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
Widget Installer

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

[Cancel] [Install]

Wikipedia

From Wikipedia, the free encyclopedia

A wiki (IPA: [ˈwɪki] <WICK-ee> or [ˈwiːki] <WEE-kee>[1]) is a type of website that allows users to easily add, remove, or otherwise edit and change some available content, sometimes without the need for any special technical skills.

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.
convenient
safe
secure
convenient
safe
secure
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.

Categories  Just Added  Top 50  Submit a Widget  Feedback  RSS

TV Forecast

**TV Forecast**

**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
58 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 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 keeping track of when each episode will air.
update checks: JSON
JavaScript
Object
Notation
Prototype is a JavaScript Framework that aims to ease development of dynamic web applications.

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

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.

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.
Writing a string to the user interface.
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

Quick and easy blog posting

**Gmail** - December 7, 2007

Your Gmail inbox at a glance

©2008 Google - [Google Home](https://www.google.com)
<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>roessler</td>
<td>hi there - lets see</td>
<td>12:08pm</td>
</tr>
<tr>
<td>ardagna</td>
<td>Intro: Claudio Ardagna - Dear All, some of you already knew me, since we are working... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Frederick Hirs</td>
<td>Updated c14n11 changes redline - undo xml:id changes to examples - Note that... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Rigo Wenning</td>
<td>Intro: Rigo Wenning - Let me continue the introduction round: I am W3C's privacy act... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Thomas Roes...</td>
<td>CA DN collisions? - Please find below the summary from the PKIX session at IETF70. ... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Ian Fette</td>
<td>11/28 Minutes - Serge, is it possible for you to do that clean-up some time soon? No... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Thomas Roes...</td>
<td>Minutes from December 5th telecon - See attached. -- Tyler W3C - DRAFT - Web Se... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Casassa Mont...</td>
<td>Intro: Marco Casassa Mont - Hi. Let me introduce myself too. I co-chair this IG with ... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Casassa Mont...</td>
<td>PLING: Suggested Discussion Topics - Dear Marco, would it be possible to set up so... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Daniel Olmed...</td>
<td>Re: Policy Negotiation - Hi, first of all, I should introduce myself. My name is Daniel ... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Daniel Olmed...</td>
<td>Re: Query/response mapping between different policy systems - Hi Somaya, coul... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Renato Iannella</td>
<td>Re: Policy Semantics: Vocabularies - On 5 Dec 2007, at 04:54, Casassa Mont, Marco ... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Renato Iannella</td>
<td>Intro: RI - Hi all, let me introduce myself. I co-chair this IG with Marco and work as... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Stephen Farrell</td>
<td>ACTION-348: cert related terminology - Hi all, Please find attached a proposed rwr... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Mary Ellen Zu...</td>
<td>Comments on: Access Control for Cross-site Requests - I've got one major comm... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Magnus Nystr...</td>
<td>Proposed work item: DerivedKey - All, If there will be work done to revise the existi... Dec 6</td>
<td></td>
</tr>
<tr>
<td>Sean Mullan</td>
<td>Consistent naming of test cases - I have finished renaming the test cases. Please do... Dec 5</td>
<td></td>
</tr>
<tr>
<td>Sean Mullan v...</td>
<td>WWW/2007/xmlesc/interop/xmlsdig/dname dnString - 6-UPC.xml,NONE,1,1 ddn5... Dec 5</td>
<td></td>
</tr>
<tr>
<td>Sean Mullan v...</td>
<td>WWW/2007/xmlesc/interop/xmlsdig/c14n11 xmlbase-c14n11spec-102-IAIK-r... Dec 5</td>
<td></td>
</tr>
<tr>
<td>William Eburn</td>
<td>Weekly WSC conference call 12/05 - regrets - Hi All, I'm afraid I must give regrets ... Dec 5</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Subject</td>
<td>Message</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>roessler</td>
<td>hi there - lets see</td>
<td></td>
</tr>
<tr>
<td>ardagna</td>
<td>Intro: Claudio Ardagna - Dear All, some of you already knew me, since we are working…</td>
<td></td>
</tr>
<tr>
<td>Frederick Hirsh</td>
<td>Updated c14n11 changes redline - undo xml:id changes to examples - Note that…</td>
<td></td>
</tr>
<tr>
<td>Rigo Wenning</td>
<td>Intro: Rigo Wenning - Let me continue the introduction round: I am W3C’s privacy act…</td>
<td></td>
</tr>
<tr>
<td>Thomas Roes</td>
<td>CA DN collisions? – Please find below the summary from the PKIX session at IETF70…</td>
<td></td>
</tr>
<tr>
<td>Ian Fette</td>
<td>11/28 Minutes – Serge, is it possible for you to do that clean-up some time soon?</td>
<td></td>
</tr>
<tr>
<td>Thomas Roes</td>
<td>Minutes from December 5th telecon – See attached. —- Tyler W3C – DRAFT – Web Se…</td>
<td></td>
</tr>
<tr>
<td>Casassa Mont</td>
<td>Intro: Marco Casassa Mont – Hi. Let me introduce myself too. I co-chair this IG with…</td>
<td></td>
</tr>
<tr>
<td>Casassa Mont</td>
<td>PLING: Suggested Discussion Topics – Dear Marco, would it be possible to set up so…</td>
<td></td>
</tr>
<tr>
<td>Daniel Olmed</td>
<td>Re: Policy Negotiation – Hi, first of all, I should introduce myself. My name is Daniel…</td>
<td></td>
</tr>
<tr>
<td>Daniel Olmed</td>
<td>Re: Query/response mapping between different policy systems – Hi Somaya, coul…</td>
<td></td>
</tr>
<tr>
<td>Renato Iannella</td>
<td>Re: Policy Semantics: Vocabularies – On 5 Dec 2007, at 04:54, Casassa Mont, Marco…</td>
<td></td>
</tr>
<tr>
<td>Renato Iannella</td>
<td>Intro: RI – Hi all, let me introduce myself. I co-chair this IG with Marco and work as…</td>
<td></td>
</tr>
<tr>
<td>Stephen Farrell</td>
<td>ACTION–348: cert related terminology – Hi all, Please find attached a proposed rewrr…</td>
<td></td>
</tr>
<tr>
<td>Mary Ellen Zu</td>
<td>Comments on: Access Control for Cross-site Requests – I’ve got one major comm…</td>
<td></td>
</tr>
<tr>
<td>Magnus Nyström</td>
<td>Proposed work item: DerivedKey – All, If there will be work done to revise the existi…</td>
<td></td>
</tr>
<tr>
<td>Sean Mullan</td>
<td>Consistent naming of test cases – I have finished renaming the test cases. Please do…</td>
<td></td>
</tr>
<tr>
<td>Sean Mullan</td>
<td>WWW/2007/xmlext/interop/xmldsig/dnString-6-UPC.xml,NONE,1,1 ddnS…</td>
<td></td>
</tr>
<tr>
<td>William Eburn</td>
<td>Weekly WSC conference call 12/05 – regrets – Hi All, I’m afraid I must give regrets…</td>
<td></td>
</tr>
</tbody>
</table>
Script injection through e-mail possible.
Just put HTML into a Subject.
Script injection through e-mail possible.
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?
Mash-ups
Client-side code processes confidential data.
<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/..."/>
<fail>
<script src="http://evil.foo/..."/>
</fail>
XMLHttpRequest

place HTTP requests from browser-side code
cross-site requests: XMLHttpRequest Level 2 access-control
XML data

responseXML
non-XML formats?
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 API?
XDomainRequest

cross-site HTTP requests
anonymous
GET

POST
advanced RESTful APIs
text/plain only

API string-based
invites eval+JSON
two sites
one DOM
invites eval JSON
postMessage

cross-window communication
cause a “message” event in another DOM
“just strings”
how about structured data?
invites eval+JSON
two sites
one DOM
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.