Web Application Security Issues

What happens when people start building security critical applications on top of HTML+CSS+JavaScript?

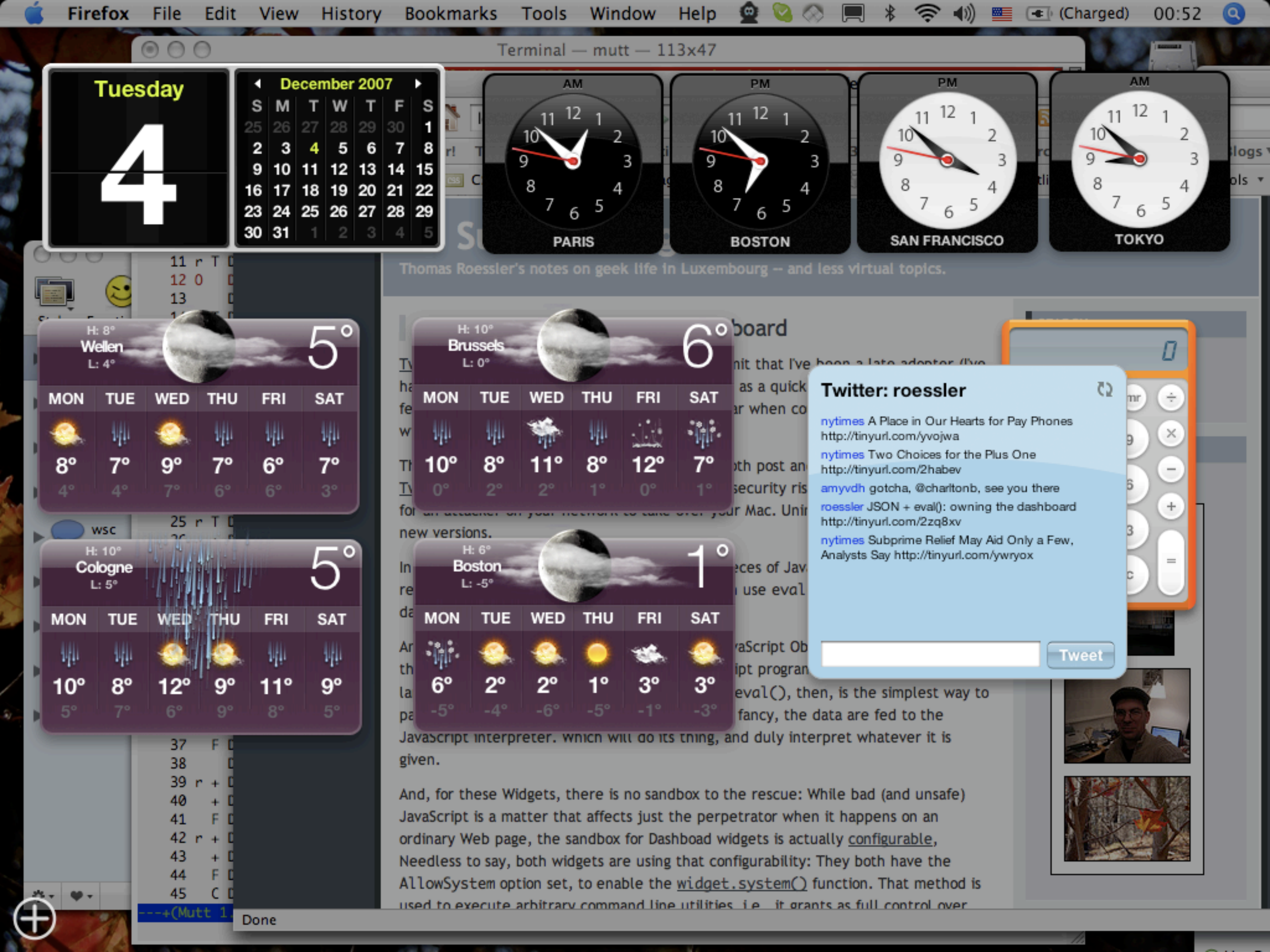
What can we learn from that for the technologies that we design?

1. Widgets
2. Mash-ups

<|>

Widgets

e.g., MacOS Dashboard



S	M	T	W	T	F	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Wellen H: 8° L: 4° 5°

MON	TUE	WED	THU	FRI	SAT
8°	7°	9°	7°	6°	7°
4°	4°	7°	6°	6°	3°

Brussels H: 10° L: 0° 6°

MON	TUE	WED	THU	FRI	SAT
10°	8°	11°	8°	12°	7°
0°	2°	2°	1°	0°	1°

Cologne H: 10° L: 5° 5°

MON	TUE	WED	THU	FRI	SAT
10°	8°	12°	9°	11°	9°
5°	7°	6°	9°	8°	5°

Boston H: 6° L: -5° 1°

MON	TUE	WED	THU	FRI	SAT
6°	2°	2°	1°	3°	3°
-5°	-4°	-6°	-5°	-1°	-3°

```
 11 r T D
 12 O   D
 13     D
 25 r T D
 37   F D
 38     D
 39 r + D
 40   + D
 41   F D
 42 r + D
 43   + D
 44   F D
 45   C D
```

Twitter: roessler

nytimes A Place in Our Hearts for Pay Phones http://tinyurl.com/yvojwa

nytimes Two Choices for the Plus One http://tinyurl.com/2habev

amyvdh gotcha, @charltonb, see you there

roessler JSON + eval(): owning the dashboard http://tinyurl.com/2zq8xv

nytimes Subprime Relief May Aid Only a Few, Analysts Say http://tinyurl.com/ywryox

Thomas Roessler's notes on geek life in Luxembourg -- and less virtual topics.

board

nit that I've been a late adopter (I've

as a quick

r when co

oth post an

security ris

for an attacker on your network to take over your Mac. Unin

new versions.

eces of Jav

use eval

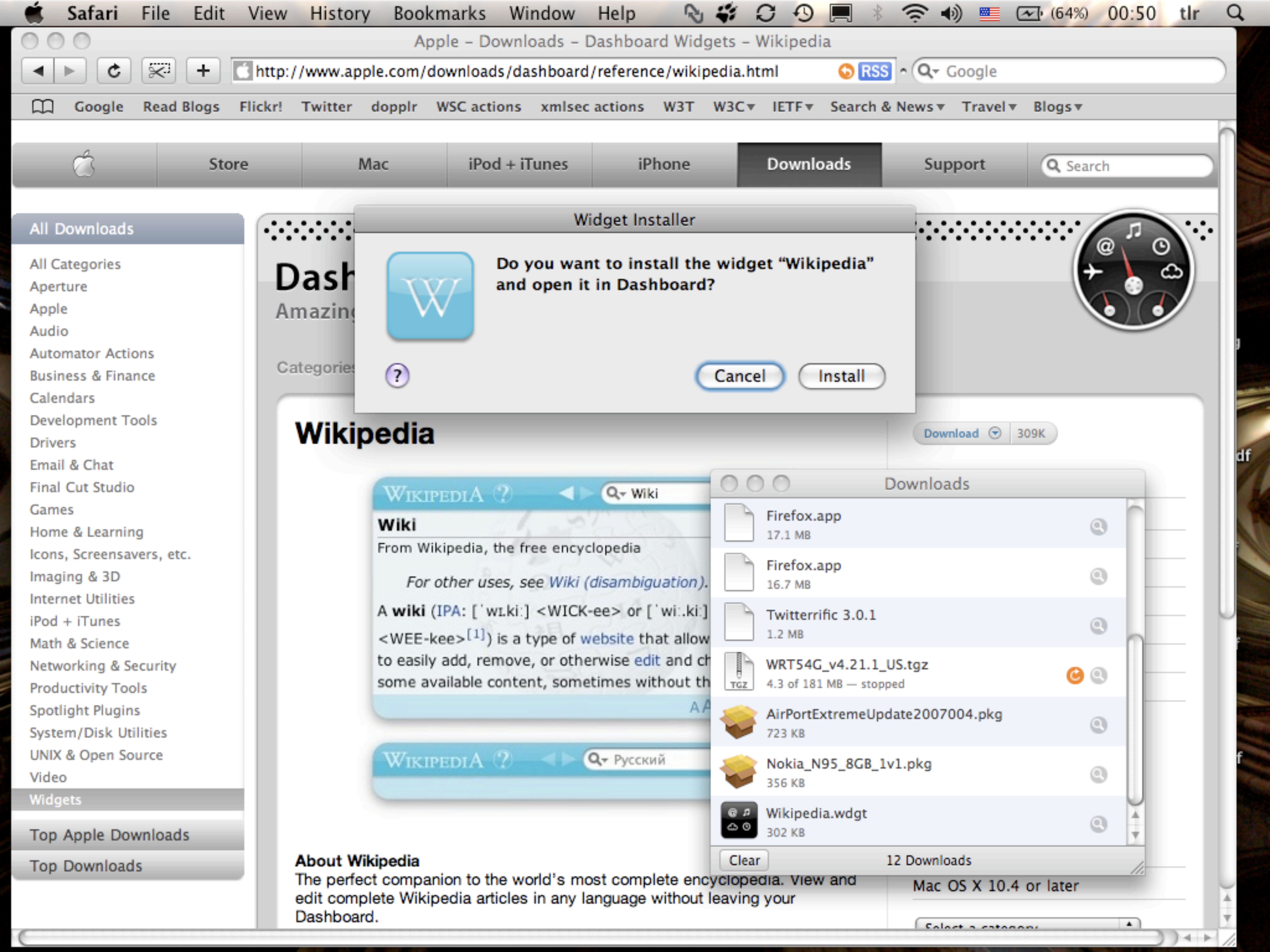
aScript Ob

ipt progran

eval(), then, is the simplest way to

fancy, the data are fed to the JavaScript interpreter. which will do its thing, and duly interpret whatever it is given.

And, for these Widgets, there is no sandbox to the rescue: While bad (and unsafe) JavaScript is a matter that affects just the perpetrator when it happens on an ordinary Web page, the sandbox for Dashboad widgets is actually configurable, Needless to say, both widgets are using that configurability: They both have the AllowSystem option set, to enable the widget.system() function. That method is used to execute arbitrary command line utilities, i.e., it grants as full control over


Safari File Edit View History Bookmarks Window Help
(64%) 00:50 tlr
Apple – Downloads – Dashboard Widgets – Wikipedia
http://www.apple.com/downloads/dashboard/reference/wikipedia.html
RSS
Google
Google Read Blogs Flickr! Twitter dopplr WSC actions xmlsec actions W3T W3C▾ IETF▾ Search & News▾ Travel▾ Blogs▾
Store Mac iPod + iTunes iPhone Downloads Support
Search
Dash
Amazin
Categorie
Cancel
Install
Download 309K
Clear

Widget Installer

Do you want to install the widget "Wikipedia" and open it in Dashboard?

All Downloads

- All Categories
- Aperture
- Apple
- Audio
- Automator Actions
- Business & Finance
- Calendars
- Development Tools
- Drivers
- Email & Chat
- Final Cut Studio
- Games
- Home & Learning
- Icons, Screensavers, etc.
- Imaging & 3D
- Internet Utilities
- iPod + iTunes
- Math & Science
- Networking & Security
- Productivity Tools
- Spotlight Plugins
- System/Disk Utilities
- UNIX & Open Source
- Video
- Widgets

Top Apple Downloads

Top Downloads

Wikipedia

WIKIPEDIA ? Wiki

Wiki

From Wikipedia, the free encyclopedia

For other uses, see Wiki (disambiguation).

A **wiki** (IPA: [ˈwɪ.ki] <WICK-ee> or [ˈwiː.ki] <WEE-kee>[1]) is a type of website that allow to easily add, remove, or otherwise edit and ch some available content, sometimes without th

WIKIPEDIA ? Русский

Downloads

Firefox.app	17.1 MB
Firefox.app	16.7 MB
Twitterrific 3.0.1	1.2 MB
WRT54G_v4.21.1_US.tgz	4.3 of 181 MB — stopped
AirPortExtremeUpdate2007004.pkg	723 KB
Nokia_N95_8GB_1v1.pkg	356 KB
Wikipedia.wdgt	302 KB

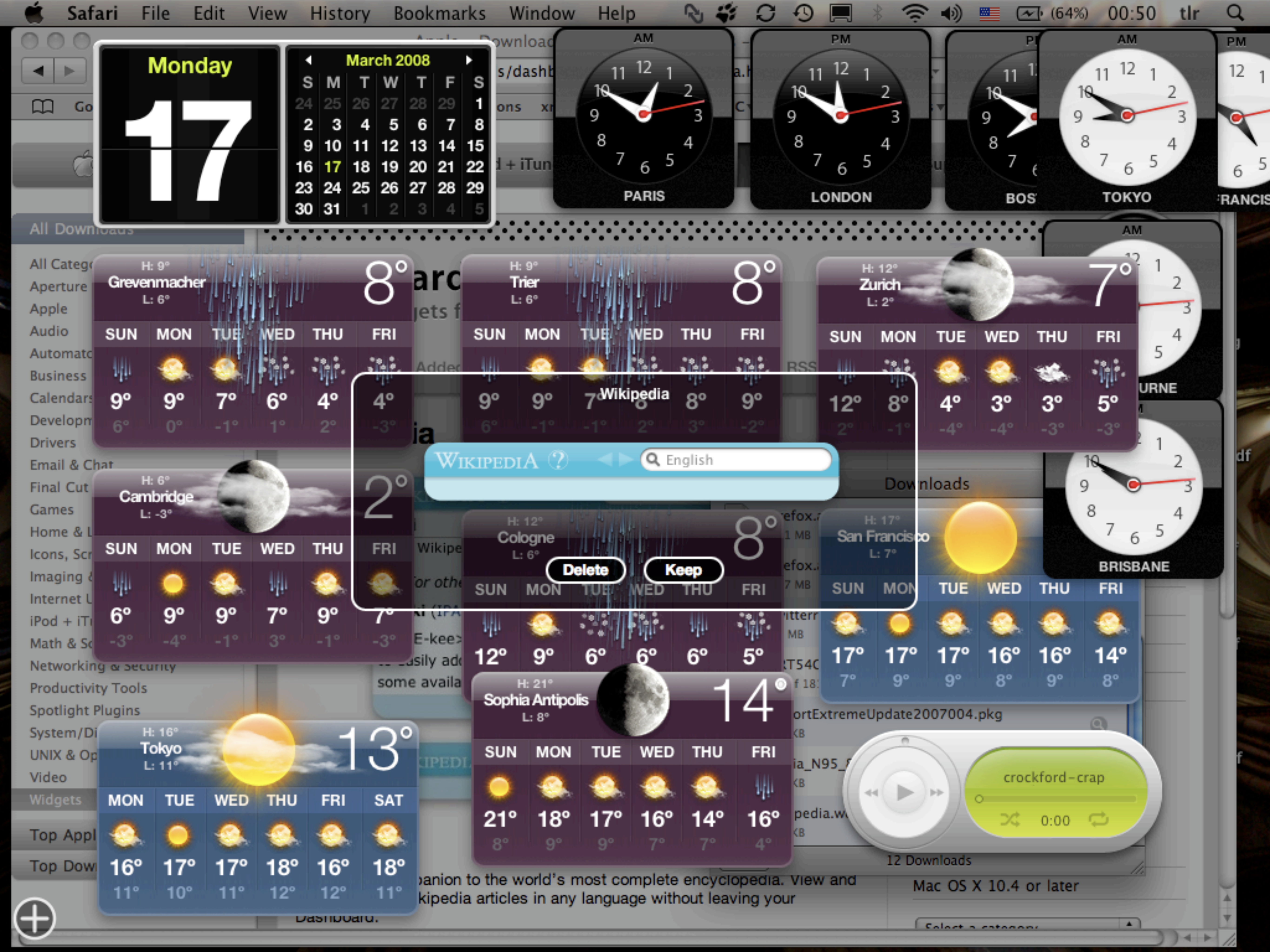
12 Downloads

About Wikipedia

The perfect companion to the world's most complete encyclopedia. View and edit complete Wikipedia articles in any language without leaving your Dashboard.

Mac OS X 10.4 or later

Select a category



Monday 17

March 2008						
S	M	T	W	T	F	S
24	25	26	27	28	29	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Grevenmacher H: 9° L: 6° 8°

SUN	MON	TUE	WED	THU	FRI
9°	9°	7°	6°	4°	4°
6°	0°	-1°	1°	2°	-3°

Trier H: 9° L: 6° 8°

SUN	MON	TUE	WED	THU	FRI
9°	9°	7°	8°	8°	9°
6°	-1°	-1°	2°	3°	-2°

Zurich H: 12° L: 2° 7°

SUN	MON	TUE	WED	THU	FRI
12°	8°	4°	3°	3°	5°
2°	-1°	-4°	-4°	-3°	-3°

Cambridge H: 6° L: -3° 2°

SUN	MON	TUE	WED	THU	FRI
6°	9°	9°	7°	9°	7°
-3°	-4°	-1°	3°	-1°	-3°

Cologne H: 12° L: 6° 8°

SUN	MON	TUE	WED	THU	FRI
12°	9°	6°	6°	6°	5°

San Francisco H: 17° L: 7°

SUN	MON	TUE	WED	THU	FRI
17°	17°	17°	16°	16°	14°
7°	9°	9°	8°	9°	8°

Sophia Antipolis H: 21° L: 8° 14°

SUN	MON	TUE	WED	THU	FRI
21°	18°	17°	16°	14°	16°
8°	9°	9°	7°	7°	4°

Tokyo H: 16° L: 11° 13°

MON	TUE	WED	THU	FRI	SAT
16°	17°	17°	18°	16°	18°
11°	10°	11°	12°	12°	11°

panion to the world's most complete encyclopedia. View and
kipedia articles in any language without leaving your
Dashboard.

convenient

safe

secure

convenient

safe

secure

FAIL

http://flickr.com/photos/good-karma/571971015/

XMLHttpRequest

to any destination
with cookies

widget.system

arbitrary shell scripts

Widget plugins: Extending what JavaScript can do.

A Widget can control your system.

Your system’s security depends on the correctness of JavaScript code.

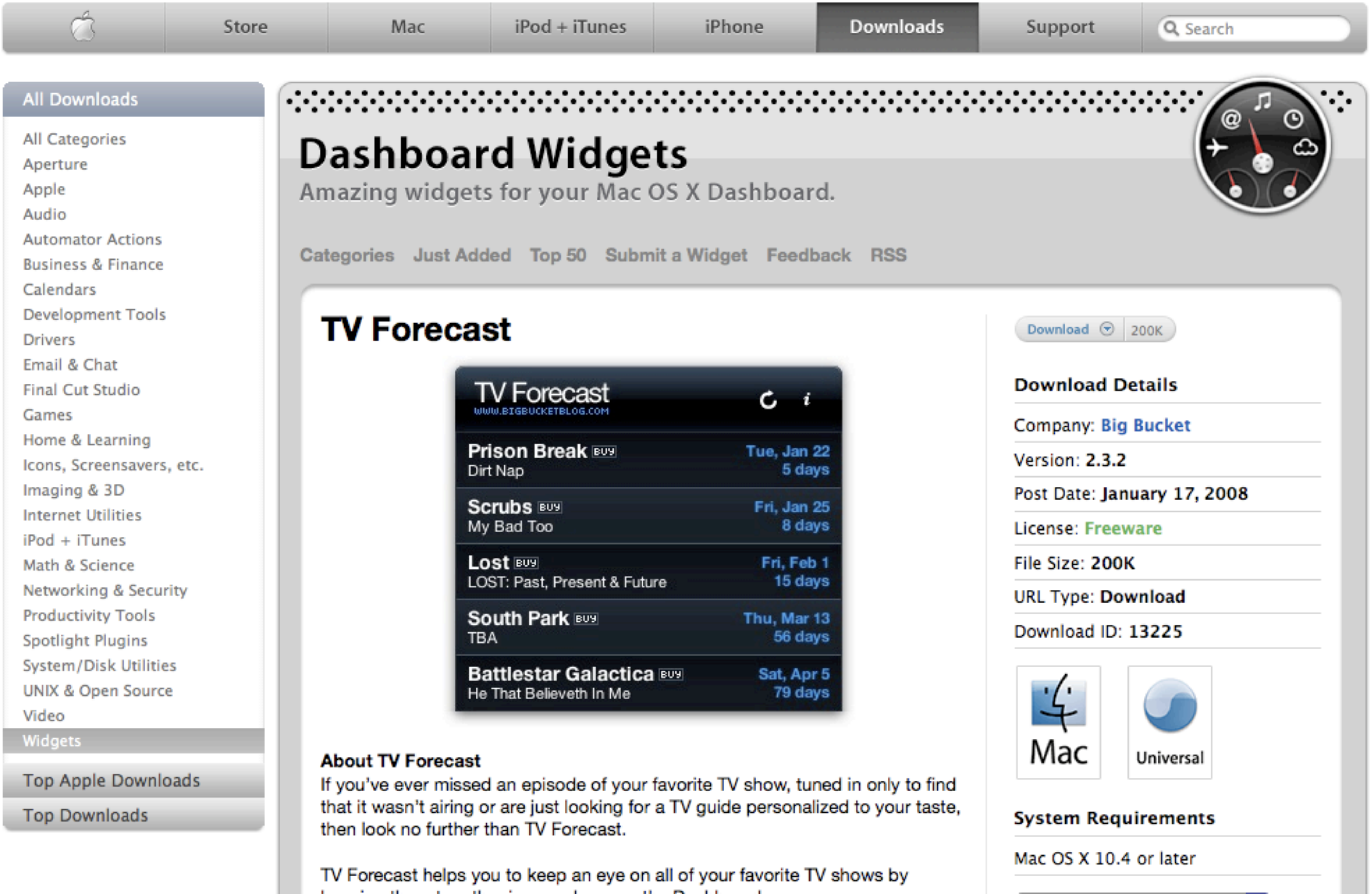
Attacker’s goal:
Control the Widget’s
DOM.

Controlling the DOM means executing arbitrary code.

Code Quality?

Parsing a number.

featured download in January 2008



Dashboard Widgets

Amazing widgets for your Mac OS X Dashboard.

TV Forecast

TV Forecast
WWW.BIGBUCKETBLOG.COM

Prison Break BUY Dirt Nap	Tue, Jan 22 5 days
Scrubs BUY My Bad Too	Fri, Jan 25 8 days
Lost BUY LOST: Past, Present & Future	Fri, Feb 1 15 days
South Park BUY TBA	Thu, Mar 13 56 days
Battlestar Galactica BUY He That Believeth In Me	Sat, Apr 5 79 days

About TV Forecast

If you've ever missed an episode of your favorite TV show, tuned in only to find that it wasn't airing or are just looking for a TV guide personalized to your taste, then look no further than TV Forecast.

TV Forecast helps you to keep an eye on all of your favorite TV shows by

Download Details

Company: Big Bucket

Version: 2.3.2

Post Date: January 17, 2008

License: Freeware

File Size: 200K

URL Type: Download

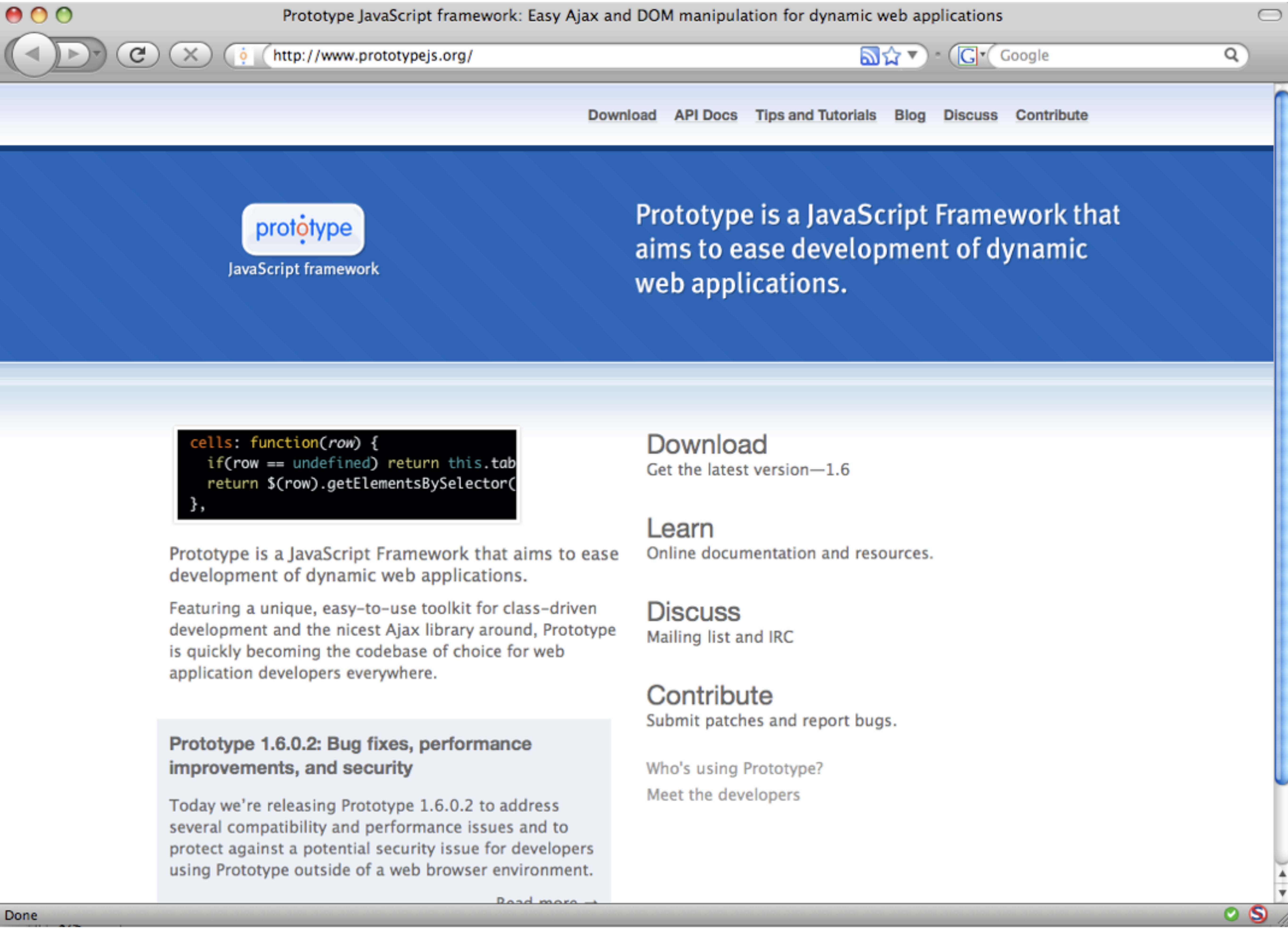
Download ID: 13225

System Requirements

Mac OS X 10.4 or later

update checks: JSON

JavaScript Object Notation



Prototype JavaScript framework: Easy Ajax and DOM manipulation for dynamic web applications
http://www.prototypejs.org/
Google
Download
API Docs
Tips and Tutorials
Blog
Discuss
Contribute
prototype
JavaScript framework
Done

Prototype is a JavaScript Framework that aims to ease development of dynamic web applications.

```
cells: function(row) {
  if(row == undefined) return this.tab
  return $(row).getElementsBySelector(
},
```

Prototype is a JavaScript Framework that aims to ease development of dynamic web applications.

Featuring a unique, easy-to-use toolkit for class-driven development and the nicest Ajax library around, Prototype is quickly becoming the codebase of choice for web application developers everywhere.

Prototype 1.6.0.2: Bug fixes, performance improvements, and security

Today we're releasing Prototype 1.6.0.2 to address several compatibility and performance issues and to protect against a potential security issue for developers using Prototype outside of a web browser environment.

Read more →

Download

Get the latest version—1.6

Learn

Online documentation and resources.

Discuss

Mailing list and IRC

Contribute

Submit patches and report bugs.

Who's using Prototype?

Meet the developers

```
this._checkVersion
  (transport.
    responseText.
      evalJSON());
```

sanity checks turned off by default

eval()

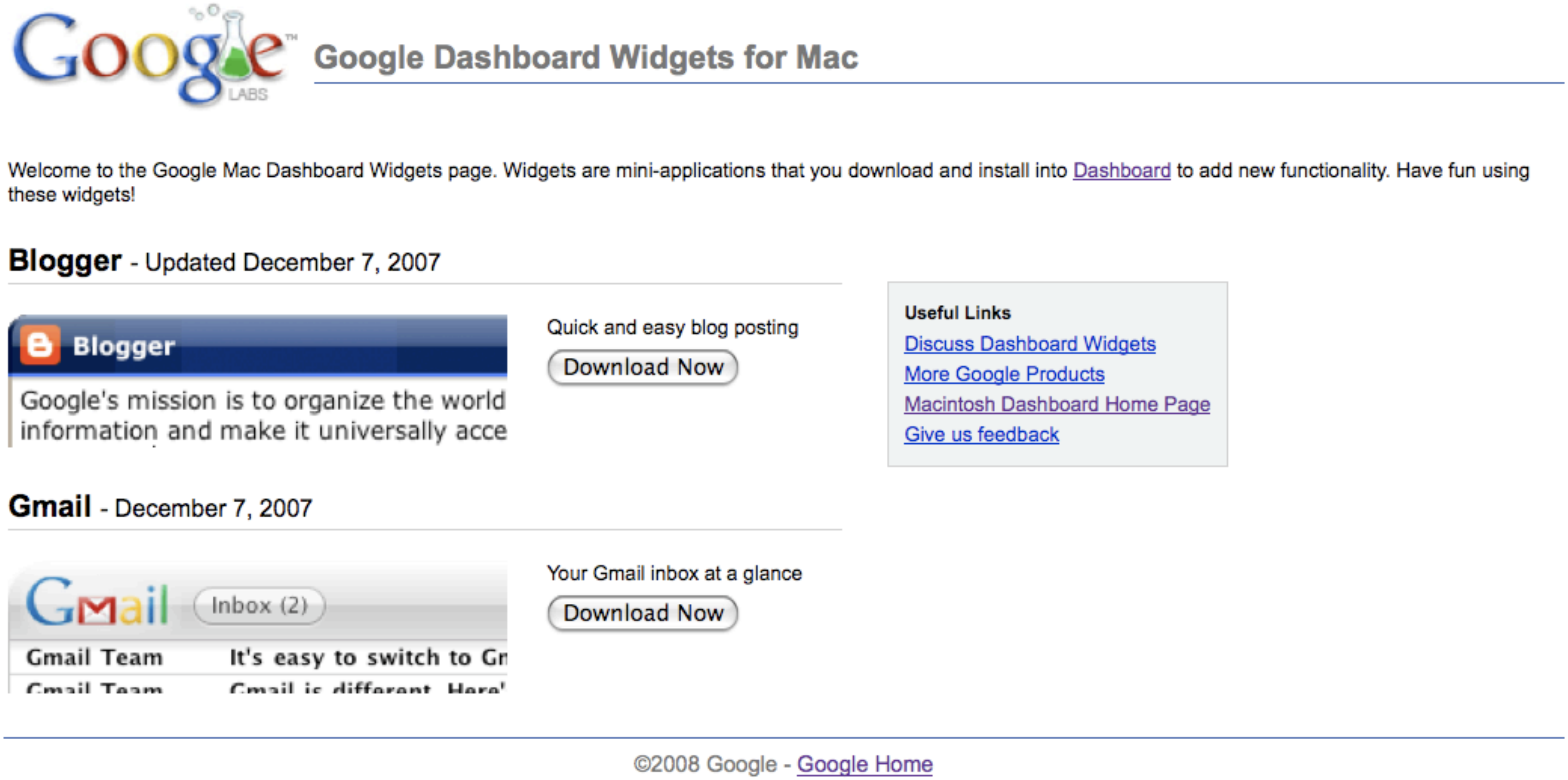
```
this._checkVersion
  (transport.
    responseText.
      evalJSON());
```

Executing arbitrary code retrieved through HTTP.

Executing arbitrary code retrieved through HTTP.

FAIL

Writing a string to the user interface.



Google Dashboard Widgets for Mac

Welcome to the Google Mac Dashboard Widgets page. Widgets are mini-applications that you download and install into Dashboard to add new functionality. Have fun using these widgets!

Blogger - Updated December 7, 2007

Blogger
Google's mission is to organize the world
information and make it universally acce

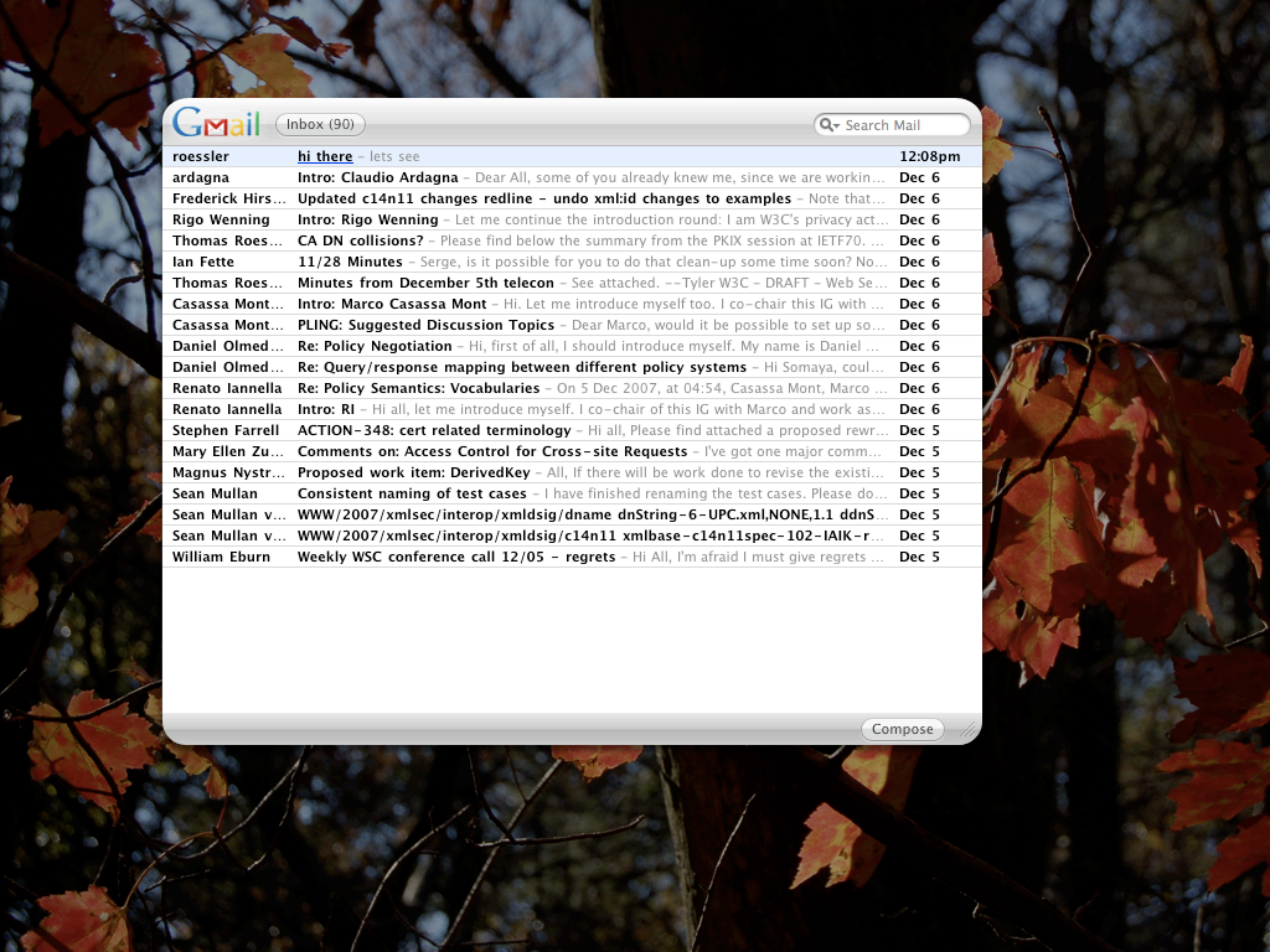
Quick and easy blog posting

Useful Links

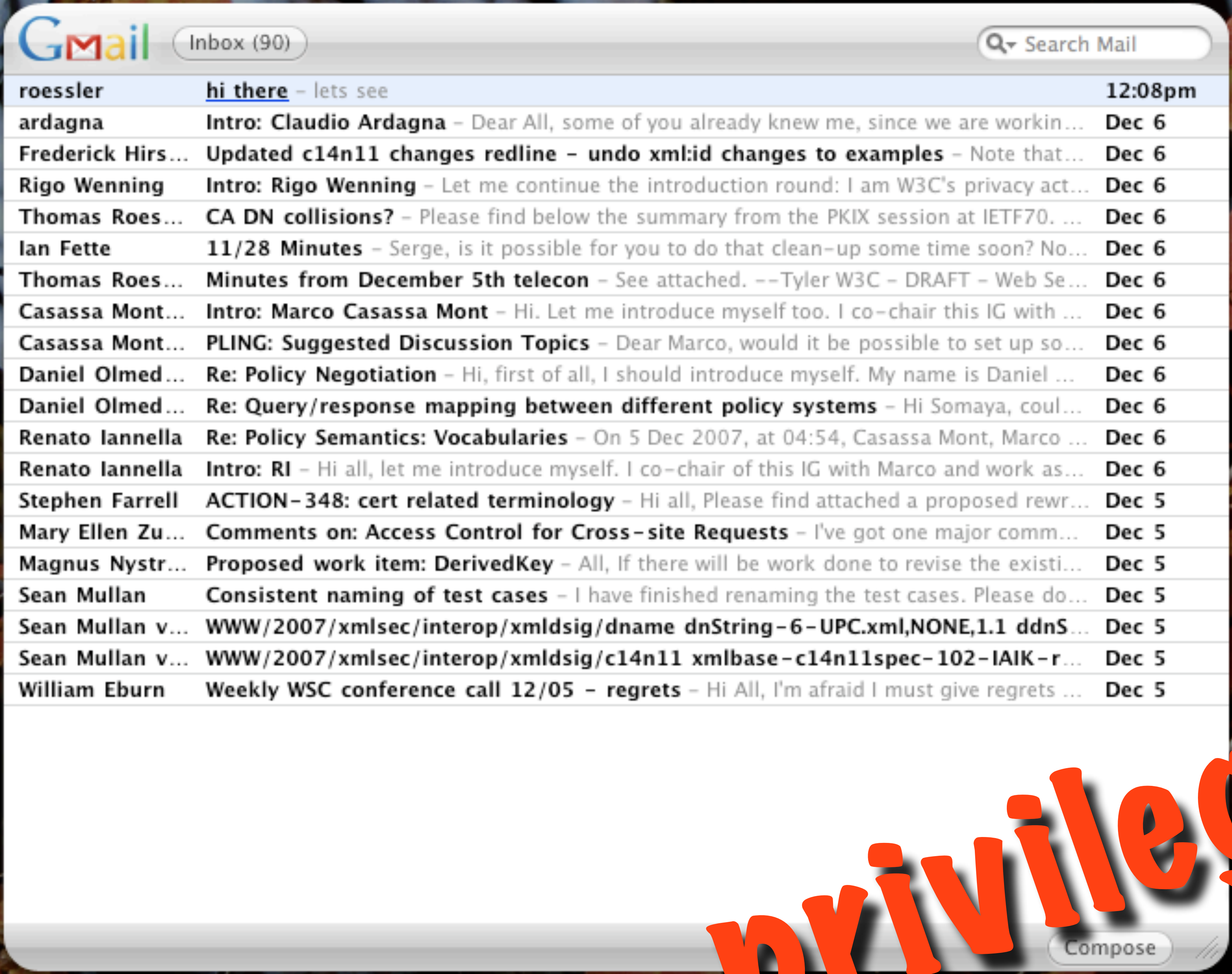
- Discuss Dashboard Widgets
- More Google Products
- Macintosh Dashboard Home Page
- Give us feedback

Gmail - December 7, 2007

Your Gmail inbox at a glance



roessler	hi there – lets see	12:08pm
ardagna	Intro: Claudio Ardagna – Dear All, some of you already knew me, since we are workin...	Dec 6
Frederick Hirs...	Updated c14n11 changes redline - undo xml:id changes to examples – Note that...	Dec 6
Rigo Wenning	Intro: Rigo Wenning – Let me continue the introduction round: I am W3C's privacy act...	Dec 6
Thomas Roes...	CA DN collisions? – Please find below the summary from the PKIX session at IETF70. ...	Dec 6
Ian Fette	11/28 Minutes – Serge, is it possible for you to do that clean-up some time soon? No...	Dec 6
Thomas Roes...	Minutes from December 5th telecon – See attached. --Tyler W3C - DRAFT - Web Se...	Dec 6
Casassa Mont...	Intro: Marco Casassa Mont – Hi. Let me introduce myself too. I co-chair this IG with ...	Dec 6
Casassa Mont...	PLING: Suggested Discussion Topics – Dear Marco, would it be possible to set up so...	Dec 6
Daniel Olmed...	Re: Policy Negotiation – Hi, first of all, I should introduce myself. My name is Daniel ...	Dec 6
Daniel Olmed...	Re: Query/response mapping between different policy systems – Hi Somaya, coul...	Dec 6
Renato Iannella	Re: Policy Semantics: Vocabularies – On 5 Dec 2007, at 04:54, Casassa Mont, Marco ...	Dec 6
Renato Iannella	Intro: RI – Hi all, let me introduce myself. I co-chair of this IG with Marco and work as...	Dec 6
Stephen Farrell	ACTION-348: cert related terminology – Hi all, Please find attached a proposed rewr...	Dec 5
Mary Ellen Zu...	Comments on: Access Control for Cross-site Requests – I've got one major comm...	Dec 5
Magnus Nystr...	Proposed work item: DerivedKey – All, If there will be work done to revise the existi...	Dec 5
Sean Mullan	Consistent naming of test cases – I have finished renaming the test cases. Please do...	Dec 5
Sean Mullan v...	WWW/2007/xmlsec/interop/xmldsig/dname dnString-6-UPC.xml,NONE,1.1 ddnS...	Dec 5
Sean Mullan v...	WWW/2007/xmlsec/interop/xmldsig/c14n11 xmlbase-c14n11spec-102-IAIK-r...	Dec 5
William Eburn	Weekly WSC conference call 12/05 - regrets – Hi All, I'm afraid I must give regrets ...	Dec 5



roessler	hi there – lets see	12:08pm
ardagna	Intro: Claudio Ardagna – Dear All, some of you already knew me, since we are workin…	Dec 6
Frederick Hirs…	Updated c14n11 changes redline - undo xml:id changes to examples – Note that…	Dec 6
Rigo Wenning	Intro: Rigo Wenning – Let me continue the introduction round: I am W3C's privacy act…	Dec 6
Thomas Roes…	CA DN collisions? – Please find below the summary from the PKIX session at IETF70. …	Dec 6
Ian Fette	11/28 Minutes – Serge, is it possible for you to do that clean-up some time soon? No…	Dec 6
Thomas Roes…	Minutes from December 5th telecon – See attached. --Tyler W3C - DRAFT - Web Se…	Dec 6
Casassa Mont…	Intro: Marco Casassa Mont – Hi. Let me introduce myself too. I co-chair this IG with …	Dec 6
Casassa Mont…	PLING: Suggested Discussion Topics – Dear Marco, would it be possible to set up so…	Dec 6
Daniel Olmed…	Re: Policy Negotiation – Hi, first of all, I should introduce myself. My name is Daniel …	Dec 6
Daniel Olmed…	Re: Query/response mapping between different policy systems – Hi Somaya, coul…	Dec 6
Renato Iannella	Re: Policy Semantics: Vocabularies – On 5 Dec 2007, at 04:54, Casassa Mont, Marco …	Dec 6
Renato Iannella	Intro: RI – Hi all, let me introduce myself. I co-chair of this IG with Marco and work as…	Dec 6
Stephen Farrell	ACTION-348: cert related terminology – Hi all, Please find attached a proposed rewr…	Dec 5
Mary Ellen Zu…	Comments on: Access Control for Cross-site Requests – I've got one major comm…	Dec 5
Magnus Nystr…	Proposed work item: DerivedKey – All, If there will be work done to revise the existi…	Dec 5
Sean Mullan	Consistent naming of test cases – I have finished renaming the test cases. Please do…	Dec 5
Sean Mullan v…	WWW/2007/xmlsec/interop/xmldsig/dname dnString-6-UPC.xml,NONE,1.1 ddnS…	Dec 5
Sean Mullan v…	WWW/2007/xmlsec/interop/xmldsig/c14n11 xmlbase-c14n11spec-102-IAIK-r…	Dec 5
William Eburn	Weekly WSC conference call 12/05 - regrets – Hi All, I'm afraid I must give regrets …	Dec 5

privileged

.innerHTML

Script injection through e-mail possible.

Just put HTML into a Subject.

Script injection through e-mail possible.

FAIL

Code Quality?

Code Quality?

FAIL

Widgets
enable
creativity

Widgets enable creativity

Good!

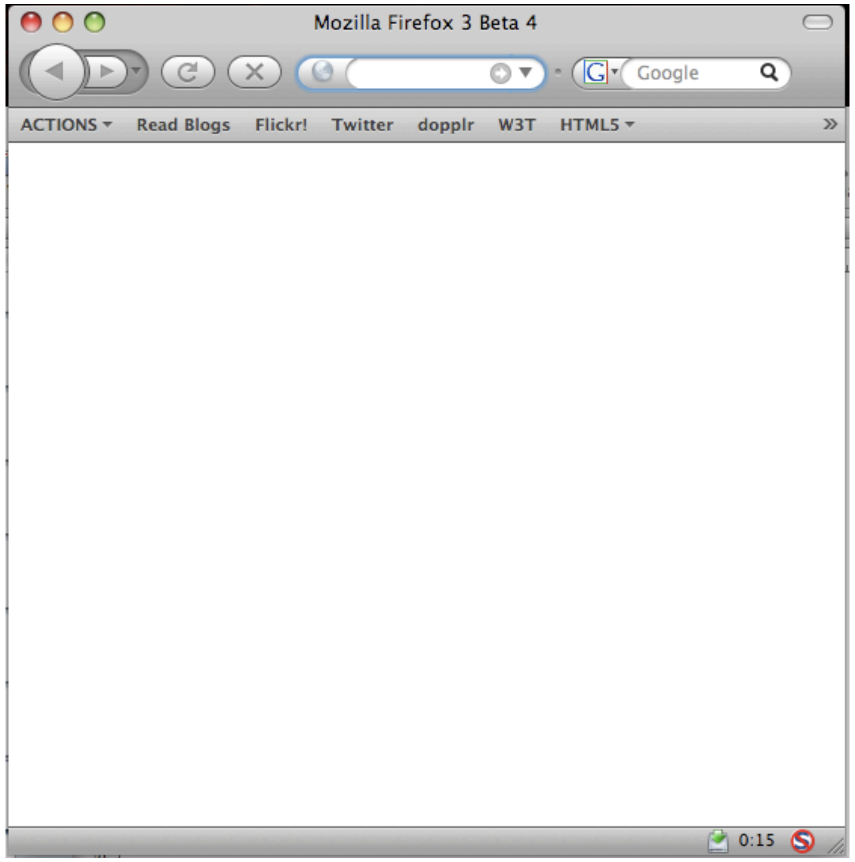
But: We need security despite bad code quality.

What do APIs invite programmers to do?

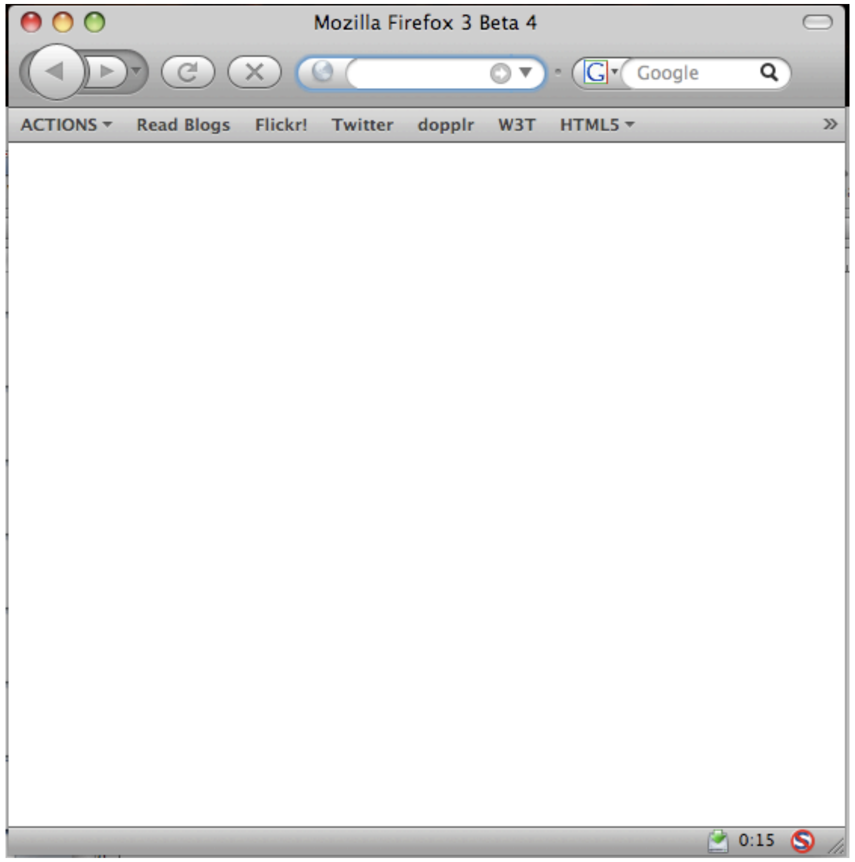
<2>

Mash-ups

Client-side code processes confidential data.



http://flickr.com/photos/onaliencinema/298243188/
http://flickr.com/photos/nickdawson/1484934955/



http://flickr.com/photos/onaliencinema/298243188/
http://flickr.com/photos/nickdawson/1484934955/

http://flickr.com/photos/mwboeckmann/2313632431/

<script>

XMLHttpRequest

JSONRequest

XDomainRequest

postMessage

```
<script src=”http://
good.foo/...”/>
<script src=”http://
evil.foo/...”/>
```

two sites
one DOM

widely popular!

```
<script src=”http://
good.foo/...”/>
<script src=”http://
evil.foo/...”/>
```

FAIL

XMLHttpRequest

place HTTP requests from browser-side code

cross-site requests:
XMLHttpReq’ Level 2
access-control

XML data

responseXML

non-XML formats?

responseText
responseBody

responseText

responseBody

raw data!

non XML formats?

FAIL

JSONRequest

place HTTP request
from client-side code

application/jsonrequest

anonymous

GET

POST

API: object is passed to call-back function.

advanced RESTful APIs?

advanced RESTful APIs?

FAIL

XDomainRequest

cross-site HTTP requests

anonymous

GET

POST

advanced RESTful

APIs?

FAIL

text/plain only

API string-based

invites eval+JSON

two sites

one DOM

invites eval JSON

FAIL

postMessage

cross-window
communication

cause a “message”
event in another DOM

“just strings”

how about structured data?

invites eval+JSON

two sites
one DOM

invites eval JSON

FAIL

The good news: probably fixable

Lots of people write JavaScript code.

Widgets, Mash-ups and Web Applications let more people be creative.

BUT

They need sane and safe APIs.

Let’s consider that in spec development.

<?>

tlr@w3.org