widgets - web vulnerabilities for all
Thomas Roessler's notes on geek life in Luxembourg -- and less virtual topics.

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 Dashboard 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
little helpers
web 2.0
html / css / javascript
easy to install
safe
secure
convenient
convenient
javascript
outside the web
with full control over the local machine
widget.system.runCommand(System.Shell.execute)
run a command in the system’s shell
when was your computer’s last cross-site scripting vulnerability?
e.g., GMail
<table>
<thead>
<tr>
<th>Sender</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>ardarka</td>
<td>Intro: Claudio Ardagna - Dear All, some of you already knew me, since we are workin... 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 Farrel</td>
<td>ACTION–348: cert related terminology - Hi all, Please find attached a proposed rewwr... Dec 5</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 5</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 5</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/xmlsec/interop/xmlsig/dname dnString–6–UPC.xml,NONE,1,1 ddnS... Dec 5</td>
<td></td>
</tr>
<tr>
<td>Sean Mullan v...</td>
<td>WWW/2007/xmlsec/interop/xmlsig/c14n11 xmlbase-c14n11spec–102–IAlK–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>
</tbody>
</table>
var titleText = MessagesTable.getTitleTextFromEntryElement(currentEntry);
titleText =
'&nbsp;&nbsp;&nbsp;<span class="title-class">' + titleText + '</span>';

// (skipping code to build message summary)

titleText =
"<div class='table-overflow-col'>" + titleText + "</div>";

titleColumn.innerHTML = titleText;
titleColumn.
innerHTML
    = titleText;
who controls titleText?
Subject: <i>hi!</i>
Hi!
we can write html into the dom, by sending e-mail
scripts?
innerHTML handles
<script>
strangely
event handlers work just fine
hacking through e-mail
output
sanitization
entity-escape
strings before writing them to the dom
Google announced fix in December
vulnerable versions don’t work any more
how about rendering html?
say, from Wikipedia
Do you want to install the widget “Wikipedia” and open it in Dashboard?

Cancel  Install

_widgetInstaller.png

Wikipedia

A wiki (IPA: [ˈwɪki]) or Wikipedia (IPA: [ˈwɪki]) is a type of website that allows contributors to edit and change content, sometimes without the need for original content. For other uses, see Wiki (disambiguation).

Wiki

From Wikipedia, the free encyclopedia

Wiki

For other uses, see Wiki (disambiguation).

Wikipedia

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

About Wikipedia

Firefox.app

17.1 MB

Firefox.app

16.7 MB

Tweettirific 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

Clear  12 Downloads
A widget engine is a software service available to users for running and displaying desktop widgets on the desktop. Desktop widgets are physically inspired applets that give access to information and frequently used functions such as clocks, calendars, news aggregators, etc.

The term widget engine is not to be confused with that of a widget toolkit. Toolkits are destined to GUI programmers, who combine several widgets to form a single application. A widget in a toolkit provide a single, low level interaction, and is prepared to communicate with other widgets in the toolkit. On the other hand, widget engines are intended for end users and each desktop widget is a stand-alone, task-oriented application which can be composed of several related interactions on its own.

The desktop widget model is attractive because of ease of development. Most of these widgets can be created with a few images and about 10 to several hundred lines of XML/JavaScript/VBScript source code. A single host software system, such as a web browser, runs all the loaded widgets. This allows several desktop widgets to be built sharing resources and code.

Contents

1 Desktop widgets
2 Mobile widgets
3 Information flow of Desktop Widgets
4 See also
5 Notes and references
6 External links

Desktop widgets

Widgets are downloadable interactive virtual tools that provide services such as showing the user the latest news, the current weather, the time, a calendar,
html parsing required by design
bake your own?
.innerHTML!
I OWNZ UR COMPUTR

say, in an
rss reader
Choose a template for your widget:

- Custom
- Countdown
- Maps
- RSS
- Podcast
- Photocast
- Quartz Composer
- Video Player
- Gauge
- Daily Feed

Custom Template

This template provides a blank widget, ready for customizing.

Place items from the Library window, such as parts and pictures, on the canvas, then use the inspector to adjust an item's appearance and assign handlers to it. Write code for your handlers in the source code editor, and when you're finished, run your widget to make sure it works as you intended.
function makeEntryDiv(content) {
    var div;
    // If it's a plain string, wrap it in a div
    if (typeof content === "string") {
        div = document.createElement("div");
        div.innerHTML = content;
    } else {
        div = content;
    }
    return div;
}
the disaster is one click away
(incidentally, forget your firewall)
can we have shrimps in that turducken?
widget.system and friends call the shell
6.3) How do I safely pass input to an external program?
“One of the biggest mistakes is to use a shell. ...”
Dashboard Widgets
Amazing widgets for your Mac OS X Dashboard.

SVN Notifier

About SVN Notifier
Version control is essential for collaborative development, and we do a lot of collaborative development at Arc90, so we rely heavily on our Subversion repositories. One of the things we’ve noticed is that it’s hard for developers to keep up with their repositories’ and working copies’ statuses: Is my copy out of date? Has someone committed something to the repository?

So we wrote a Dashboard widget that monitors working copies and repositories to make sure that it’s always clear what’s what. And we threw in Growl support to make the package extra appealing. It’s a great way to keep tabs on your development efforts.
what’s new in that svn repository?
notification
through growl
command = baseCommand
    // title (note the trailing space)
    + '"' + projLabel + ' is out of date"'

    // message
    + '"You have revision r'
    + my_rev
    + ' , and the repository has been updated to r'
    + repos_rev + ' by '
    + repos_rev_author
    + ' with the following message:\n\n'
    + repos_rev_msg + '"';
"; touch /tmp/gotcha; echo "
hacking through svn commit messages
there’s similar code in the wikipedia widget
web
2.0
JSON
eval
twitgit
twitterlex
facebook
Dashboard Widgets
Amazing widgets for your Mac OS X Dashboard.

Facebook

About Facebook
Look up student information on the facebook.com community. Limitations:
- If not already specified, users must set their Safari preferences to accept cookies “Always.” If not already set to “Always,” the widget will facilitate changing this setting upon a first attempt at searching using the widget.
- When searching by attributes other than name, results are limited to only those in the user's personal network. This limitation is imposed by facebook.com, not by the Facebook Search Widget.

What's Next?
Look for the following features in future releases:
- Bug fixes
- Results displayed as a list of names in a drop-down drawer within the widget interface itself, rather than linking to an external browser window.

What's New in this Version
- Fixed a bug in which users would be directed to the cookies setup page even after correctly configuring their cookies.
- Fixed a bug that caused the widget to begin a search with no user input.
- Added support for searching only within your personal network.
json based apis
XMLHttpRequest
eval
twitter
facebook
not quite a JSON example
Dashboard Widgets
Amazing widgets for your Mac OS X Dashboard.

Hockey Widget

About Hockey Widget
Allows you to keep track of your favorite NHL team - daily schedules (game times are converted to your local time zone) with past and current results and upcoming schedules as well as current standings (both division and full conference). Hovering the pointer over a game that has concluded (or is currently in progress) shows the period by period breakdown of scores as well as game leaders (or last play and last goal for games in progress).
var xmlResponse = xmlRequest.responseText
xmlResponse = xmlResponse.replace(/\[\n\r]/g,"");
var NHLatl = null;
var gameData = xmlResponse.match(/script[^<]*var NHLatl.*?<script>/)[0].replace(/.*?var /,"").replace(/>.*/s*myScoresIcon.*/,"}"));
eval(gameData);
screen-scraping through eval
another pattern:
use JSON to check for updates
Dashboard Widgets
Amazing widgets for your Mac OS X Dashboard.

Categories    Just Added    Top 50    Submit a Widget    Feedback    RSS

TV Forecast

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 tracking airing dates and providing detailed information.
this._checkVersion
(transport.
responseText.
evalJSON());
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
default json
parser: eval
widget doesn’t turn on sanitization
frameworks may be less secure than you think
“You’re trusting them anyway, so why bother?”
leverage network attack into machine takeover
security of update servers at all times
robustness against cross-site scripting
More High Profile Sites IFRAME Injected

The ongoing monitoring of this campaign reveals that the group is continuing to expand the campaign, introducing over a hundred new bogus .info domains acting as traffic redirection points to the campaigns hardcoded within the secondary redirection point, in this case radt.info where a new malware variant of Zlob is attempting to install though an ActiveX object. These are the high profile sites targeted by the same group within the past 48 hours, with number of locally cached and IFRAME injected pages within their search engines:

NCSU Libraries - lib.ncsu.edu - 372,000 pages
FullDownloads.us - fulldownloads.us - 13,000 pages
Central Statistics Office Ireland - cso.ie - 10,300 pages
DBLife Frontpage - dblife.cs.wisc.edu - 1,130 pages

School of Mathematics and Statistics - www-history.mcs.st-andrews.ac.uk - 1040 pages
The World Clock - timeanddate.com - 944 pages
Boise State University - boisestate.edu - 471 pages
The U.S. Administration on Aging (AoA) - aoa.gov - 425 pages
Gustavus Adolphus College - gustavus.edu - 312 pages

http://ddanchev.blogspot.com/2008/03/more-high-profile-sites-iframe-injected.html
“more high profile sites iframe injected”
widgets are a predictor
javascript as programming language of choice?
sms application, web-based, widget-style?
social network worms that create zombies?
targeted attacks with plausible deniability?
the flaws aren’t rocket science
widespread
trivial to exploit
easy to find
json-based api?
shows html?
uses external programs?
ooooops