

# Origin Policy Enforcement in Modern Browsers

## A Case Study in Same Origin Implementations

Frederik Braun

# Table of Contents

## 1 about:me

## 2 Motivation

- Ambient Authentication
- The Severity of a Same Origin Policy Bypass

## 3 The Same Origin Policy

- What is an Origin?
- What is the Same Origin Policy?
- Examples

## 4 Evaluation

- SOP Bypass: Firefox (2007)
- SOP Bypass: Flash (2010)
- SOP Bypass: Java 7 Update 5-X (2012)

## 5 Conclusion

# Table of Contents

## 1 about:me

## 2 Motivation

- Ambient Authentication
- The Severity of a Same Origin Policy Bypass

## 3 The Same Origin Policy

- What is an Origin?
- What is the Same Origin Policy?
- Examples

## 4 Evaluation

- SOP Bypass: Firefox (2007)
- SOP Bypass: Flash (2010)
- SOP Bypass: Java 7 Update 5-X (2012)

## 5 Conclusion

- Dipl. Ing. in IT-Security at Ruhr-Uni Bochum (2012)
  - ▶ this research!
  - ▶ <https://frederik-braun.com/thesis>
- Security Engineer at Mozilla in Berlin
- likes to play CTFs (hi FluxFingers!)
- @freddyb on twitter

# Table of Contents

## 1 about:me

## 2 Motivation

- Ambient Authentication
- The Severity of a Same Origin Policy Bypass

## 3 The Same Origin Policy

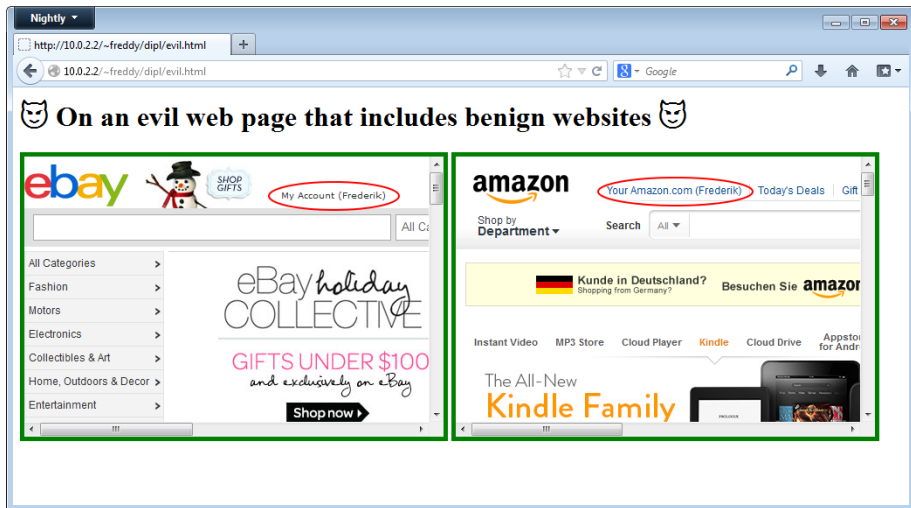
- What is an Origin?
- What is the Same Origin Policy?
- Examples

## 4 Evaluation

- SOP Bypass: Firefox (2007)
- SOP Bypass: Flash (2010)
- SOP Bypass: Java 7 Update 5-X (2012)

## 5 Conclusion

# Ambient Authentication



# The Severity of a Same Origin Policy Bypass



## Security Vulnerability in Firefox 16

### Issue:

Mozilla is aware of a security vulnerability in the current release version of Firefox (version 16). We are actively working on a fix and plan to ship updates tomorrow. Firefox version 15 is unaffected.

### Impact:

The vulnerability could allow a malicious site to potentially determine which websites users have visited and have access to the URL or URL parameters. At this time we have no indication that this vulnerability is currently being exploited in the wild.

### Status:

Firefox 16 has been temporarily removed from the current installer page and users will automatically be upgraded to the new version as soon as it becomes available. As a precaution, users can downgrade to version 15.0.1 by following these instructions <http://www.mozilla.org>

# Table of Contents

## 1 about:me

## 2 Motivation

- Ambient Authentication
- The Severity of a Same Origin Policy Bypass

## 3 The Same Origin Policy

- What is an Origin?
- What is the Same Origin Policy?
- Examples

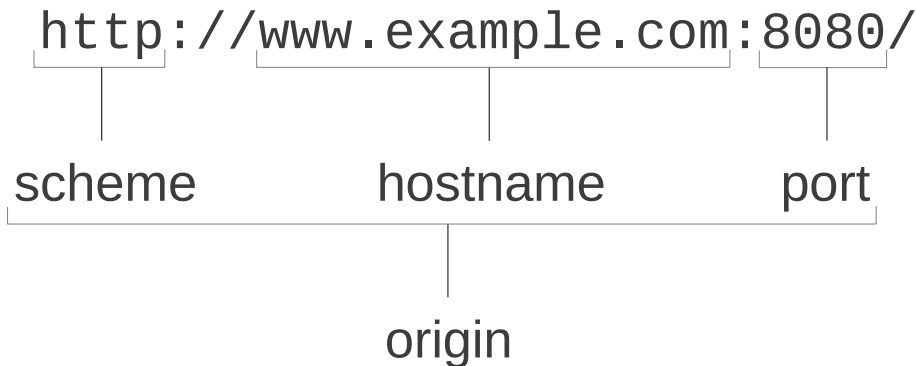
## 4 Evaluation

- SOP Bypass: Firefox (2007)
- SOP Bypass: Flash (2010)
- SOP Bypass: Java 7 Update 5-X (2012)

## 5 Conclusion



# What is an Origin?



# The Same Origin Policy (SOP)

“An ‘origin’ (...) is often used as the scope of authority or privilege by user agents. ” — Barth

“The same-origin policy is the most important mechanism we have to keep hostile web applications at bay, but it’s also an imperfect one.” — Zalewski

# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	

# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	✓

# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	✓
<code>https://www.example.com/</code>	

# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	✓
<code>https://www.example.com/</code>	✗

# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	✓
<code>https://www.example.com/</code>	✗
<b><code>about:blank</code></b>	

# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	✓
<code>https://www.example.com/</code>	✗
<b><code>about:blank</code></b>	✓



# Examples

Compare for <http://www.example.com/>

URL	same-origin?
<a href="http://www.example.com/help">http://www.example.com/help</a>	✓
<a href="https://www.example.com/">https://www.example.com/</a>	✗
<b>about:blank</b>	✓
<a href="http://www.example.com:8000/phpMyAdmin">http://www.example.com:8000/phpMyAdmin</a>	

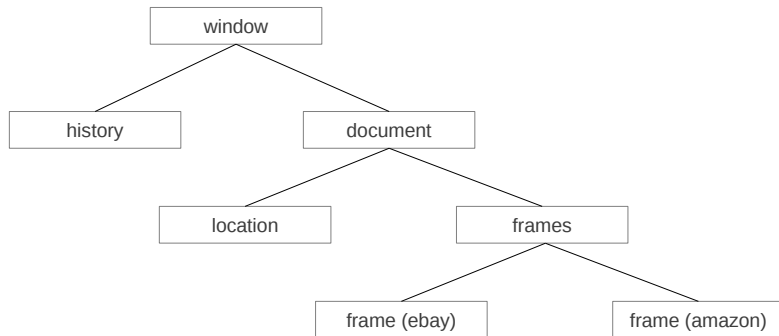
# Examples

Compare for `http://www.example.com/`

URL	same-origin?
<code>http://www.example.com/help</code>	✓
<code>https://www.example.com/</code>	✗
<b><code>about:blank</code></b>	✓
<code>http://www.example.com:8000/phpMyAdmin</code>	✗/✓ <sup>a</sup>

<sup>a</sup>Internet Explorer doesn't care about ports.

# JavaScript Object Hierarchy





# SOP Wrap-Up

## Summary

- read access
- vendor specific
- JavaScript Engine (Object Capability) vs. DOM (Access Control)
- the SOP is highly inhomogenous
- no consistent reference implementation

# Table of Contents

## 1 about:me

## 2 Motivation

- Ambient Authentication
- The Severity of a Same Origin Policy Bypass

## 3 The Same Origin Policy

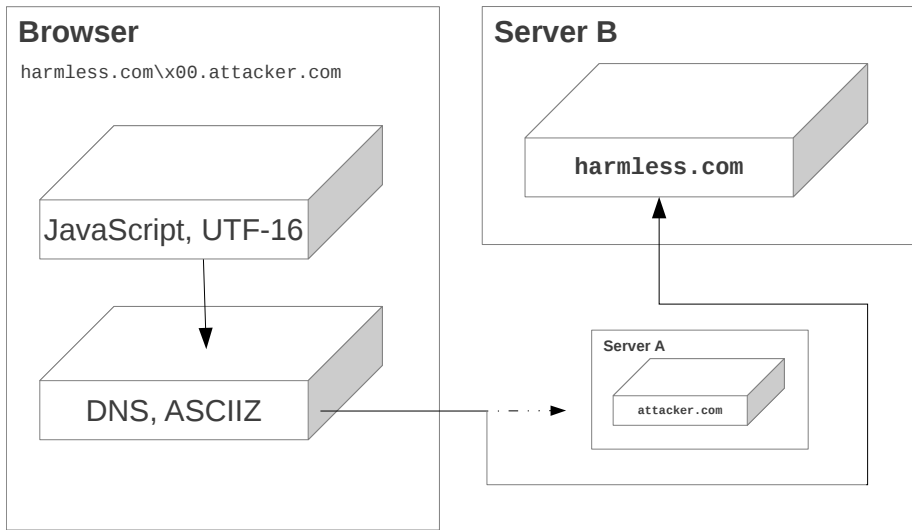
- What is an Origin?
- What is the Same Origin Policy?
- Examples

## 4 Evaluation

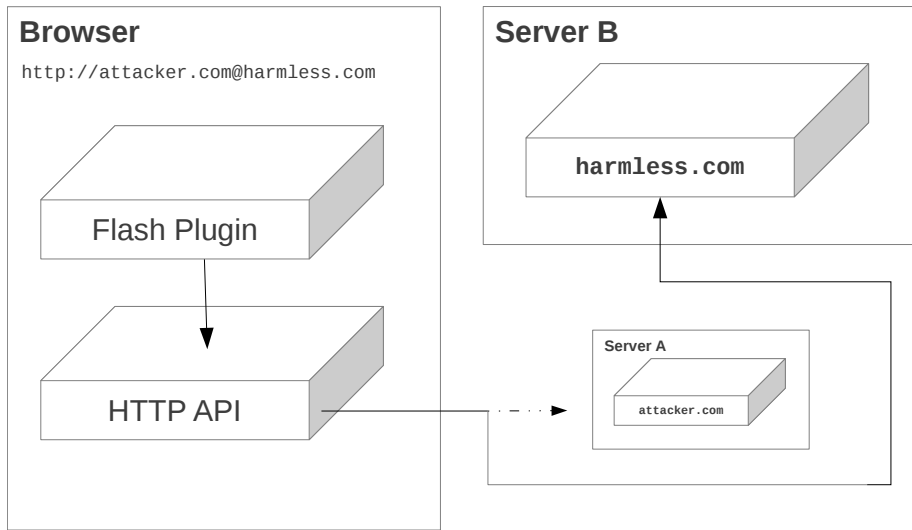
- SOP Bypass: Firefox (2007)
- SOP Bypass: Flash (2010)
- SOP Bypass: Java 7 Update 5-X (2012)

## 5 Conclusion

# All SOP Flaws are alike (CVE-2007-0981)

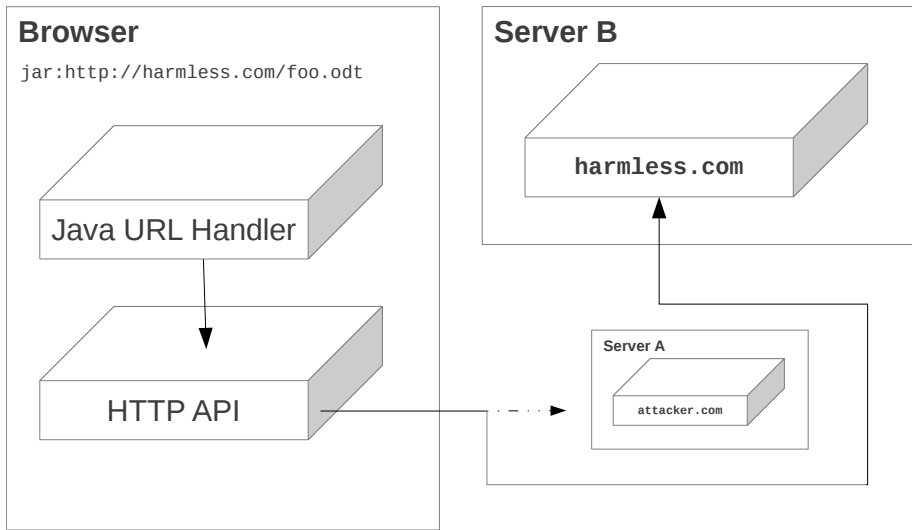


# All SOP Flaws are alike (CVE-2010-2179)





# All SOP Flaws are alike (CVE TBA)



# Demo

# Table of Contents

## 1 about:me

## 2 Motivation

- Ambient Authentication
- The Severity of a Same Origin Policy Bypass

## 3 The Same Origin Policy

- What is an Origin?
- What is the Same Origin Policy?
- Examples

## 4 Evaluation

- SOP Bypass: Firefox (2007)
- SOP Bypass: Flash (2010)
- SOP Bypass: Java 7 Update 5-X (2012)

## 5 Conclusion

# Conclusion: Same Origin Policy

- an inconsistent policy
- vendor specific
- theoretically, it's a black list
- plugins
- late 2012: Java in nearly 70% of all browsers
- but only 0.2% of websites
- 2013: exploits, Click-To-Play, ..
- But: There are safe & well designed security models on the horizon

# Future Work: Automation?



Picture by Jason Huggins on flickr

“This same origin policy is the dumbest thing ever. . . . All this ‘protection’ serves to do is aggravate legitimate developers trying to get JavaScript to do the simplest of tasks.” — Somebody on [stackoverflow.com](https://stackoverflow.com)

Thanks

# References



Barth, Adam.

The web origin concept.

<http://tools.ietf.org/html/rfc6454>, December 2011.



Q-Success.

Usage of client-side programming languages for websites.

[http://w3techs.com/technologies/overview/client\\_side\\_language/all](http://w3techs.com/technologies/overview/client_side_language/all).

Last visited 2012-10-17.



Michal Zalewski.

*The Tangled Web: A Guide to Securing Modern Web Applications.*

No Starch Press, November 2011.

- For all references please see full thesis on <https://frederik-braun.com/thesis>