

The logo for SecTheory features the word "SecTheory" in a bold, italicized sans-serif font. Below it, the words "Internet Security" are written in a smaller, plain sans-serif font. A large, light gray, stylized graphic element, resembling a thick, irregular oval or a stylized letter 'O', is positioned behind the text.

SecTheory
Internet Security

The logo for CENZIC consists of a red circular icon on the left, made of three concentric, slightly irregular lines. To the right of the icon, the word "CENZIC" is written in a large, bold, uppercase sans-serif font. Below "CENZIC", the tagline "Securing Enterprise Applications" is written in a smaller, plain sans-serif font.

CENZIC
Securing Enterprise Applications

About Us

- ▣ Tom “Strace” Stracener – Sr. Security Analyst
- ▣ Cenzic
 - ▣ <http://www.cenzic.com>
 - ▣ <http://www.badgadgets.net>
- ▣ Robert “RSnake” Hansen - CEO
- ▣ SecTheory LLC
 - ▣ <http://www.sectheory.com>
 - ▣ <http://ha.ckers.org> – the lab
 - ▣ <http://sla.ckers.org> – the forum

Xploiting Google Gagets

- ▣ iHumble
- ▣ I want to explain the history...
- ▣ Only a few know the whole story.
- ▣ Sit back and relax, it's story time.



Before We Start...

- ▣ We've all heard these sentiments: "If you find a vulnerability, we ask that you share it with us. If you share it with us, we will respond to you with a time we will fix that hole." Scott Petry - Director @ Google
 - (We'll be coming back to this!)



Ah, Memories...

- ▣ It all started four years ago...
- ▣ We found that redirection vulnerabilities were being used by phishers in a number of sites, Visa, Doubleclick, eBay and of course, Google to confuse consumers.
- ▣ Timeframes for fixes:
 - Visa closed their hole down within hours
 - Double Click within days (partially)
 - eBay within weeks
 - Google still hasn't closed them (~4 years later)
- ▣ Every company agrees it's a hole. Everyone

It's out there!

▣ Word gets out – fast!

- <http://lists.virus.org/dshield-0602/msg00156.html>
- http://blog.eweek.com/blogs/larry_seltzer/archive/2006/03/05/8240.aspx
- <http://thespamdiaries.blogspot.com/2006/03/google-used-as-url-cloaking-device-in.html>
- <http://www.docuverse.com/blog/donpark/EntryViewPage.aspx?guid=e08af74b-8b86-418c-94e0-7d29a7cb91e2>
- <http://email.about.com/od/outlooktips/qt/et043005.htm>
- <http://listserv.educause.edu/cgi-bin/wa.exe?A2=ind0511&L=security&T=0&F=&S=&P=15599>
- <http://blogs.geekdojo.net/brian/archive/2004/10/14/googlephishing.aspx>
- <http://www.zataz.com/news/13296/google-corrige-une-faille.html>
- <http://google.blognewschannel.com/archives/2007/02/22/google-changes-redirects-adds-nofollow-to-blogger/>
- <http://googlesystem.blogspot.com/2007/02/google-redirect-notice.html>

▣ And others...

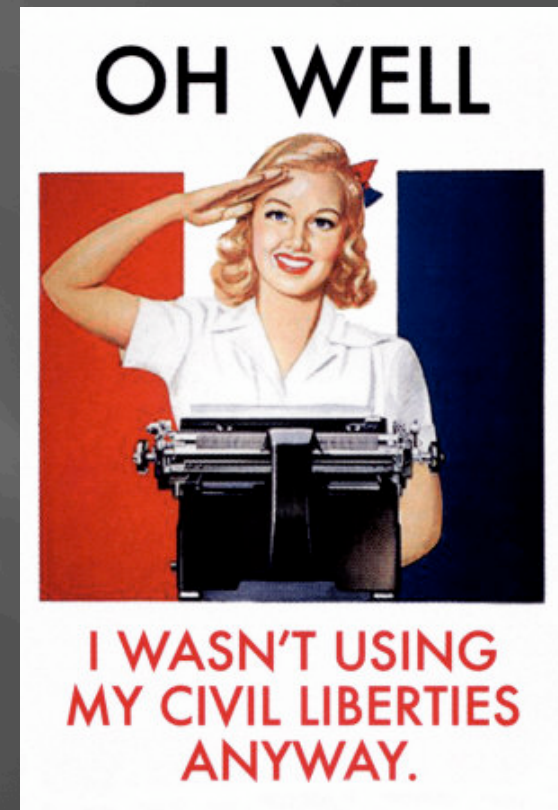
Google, Failure #1

- ❑ Everyone has vulns. But in this case...
- ❑ We informed Google that their own users were being exploited, to which we were told that they were putting a blacklist in place.
- ❑ Yes, you heard me, a blacklist...
- ❑ Blacklists only block what you know, not what you don't know – they refused to fix the problem properly. Add one character, you evade their blacklist. Best engineers in the world, eh?



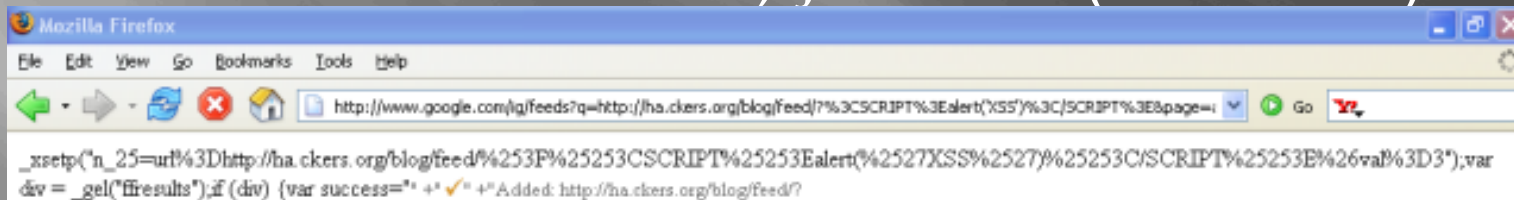
Google, Failure #2

- ▣ Why not fix it?
 - Money: Expensive to fix
 - Money: Useful for tracking users
 - Money: Would break “feeling lucky” and other tools that drive ‘stickiness’
- ▣ Why fix it?
 - Altruism: It’s the right thing to do (Google != Evil)
 - Altruism: It’s hole being actively used (not theory)
 - Altruism: Stop contributing to the problem
- ▣ So what did I do? I waited two years...



...and then I Went FD on Their *ss


- ❑ I don't hate Google, I just crush a lot.
- ❑ Disclosed 4 redirects 11th, Jan 2006 (with no reaction)
- ❑ Disclosed XSS on 4th, Jul 2006 (reaction!)



Wait, You Agree?!

- ▣ “Just to close this subject out, I think the open url redirection ... has been closed.... To the extent that open url redirection was being used by phishers, closing the most-used url should make a difference.” – Matt Cutts
- ▣ “Given that tons of different internal groups at Google used this redirector for quite a while, it’s understandable that it took a little while to close this.” – Matt Cutts



 [Matt Cutts](#) said on February 23, 2007 2:00 PM PDT:

<#>

Yup, it's good that Google made this change, because some bad guys were using this url redirector for things like phishing.

Why Do I Care About Redirects?

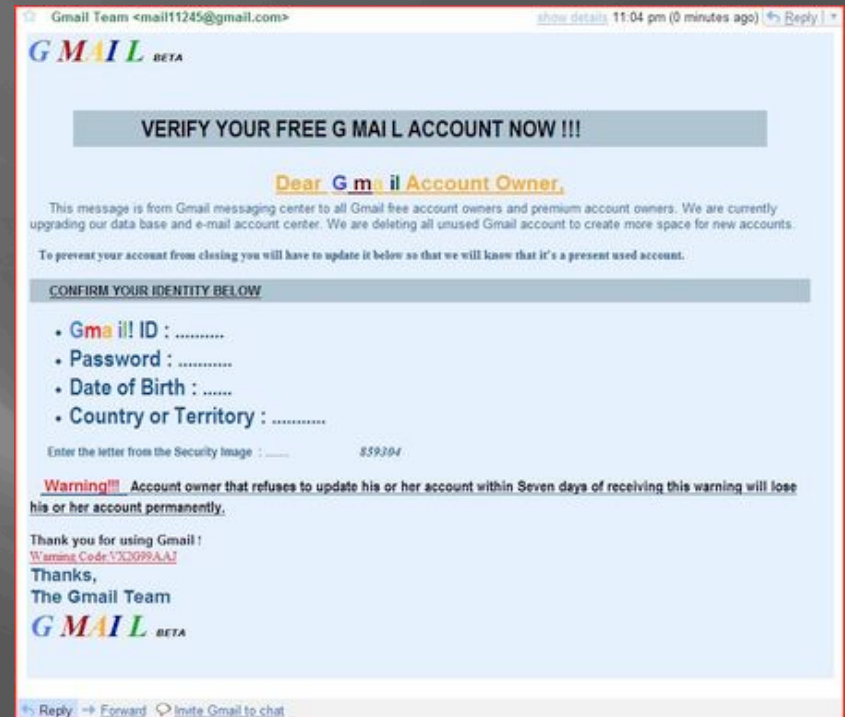
□ Anti-Phishing Primer:

- Whitelist first
 - Known good sites
 - False positives
 - Webmail
- Blacklist second
 - Known bad URLs (not domains)
- Heuristics last
- DNS sometimes

□ Google is litigious.

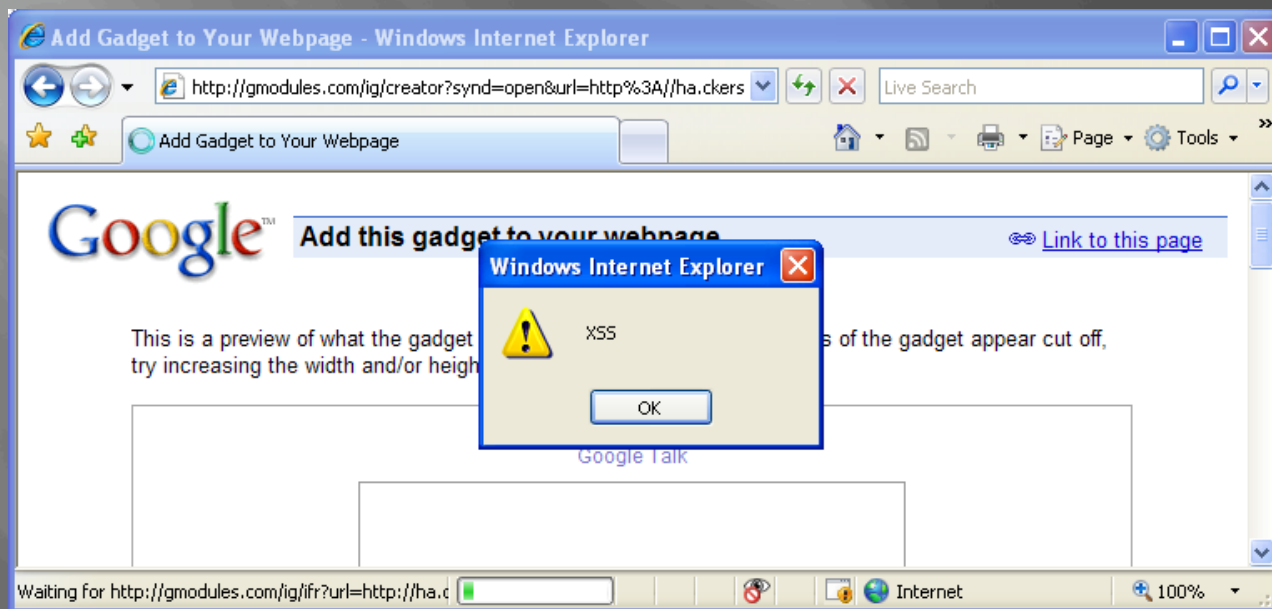
- We marked Google as a phishing site, but guess why?
- It WAS a phishing site! Duh!

□ Consumers put misguided trust in Google. ☹

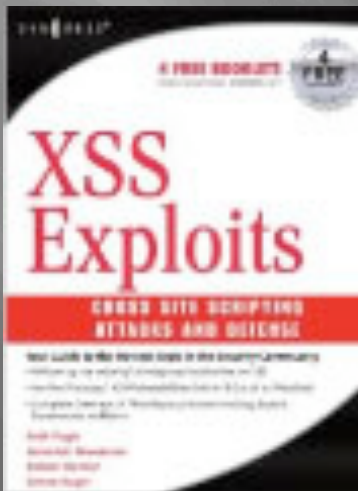


Google Gadgets

- ❑ Well, it just so happens that JavaScript can redirect too.
- ❑ But this time, I'm nice! Remember Mr. Petry, if you disclose it to us responsibly, "we will fix that hole".



Their Response



- “On further review, it turns out that this is not a bug, but instead the expected behavior of this domain.”
- “Since these modules reside on the gmodules.com domain instead of the Google domain, cross-domain protection stops them from being used to steal Google-specific cookies, etc.”
- Uh... Bueller?

My Response:

[-] **Subject:** Re: [#188242313] Another XSS hole

From: [RSnake](#)

Date: 8/17/2007 1:17 PM

To: [Google Security](#)

content-transfer-encoding: 7bit

Wow.

Google Security wrote:

Hi RSnake,

On further review, it turns out that this is not a bug, but instead the expected behavior of this domain. Javascript is a supported part of

Wow.

Shame On You Google

- ❑ Google already agreed redirection was bad.
- ❑ Google is still an evil litigious company (maybe more so now than ever).
- ❑ Google doesn't have the first clue what XSS is or what it can be used for.
- ❑ Google lied about the definition of a vulnerability that they already agreed to fix.
- ❑ Bad guys are STILL using it!



Google Ads Abused to Serve Spam and Malware

Monday March 17, 2008 at 9:05 am CST

Posted by [Vinoos Thomas](#)

[Trackback](#)

Early this year we observed spammers using Google page ads in [HTML-formatted emails](#) to redirect users who click the spammed URL to the spammers' sites.

[http://www.google.com/pagead/clk?sa=l&ai=MfeNYs
&num=123456&adurl=http://www.spammersite.com](http://www.google.com/pagead/clk?sa=l&ai=MfeNYs&num=123456&adurl=http://www.spammersite.com)

At first we thought Google page ads were being used to conceal the actual URL and subvert traditional anti-spam detection techniques. However, it seems one can change the linked URL to point to any site of your choice—as no validation appears to be done on Google's end.

Stupidity

- ▣ Others: “This issue you describe is not actually a vulnerability (and is not cross site scripting).... In this case, you are simply including allowed script in your blog. This does not constitute a security breach.” - Blogspot
- ▣ “I think it is irresponsible for RSnake to hint that...” - ‘bob’ 72.14.224.1 (Google Corp IT)
- ▣ Meanwhile more holes are opening!
- ▣ Stop fighting us, Google. We’re the good guys!

Top Infected IP Addresses for March 2008

Posted by Oliver Day Sun, 06 Apr 2008 01:48:00 GMT

| IP Address | Infections | CC AS Name |
|-----------------|------------|------------------------------|
| 72.14.207.191 | 3722 | US GOOGLE - Google Inc. |
| 60.28.237.31 | 1403 | CN CHINA169-BACKBONE C |
| 218.244.142.168 | 1201 | CN DXTNET Beijing Dian Xin T |

Press Worthy Mentions

- ▣ The Google Desktop Vuln (May 31st, 2007)
'Regarding security-flaw disclosure, Mr. Merrill says Google hasn't provided much because consumers, its primary users to date, often aren't tech-savvy enough to understand security bulletins and find them "distracting and confusing." Also, because fixes Google makes on its servers are invisible to the user, notification hasn't seemed necessary, he says.' – Wall Street Journal
- ▣ Phishing problem (Nov 1st 2007) "in the two months since RSnake first made his concerns public, no one from Google has publicly disputed anything he has said" – News.com

On with the show...

- ▣ We are simply exacerbating the points already known:
 - Google is, was and will be vulnerable
 - Google hasn't been open about it with consumers
 - Google hasn't fixed their holes in a timely manner
 - Google lies to security researchers
 - ▣ "If you share it with us, we will respond to you with a time we will fix that hole." (April 10th, 2008)
 - ▣ This has NEVER happened, holes may get fixed but I have never been given a timeline for any of the redirects.
 - Google cares more about tracking users than safety.
 - This isn't the whole history... there's lots more...

Evil?

“If today’s malware mostly runs on Windows because it’s the commonest executable platform, tomorrow’s will likely run on the Web, for the very same reason. Because, like it or not, Web is already a huge executable platform, and we should start thinking at it this way, from a security perspective.”

PDP, Architect, GNUCITIZEN, quoting Giorgio Maone

XSS, SO WHAT?

Execute arbitrary code

“Use JavaScript and HTML to craft custom payloads”

Content Spoofing

“Make users believe that content is legitimate when in fact it is controlled by an attacker with malicious intent.”

Phishing

“Steal user passwords by faking login portals to web based services, devices, or web sites.”

Arbitrary JavaScript executes whenever the user follows a link to the gadget or if the gadget is embedded within a web page.

GOOGLE'S ARGUMENT

“On further review, it turns out that this is not a bug, but instead the expected behavior of this domain. Javascript is a supported part of Google modules, as seen, for example, here: http://www.google.com/apis/maps/documentation/mapplets/#Hello_World_of_Mapplets. Since these modules reside on the gmodules.com domain instead of the Google domain, cross-domain protection stops them from being used to steal Google-specific cookies, etc. **If you do find a way of executing this code from the context of a google.com domain, though, please let us know.**”

- Google Security

We are going to spend a few minutes and take their reasoning apart piece by piece and then show you why they are wrong.

GOOGLE'S REASONING ABOUT THE XSS VULN (DOMAIN ARGUMENT)

Premise (Google): Gmodules is a different domain from Google or Gmail.

Premise (Google): You can only attack Gmodules with this vulnerability

Conclusion (Google): The vulnerability is insignificant

Response: This begs the questions *that there is nothing worth exploiting on Gmodules, and that phishing attacks should not be a concern.*

GOOGLE'S REASONING ABOUT THE XSS VULN (RESEMBLANCE ARGUMENT)

Premise (Google): Gmodules does not look like a Google domain

Premise (Google): Users who would follow a link to Gmodules (a Google domain) would be just as likely to follow a link to BadGmodules (not a Google domain).

Conclusion (Google): Fixing the vulnerability would not reduce risk to the user

Response: *Does Gmail look like a Google domain?*

GOOGLE'S REASONING ABOUT THE XSS VULN (EXPECTED BEHAVIOR)

Premise (Google): Gmodules needs JavaScript to serve and cache Gadgets

Premise (Google): There is no harm in using JavaScript to host our Gadgets

Conclusion (Google): The XSS is expected behavior and should not be fixed.

Response: The issue is

- 1) Not JavaScript, but JavaScript security.
- 2) Placing additional security measures could make the hosted code more Secure.
- 3) The current architecture creates an environment of significant risk.

IMPACT OF GMODULES XSS

Attackers can exploit the Gmodules XSS to attack Google Gadgets and potentially the users desktop

Attackers can use Gmodules as a place to host their malware

This makes it virtually impossible to tell bad or dangerous Gmodules code from good or safe code.

Attackers can use Gmodules as a host for Phishing sites

UNDERSTANDING GADGETS

Part of a new world view of *how the web* should operate...

Gadgets are often
talked about in
ideological terms

Google Seed
Money!



GOOGLE GADGETS OVERVIEW



1. Simple to build

“ create gadgets that include tabs, Flash content, persistent storage, dynamic resizing, and more”



2. Access and Run on Multiple Sites

“Your gadget can run on multiple sites and products including iGoogle, Google Maps, Orkut, or any webpage.”



3. Reach Millions of Users

“Gadgets are viewed millions of times per week and generate significant traffic”



GADGETS SOCIAL DESIGN

“OpenSocial is built upon gadgets, so you can build a great viral social app with little to no serving costs.”

1) Viral Spread via ‘Social Graph’

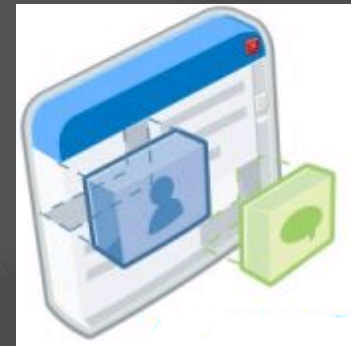
Gadget-as-a-Meme

2) Decentralized Architecture Distributed Processing

Gadget-as-an-Agent

3) Content Rich, Self-Expression

Gadget-as-Expression



<http://code.google.com/apis/opensocial/articles/bestprac.html>



GADGETS SOCIAL DESIGN

4) Dynamic, Organic Change

Gadget-as-an-Organism

5) Expose the Activity Stream

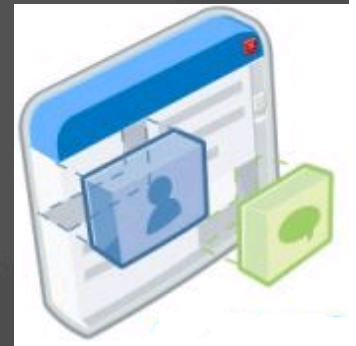
Gadget-as-'Social Information'

Gadget-as-a-'Record of Activity'

6) Browse the Social Graph

Gadget-as-Graph

- *Monitoring without centralization*



<http://code.google.com/apis/opensocial/articles/bestprac.html>



GADGETS SOCIAL DESIGN

7) Drive Interactions and Communication

Gadget-as-Communication

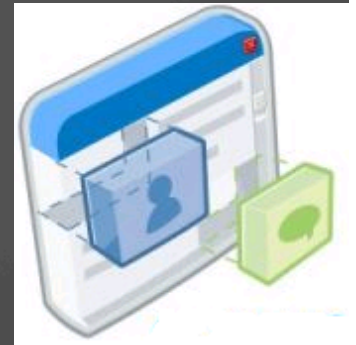
8) Build Relationships and Communities

Gadget-as-a-Community

9) Solve Real World Tasks

Gadget-as-Tool

- *Problem Solving*
- *Revenue Generating*



<http://code.google.com/apis/opensocial/articles/bestprac.html>

TYPES OF GOOGLE GADGETS

- 1) Gadgets for iGoogle
- 2) Gadgets for the web
- 3) OpenSocial API
- 4) Desktop Gadgets



<http://code.google.com/apis/gadgets/>

HIGH LEVEL SECURITY CONCERNS



Gadgets can be easily “weaponized” into attack tools or payloads



Gadgets are largely 3rd party code and potentially malicious



Gadgets can attack other gadgets, the desktop, or web sites



Gadgets can have (most of) the same vulnerabilities as web applications

DISTURBING DISCLAIMERS: GADGET FAQ

What if my Gadget is broken or displays offensive or inappropriate content?

Most of our gadgets are created and maintained by third parties. If you have questions or concerns about the functionality or content of a particular gadget, we suggest you contact the gadget's author directly. You may be able to locate contact information for the gadget's creator

Perfomance-Meter [dropdown] [minimize] [close]

Requires the latest Google Desktop software.

Install

[Why does this gadget require Google Desktop?](#)

By installing, you agree to Google's [Terms of Service](#).

Google has not verified the features or security of third party gadgets, which may use [Advanced APIs](#).



GADGETS THREAT MODEL



1. JavaScript/HTML/Script Injection

- Gadget-to-Gadget Vectors
- Gadget-to-Desktop Vectors

2. Defacement

- Content/Data Manipulation Attacks

3. Poisoning

- Data Pollution
- Social Graph Attacks
- 'click fraud' corollaries

GADGETS THREAT MODEL

4. Content/Gateway Spoofing

- Masquerading, Redirection
- Gateways to other apps
- Phishing



5. Surveillance/Spyware

- Spyware/ Adware
- User tracking/monitoring
- Unauthorized Data collection & Export

6. Exposures

- Exposing “low-interaction” user data
- Personal information theft + leaks

GADGETS THREAT MODEL



7. Malware “Gmalware”

- targeted attacks, DDOS
- Cookie Theft, Zombies
- Exploits, Wrappers
- Browser attacks + Hijacking

8. Worms

- Social Networks

9. Abusive/Coercive Functionality

- Tracking gadgets, privacy concerns, unfriendly gadgets

DEVELOPER HUMOR

Take a close look at the Gadget's *Options*. Someone at Google has a sense of humor...

Gadget testing container

Displaying gadget:

cache use caja use permissive

Using state: **do evil**

Viewer id: Owner id:

Decisions decisions...

```
if ((too_be($evil) ) || (!too_be($evil))) {  
    $that = $the->question();  
}
```

ADVANCED API

[Google Desktop Gadget API](#)

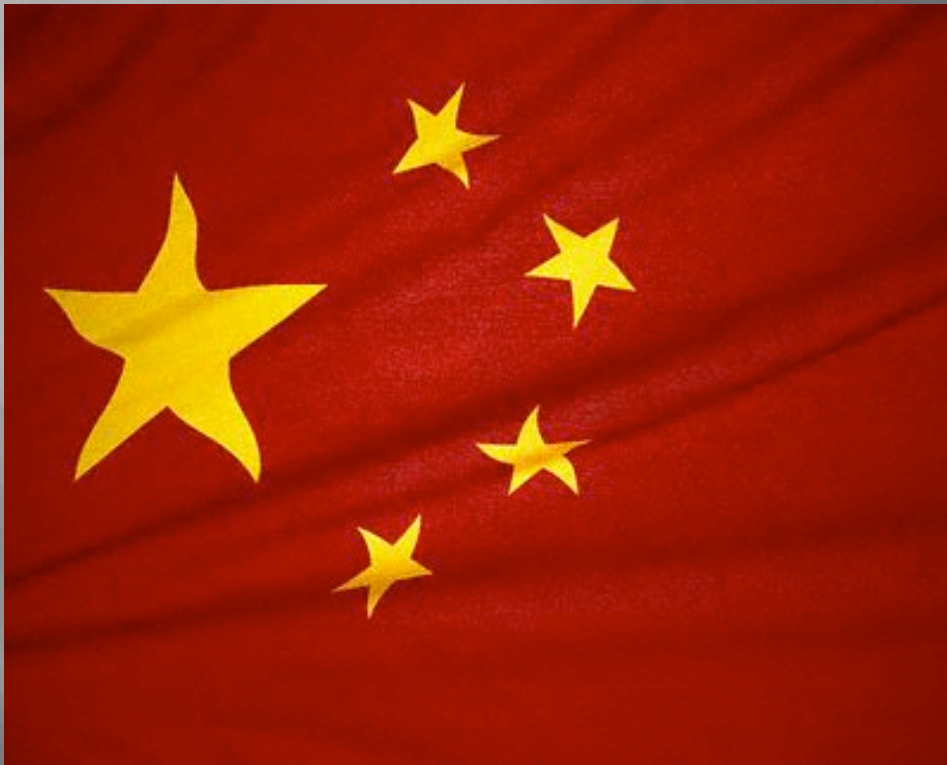
<http://code.google.com/apis/desktop/>

Desktop gadgets are powerful mini-applications that can live within the Google Desktop sidebar, or right on the user's desktop, or even inside iGoogle home pages. You create Desktop gadgets using XML and JavaScript, optionally adding native code for access to Windows APIs. The Desktop Gadget API enables advanced functionality such as transparency, animation, custom fonts, and personalization.

<http://desktop.google.com/en/dev/advancedapi.html>

<http://code.google.com/more/#products-gadgets-gdgadgets>

THE PEOPLE'S GADGET...



Crackdown Gadget..

THE PEOPLE'S GADGET...

The Joy of Tech™

by Nitrozac & Snaggy



Google in China... search no evil?

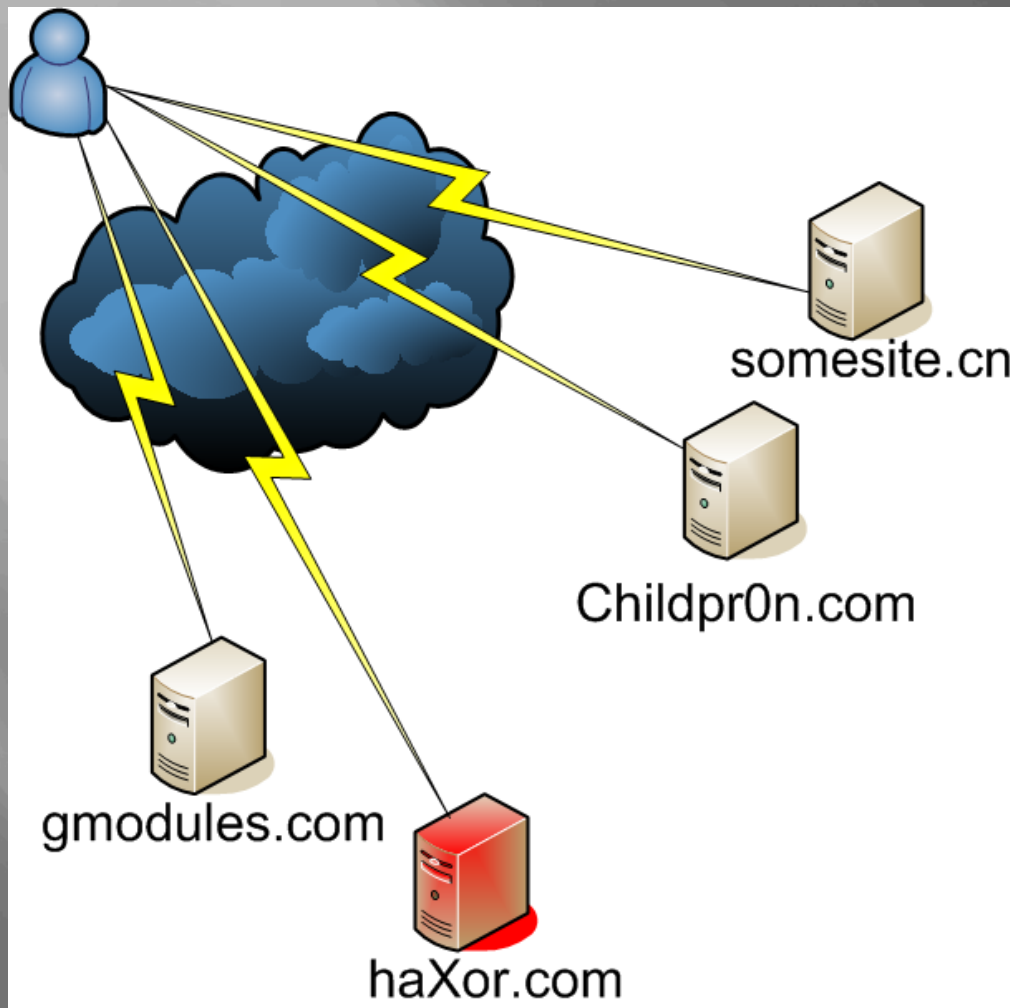
THE PEOPLE'S GADGET...



M.U.S.H.U!

1. **Monitors** feeds/web sites for subversive content
2. **Uploads** search terms (via CSS history hack, etc...) and IP address to state server
3. **Spiders** Web Sites from which content originates and determines how “Red” a domain is
4. **Hinders** freedom movements and suppresses Anti-Communist rhetoric
5. **Updates** state database with data from the “Social Grid”

CSRF GADGET



- 1) Or SQL injection CSRF
- 2) Or RFI injection CSRF
- 3) Or Exponential (Xdomain) XSS worms
- 4) Etc.. Etc..

Demo time...

YAHOO SITE EXPLORER SPIDER GADGET

1. Port of PDPs Yahoo Spider Gadget

On this page you will find a small POC (Proof of Concept) of a client-side (only JavaScript) spider that is based on the top of Yahoo Site Explorer PageData service

2. Gadget

We created a gadget for PDPs spider example

3. Client-Side JavaScript Spider

The Page Data service allows you to retrieve information about the subpages in a domain or beneath a path that exist within the Yahoo! index.

SIMPLE PHP SPIDER GADGET



- Demonstrates ability to call an external PHP script to include functionality within a Gadget
- One of a number of useful web hacking Gadgets we've ported
- Gadget Code & Spider Code is available for download

Gadget Spider

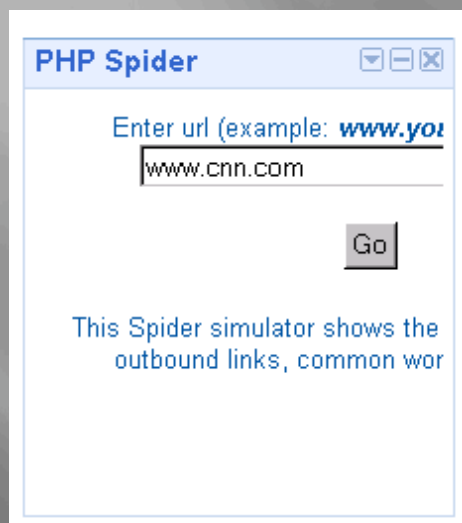
<http://www.seoish.com/spider-simulator-google-gadget/>

SIMPLE PHP SPIDER

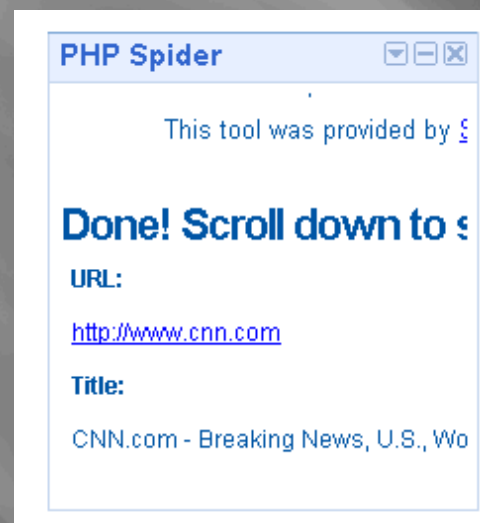
We fetch a PHP script within the Gadget

Configuration

Results



The screenshot shows a window titled "PHP Spider" with a text input field containing "www.cnn.com" and a "Go" button. Below the input field, there is a descriptive text: "This Spider simulator shows the outbound links, common wor".

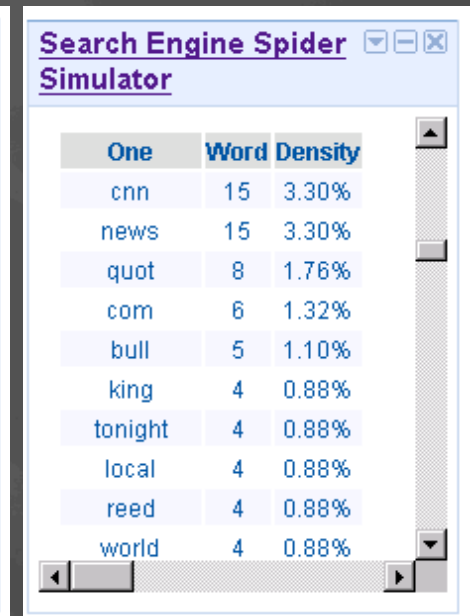


The screenshot shows a window titled "PHP Spider" displaying the results of the spider simulation. It includes the text "Done! Scroll down to s" and "URL: <http://www.cnn.com>". Below this, the "Title:" is shown as "CNN.com - Breaking News, U.S., Wo".



The screenshot shows a window titled "Search Engine Spider Simulator" displaying a list of links. The list includes:

- <http://www.cnn.com/>
- <http://www.cnn.com/WORLD/>
- <http://www.cnn.com/US/>
- <http://www.cnn.com/POLITICS/>
- <http://www.cnn.com/CRIME/>
- <http://www.cnn.com/SHOWBIZ/>
- <http://www.cnn.com/HEALTH/>
- <http://www.cnn.com/TECH/>
- <http://www.cnn.com/TRAVEL/>
- <http://www.cnn.com/LIVING/>
- <http://money.cnn.com/?cnn=ves>

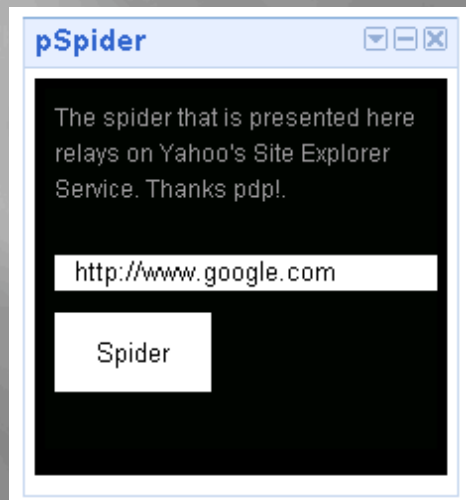


The screenshot shows a window titled "Search Engine Spider Simulator" displaying a table of word density. The table has three columns: "One", "Word", and "Density".

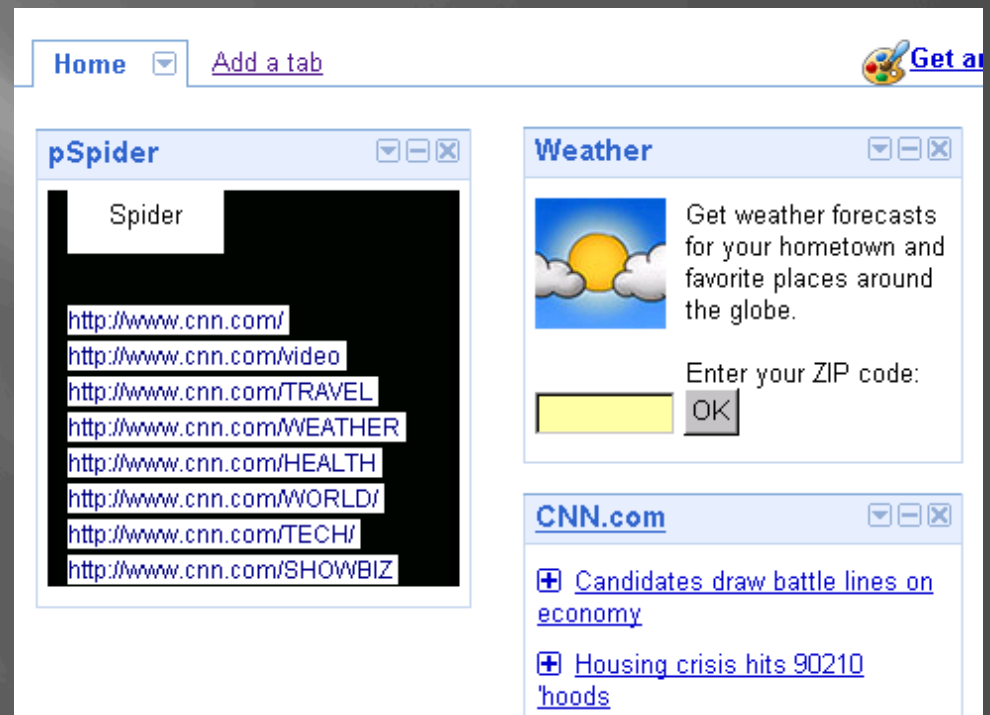
| One | Word | Density |
|---------|------|---------|
| cnn | 15 | 3.30% |
| news | 15 | 3.30% |
| quot | 8 | 1.76% |
| com | 6 | 1.32% |
| bull | 5 | 1.10% |
| king | 4 | 0.88% |
| tonight | 4 | 0.88% |
| local | 4 | 0.88% |
| reed | 4 | 0.88% |
| world | 4 | 0.88% |

YAHOO SITE EXPLORER SPIDER GADGET (PSPIDER)

Configuration



Results



<http://exgenesis.com/wonderbread/pspider.xml>

JS PORT SCANNER GADGET

- 1) Demonstrates port scanning via a javascript embedded within a gadget
- 2) We ported PDPs nice JS Scanner into a Gadget
- 3) Port scanner Gadget code is available for download

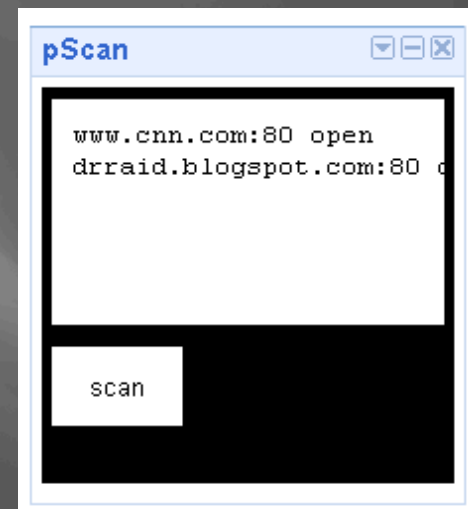
Gadget Port Scanner

JS PORT SCANNER GADGET

pScan Configuration



Results



PHISHING GADGET


Gmail: Email from Google - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Reload Print Mail Stop




Address <http://gmodules.com/ig/creato?synd=open&url=http%3A//ha.ckers.org/asdf2.xml&pt=&context=b&synd=open&lang=en&.lang=en&country=us&.country=us&cat=all&num=24&st> Go Links >>

Google G Go Bookmarks 2 blocked Check AutoLink AutoFill Send to Settings

 **Welcome to Gmail**

A Google approach to email.

Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

-  **Less spam**
Keep unwanted messages out of your inbox with Google's innovative technology.
-  **Mobile access**
Read Gmail on your mobile phone by pointing your phone's web browser to <http://gmail.com/app>.
[Learn more](#)
-  **Lots of space**
Over 6922.042211 megabytes (and counting) of free storage so you'll never need to delete another message.


Sign in to Gmail with your Google Account

Username:

Password:

Remember me on this computer.

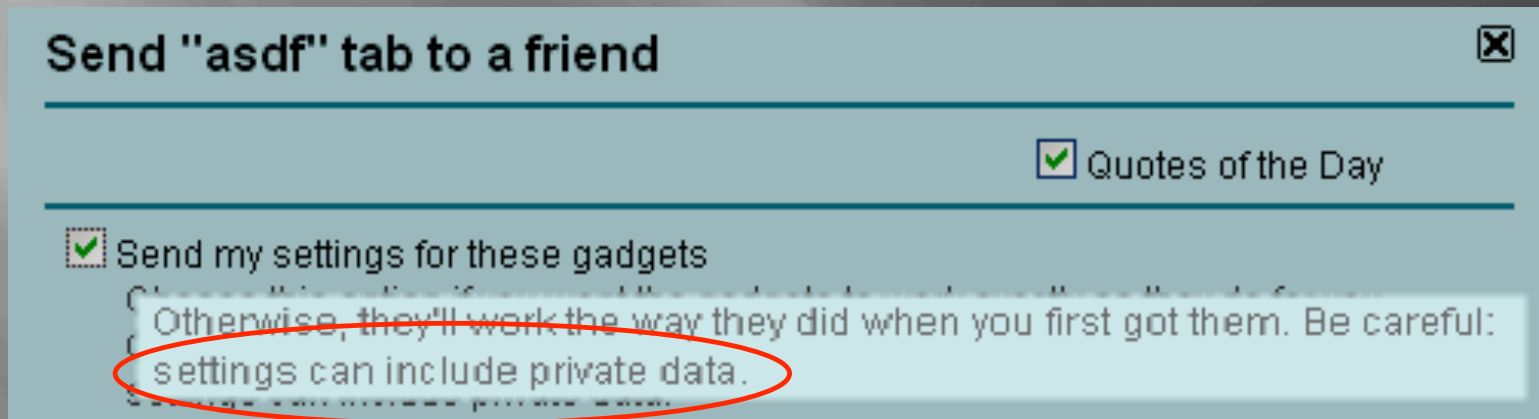
[I cannot access my account](#)

Latest News from the Gmail Blog 

[Chat with your Gmail contacts on the iPhone](#)

CROSS-GADGET ATTACKS

1. Gadgets can attack one another, steal cookies and/or data, manipulate the content of other gadgets.



Demo time...

Referrers

http://89.gmodules.com/ig/ifr?url=http://www3.sympatico.ca/mjdresser/Delicious.xml&nocache=0&up_username=wipeouter&up_tag=&up_count=15&upt_count=enum&up_images=0&upt_images=bool&lang=de&country=de&.lang=de&.country=de&synd=ig&mid=89&ifpctok=6968901372936289341&parent=http://www.google.de&extern_js=/extern_js/f/CgJlbhICdXMrMAo4ACw/8IKVf7DB5CY.js

http://98.gmodules.com/ig/ifr?url=http://customrss.googlepages.com/customrss.xml&nocache=0&up_rssurl=http://ha.ckers.org/blog/feed/&up_title=ha.ckers.org&up_titleurl=http://ha.ckers.org&up_num_entries=10&up_linkaction=openlink&upt_linkaction=enum&up_background=E1E9C3&up_border=CFC58E&up_round=1&upt_round=bool&up_fontfamily=Arial&up_fontsize=8pt&up_openfontsize=9pt&up_itempadding=3px&up_bullet=icon&upt_bullet=enum&up_custicon=Overrides+favicon.ico&up_boxicon=1&upt_boxicon=bool&up_opacity=20&upt_opacity=enum&up_itemlinkcolor=596F3E&up_itemlinkweight=Normal&upt_itemlinkweight=enum&up_itemlinkdecoration=None&upt_itemlinkdecoration=enum&up_vlinkcolor=C7CFA8&up_vlinkweight=Normal&upt_vlinkweight=enum&up_vlinkdecoration=None&upt_vlinkdecoration=enum&up_showdate=1&upt_showdate=bool&up_datecolor=9F9F9F&up_tcolor=1C57A9&up_thighlight=FFF19D&up_desclinkcolor=1B5790&up_color=000000&up_dback=FFFFFF&up_dborder=DFCE6F&up_desclinkweight=Bold&upt_desclinkweight=enum&up_desclinkdecoration=None&upt_desclinkdecoration=enum&lang=nl&country=us&.lang=nl&.country=us&synd=ig&mid=98&ifpctok=-5944482123251000084&parent=http://www.google.com&extern_js=/extern_js/f/CgJlbhICdXMrMBI4ACwrMBM4ACw/v3vgcgA0x8g.js

Seriously, is this a problem?

- ▣ How can you get a malicious Google Gadget on someone's iGoogle?
 - They can add something that they think is good but turns into something bad.
 - We can hack any one of the hundreds of domains that already host Google gadgets (remember how easy it is to hack into websites)?
 - Since Google's base domain is vulnerable to XSS fairly frequently, we could use XMLHttpRequest if we know of one. But if we have that, we don't need any of this other stuff, so that's not a practical argument although it would add persistence to your attack if necessary (turning reflected XSS into persistent).
 - Annnnd, we can force people to add it subversively...
 - ▣ Demo time.

Anyone?

- ▣ Is anyone from Google in the audience?
- ▣ Is this Expected Behavior™?
- ▣ Get to the point already:
 - It's "bad".

Robert Hansen Loses His Sh*t Over Google Gadgets

1. [RSnake discovers](#) that Google gadgets can be coerced into rendering [arbitrary tags](#), and reports it to Google.
2. Google responds, in effect, "that's one of the reasons why they live under gm continuing. "If you do find a way of executing this code from the context of a

- ▣ We know you have choices in the speeches you listen to. Thank you for flying Google Gadgets airlines.

Questions/Comments?

- ▣ Tom “Strace” Stracener
 - ▣ <http://www.cenzic.com>
 - ▣ <http://www.badgadgets.net>
 - ▣ strace_aT_gmail_d0t_org

- ▣ Robert “RSnake” Hansen
 - ▣ <http://www.sectheory.com>
 - ▣ <http://ha.ckers.org> – the lab
 - ▣ <http://sla.ckers.org> – the forum
 - ▣ h_aT_ckers_d0t_org