One Click to Rule Them All:
Warum ein Mausklick Schaden anrichten kann

Marcus Niemietz
CEO / Co-Founder

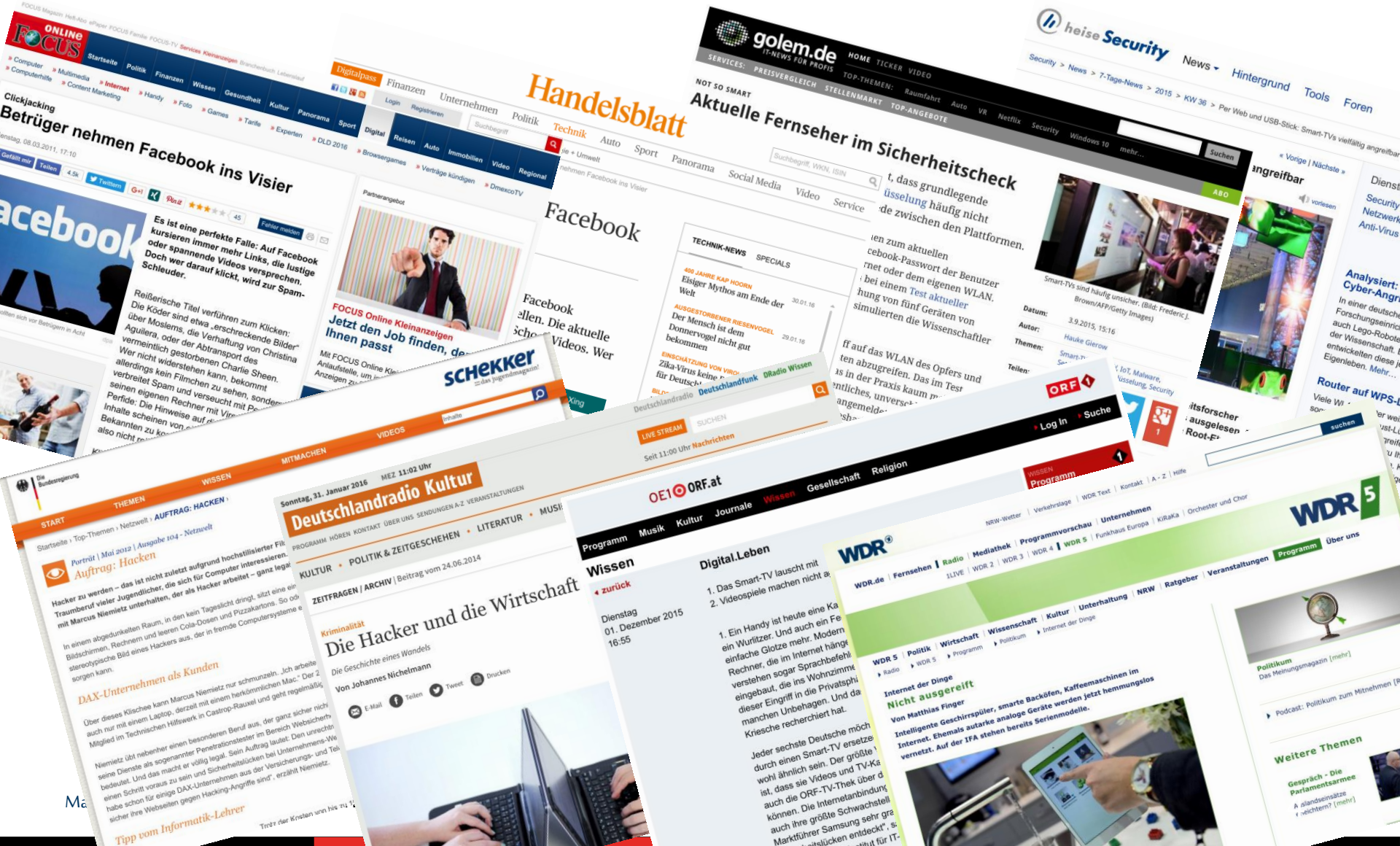
Hackmanit GmbH
www.hackmanit.de

Marcus Niemietz

- Horst Görtz Institute für IT-Sicherheit
- Hackmanit GmbH
- Buch über UI-Redressing
- Sprecher auf Black Hat, BlueHat, PHDays, Zeronights, OWASP, ...
- Twitter: @mniemietz
- mail@mniemietz.de

Mit einem Klick zum Erfolg?

Mit einem Klick zum Erfolg?



Firefox hat diese Website daran gehindert, ein Pop-up-Fenster zu öffnen. Einstellungen

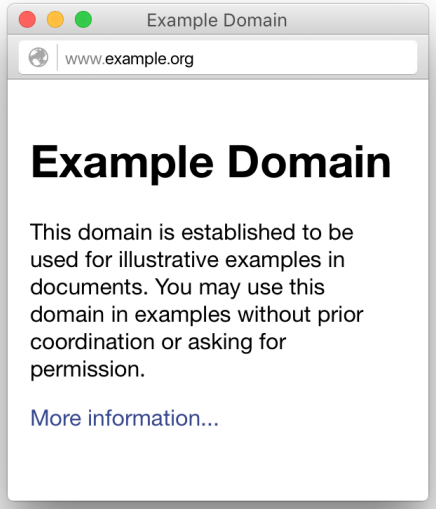
Pop-Up in Firefox

```
<script>
   window.open(
   'http://rub.de', null,
   'height=200, width=400');
</script>
```

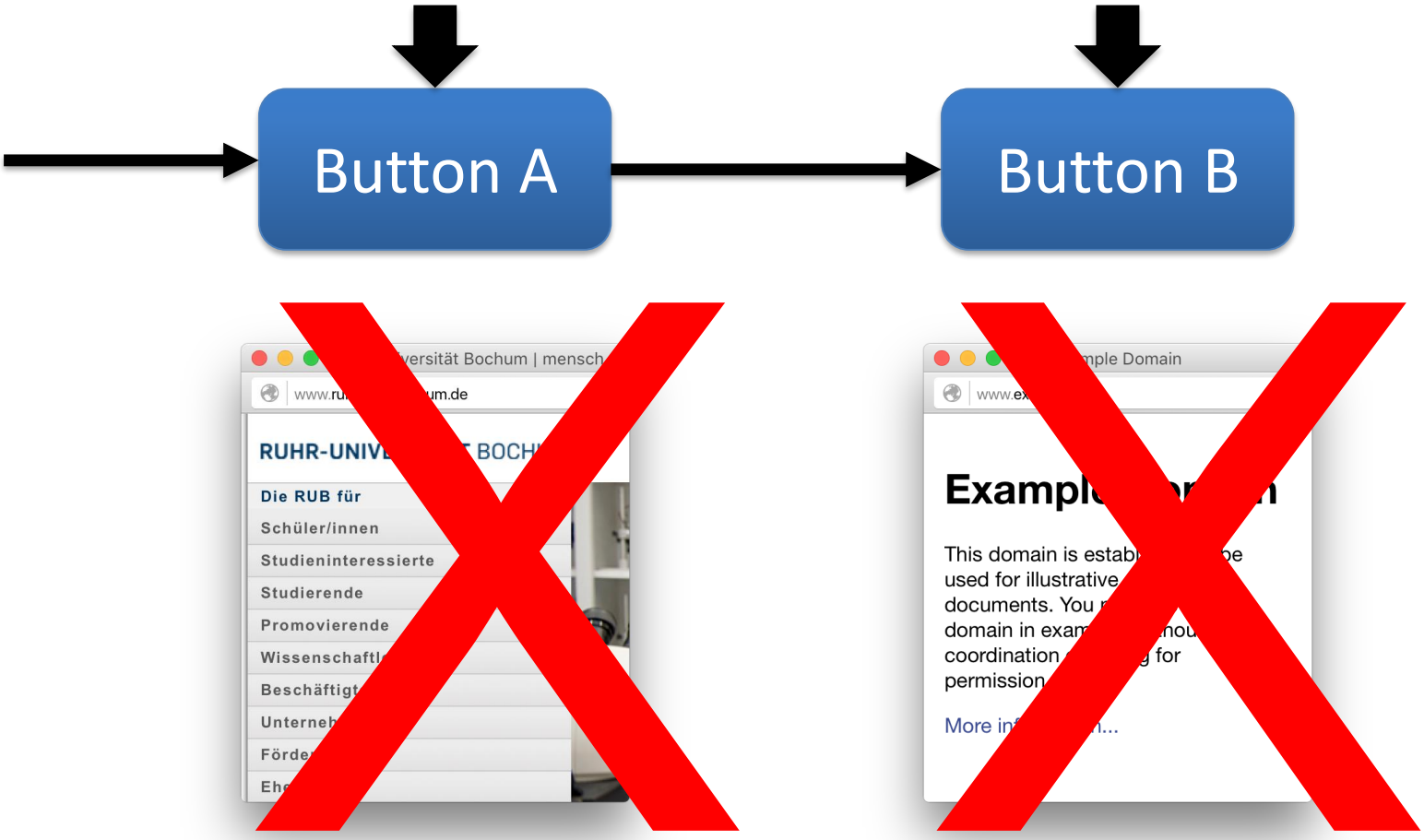
Pop-Up in Firefox: Trusted Events

Button A

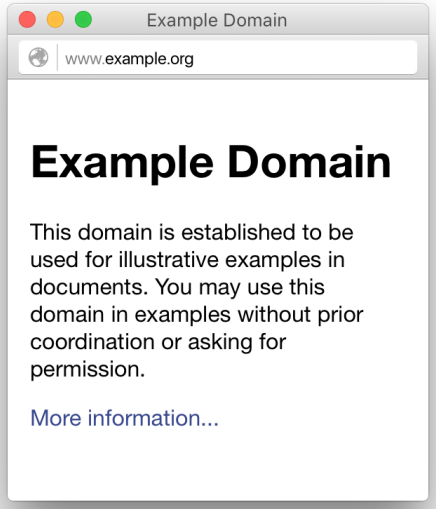
Button B



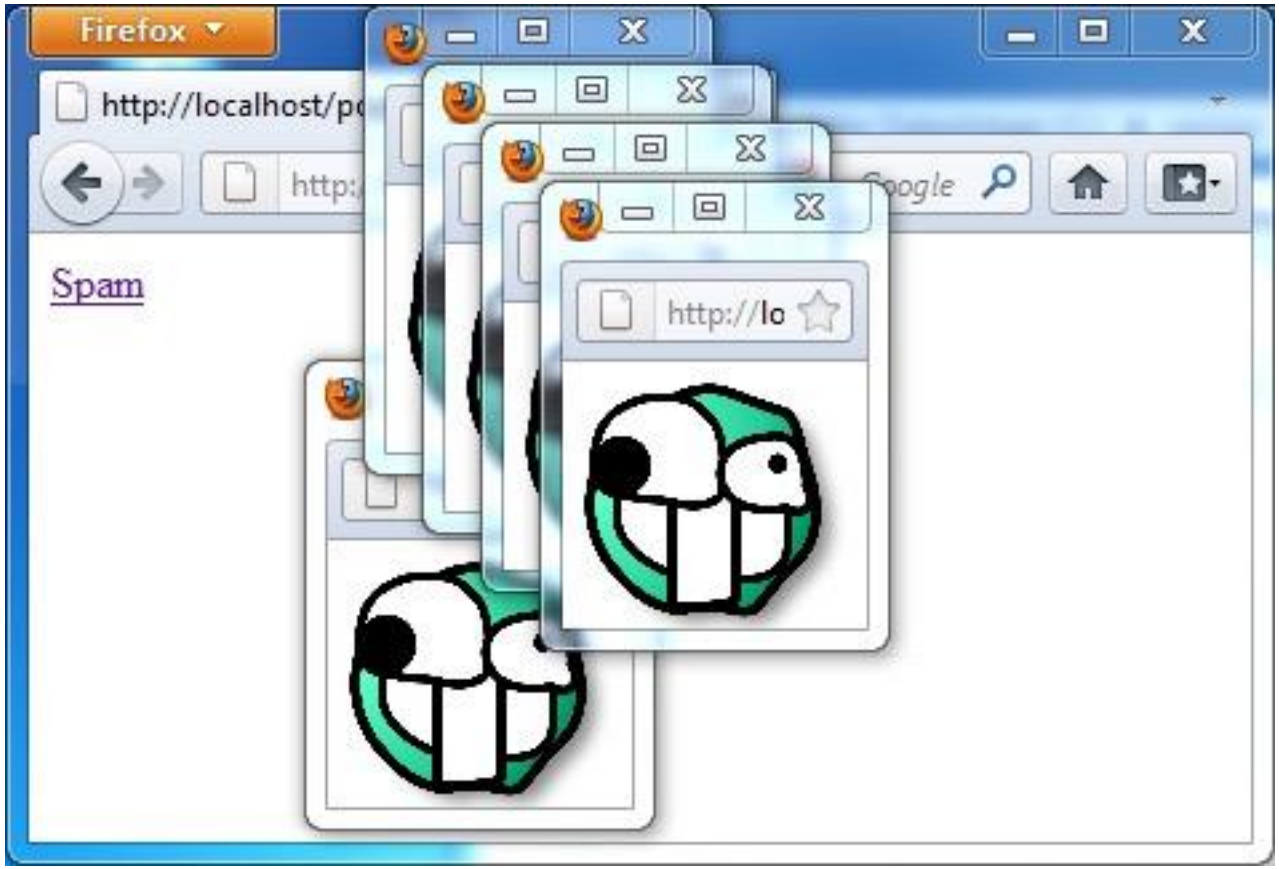
Pop-Up in Firefox: Script Events



Pop-Up in Firefox: Benutzer / Script



Flooding via Trusted Events



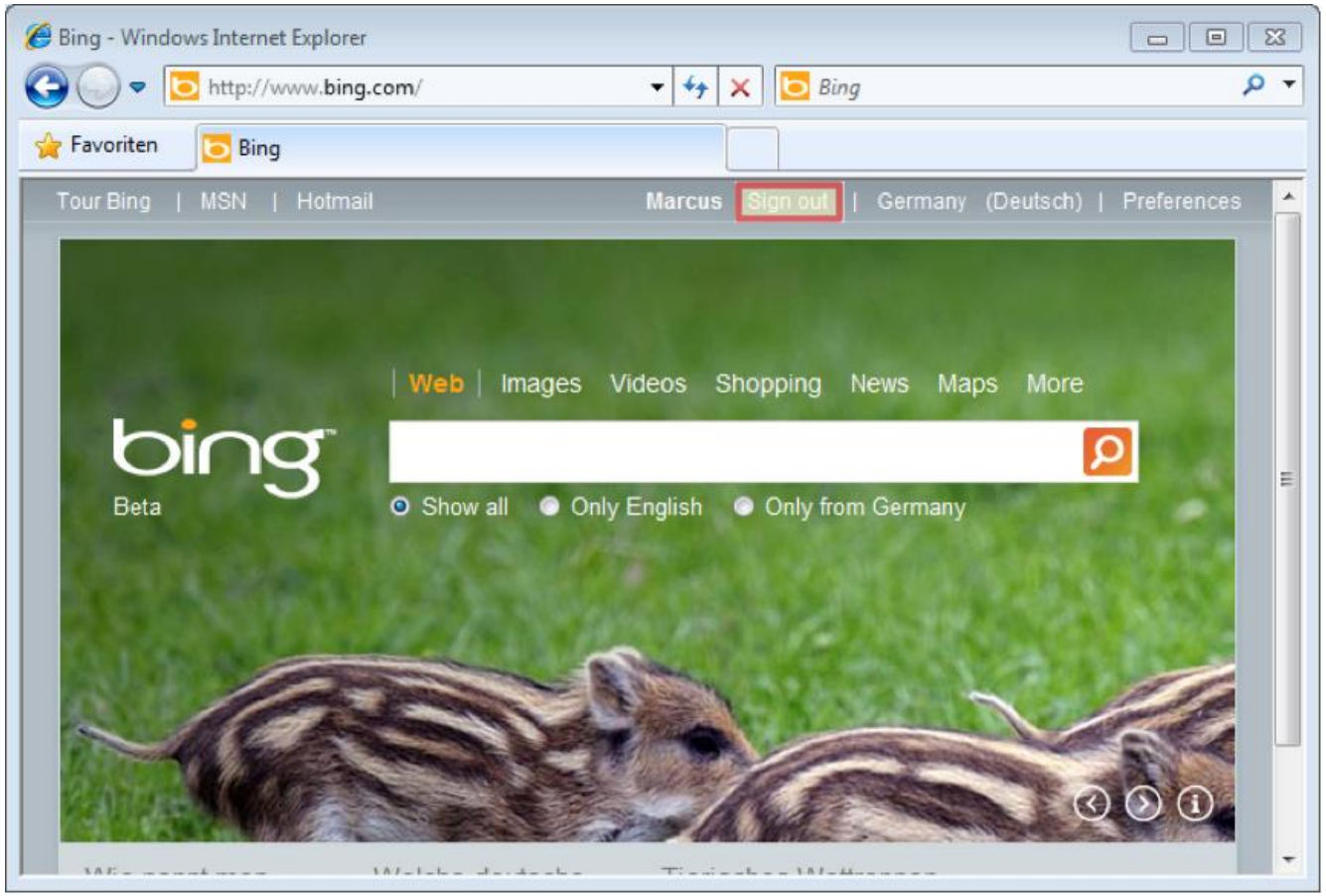
Evaluation von „Pop-Up“-Fenstern

Events	Type	IE 11	FF 47	GC 54	OP 41
load, error, unload	UI	✗			
click, dblclick, mousedown, mouseup (left-click)	Mouse	✓			
contextmenu (right-click)		✓	✗		
mouseenter, mouseleave, mousemove, mouse-out, mouseover (movement)		✗			
drag, dragstart (dragging)		✗			
wheel		✗			
keydown, keyup, keypress	Keyboard	✗		✓	
search (keyboard, left-click)	Multiple	–		(✗,✓)	
select (keyboard, left-click)		(✗,✓)		✓	
input (keyboard, right-click paste)		✗	(✗, ✓)	(✓, ✗)	
focus (keyboard, left-click)		✗		✓	
focusin, focusout (keyboard, left-click)		✗	–	✓	
blur (keyboard, left-click)		✗		✓	(✗, ✓)
scroll (keyboard, wheel)		✗			

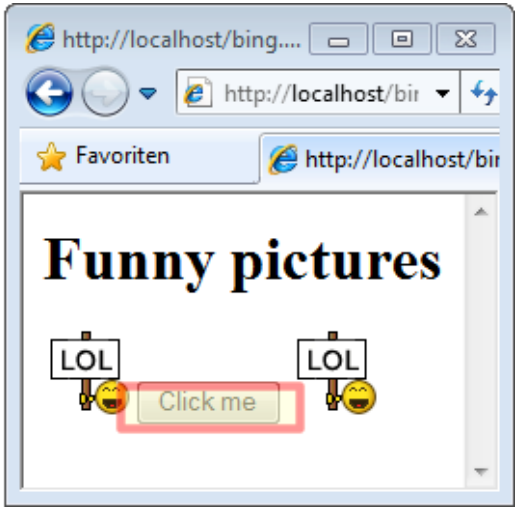
Mehr Klicks, mehr Schaden?

Clickjacking

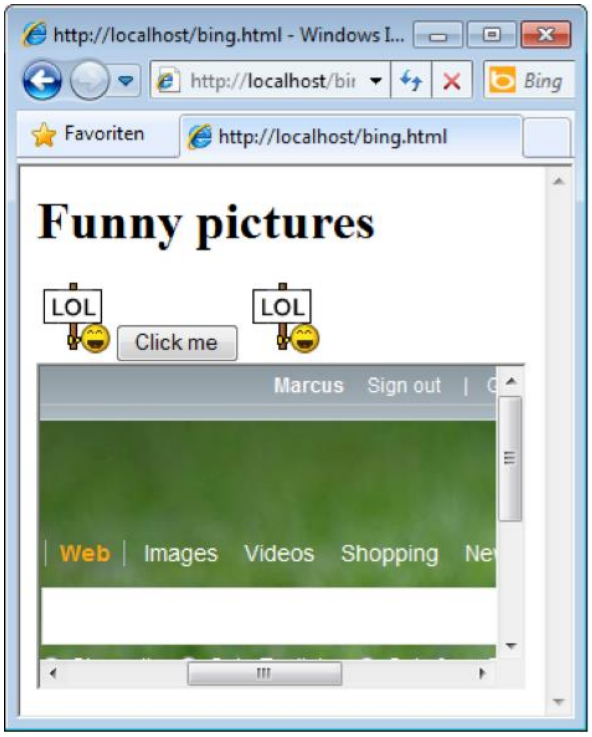
Clickjacking

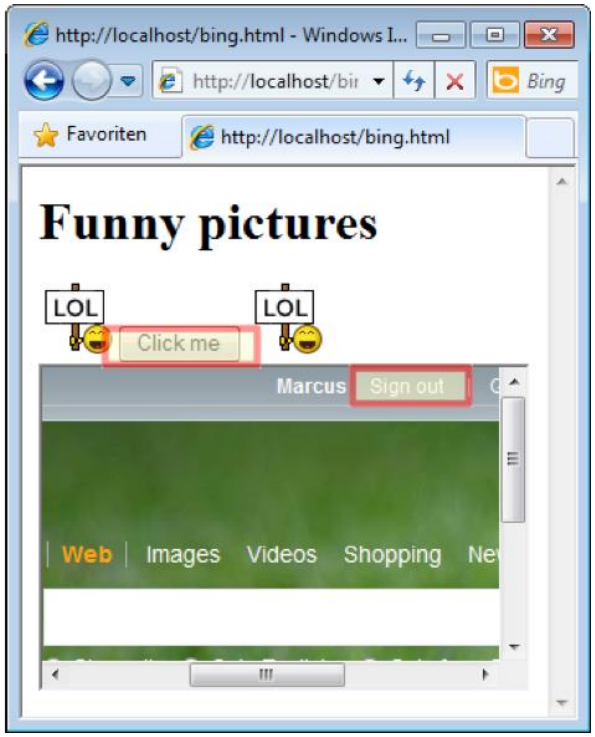


Clickjacking

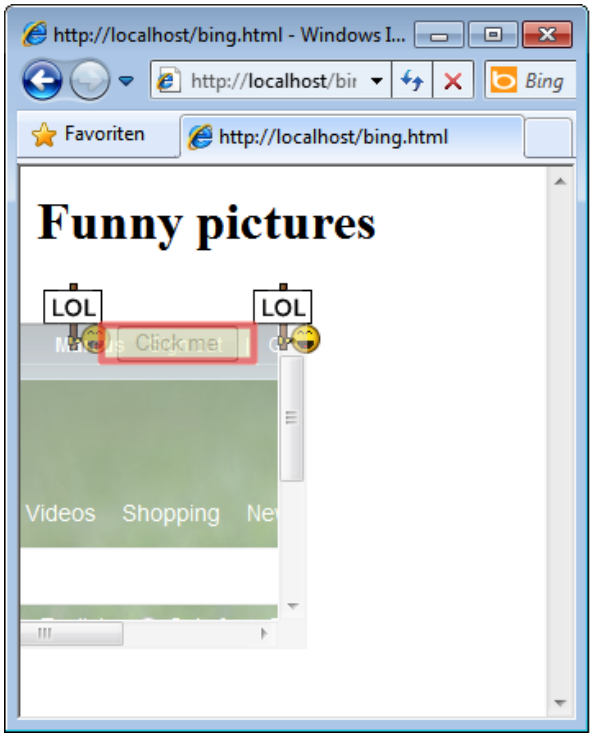


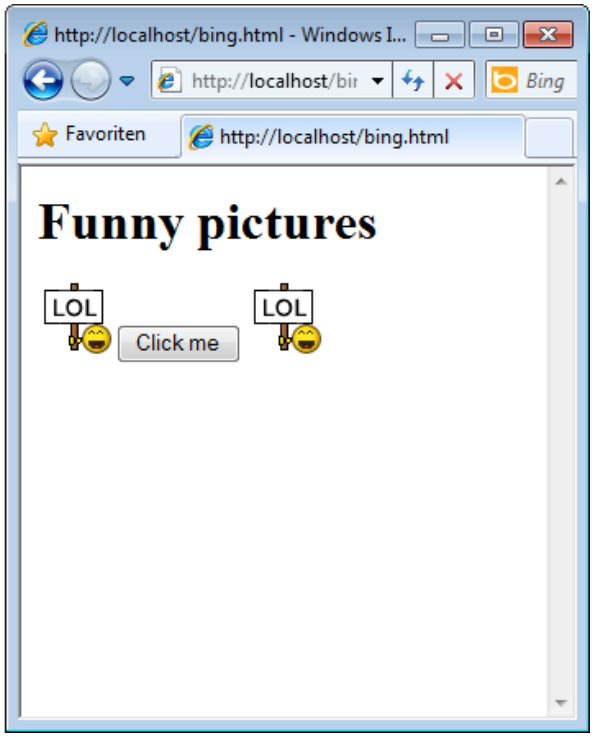
Clickjacking





Clickjacking





Clickjacking

```
<h1>Funny pictures</h1>
<img src="lol.gif">
<button>Click me</button>
<img src="lol.gif">
<iframe style="position:absolute;
opacity:0.0; filter:alpha(opacity=0);
left:-120px; top:95px;" width="300"
height="200“
src="http://www.bing.com"></iframe>
```

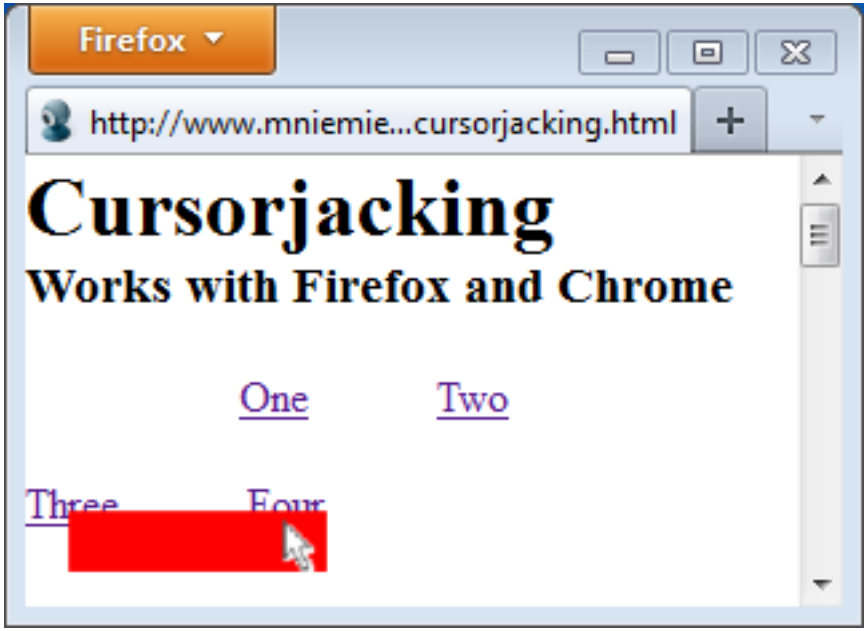
Drag-and-Drop

OWASP: X-Frame-Options

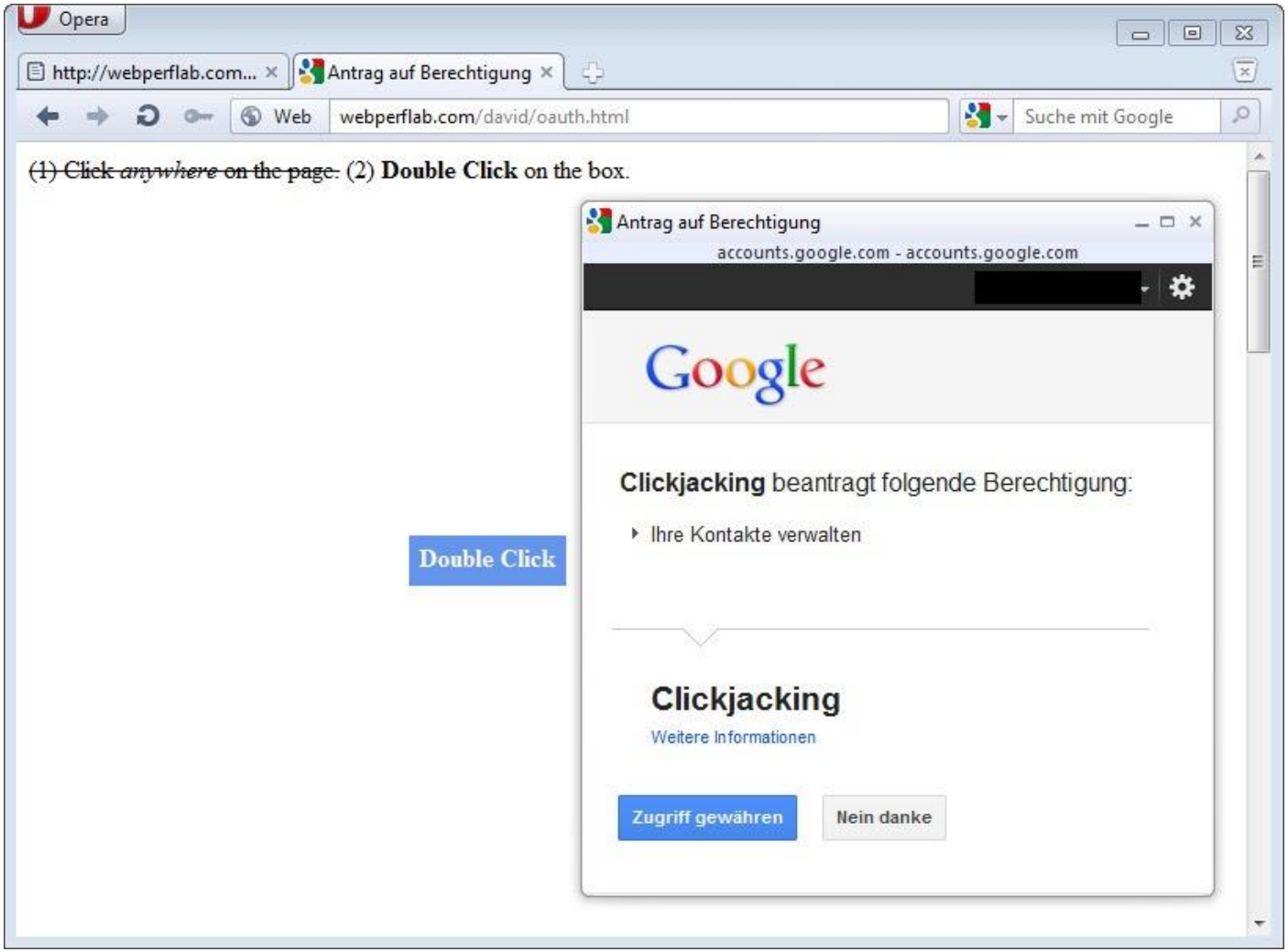
- Eingeführt von Microsoft in 2008
- Seit Oktober 2013: RFC 7034
- Drei Werte
  - DENY
  - SAMEORIGIN
  - ALLOW-FROM URI
- Example:

```
<?php header ("X-Frame-Options: DENY"); ?>
```

Cursorjacking



Double Clickjacking



Clickjacking

- Defacto standardisierte Gegenmaßnahmen mildern Angriffe
  - Helfen nicht vollständig: es bleibt kompliziert
- Neue Standards und Features verschärfen die Problematik
- Content-Security-Policy ist kein Allheilmittel

Hackmanit GmbH

Penetrationstests

Schulungen

Gutachten

- Web Security, Single Sign-On, Applied Crypto
- OAuth, OpenID Connect, SAML, SOAP, XML, REST, SSL/TLS
- https://www.hackmanit.de

Vielen Dank für Ihre Aufmerksamkeit.
Fragen?

marcus.niemietz@hackmanit.de