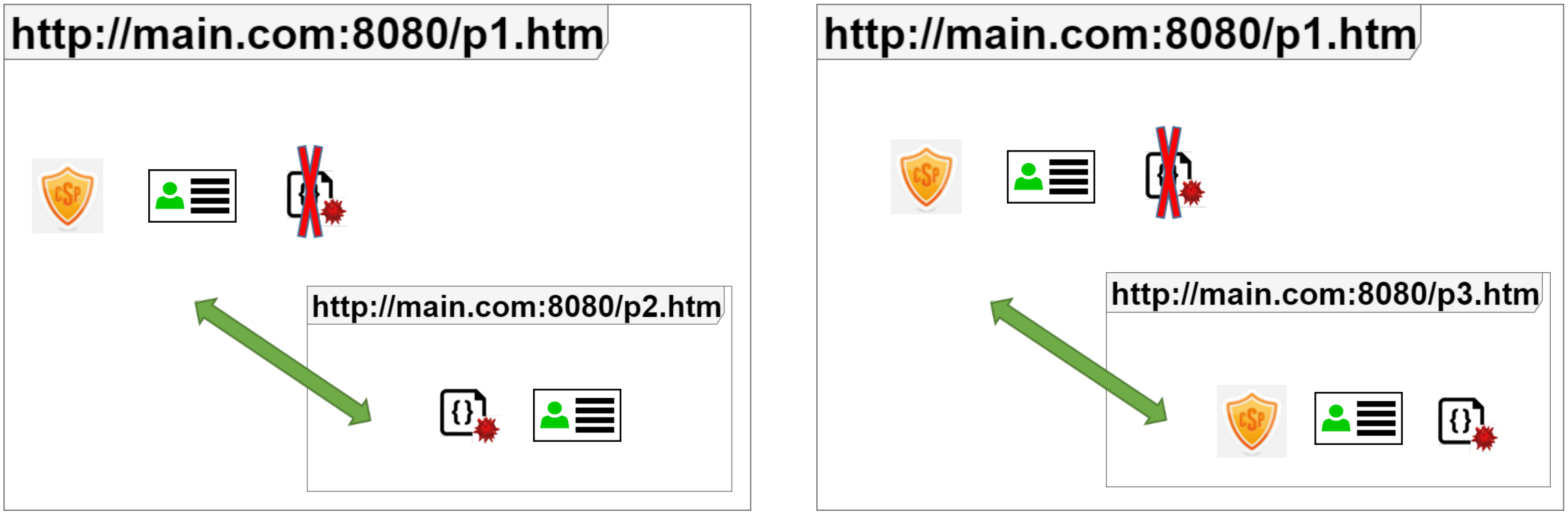


```
Refused to load the script 'http://attacker.com/evil.js' because it      p1.htm:1
violates the following Content Security Policy directive: "script-src 'self'
third.com".
```

Outline

1. Problem: CSP can be bypassed by Same Origin Policy
2. Empirical study: how many sites are vulnerable to this problem?
3. Defense: origin-wide CSP and sandboxing
4. Conclusion

Problem: Efficient CSP can be bypassed



http://main.com:8080/p1.htm

http://main.com:8080/p2.htm

http://main.com:8080/p1.htm

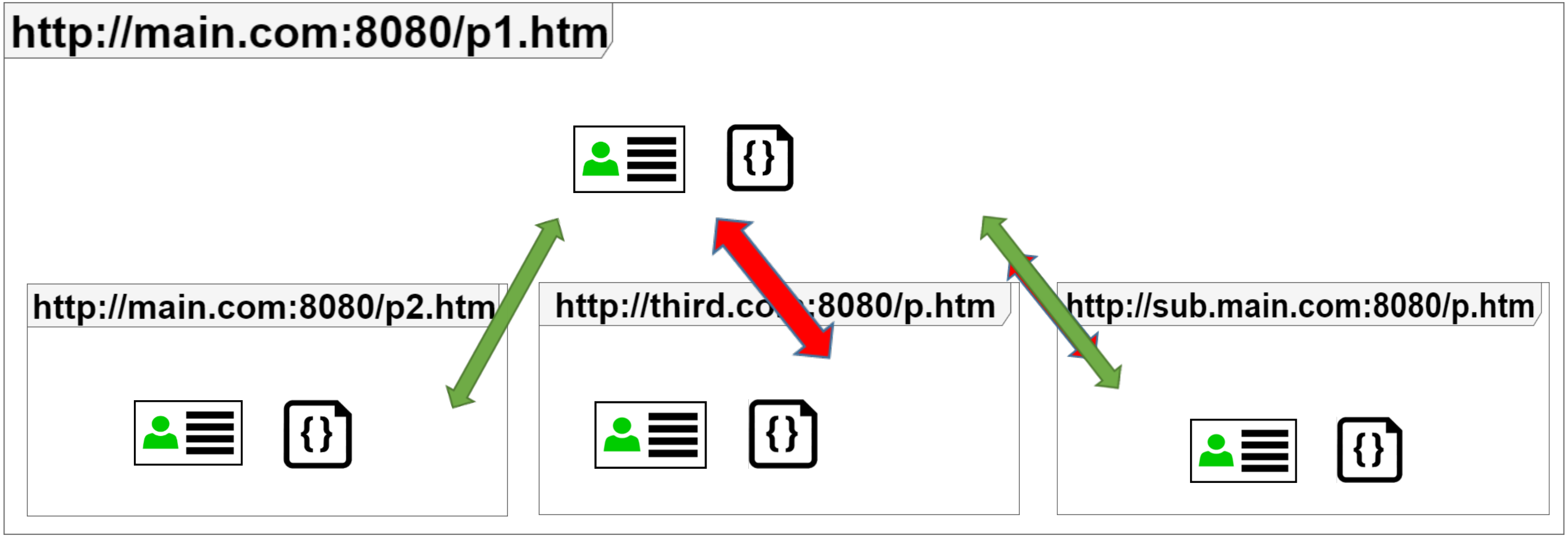
http://main.com:8080/p3.htm

Problem extends to subdomains

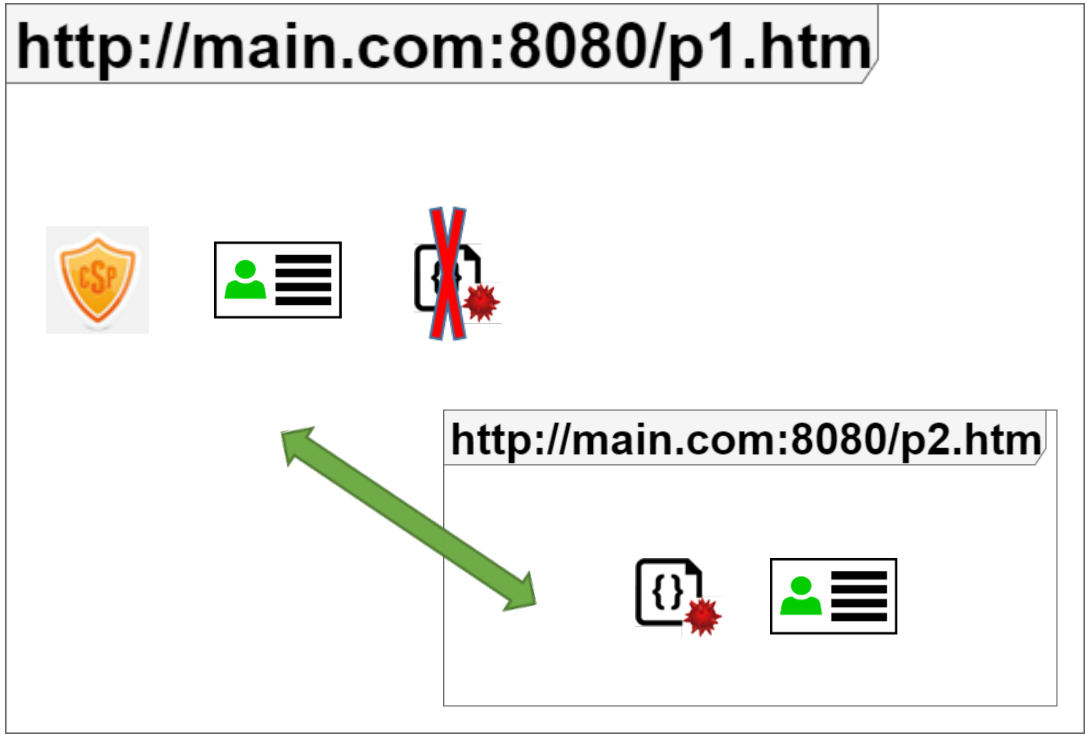
Origin
-scheme, host, port

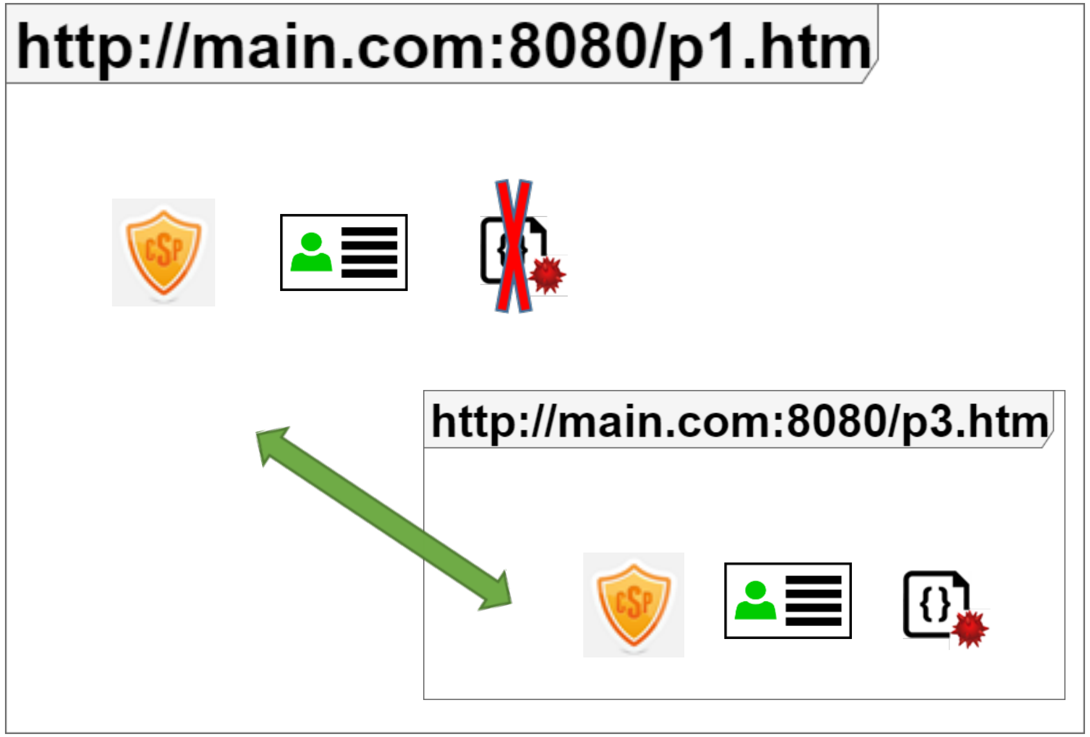
Security
-isolate unstrusted content

Origin relaxation
`-document.domain="main.com";`


http://main.com:8080/p1.htm
http://main.com:8080/p2.htm
http://third.co :8080/p.htm
http://sub.main.com:8080/p.htm

Problem: in the Wild

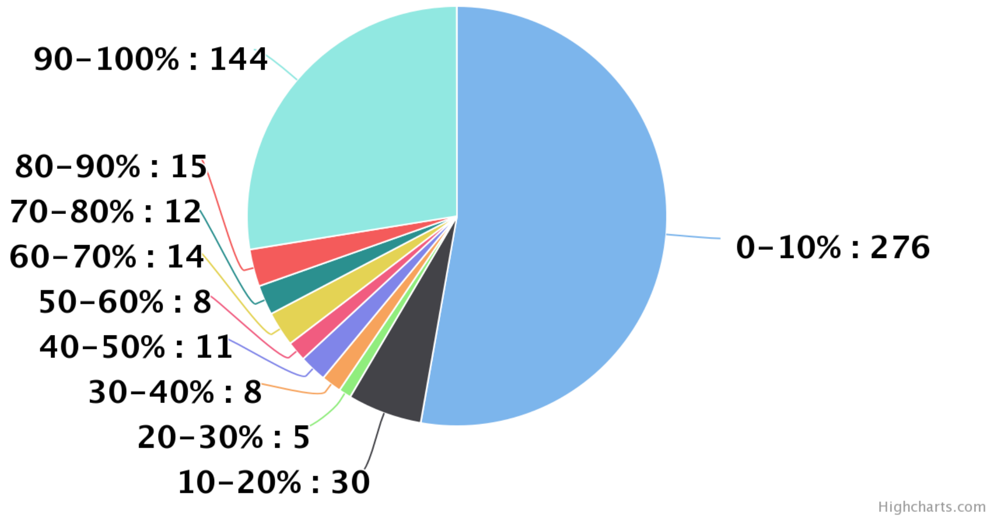




Empirical Study: preliminary results

Sites	9,885 (99%)
Pages	1,090,226
Pages with CSP	21,961 (2.00%)
Pages with CSP in enforcement mode	18,035
Sites with CSP on some pages	523 (5.29%)

CSP Coverage by site



Same origin pages do not have CSP

Same origin page	4,381
Sub domain page	4,728
Total	9,109 (50.51%)

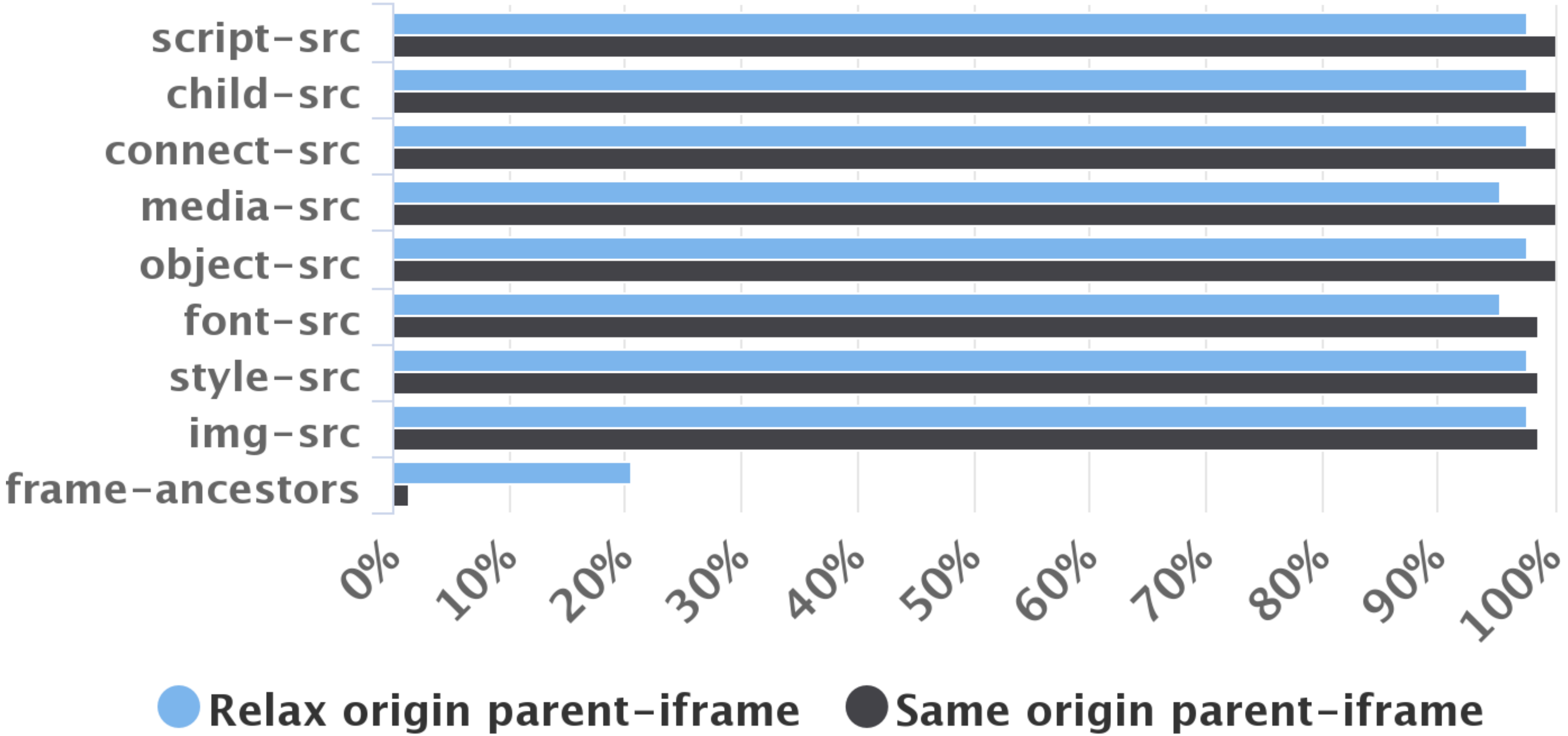
Same origin pages have a different CSP

Same origin page	1,223
Sub domain page	2,567
Total	3,790 (21.01%)

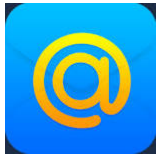
Empirical Study: Main Results

	Same Origin parent-iframe	**Same Origin parent-iframe (on origin relaxation)**
Couples Parent-iframe	**720**	**1781**
Only parent has CSP	**83**	**1,388**
Only iframe has CSP	16	240
Different CSPs	**70**	**44**
CSP problem total	**169 (23.5%)**	**1,672 (94%)**

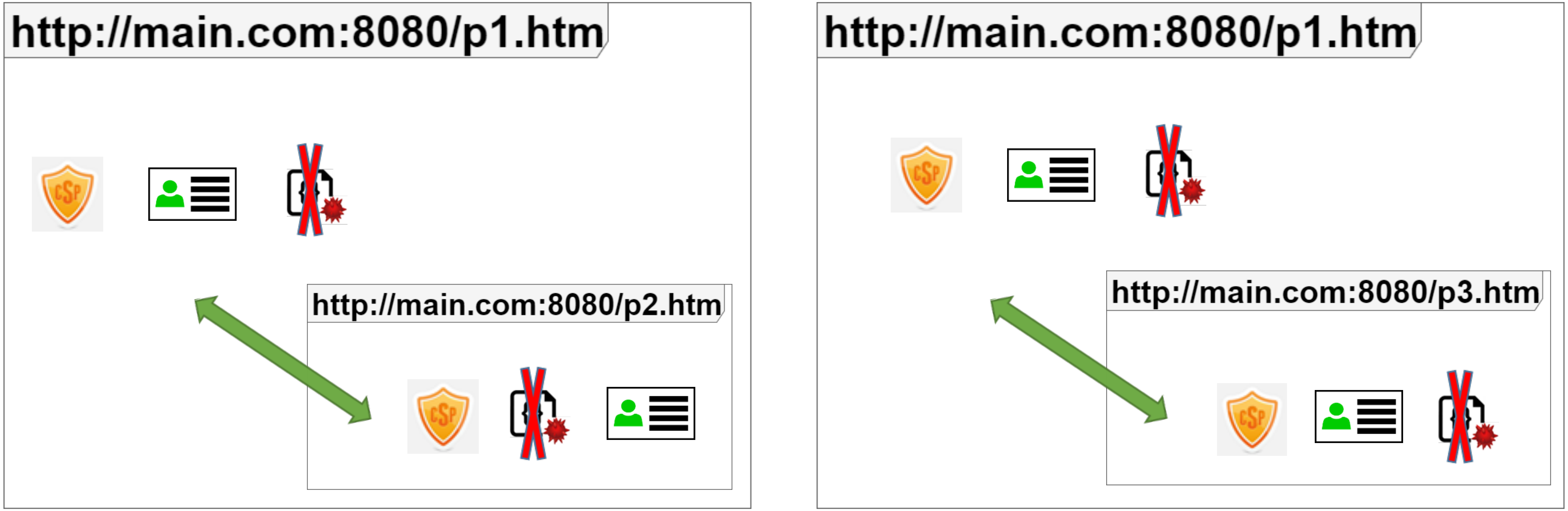
Empirical Study: CSP Directives Differences



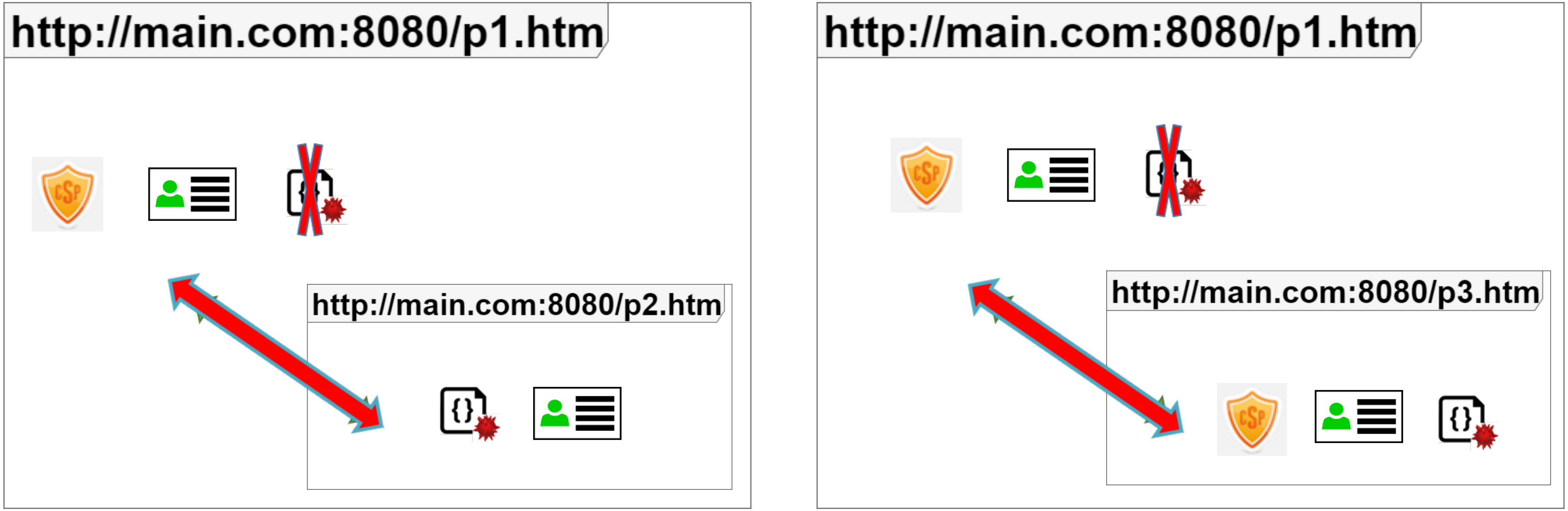
Websites concerned with this problem



Defense[1]: Same Efficient CSP


http://main.com:8080/p1.htm
http://main.com:8080/p2.htm
http://main.com:8080/p1.htm
http://main.com:8080/p3.htm

Defense[2]: Sandboxing


http://main.com:8080/p1.htm
CSP
http://main.com:8080/p2.htm
http://main.com:8080/p1.htm
CSP
http://main.com:8080/p3.htm
CSP

Browser Subtleties

- Bug in Firefox CSP implementation
  - `srcdoc` iframes
  - sandboxing to refine SOP
- Filed to Mozilla
- Details in paper

Conclusions

- Problem: CSP can be violated due to SOP
- Empirical study: 72% of pages with CSP of top 10K Alexa are vulnerable
- Defense
  - Same CSP on same-origin pages
  - Different CSP with sandboxing
- Additional discovery
  - Implementation error in Firefox regarding `srcdoc` iframes.
- Recommendation: use sandbox as a CSP directive instead of iframe attribute