About Me

- Robert Hansen - CEO
- SecTheory LLC
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - http://www.sectheory.com/
- Advisory capacity to VCs/start-ups
- Founded the web application security lab
  - http://ha.ckers.org/ - the lab
  - http://sla.ckers.org/ - the forum
Xploiting Google Gagets, and Clickjacking

- 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!)
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
Word gets out – fast!

- 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://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

And others…
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…
I like consumers more than Google.
I disclosed 4 redirects 11\textsuperscript{th}, Jan 2006 (with no reaction)
I then disclosed 1 XSS hole on 4\textsuperscript{th}, Jul 2006 (reaction!)
“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”.

![Google Gadgets Image]

This is a preview of what the gadget may look like. If parts of the gadget appear cut off, try increasing the width and/or height.
“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?
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...
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 JavaScript can be used for, apparently (redirection).

Google lied about the danger of a vulnerability that they already agreed to fix.

Bad guys are STILL using it!
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
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 by following the links provided.

![Performance-Meter]

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](#).
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://code.google.com/more/#products-gadgets-gdgadgets
**SIMPLE PHP SPIDER**

We fetch a PHP script within the Gadget

Configuration

Results

**PHP Spider**

Enter url (example: www.you

www.cnn.com

Go

This tool was provided by $

**Done! Scroll down to see**

URL:

http://www.cnn.com

Title:

CNN.com - Breaking News, U.S., Wo

**Search Engine Spider Simulator**

Links:

http://www.cnn.com/
http://www.cnn.com/WORLD/
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=yes

**Search Engine Spider Simulator**

<table>
<thead>
<tr>
<th>One</th>
<th>Word Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>cnn</td>
<td>15</td>
</tr>
<tr>
<td>news</td>
<td>15</td>
</tr>
<tr>
<td>quot</td>
<td>8</td>
</tr>
<tr>
<td>com</td>
<td>6</td>
</tr>
<tr>
<td>bull</td>
<td>5</td>
</tr>
<tr>
<td>king</td>
<td>4</td>
</tr>
<tr>
<td>tonight</td>
<td>4</td>
</tr>
<tr>
<td>local</td>
<td>4</td>
</tr>
<tr>
<td>reed</td>
<td>4</td>
</tr>
<tr>
<td>world</td>
<td>4</td>
</tr>
</tbody>
</table>
YAHOO SITE EXPLORER SPIDER GADGET (PSPIDER)

Configuration

The spider that is presented here relays on Yahoo's Site Explorer Service. Thanks pdpl.

http://www.google.com

Spider

Results

http://www.cnn.com/
http://www.cnn.com/video
http://www.cnn.com/TRAVEL
http://www.cnn.com/WEATHER
http://www.cnn.com/HEALTH
http://www.cnn.com/WORLD/
http://www.cnn.com/TECH/
http://www.cnn.com/SHOWBIZ

Get weather forecasts for your hometown and favorite places around the globe.
Enter your ZIP code:

CNN.com
- Candidates draw battle lines on economy
- Housing crisis hits 90210 hoods

http://exgenesis.com/wonderbread/pspider.xml
JS PORT SCANNER GADGET

pScan Configuration

JAVA SCRIPT PORT SCANNER

target: drraid.blogspot.com

ports: 80 (you can use multiple ports such as 80, 81, 8080, 1024)

Results

www.cnn.com:80 open
drraid.blogspot.com:80 open

scan
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 6022.042211 megabytes (and counting) of free storage so you’ll never need to delete another message.

Welcome to Gmail

Sign in to Gmail with your Google Account
Username:
Password:
Remember me on this computer:
Sign in

I cannot access my account

Click to sign up for Gmail
CROSS-GADGET ATTACKS

1. Gadgets can attack one another, steal cookies and/or data, manipulate the content of other gadgets.
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://hacker.org/blog/feed/&up_title=ha.cackers.org&up_titleurl=http://hacker.org&up_num_entries=10&up_linkaction=openlink&upt_linkaction=enum&up_background=E1E9C3&up_border=CFC58E&up_round=1&upt_round=boool&up_fontfamil=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=boool&up_opacity=20&upt_opacity=enum&up_itemlinkcolor=596F3E&up_itemlinkweight=Normal&up_itemlinkweight=enum&up_itemlinkdecoration=Normal&up_vlinkcolor=C7CFA8&up_vlinkweight=Normal&up_vlinkweight=enum&up_vlinkdecoration=enum&up_vlinkcolor=000000&up_vlinkweight=Normal&up_vlinkweight=enum&up_vlinkdecoration=enum&up_dcolor=9F9F9F&up_tcolor=1C57A9&up_highlight=FFF19D&up_desclinkcolor=1B5790&up_color=000000&up_dback=FFFFFF&up_dborder=DFCE6F&up_desclinkweight=Bold&up_desclinkweight=enum&up_desclinkdecoration=enum&up_lang=nl&country=us&lang=us&country=nl&synd=ig&mid=98&ifpctok=-5944482123251000084&parent=http://www.google.com&extern_js=/extern_js/f/CgJlbhICdXMrMBI4ACwrMBM4ACw/v3vgcgA0x8g.js
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.
Clickjacking 101

Flash Player Help

Global Security Settings panel

TABLE OF CONTENTS

Flash Player Help
Settings Manager
- Global Privacy Settings Panel
- Global Storage Settings Panel
- Global Security Settings Panel
- Global Notifications Settings Panel
- Website Privacy Settings Panel
- Website Storage Settings Panel
Display Settings
Local Storage Settings
Microphone Settings

Adobe Flash Player™ Settings Manager

Global Security Settings

Some websites may access information from other sites using an older system of security. This is usually harmless, but it is possible that some sites could obtain unauthorized information using the older system. When a website attempts to use the older system to access information:

- Always ask
- Always allow
- Always deny

Always trust files in these locations: Edit locations...
Clickjacking 101
Clickjacking Issues

- JavaScript is not required
- Flash vulnerable
- Flash security settings manager is also vulnerable
- IE7.0 and IE8.0 could be overlayed, plus IE8.0 persistence (demo x2…)
- Framebusting code does not work well in IE8.0 Beta.
- Clicks can be monitored
- Can promote “Unlikely” XSS vulnerabilities
- Prior to 1.8.1.9 Noscript was vulnerable
- CSRF protection using nonces can often be overcome
Clickjacking 101

- Ronald’s flash settings manager subversion...

This is a non-malicious proof of concept based upon clickjacking, this poc leverages all security settings, which allow cross domain access. Please do notice that once you checked, your Flash settings will allow for cross domain access! to un-check go to this page: unio flash settings credits: Robert Hansen, Jeremiah Grossman, FPDF, rydh

Login please

Hello! welcome back!

username: test
password: 

Do you want to remember your login? please check to allow: Always allow

Login!
Clickjacking 101

- Typical security dialog...
PDP’s version…

All your sites are belong to us!

Do you allow AJAX?
AJAX will improve your user experience!

☐ Never ask again
☑ Allow
Clickjacking 101

- Demo time...

Click Jacking Demo

Click

here

please.
Oracle Webforms

Customer Information Maintenance

Edit Customer Information

Customer Id: 101
First Name: Constantin
Last Name: Wellesil
Credit Limit: $101.00
eMail: Constantin.Wellesil@AN

[Buttons: OK, Cancel]
Delete User Accounts

<table>
<thead>
<tr>
<th>NAME</th>
<th>MEMBER ID/EMAIL ADDRESS</th>
<th>(Delete)</th>
</tr>
</thead>
<tbody>
<tr>
<td>mike tadlo...</td>
<td><a href="mailto:mikel@verizon.net">mikel@verizon.net</a></td>
<td></td>
</tr>
<tr>
<td>Chris Miller</td>
<td>chris9441@verizon...</td>
<td>(Delete)</td>
</tr>
<tr>
<td>Jan Miller</td>
<td>jan9441@verizon...</td>
<td>(Delete)</td>
</tr>
<tr>
<td>Curran Smi...</td>
<td>curran9721@verizon...</td>
<td>(Delete)</td>
</tr>
</tbody>
</table>
**Auto-purchase**

**Shopping Cart Contents**

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 x Heritage Grunge Clikit</td>
<td>$3.50</td>
</tr>
<tr>
<td>- Zip Part 1: Download</td>
<td></td>
</tr>
</tbody>
</table>

**Sub-Total:** $3.50

**Free Shipping:** $0.00

**Discount Coupons:** couponcode - $3.50

**Total:** $0.00

**Shipping Method:** Free Shipping

**Payment Method:**

**Final Step**
- continue to confirm your order. Thank you!
Auto download

Checkout Success!
Congratulations on completing checkout. Your files will be accessible from your account for the next 7 days. Should you have any problems please do not hesitate to email us.

Please notify me of updates to the products I selected below:

- [ ] Heritage Grunge Click

Your Order Number:

You can view your order history by going to the My Account page and by clicking on View Orders.

Please direct any questions you have to customer service.

Thanks for shopping with us online!

Download your products here:

<table>
<thead>
<tr>
<th>Product</th>
<th>Link</th>
<th>Downloads remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heritage Grunge Click</td>
<td>02/04/2006</td>
<td>5</td>
</tr>
</tbody>
</table>
## Confirm Order

<table>
<thead>
<tr>
<th>Date</th>
<th>06/06/2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>07:38 AM</td>
</tr>
</tbody>
</table>

### Details

- **Buy PCU 1 Share**
- **Market N/A DAY**
- **Estimated total cost $91.73**
- **Southern Copper Corporation Common Stock (PCU:NYSE)**
- **Bid 78.26 Ask 91.73 Last trade 91.73**

### Buttons

- CANCEL ORDER
- SEND ORDER
Auto-call
Webex/Meetingplace
OWA
Router Reset

D-Link

DFL-700
Network Security Firewall

Restart / Reset

- Quick restart - reset interfaces and restore configuration
- Full restart - restart from power on state

Reset to factory defaults

You can restore the unit to factory defaults. This means that all configuration parameters will be wiped, and all firmware upgrades removed.

On the next startup, its LAN IP address will be 192.168.1.1, and the web GUI will begin with the setup wizard. It will not accept connections on any interface other than the LAN interface.

Reset to Factory Defaults
Delete Firewall Rules

[Image of SonicWall Firewall interface showing access rules]

<table>
<thead>
<tr>
<th>Priority</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Options</th>
<th>Enable</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WLAN</td>
<td>192.168.168</td>
<td>HTTP Management</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>LAN</td>
<td>192.168.168</td>
<td>HTTPS Management</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>LAN</td>
<td>192.168.168</td>
<td>HTTP Management</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>WLAN</td>
<td>192.168.168</td>
<td>HTTPS Management</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>*</td>
<td>192.168.168</td>
<td>Key Exchange (IKE)</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>192.168.168</td>
<td>* Key Exchange (IKE)</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>WLAN</td>
<td>WLAN</td>
<td>Any</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>WLAN</td>
<td>LAN</td>
<td>Any</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>LAN</td>
<td>WLAN</td>
<td>Any</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>LAN</td>
<td>*</td>
<td>Any</td>
<td>DENY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>*</td>
<td>LAN</td>
<td>Any</td>
<td>ALLOW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Delete Logs

Login Logs

All log files:  [Graphs]  [Log Data]  [Admin Logins]

<table>
<thead>
<tr>
<th>File name</th>
<th>Last modified</th>
<th>File size</th>
<th>Graphs</th>
<th>Log Data</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current log</td>
<td>log.txt Mon 09/29/2003 04:02 PM</td>
<td>284</td>
<td>[Graphs]</td>
<td>[Log Data]</td>
<td></td>
</tr>
<tr>
<td>Older logs</td>
<td>log_29Sep2003_0926 Mon 09/29/2003 09:26 AM</td>
<td>1603</td>
<td>[Graphs]</td>
<td>[Log Data]</td>
<td>[Delete]</td>
</tr>
</tbody>
</table>
Make Your Profile Public

Who Can View My Full Profile

- My Friends Only
- Public
- Only Users Over 18

Privacy Settings

- Friend Requests - Require email or last name
- Comments - approve before posting
- Hide Online Now
- Show My Birthday to my Friends
- Photos - No Forwarding
- Blog Comments - Friends Only
- Friend Requests - No Bands
- Block Users Under 18 From Contacting Me
Deactivate Wordpress Plugins

Plugin Management

Plugins extend and expand the functionality of Wordpress. Once a plugin is installed, you may activate it or deactivate it here.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Version</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akismet</td>
<td>2.1.4</td>
<td>Akismet checks your comments against the Akismet web service to see if they look like spam or not. You need a WordPress.com API key to use it. You can review the spam it catches under “Comments.” To show off your Akismet stats, just put <code>&lt;php akismet_counter(); ?&gt;</code> in your template. See also: <a href="http://matt.mullenweg.com">wp stats plugin</a> by Matt Mullenweg.</td>
<td>Activate Edit</td>
</tr>
<tr>
<td>Hello Dolly</td>
<td>1.5</td>
<td>This is not just a plugin; it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong. Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. By Matt Mullenweg.</td>
<td>Deactivate Edit</td>
</tr>
</tbody>
</table>

If something goes wrong with a plugin and you can’t use Wordpress, delete or rename that file in the wp-content/plugins/ folder and it will be automatically deactivated.

www.themetalab.com
Demo time...
not dead, just got back from burning man this am, catching up and recoverinh
Add Friends on Orkut

Friend confirmation
Please make sure that this person is your friend before you confirm

- haven't met
- acquaintance
- friend
- good friend
- best friend

Note: This selection is used to let you categorize your friends list and is only visible to your friends.
MySpace

Bob wants to be your friend!

- Approve
- Deny
- Spam

Send Message | View Mutual Friends
Flashblock
Clickjacking 101

- Use Noscript++/Upgrade Flash
- Fix the browsers (all of them)
- Put tape over your video camera
Thank you!

- Robert Hansen
- http://www.sectheory.com – the company
- http://ha.ckers.org – the lab
- http://sla.ckers.org – the forum
- XSS Exploits – the book
- robert_aT_sectheory_d0t_org – the email