Same-Origin Policy: Evaluation in Modern Browsers

Jörg Schwenk, **Marcus Niemietz**, Christian Mainka

Ruhr-University Bochum

hgi
Horst Görtz Institute
for IT-Security

RUB

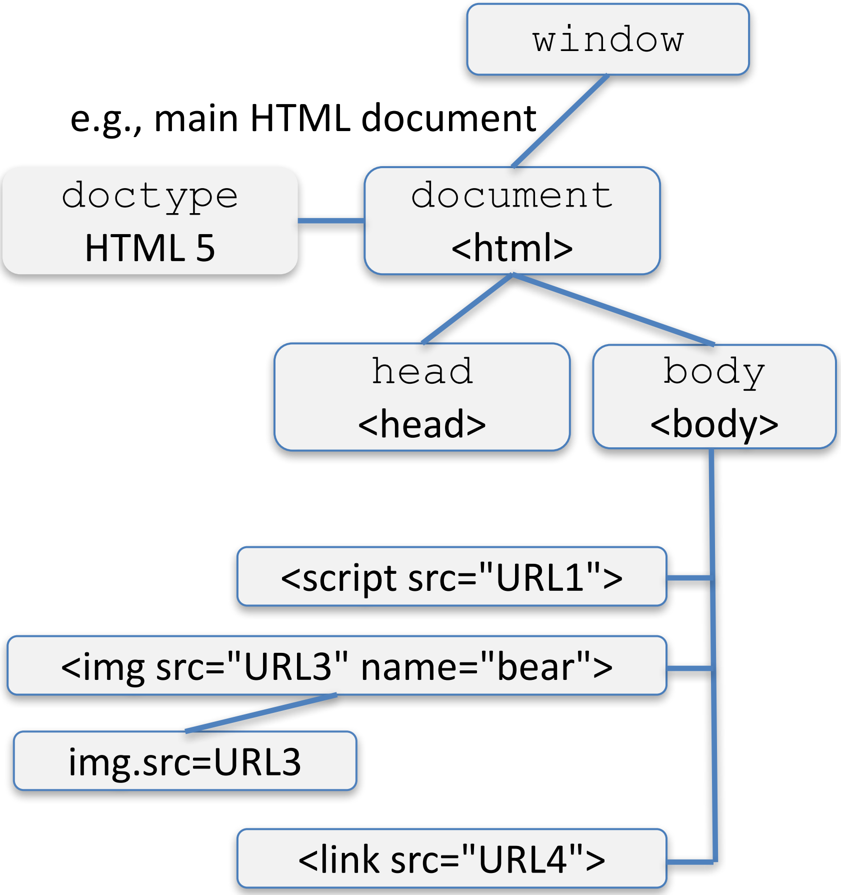
Contents

1. Introduction & Foundations
2. Methodology & Evaluation
3. Limitations & Access Control Policies
4. Conclusions & Future Work

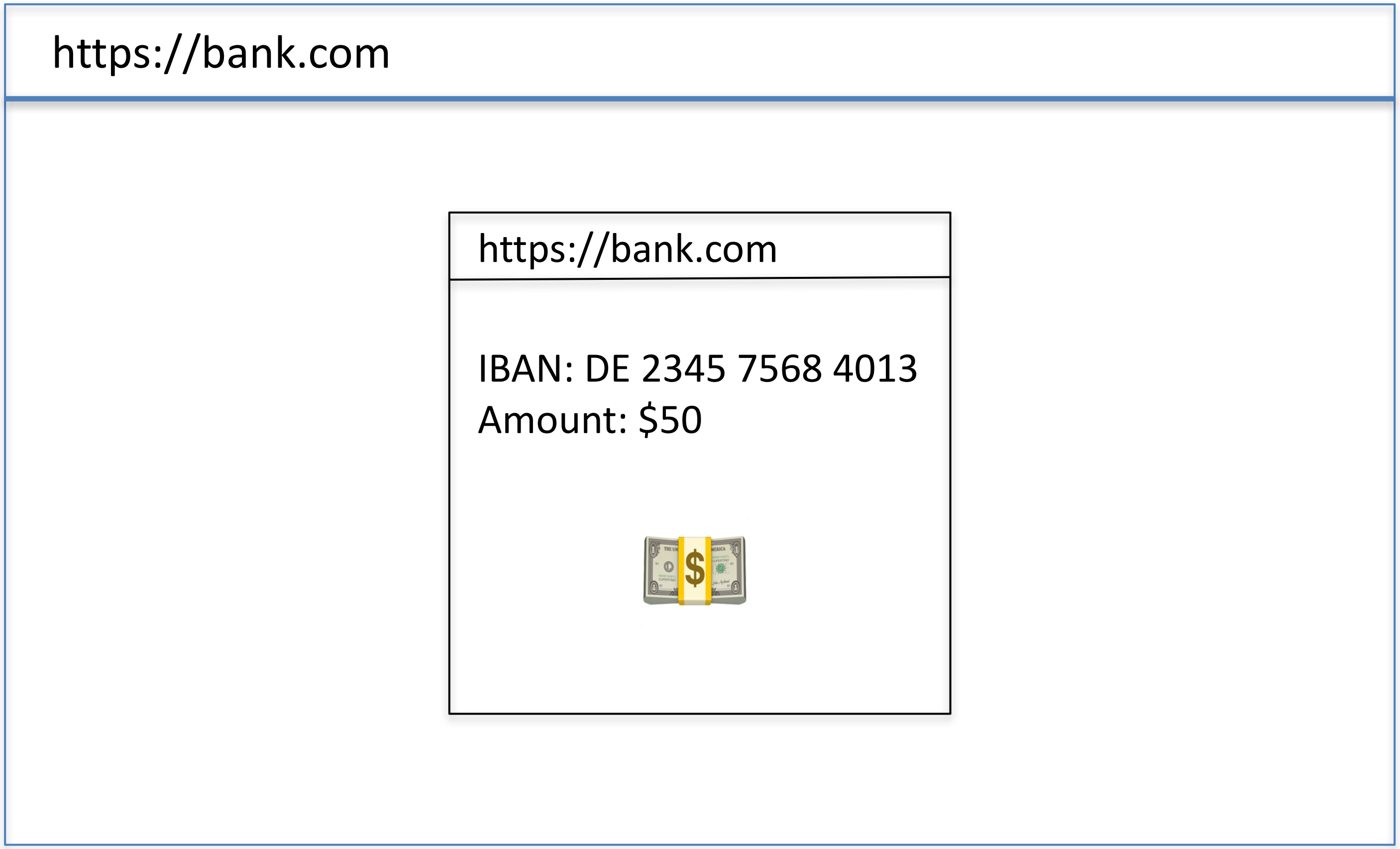
1. Introduction & Foundations

Same-Origin Policy

https://bank.com



Same-Origin Policy

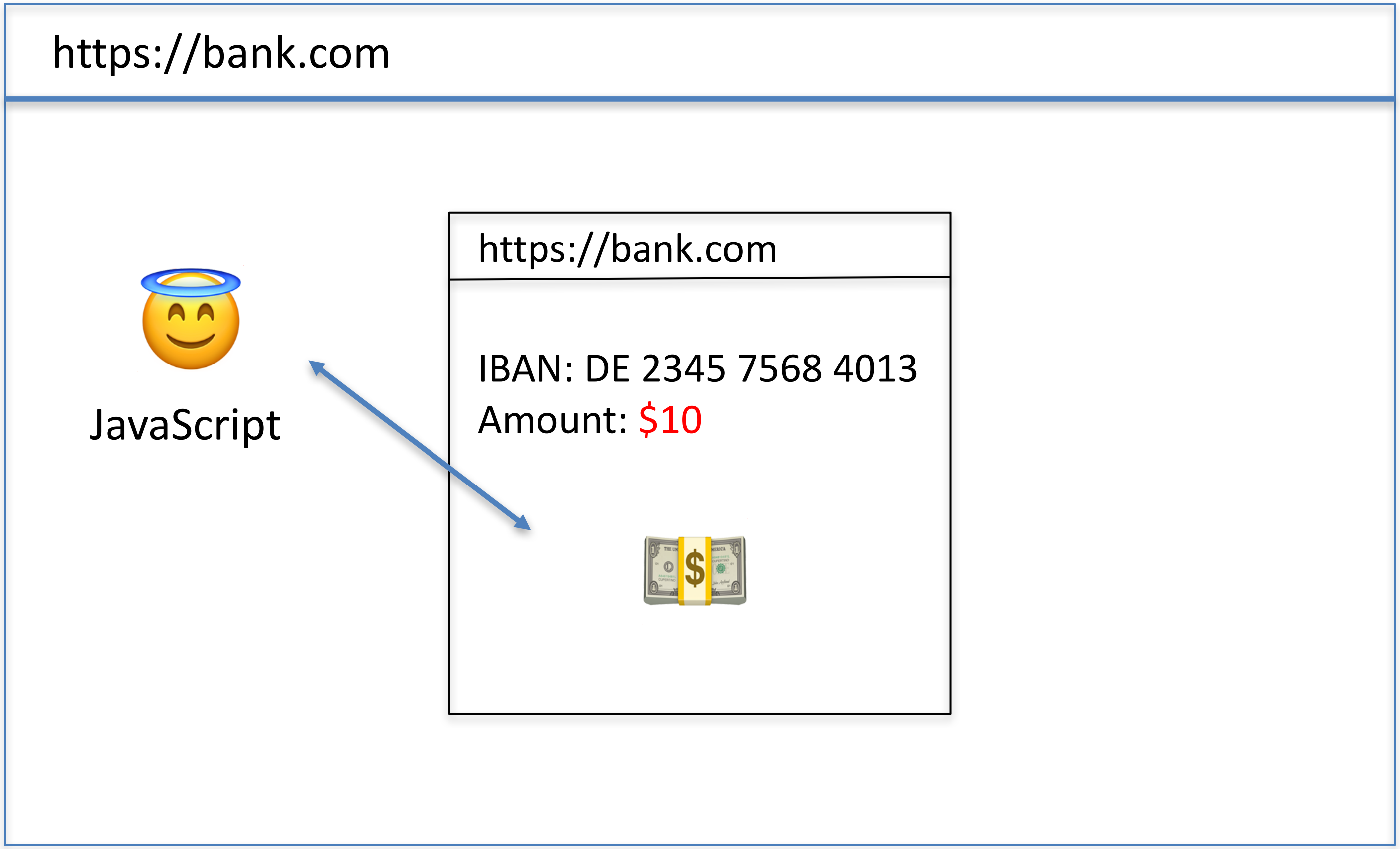


https://bank.com

https://bank.com

IBAN: DE 2345 7568 4013
Amount: $50

Same-Origin Policy



https://bank.com

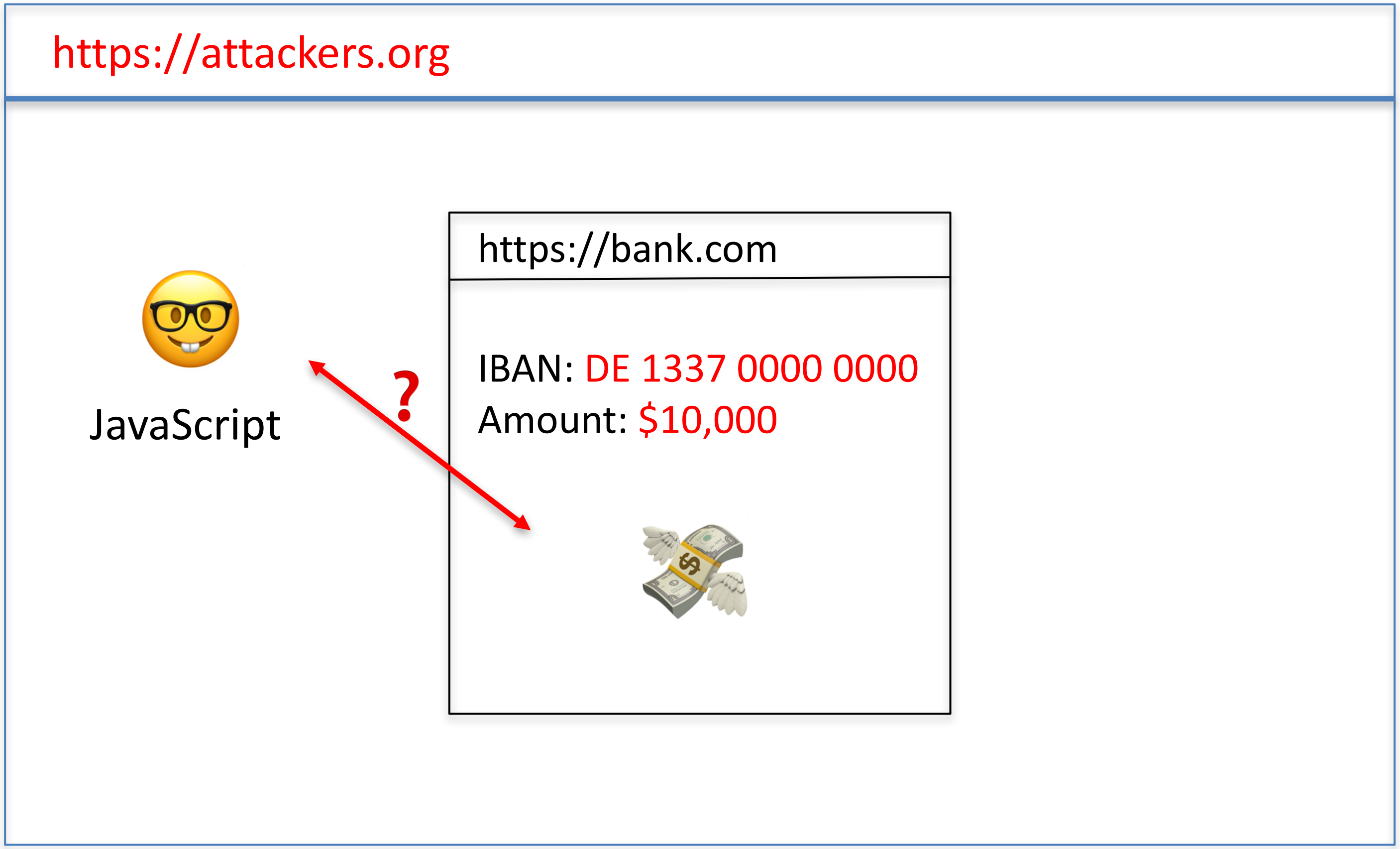
JavaScript

https://bank.com

IBAN: DE 2345 7568 4013

Amount: $10

Same-Origin Policy



https://attackers.org

JavaScript

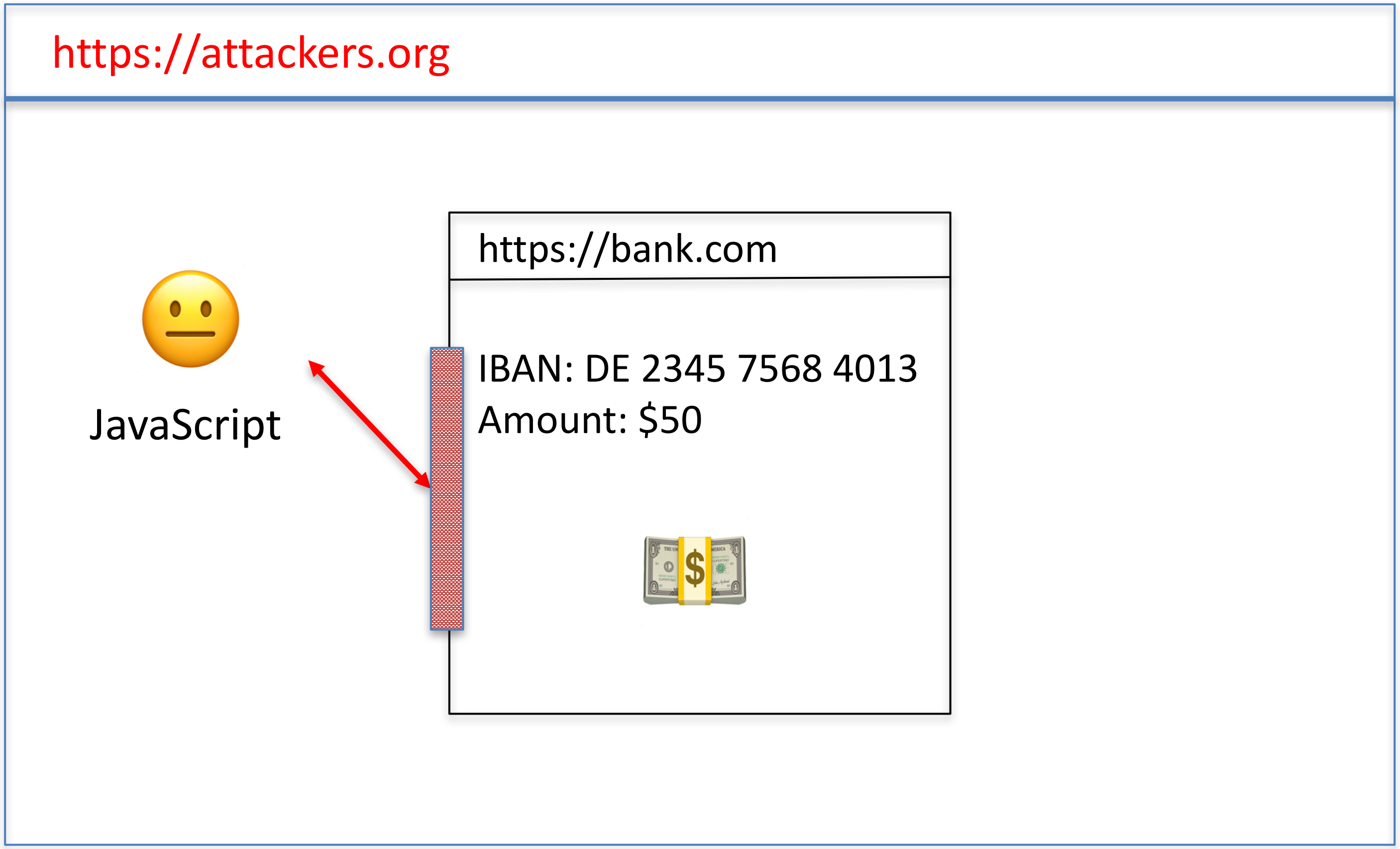
?

https://bank.com

IBAN: DE 1337 0000 0000

Amount: $10,000

Same-Origin Policy



https://attackers.org

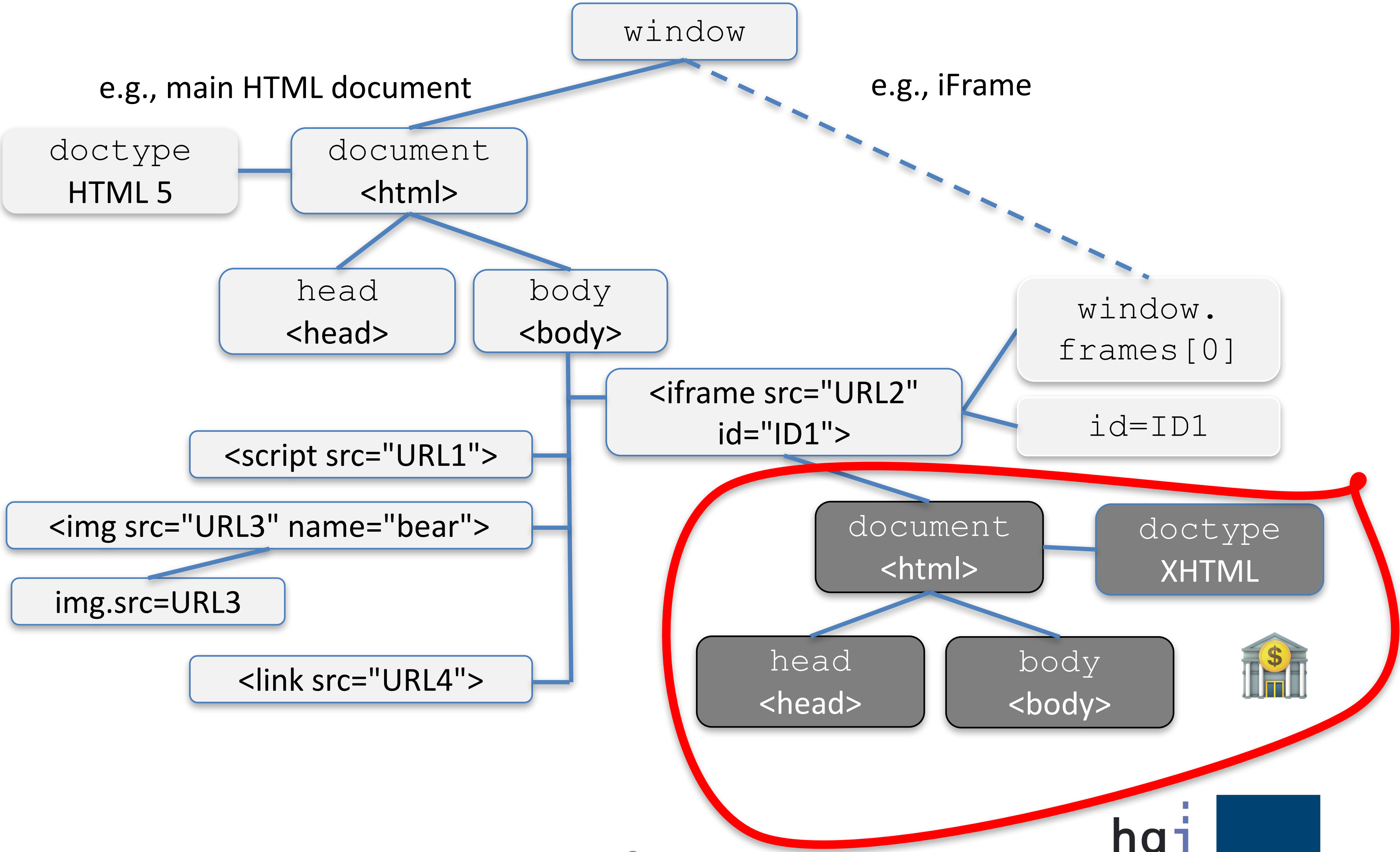
JavaScript

https://bank.com

IBAN: DE 2345 7568 4013

Amount: $50

DOM-SOP


window
e.g., main HTML document
e.g., iFrame
doctype
HTML 5
document
<html>
head
<head>
body
<body>
window.
frames[0]
<iframe src="URL2"
id="ID1">
id=ID1
<script src="URL1">
<img src="URL3" name="bear">
img.src=URL3
<link src="URL4">
document
<html>
doctype
XHTML
head
<head>
body
<body>
🏦

Different Subsets Of SOP Rules

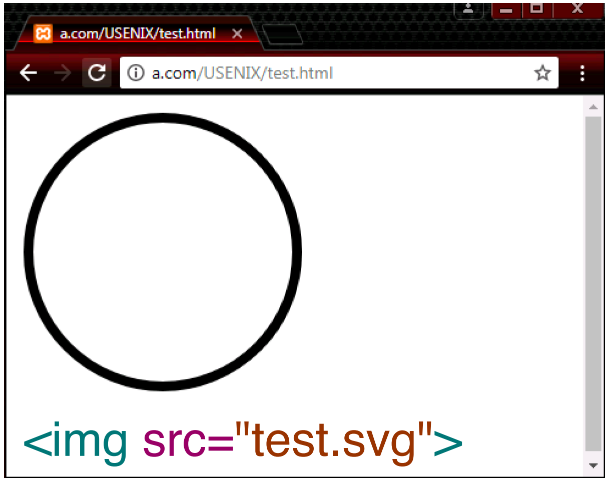
- **DOM access (SOP-DOM)**
- Local storage and session storage
- XMLHttpRequest
- Pseudoprotocols
- Plugins (e.g., Flash, Silverlight, PDF)
- Window/tab
- HTTP cookies

Focus

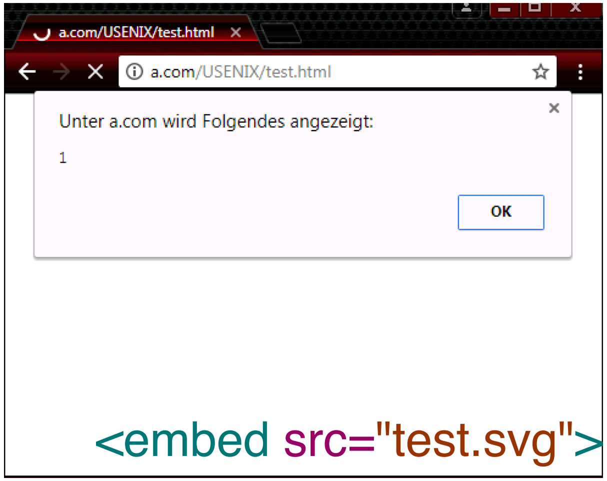
- Subset of SOP rules according to these criteria
  - Browser Interactions
    - Interaction of web objects once they have been loaded
  - Web Origins (RFC 6454 as a foundation)
    - "An image is passive content and, therefore, carries no authority, meaning the image has no access to the objects and resources available to its origin"

Scalable Vector Graphics

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<svg xmlns="http://www.w3.org/2000/svg" width="300" height="300">
<script>alert(1)</script>
<circle cx="120" cy="120" r="110" fill="#fff" stroke="#000" stroke-width="8"/>
</svg>
```



<img src="test.svg">



Unter a.com wird Folgendes angezeigt:

1

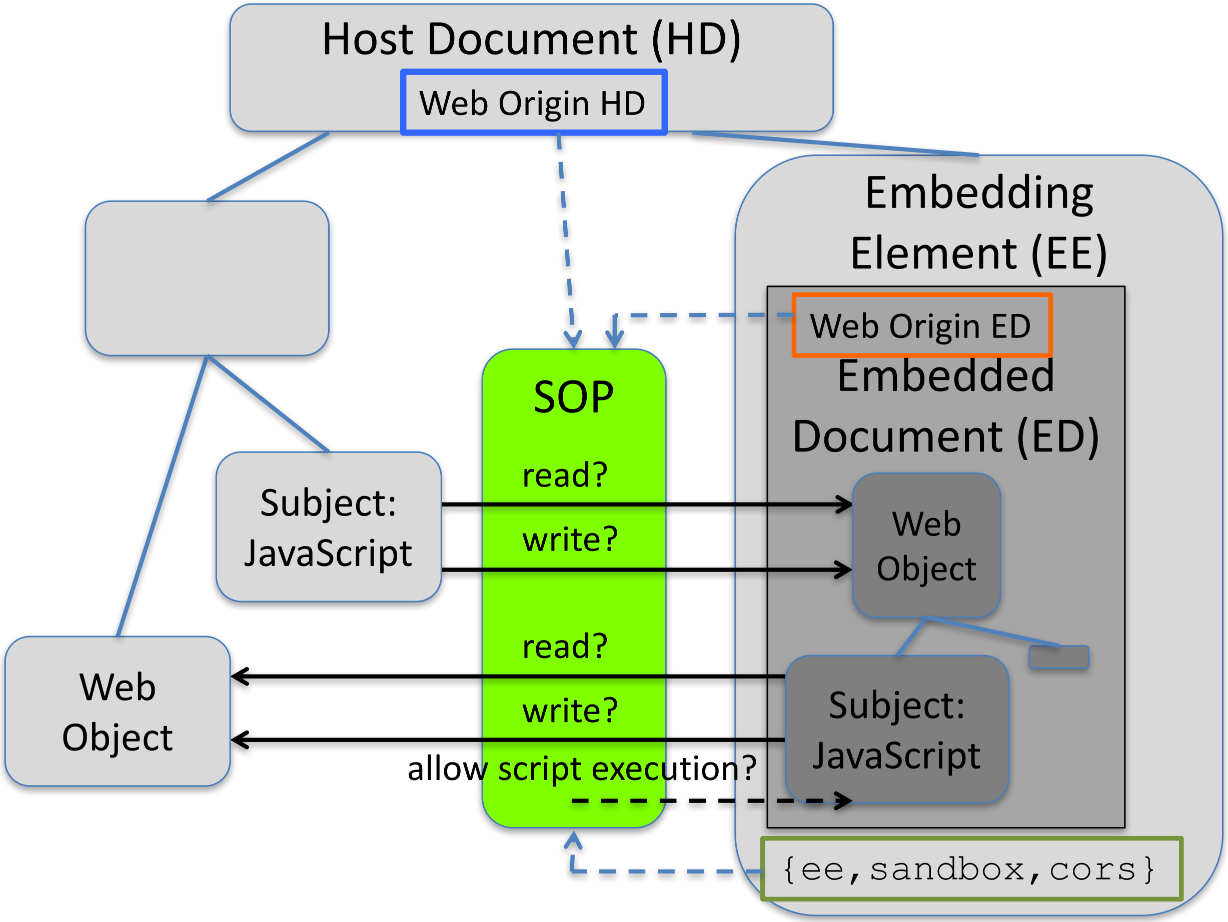
<embed src="test.svg">

Research Questions

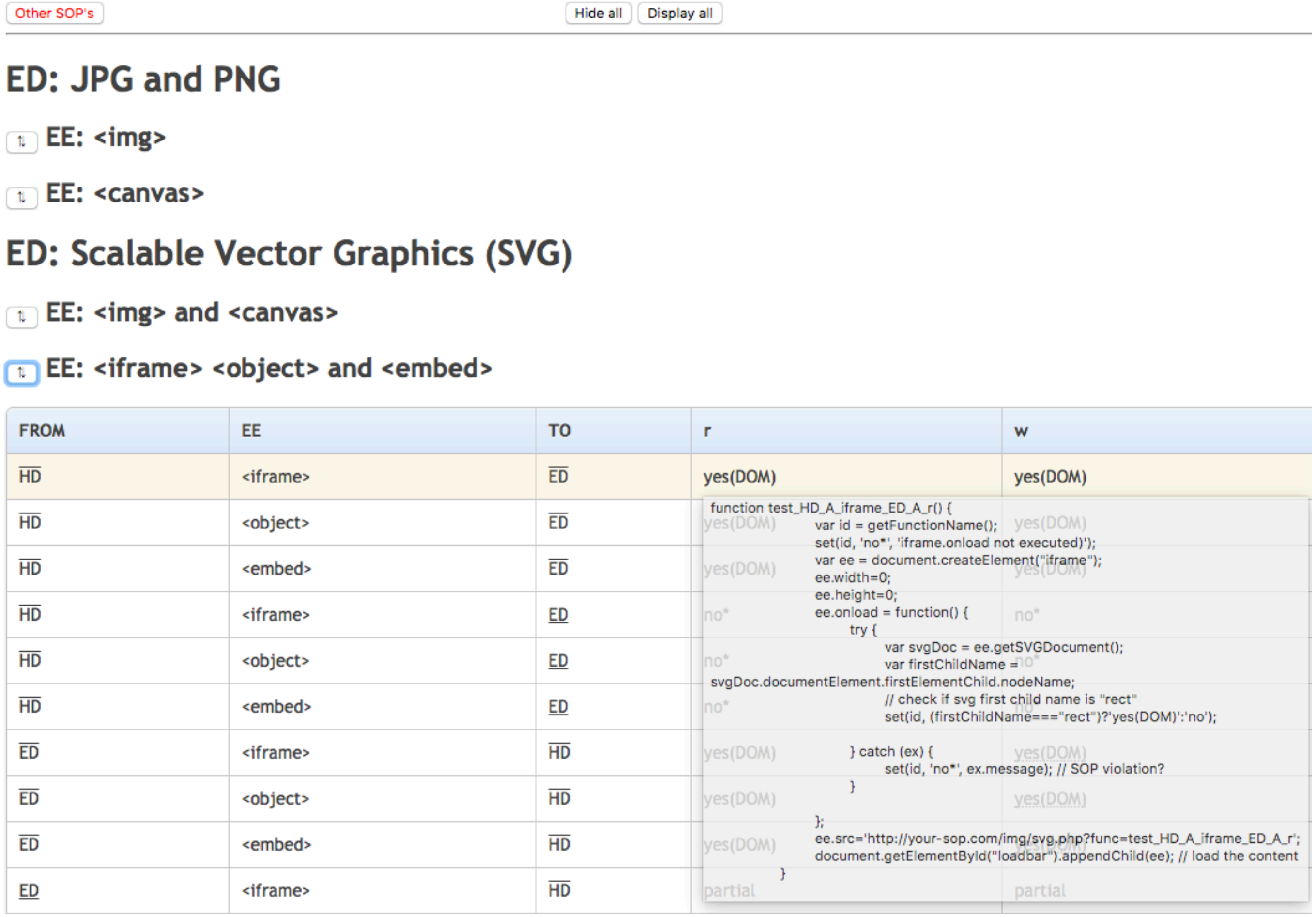
- How is SOP for DOM access (SOP-DOM) implemented in modern browsers?
- Which parts of the HTML markup influences SOP-DOM?
- How does the detected behavior match known access control policies?

2. Methodology & Evaluation

SOP-DOM Setup: Test Cases



Your-SOP.com Testbed



ED: JPG and PNG

⇅ EE: <img>

⇅ EE: <canvas>

ED: Scalable Vector Graphics (SVG)

⇅ EE: <img> and <canvas>

⇅ EE: <iframe> <object> and <embed>

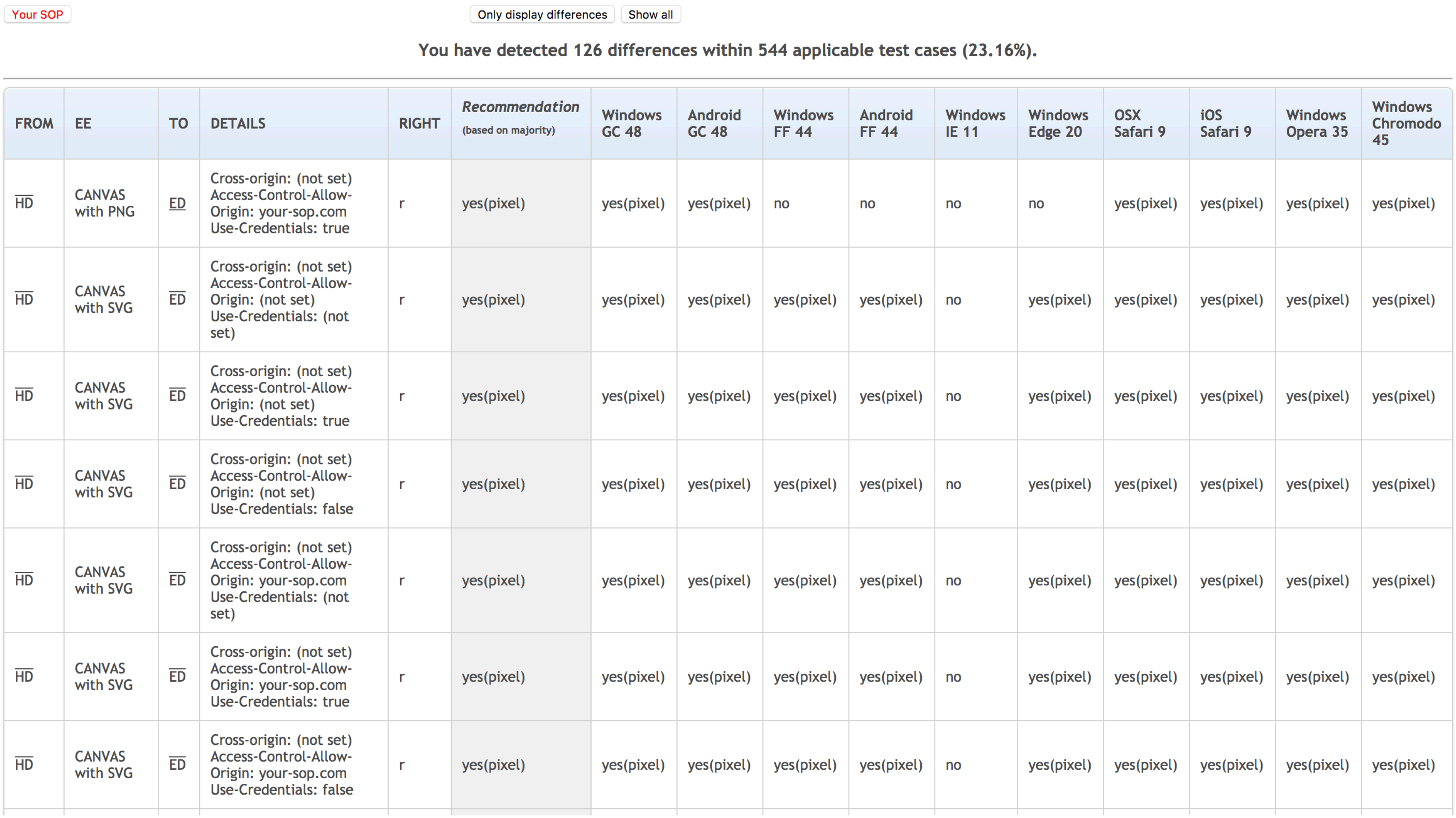
FROM	EE	TO	r	w
$\overline{HD}$	<iframe>	$\overline{ED}$	yes(DOM)	yes(DOM)
$\overline{HD}$	<object>	$\overline{ED}$	yes(DOM)	yes(DOM)
$\overline{HD}$	<embed>	$\overline{ED}$	yes(DOM)	yes(DOM)
$\overline{HD}$	<iframe>	$\underline{ED}$	no*	no*
$\overline{HD}$	<object>	$\underline{ED}$	no*	no*
$\overline{HD}$	<embed>	$\underline{ED}$	no*	no
$\overline{ED}$	<iframe>	$\overline{HD}$	yes(DOM)	yes(DOM)
$\overline{ED}$	<object>	$\overline{HD}$	yes(DOM)	yes(DOM)
$\overline{ED}$	<embed>	$\overline{HD}$	yes(DOM)	yes(DOM)
$\underline{ED}$	<iframe>	$\overline{HD}$	partial	partial

```
function test_HD_A_iframe_ED_A_r() {
        var id = getFunctionName();
        set(id, 'no*', 'iframe.onload not executed)');
        var ee = document.createElement("iframe");
        ee.width=0;
        ee.height=0;
        ee.onload = function() {
            try {
                var svgDoc = ee.getSVGDocument();
                var firstChildName =
svgDoc.documentElement.firstElementChild.nodeName;
                // check if svg first child name is "rect"
                set(id, (firstChildName==="rect")?'yes(DOM)':'no');

            } catch (ex) {
                set(id, 'no*', ex.message); // SOP violation?
            }

        };
        ee.src='http://your-sop.com/img/svg.php?func=test_HD_A_iframe_ED_A_r';
        document.getElementById("loadbar").appendChild(ee); // load the content
    }
```

Your-SOP.com Testbed



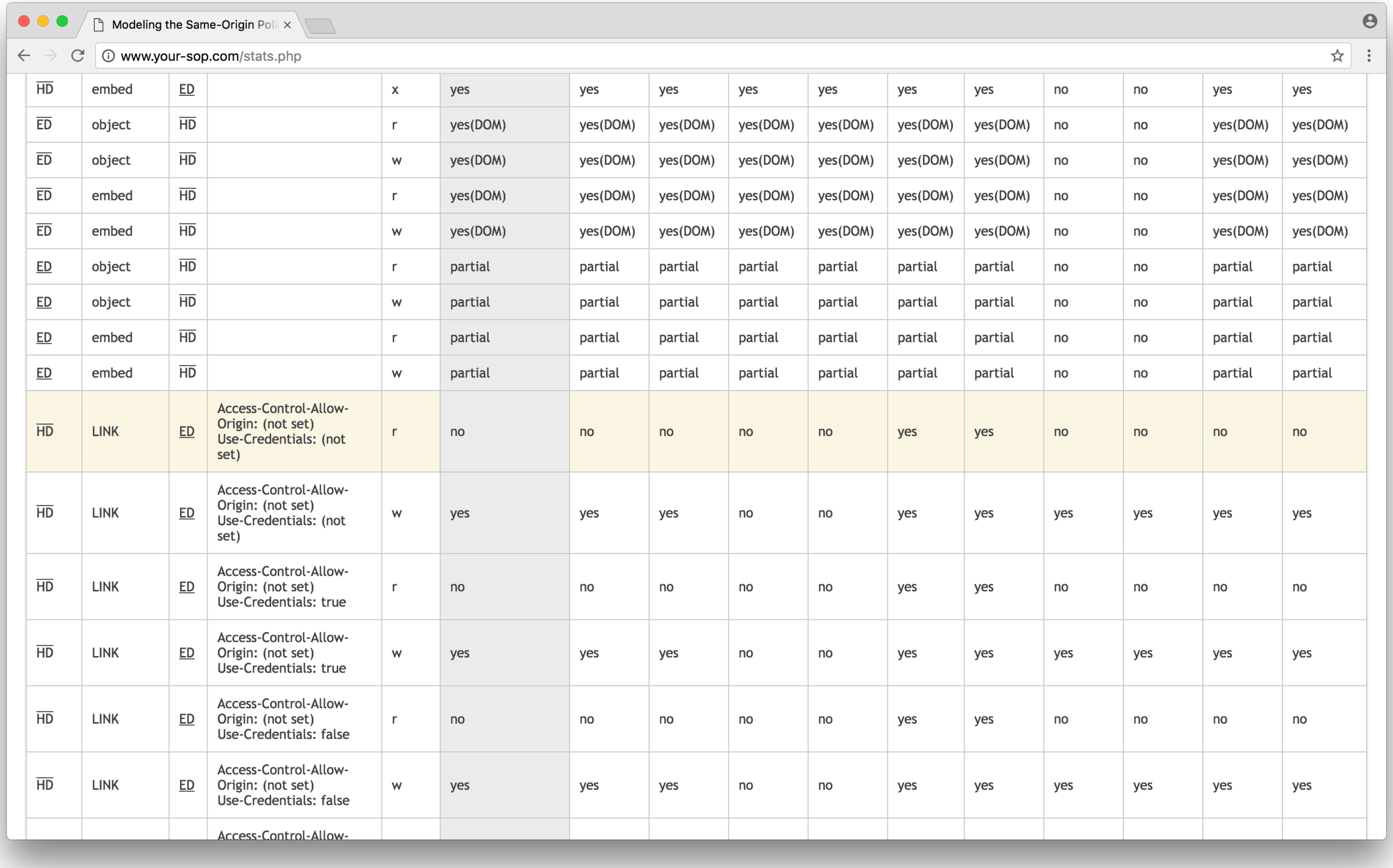
You have detected 126 differences within 544 applicable test cases (23.16%).

FROM	EE	TO	DETAILS	RIGHT	*Recommendation* (based on majority)	Windows GC 48	Android GC 48	Windows FF 44	Android FF 44	Windows IE 11	Windows Edge 20	OSX Safari 9	iOS Safari 9	Windows Opera 35	Windows Chromodo 45
$\overline{\text{HD}}$	CANVAS with PNG	$\underline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: your-sop.com Use-Credentials: true	r	yes(pixel)	yes(pixel)	yes(pixel)	no	no	no	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)
$\overline{\text{HD}}$	CANVAS with SVG	$\overline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: (not set) Use-Credentials: (not set)	r	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)
$\overline{\text{HD}}$	CANVAS with SVG	$\overline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: (not set) Use-Credentials: true	r	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)
$\overline{\text{HD}}$	CANVAS with SVG	$\overline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: (not set) Use-Credentials: false	r	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)
$\overline{\text{HD}}$	CANVAS with SVG	$\overline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: your-sop.com Use-Credentials: (not set)	r	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)
$\overline{\text{HD}}$	CANVAS with SVG	$\overline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: your-sop.com Use-Credentials: true	r	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)
$\overline{\text{HD}}$	CANVAS with SVG	$\overline{\text{ED}}$	Cross-origin: (not set) Access-Control-Allow-Origin: your-sop.com Use-Credentials: false	r	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	no	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)	yes(pixel)

Different Browser Behaviors

- >12%: Safari 9
  - Missing type: `image/svg+xml`
  - Fixed in Safari 10.1
- >35%: `<canvas>` and PNG/SVG (CORS)
- >51%: `<link>` (CORS)
- One IE/Edge vulnerability without using CORS

Cross-Origin Login Oracle Attack



$\overline{\text{HD}}$	embed	$\underline{\text{ED}}$		x	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes
$\overline{\text{ED}}$	object	$\overline{\text{HD}}$		r	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	no	no	yes(DOM)	yes(DOM)
$\overline{\text{ED}}$	object	$\overline{\text{HD}}$		w	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	no	no	yes(DOM)	yes(DOM)
$\overline{\text{ED}}$	embed	$\overline{\text{HD}}$		r	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	no	no	yes(DOM)	yes(DOM)
$\overline{\text{ED}}$	embed	$\overline{\text{HD}}$		w	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	yes(DOM)	no	no	yes(DOM)	yes(DOM)
$\underline{\text{ED}}$	object	$\overline{\text{HD}}$		r	partial	partial	partial	partial	partial	partial	partial	no	no	partial	partial
$\underline{\text{ED}}$	object	$\overline{\text{HD}}$		w	partial	partial	partial	partial	partial	partial	partial	no	no	partial	partial
$\underline{\text{ED}}$	embed	$\overline{\text{HD}}$		r	partial	partial	partial	partial	partial	partial	partial	no	no	partial	partial
$\underline{\text{ED}}$	embed	$\overline{\text{HD}}$		w	partial	partial	partial	partial	partial	partial	partial	no	no	partial	partial
$\overline{\text{HD}}$	LINK	$\underline{\text{ED}}$	Access-Control-Allow-Origin: (not set) Use-Credentials: (not set)	r	no	no	no	no	no	yes	yes	no	no	no	no
$\overline{\text{HD}}$	LINK	$\underline{\text{ED}}$	Access-Control-Allow-Origin: (not set) Use-Credentials: (not set)	w	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes
$\overline{\text{HD}}$	LINK	$\underline{\text{ED}}$	Access-Control-Allow-Origin: (not set) Use-Credentials: true	r	no	no	no	no	no	yes	yes	no	no	no	no
$\overline{\text{HD}}$	LINK	$\underline{\text{ED}}$	Access-Control-Allow-Origin: (not set) Use-Credentials: true	w	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes
$\overline{\text{HD}}$	LINK	$\underline{\text{ED}}$	Access-Control-Allow-Origin: (not set) Use-Credentials: false	r	no	no	no	no	no	yes	yes	no	no	no	no
$\overline{\text{HD}}$	LINK	$\underline{\text{ED}}$	Access-Control-Allow-Origin: (not set) Use-Credentials: false	w	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes
			Access-Control-Allow-												

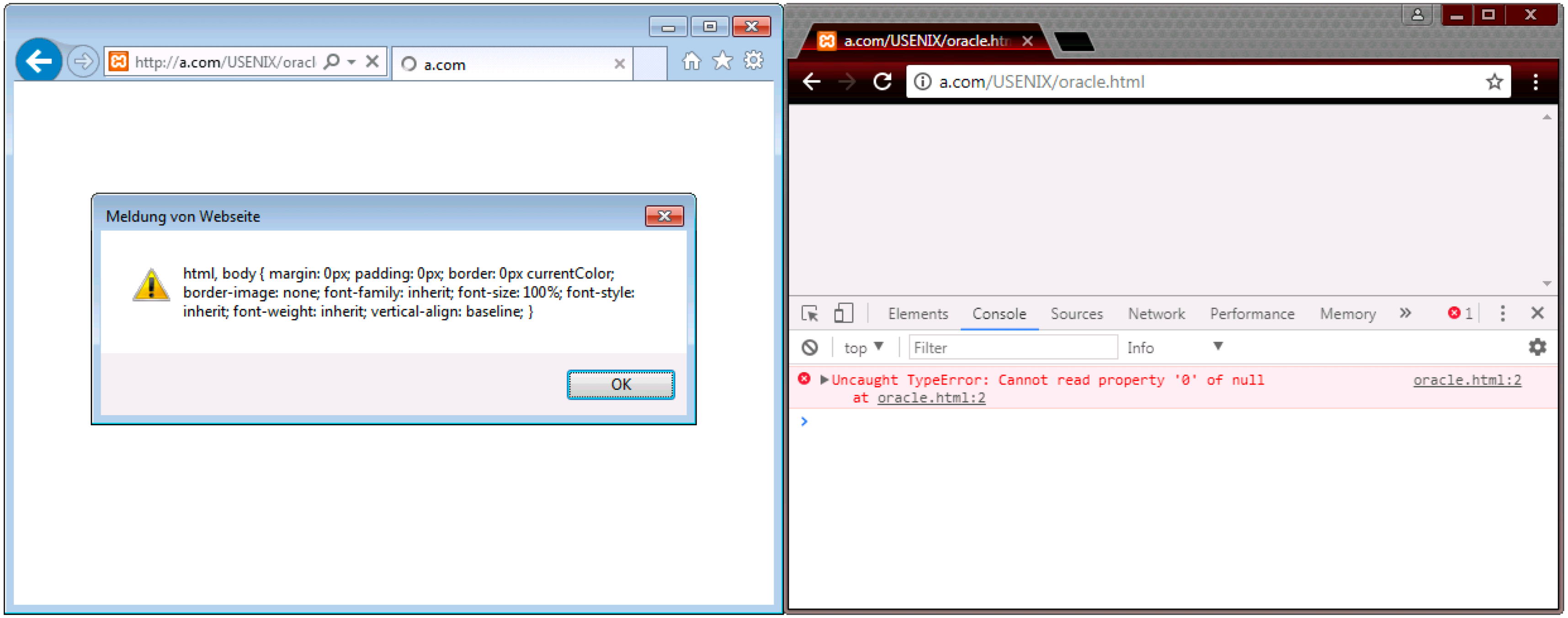
Cross-Origin Login Oracle Attack

- Webserver delivers different CSS files
  - User *logged in* or *logged out*?
- *a.com* attacks *victim.com*

  -
    ```
    <link type="text/css" rel="stylesheet" href="//victim.com/style.css" />
    ```

  -
    ```
    <script>alert(document.styleSheets[0].cssRules[0].cssText)</script>
    ```

Cross-Origin Login Oracle Attack



html, body { margin: 0px; padding: 0px; border: 0px currentColor; border-image: none; font-family: inherit; font-size: 100%; font-style: inherit; font-weight: inherit; vertical-align: baseline; }

```
▶Uncaught TypeError: Cannot read property '0' of null          oracle.html:2
   at oracle.html:2
>
```

3. Limitations & Access Control Policies

Limitations

- 15 HTML elements with `src` attributes
  - Several more with a similar functionality
- Many sandbox attributes, ways to embed a document, MIME types, and pseudoprotocols
- `<link>`: imports, worker
- `<svg>`: JavaScript via xlink
- Growing surface with each new feature

Access Control Policies

- Discretionary Access Control (DAC)
- Role-Based Access Control (RBAC)
  - Enhanced RBAC
- Attribute-Based Access Control (ABAC)

4. Conclusions & Future Work

Conclusions & Future Work

- Different browser data sets to identify inconsistencies (edge cases are important)
- Discussion about access control policies may help to understand the SOP-DOM
- Future Work
  - Other SOP subsets, HTML elements/attributes
  - Pseudoprotocols

Thank you for your attention

✉ marcus.niemietz@rub.de
🐦 @mniemietz