Making Sense of CORS using web.py

zach wick
zwick@bareo.io

July 28, 2015

Agenda

- About the speaker
- HTTP Primer
- What is CORS
- Why is CORS useful
- How does CORS work
  - HTTP
  - Simple Requests
  - Other Requests
- Worked Example
- Best Practices
- Questions (and hopefully answers)

About the Speaker

HTTP Primer

- application protocol

HTTP Primer

- application protocol
- uses request verbs

HTTP Primer

- application protocol
- uses request verbs
  - HTTP/1.0 — GET POST HEAD

HTTP Primer

- application protocol
- uses request verbs
    - HTTP/1.0 — GET POST HEAD
    - HTTP/1.1 — OPTIONS PUT DELETE TRACE CONNECT

HTTP Primer

- application protocol
- uses request verbs
  - HTTP/1.0 — GET POST HEAD
  - HTTP/1.1 — OPTIONS PUT DELETE TRACE CONNECT
  - RFC 5789 — PATCH

HTTP Primer

- application protocol
- uses request verbs
  - HTTP/1.0 — GET POST HEAD
  - HTTP/1.1 — OPTIONS PUT DELETE TRACE CONNECT
  - RFC 5789 — PATCH
  - Other specs & RFC's

HTTP Primer

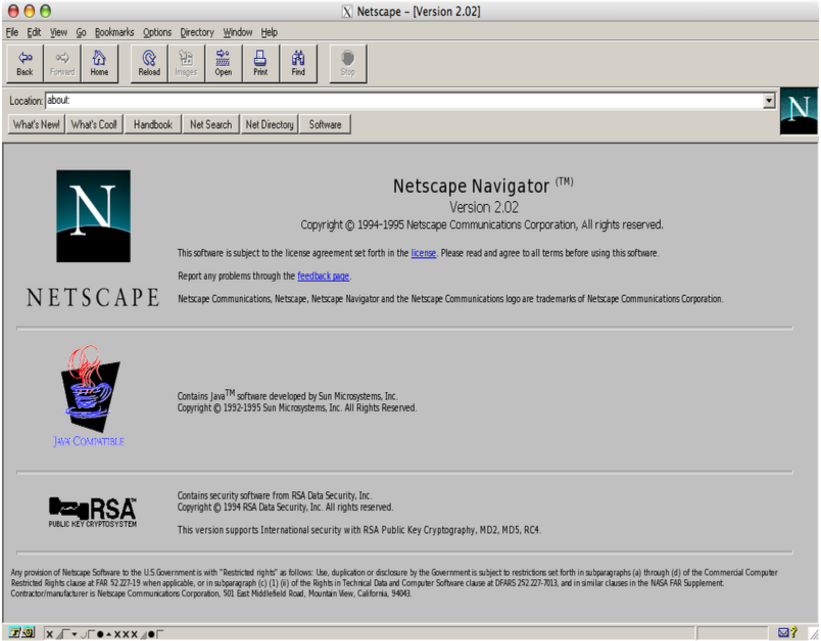
- application protocol
- uses request verbs
  - HTTP/1.0 — GET POST HEAD
  - HTTP/1.1 — OPTIONS PUT DELETE TRACE CONNECT
  - RFC 5789 — PATCH
  - Other specs & RFC's
  - * Other user defined verbs *

HTTP Primer

- application protocol
- uses request verbs
  - HTTP/1.0 — GET POST HEAD
  - HTTP/1.1 — OPTIONS PUT DELETE TRACE CONNECT
  - RFC 5789 — PATCH
  - Other specs & RFC's
  - * Other user defined verbs *
- idempotent vs. non-idempotent

HTTP Primer

- application protocol
- uses request verbs
  - HTTP/1.0 — GET POST HEAD
  - HTTP/1.1 — OPTIONS PUT DELETE TRACE CONNECT
  - RFC 5789 — PATCH
  - Other specs & RFC's
  - * Other user defined verbs *
- idempotent vs. non-idempotent
- status codes



about:

Netscape Navigator (TM)

Version 2.02

Copyright © 1994-1995 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

Report any problems through the feedback page.

Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.

Contains Java^{TM} software developed by Sun Microsystems, Inc.
Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.

Contains security software from RSA Data Security, Inc.
Copyright © 1994 RSA Data Security, Inc. All rights reserved.

This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.

Any provision of Netscape Software to the U.S.Government is with "Restricted rights" as follows: Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Netscape Communications Corporation, 501 East Middlefield Road, Mountain View, California, 94043.

In the Beginning There Was Netscape Navigator 2

- LiveScript (now called JavaScript)

In the Beginning There Was Netscape Navigator 2

- LiveScript (now called JavaScript)
- Plugin Support

In the Beginning There Was Netscape Navigator 2

- LiveScript (now called JavaScript)
- Plugin Support
- HTML Frames (iframes)

In the Beginning There Was Netscape Navigator 2

- LiveScript (now called JavaScript)
- Plugin Support
- HTML Frames (iframes)
- Same-Origin Policy

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) $=$ Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	Origin Tuple Matches
http://www.example.com/d2/p3.html	

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	Origin Tuple Matches
http://www.example.com/d2/p3.html	Origin Tuple Matches
https://www.example.com/dir/p2.html	

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	Origin Tuple Matches
http://www.example.com/d2/p3.html	Origin Tuple Matches
https://www.example.com/dir/p2.html	Protocol Differs
http://www.example.com:82/dir/p2.html	

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	Origin Tuple Matches
http://www.example.com/d2/p3.html	Origin Tuple Matches
https://www.example.com/dir/p2.html	Protocol Differs
http://www.example.com:82/dir/p2.html	Port Differs
http://example.com/dir/p2.html	

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	Origin Tuple Matches
http://www.example.com/d2/p3.html	Origin Tuple Matches
https://www.example.com/dir/p2.html	Protocol Differs
http://www.example.com:82/dir/p2.html	Port Differs
http://example.com/dir/p2.html	Host Differs
http://www.example.com:80/dir/p2.html	

Same-Origin Policy

- Applies to DOM manipulation and others (XMLHttpRequest)
- (protocol, host, port) = Origin
- Tuples must match

http://www.example.com/dir/page.html

Compared URL	Reason
http://www.example.com/dir/p2.html	Origin Tuple Matches
http://www.example.com/d2/p3.html	Origin Tuple Matches
https://www.example.com/dir/p2.html	Protocol Differs
http://www.example.com:82/dir/p2.html	Port Differs
http://example.com/dir/p2.html	Host Differs
http://www.example.com:80/dir/p2.html	Implementation Based

How to Get Around Same-Origin Policy

What Do We Want?

Any Domain

What Do We Want?

Any Domain

- images

What Do We Want?

Any Domain

- images
- scripts

What Do We Want?

Any Domain

- images
- scripts
- stylesheets

What Do We Want?

Any Domain

- images
- scripts
- stylesheets
- iframes

What Do We Want?

Any Domain

- images
- scripts
- stylesheets
- iframes
- videos

What Do We Want?

Any Domain

- images
- scripts
- stylesheets
- iframes
- videos
- some plugin content

What Do We Want?

Any Domain

- images
- scripts
- stylesheets
- iframes
- videos
- some plugin content

Only Special Domains

What Do We Want?

Any Domain

- images
- scripts
- stylesheets
- iframes
- videos
- some plugin content

Only Special Domains

- embedded web fonts

What Do We Want?

Any Domain

- images
- scripts
- stylesheets
- iframes
- videos
- some plugin content

Only Special Domains

- embedded web fonts
- AJAX

What about JSONP?

- JSON with padding

What about JSONP?

- JSON with padding
- works via HTML script tags (in the 'Any Domain' column)

What about JSONP?

- JSON with padding
- works via HTML script tags (in the 'Any Domain' column)
- only GET

Why is CORS useful?

- AJAX to non-origin domains

How does CORS work?