SecTheory

Internet Security

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!)

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://blogs.geekdojo.net/brian/archive/2004/10/14/googlephishing.aspx
  - 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://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

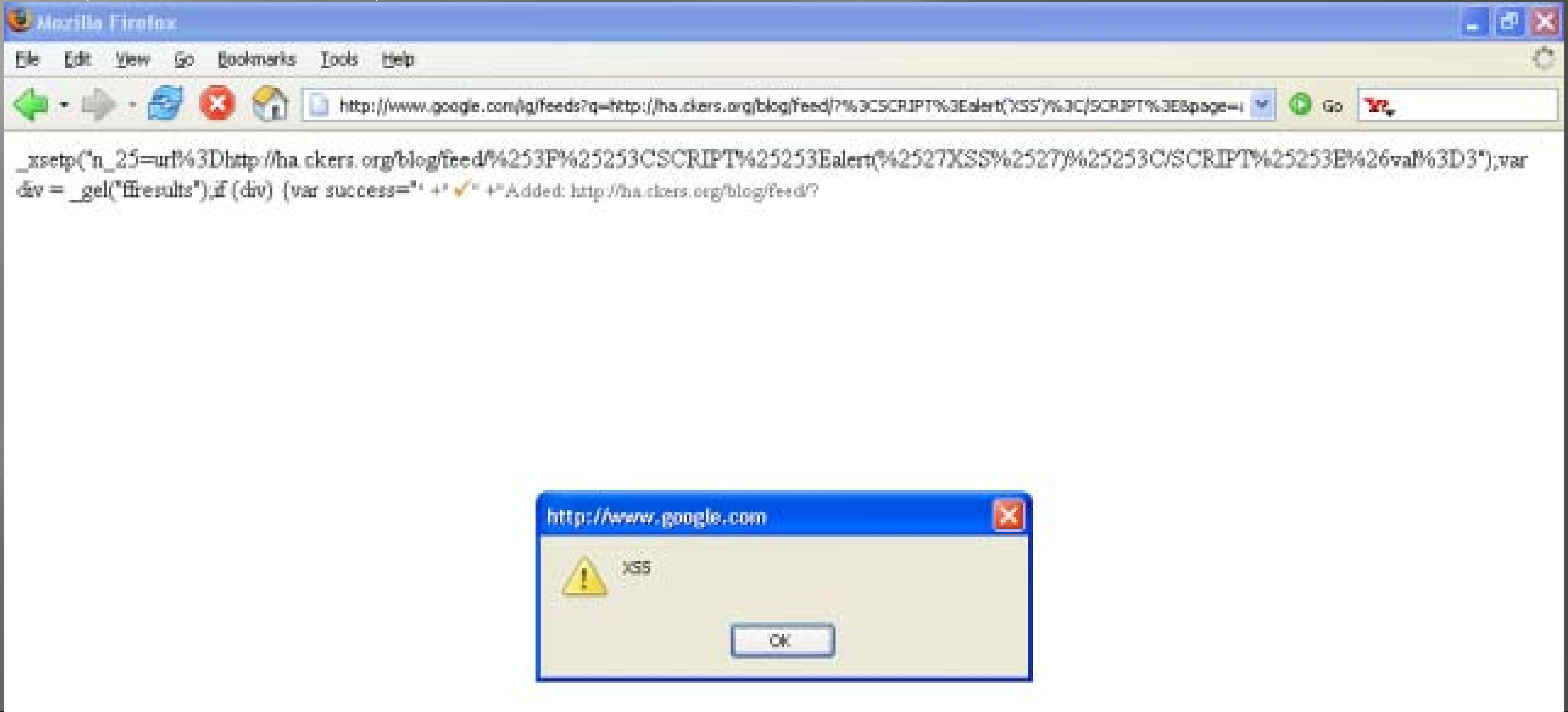
- Everyone has vulns. But in this case…
- We informed Google that their own users were being exploited, to which we were told that they were putting a blacklist in place.
- Yes, you heard me, a blacklist…
- Blacklists only block what you know, not what you don't know – they refused to fix the problem 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

- I like consumers more than Google.
- I disclosed 4 redirects 11th, Jan 2006 (with no reaction)
- I then disclosed 1 XSS hole on 4th, Jul 2006 (reaction!)



http://www.google.com/ig/feeds?q=http://ha.ckers.org/blog/feed/?%3CSCRIPT%3Ealert('XSS')%3C/SCRIPT%3E&page=

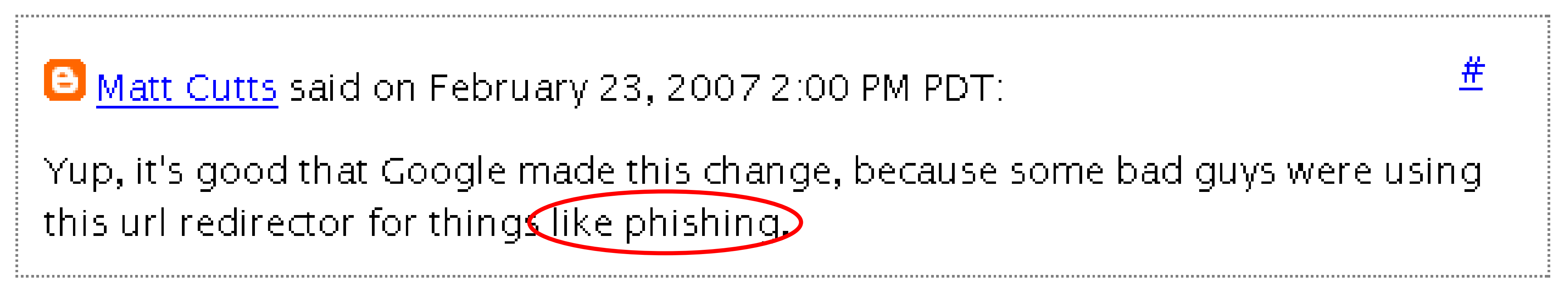
```
_xsetp("n_25=url%3Dhttp://ha.ckers.org/blog/feed/%253F%25253CSCRIPT%25253Ealert(%2527XSS%2527)%25253C/SCRIPT%25253E%26val%3D3");var
div = _gel("ffresults");if (div) {var success="' +' ✓' +"Added: http://ha.ckers.org/blog/feed/?
```

http://www.google.com

XSS

Wait, You Agree?!

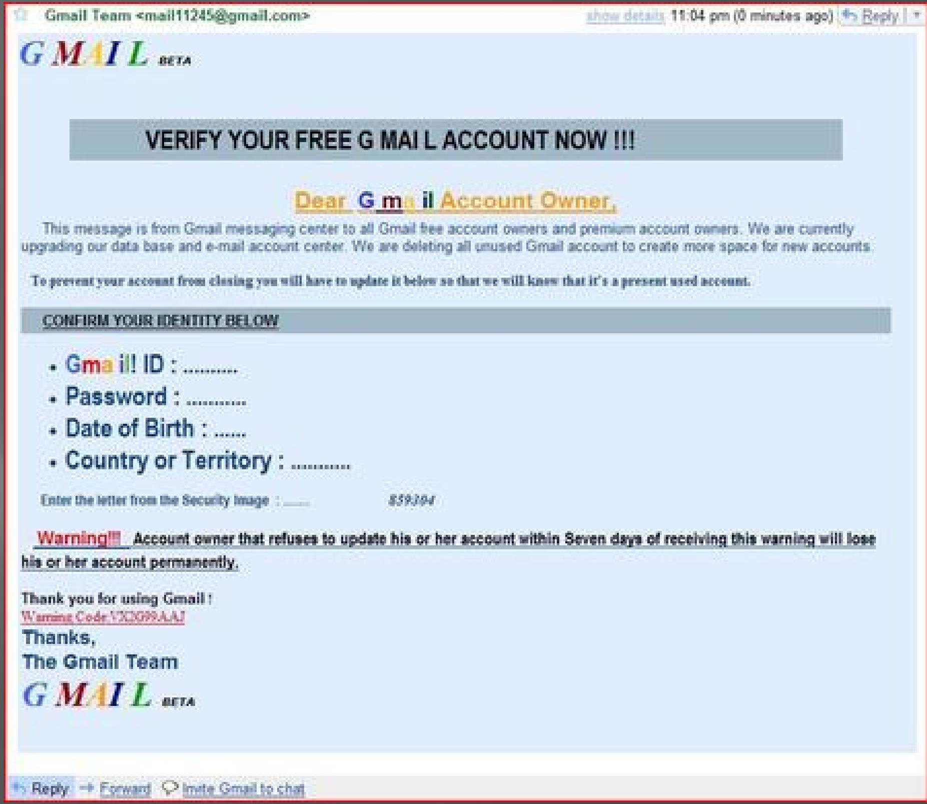
- "Just to close this subject out, I think the open url redirection … has been closed.... To the extent that open url redirection was being used by phishers, closing the most-used url should make a difference." – Matt Cutts
- "Given that tons of different internal groups at Google used this redirector 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



Gmail Team <mail11245@gmail.com> 11:04 pm (0 minutes ago)

G MAIL BETA

VERIFY YOUR FREE G MAI L ACCOUNT NOW !!!

Dear G ma il Account Owner,

This message is from Gmail messaging center to all Gmail free account owners and premium account owners. We are currently upgrading our data base and e-mail account center. We are deleting all unused Gmail account to create more space for new accounts.

To prevent your account from closing you will have to update it below so that we will know that it's a present used account.

CONFIRM YOUR IDENTITY BELOW

- Gma il! ID : ....
- Password : ....
- Date of Birth : ......
- Country or Territory : ....

Enter the letter from the Security Image : 859304

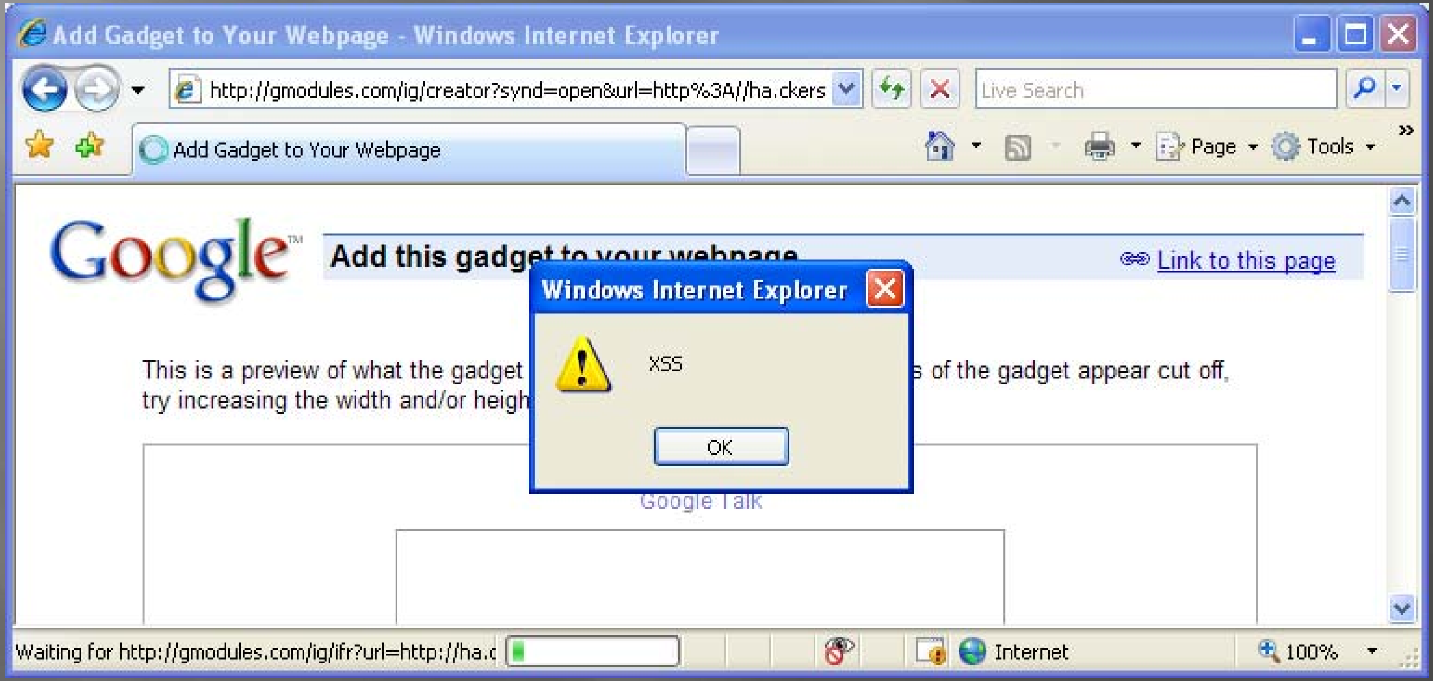
Warning!!! Account owner that refuses to update his or her account within Seven days of receiving this warning will lose his or her account permanently.

Thank you for using Gmail !
Warning Code:VX2G99AAJ
Thanks,
The Gmail Team
G MAIL BETA

- 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 Gagdets

- 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".



Add Gadget to Your Webpage - Windows Internet Explorer

http://gmodules.com/ig/creator?synd=open&url=http%3A//ha.ckers

Add this gadget to your webpage

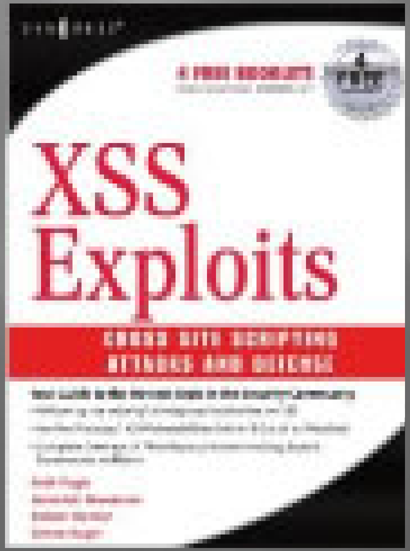
This is a preview of what the gadget … s of the gadget appear cut off, try increasing the width and/or heigh

Windows Internet Explorer

XSS

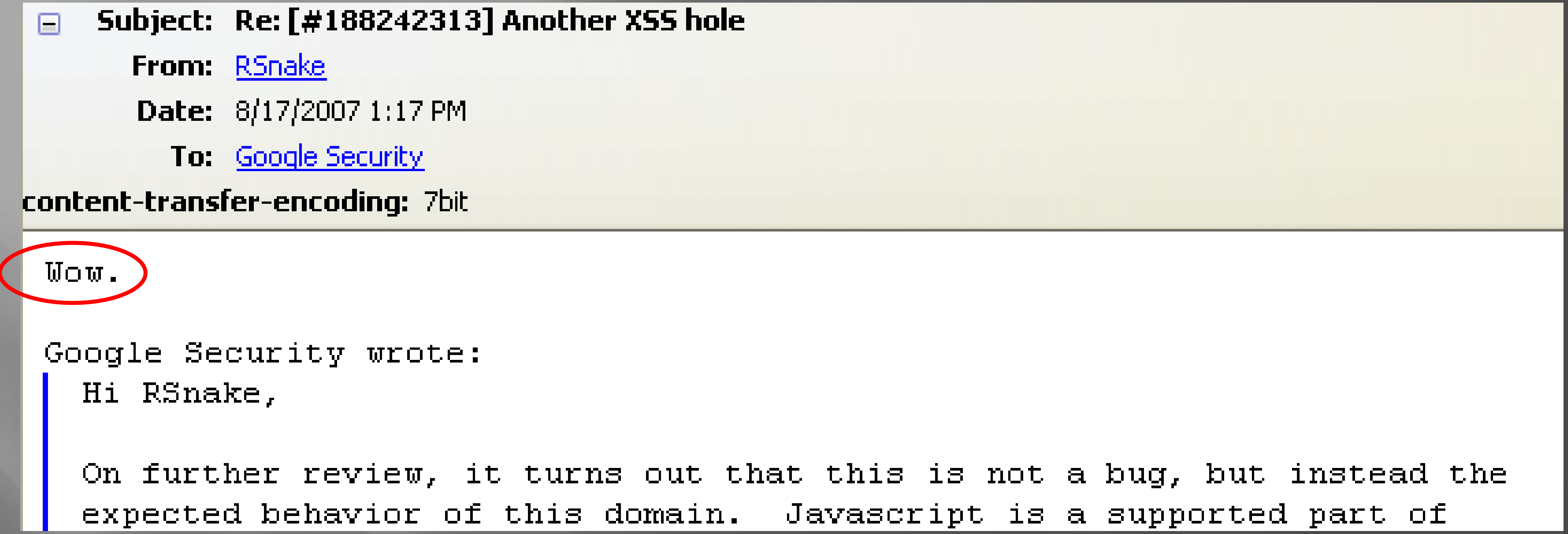
Waiting for http://gmodules.com/ig/ifr?url=http://ha.c

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

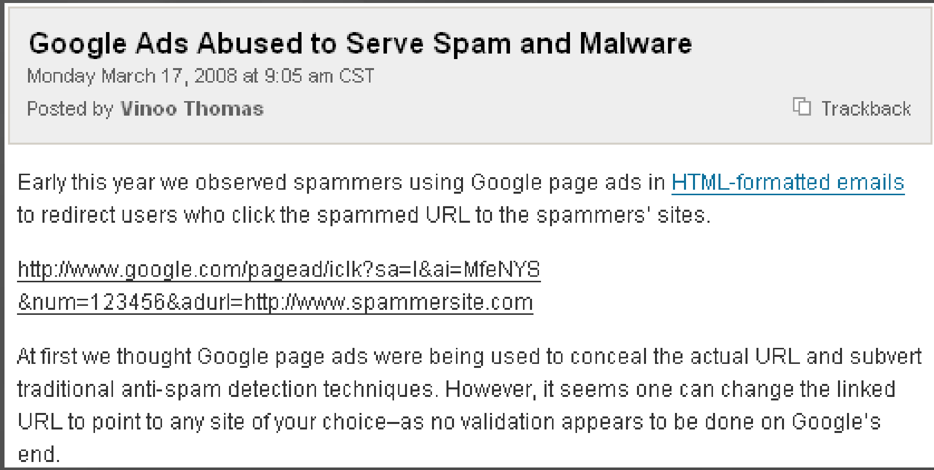
content-transfer-encoding: 7bit

```
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 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!



Google Ads Abused to Serve Spam and Malware

Monday March 17, 2008 at 9:05 am CST

Posted by **Vinoo Thomas**

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/iclk?sa=l&ai=MfeNYS
&num=123456&adurl=http://www.spammersite.com

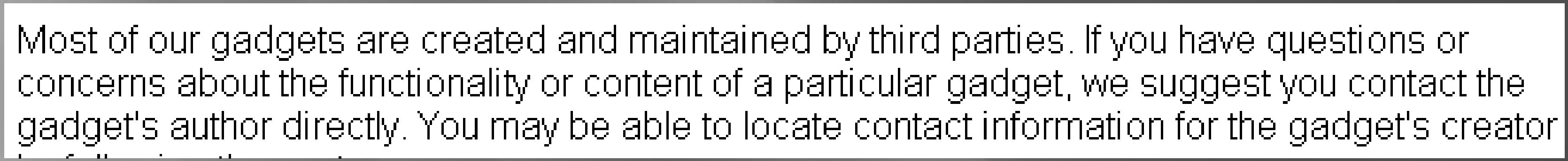
At first we thought Google page ads were being used to conceal the actual URL and subvert traditional anti-spam detection techniques. However, it seems one can change the linked URL to point to any site of your choice–as no validation appears to be done on Google's end.

Press Worthy Mentions

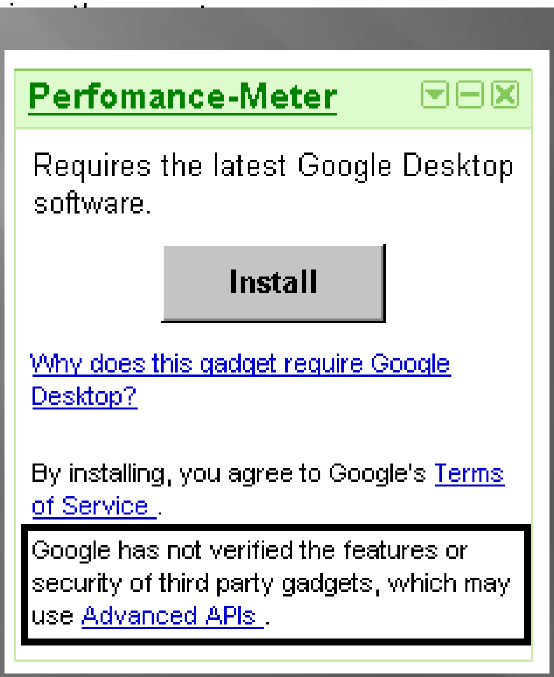
- The Google Desktop Vuln (May 31st, 2007) ‘Regarding security-flaw disclosure, Mr. Merrill says Google hasn’t provided much because consumers, its primary users to date, often aren’t tech-savvy enough to understand security bulletins and find them “distracting and confusing.” Also, because fixes Google 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

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

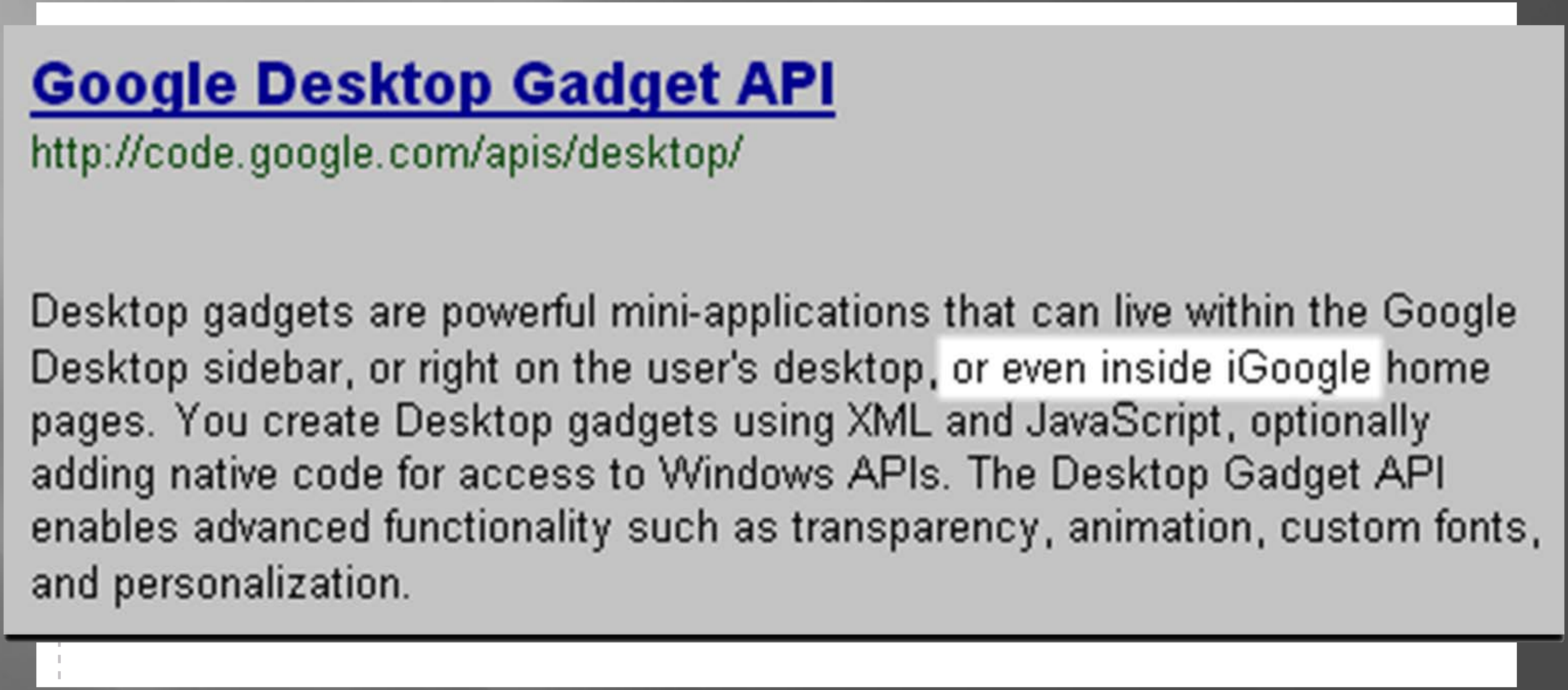
Requires the latest Google Desktop software.

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



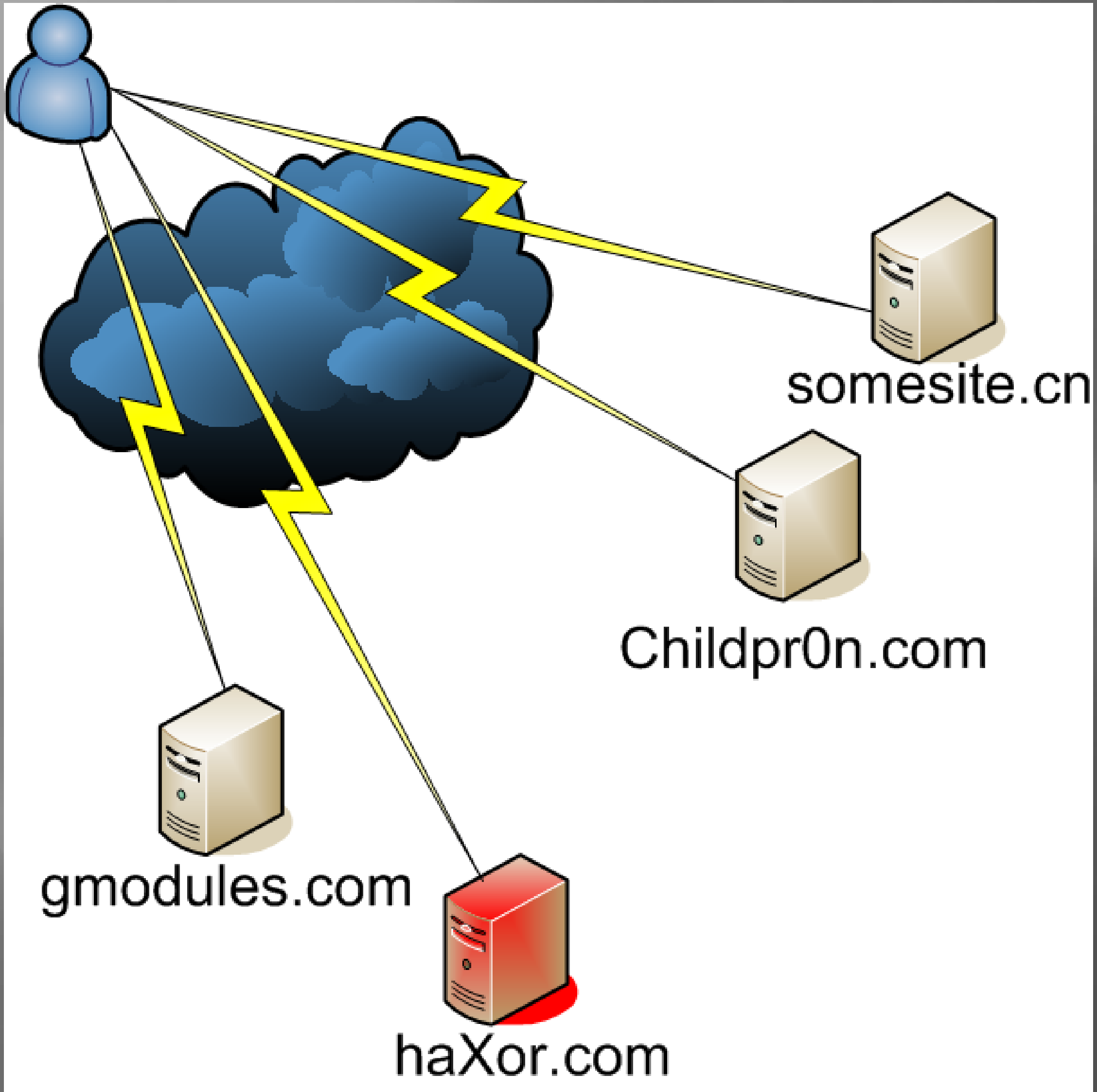
Google Desktop Gadget API

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://desktop.google.com/en/dev/advancedapi.html
http://code.google.com/more/#products-gadgets-gdgadgets

CSRF GADGET



1) Or SQL injection CSRF

2) Or RFI injection CSRF

3) Or Exponential (Xdomain) XSS worms

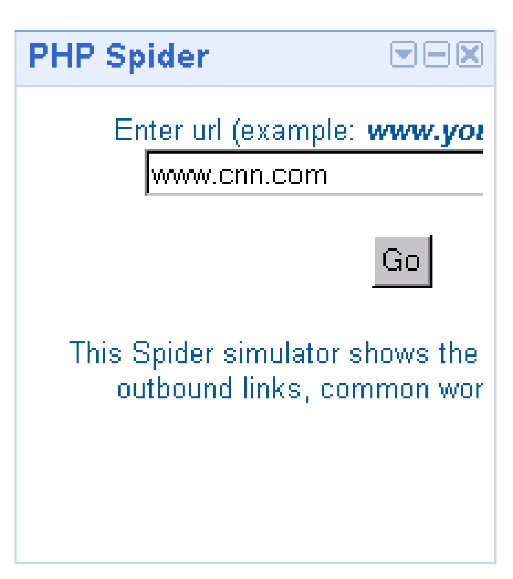
4) Etc... Etc...

Demo time…

SIMPLE PHP SPIDER

We fetch a PHP script within the Gadget

Configuration **Results**



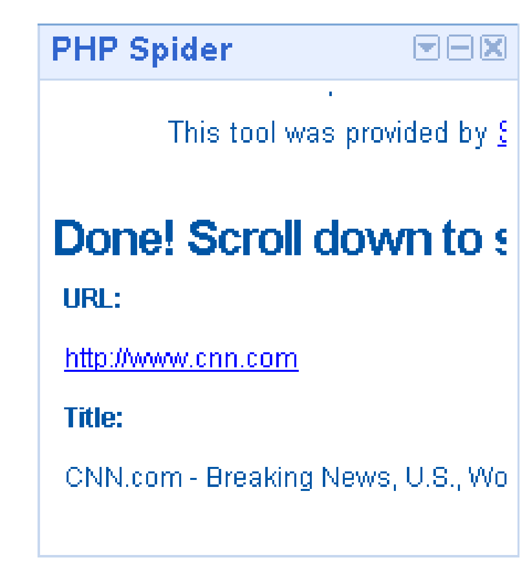
PHP Spider

Enter url (example: *www.you*

www.cnn.com

Go

This Spider simulator shows the outbound links, common wor



PHP Spider

This tool was provided by S

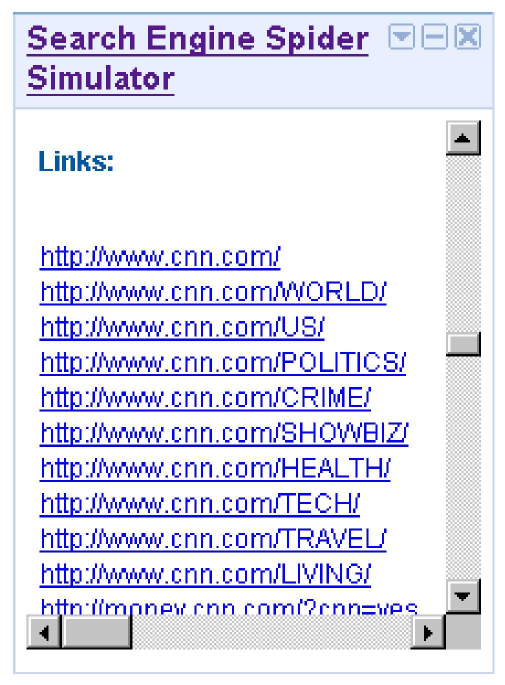
Done! Scroll down to s

URL:

http://www.cnn.com

Title:

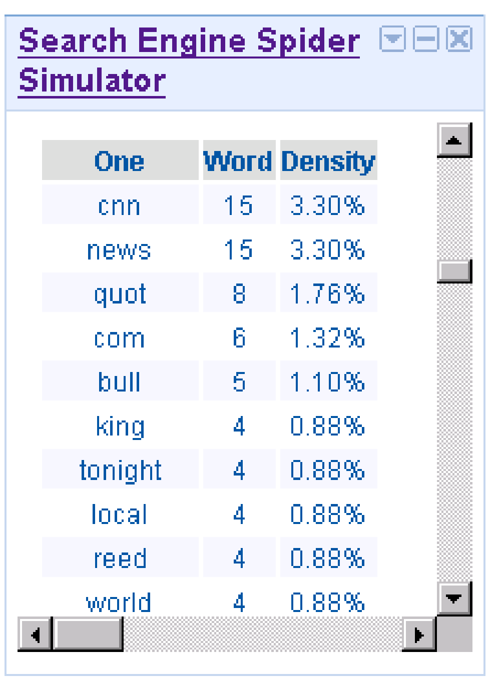
CNN.com - Breaking News, U.S., Wo



Search Engine Spider Simulator

Links:

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

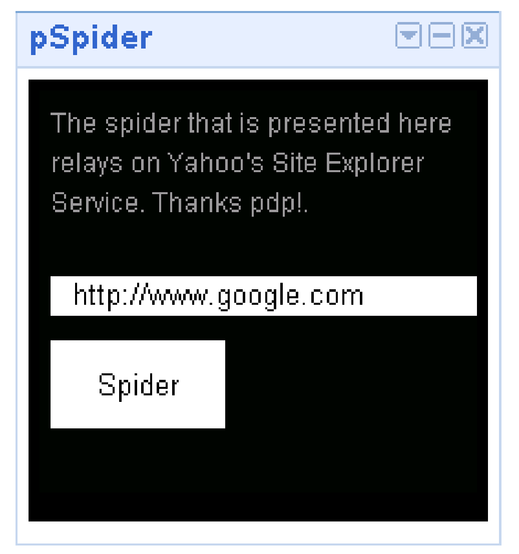


Search Engine Spider Simulator

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)

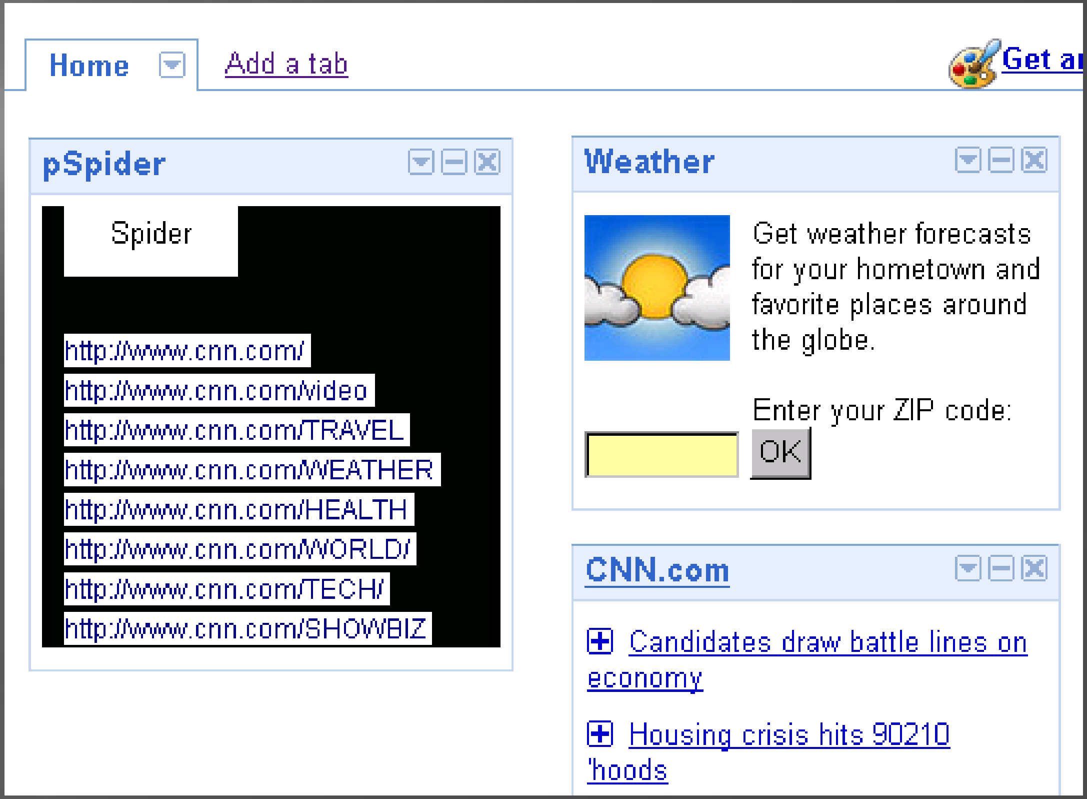
Configuration



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

http://www.google.com

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:

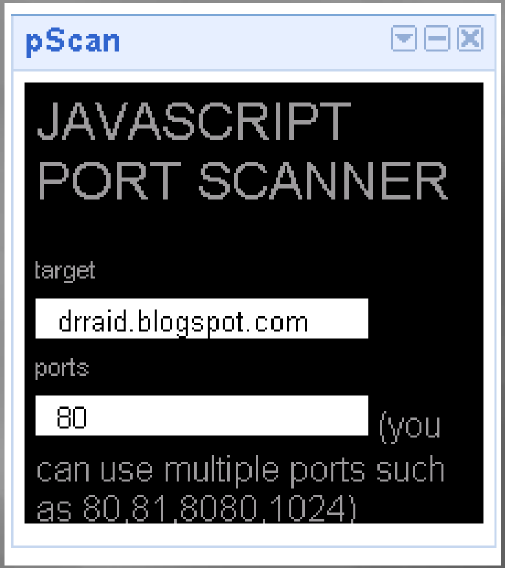
⊞ Candidates draw battle lines on economy

⊞ Housing crisis hits 90210 'hoods

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

JS PORT SCANNER GADGET

pScan Configuration



pScan

JAVASCRIPT
PORT SCANNER

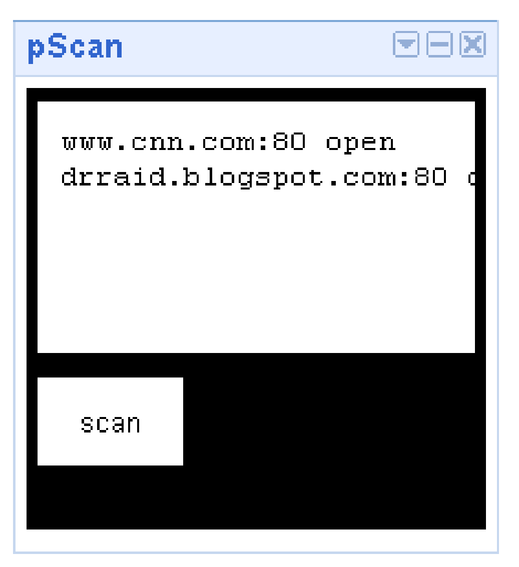
target

drraid.blogspot.com

ports

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

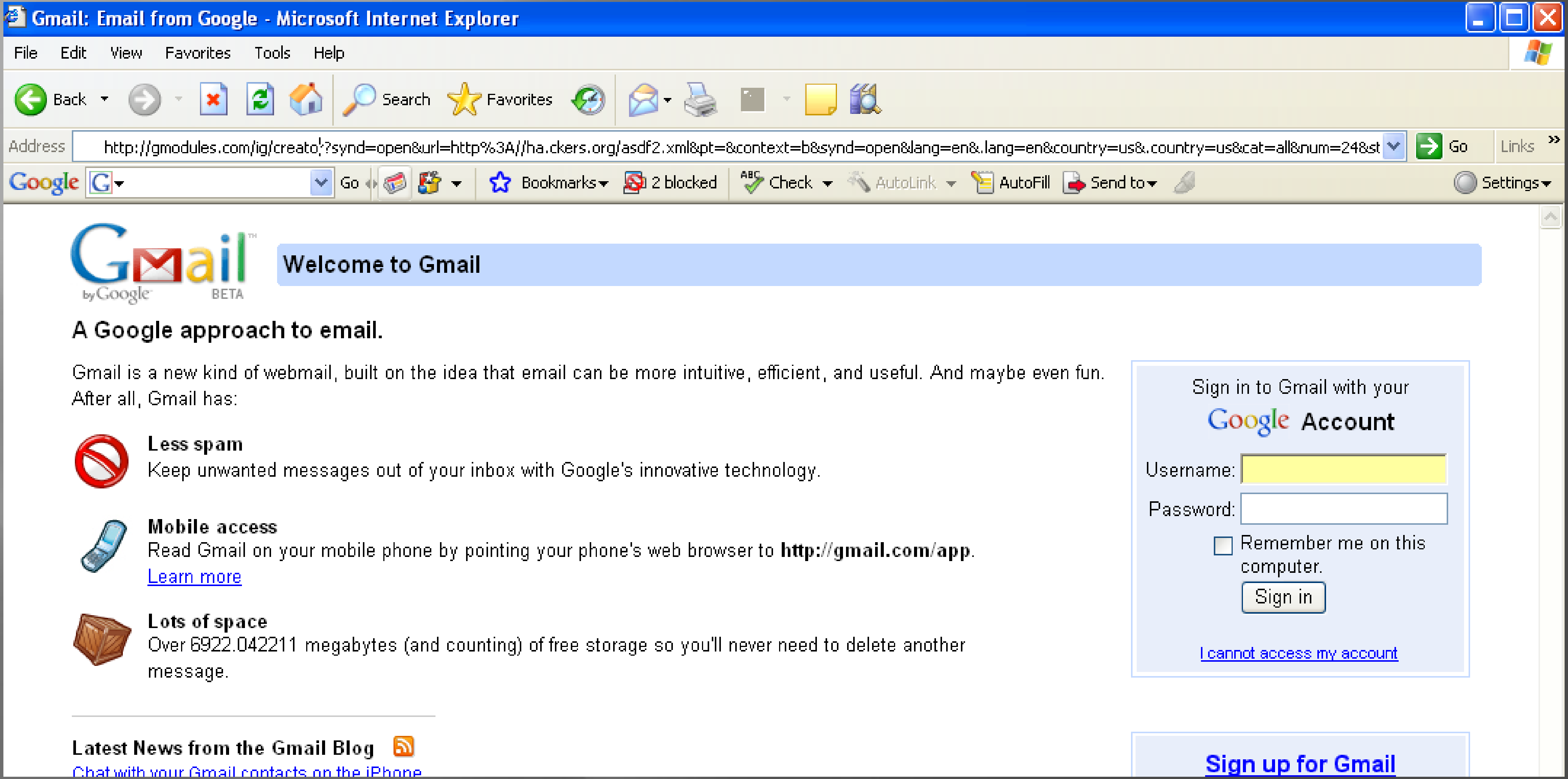
Results



pScan

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

PHISHING GADGET



http://gmodules.com/ig/creator?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

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.

Latest News from the Gmail Blog
Chat with your Gmail contacts on the iPhone

Sign in to Gmail with your Google Account

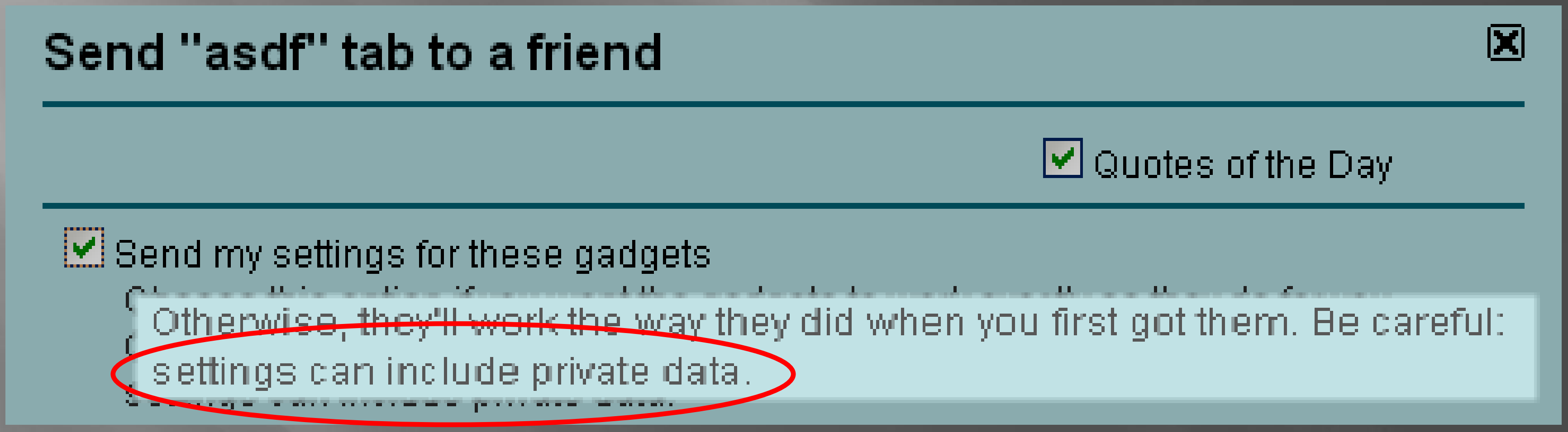
Username:
Password:
□ Remember me on this computer.

I cannot access my account

Sign up for Gmail

CROSS-GADGET ATTACKS

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



Send "asdf" tab to a friend

☑ Quotes of the Day

☑ Send my settings for these gadgets

Otherwise, they'll work the way they did when you first got them. Be careful: settings can include private data.

Demo time…

Referrers

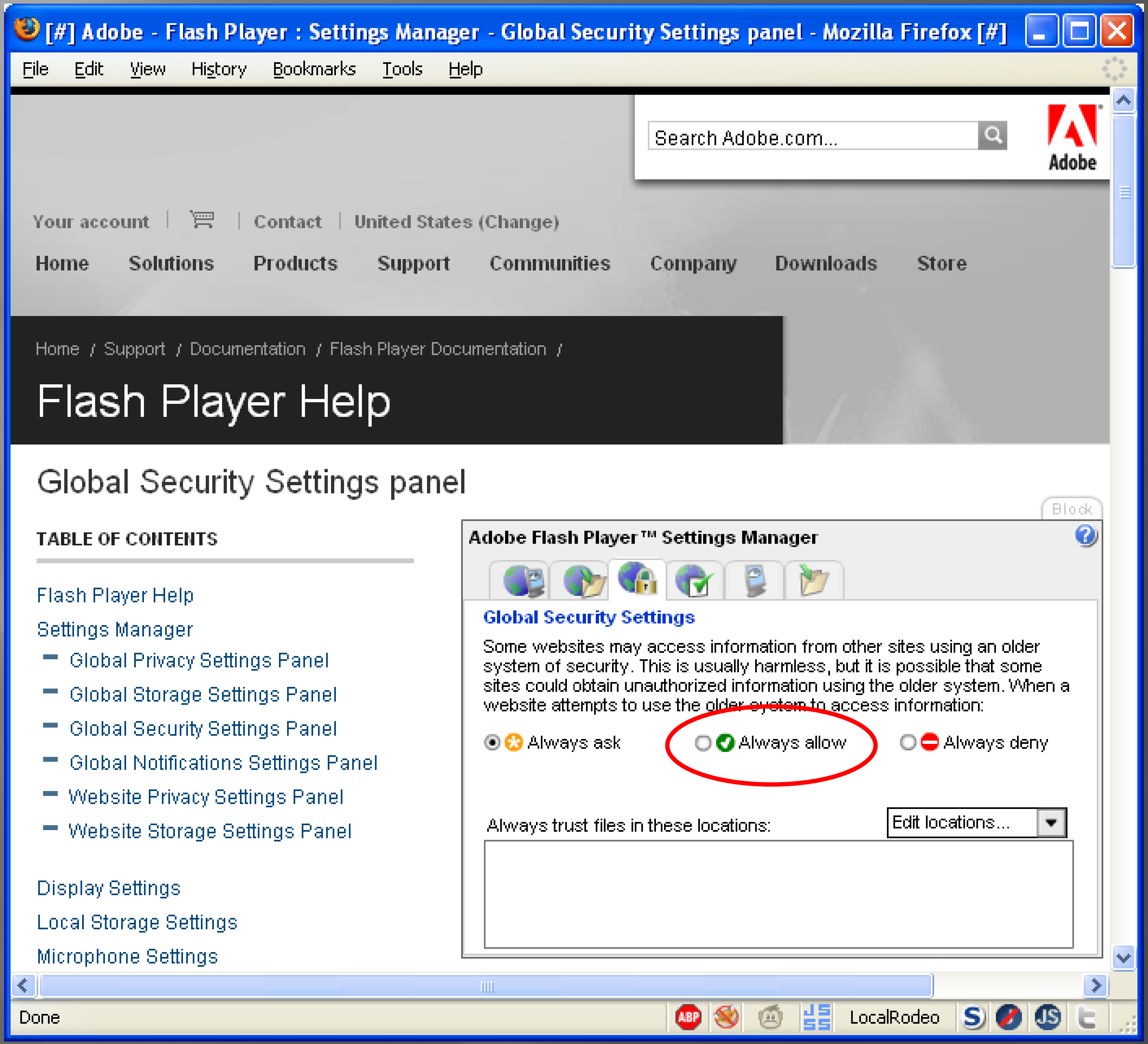
http://89.gmodules.com/ig/ifr?url=http://www3.sympatico.ca/mjdresser/Delicious.xml&nocache=0&up_username=wipeouter&up_tag=&up_count=15&upt_count=enum&up_images=0&upt_images=bool&lang=de&country=de&.lang=de&.country=de&synd=ig&mid=89&ifpctok=6968901372936289341&parent=http://www.google.de&extern_js=/extern_js/f/CgJlbhICdXMrMAo4ACw/8IKVf7DB5CY.js

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.

Clickjacking 101



[#] Adobe - Flash Player : Settings Manager - Global Security Settings panel - Mozilla Firefox [#]
File Edit View History Bookmarks Tools Help
Search Adobe.com...
Adobe
Your account | Contact | United States (Change)
Home Solutions Products Support Communities Company Downloads Store
Home / Support / Documentation / Flash Player Documentation /
Block
Done
LocalRodeo

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

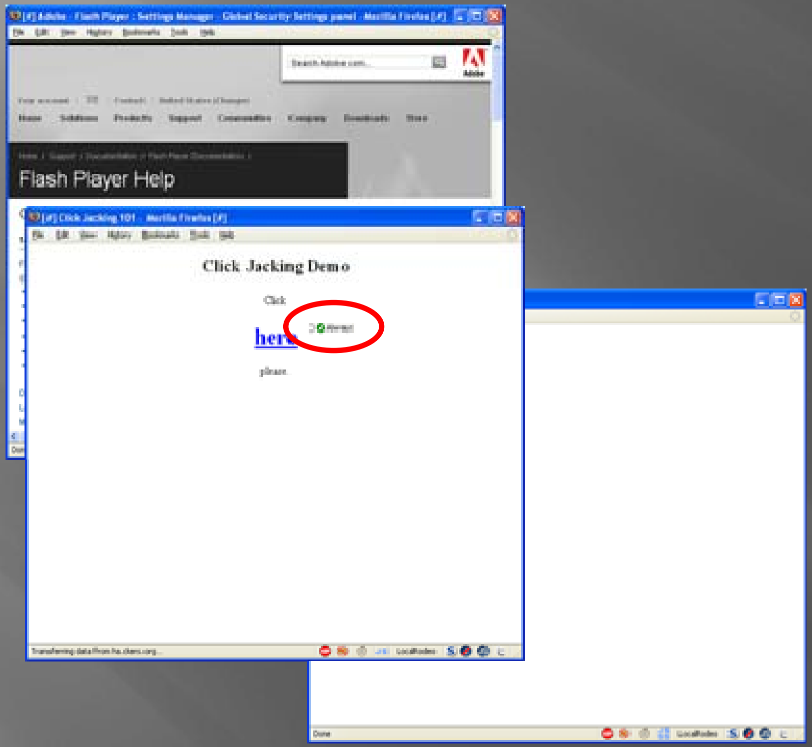
Global Security Settings

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



Click Jacking Demo

Click

here

please

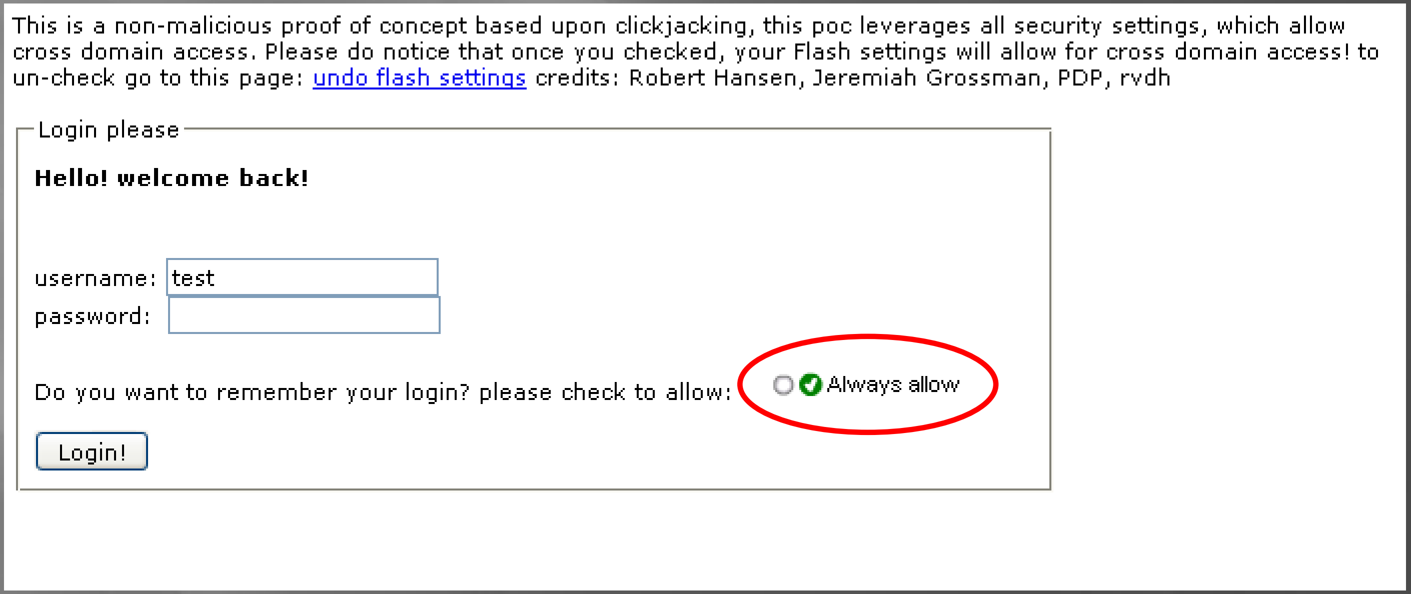
[#] Adobe - Flash Player : Settings Manager - Global Security Settings panel - Mozilla Firefox [#]
File Edit View History Bookmarks Tools Help
Search Adobe.com...
Adobe
Home Solutions Products Support Communities Company Downloads Store
Flash Player Help
[#] Click Jacking 101 - Mozilla Firefox [#]
File Edit View History Bookmarks Tools Help
Always
Transferring data from ha.ckers.org...
LocalRodeo
Done

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: undo flash settings credits: Robert Hansen, Jeremiah Grossman, PDP, rvdh

Login please

Hello! welcome back!

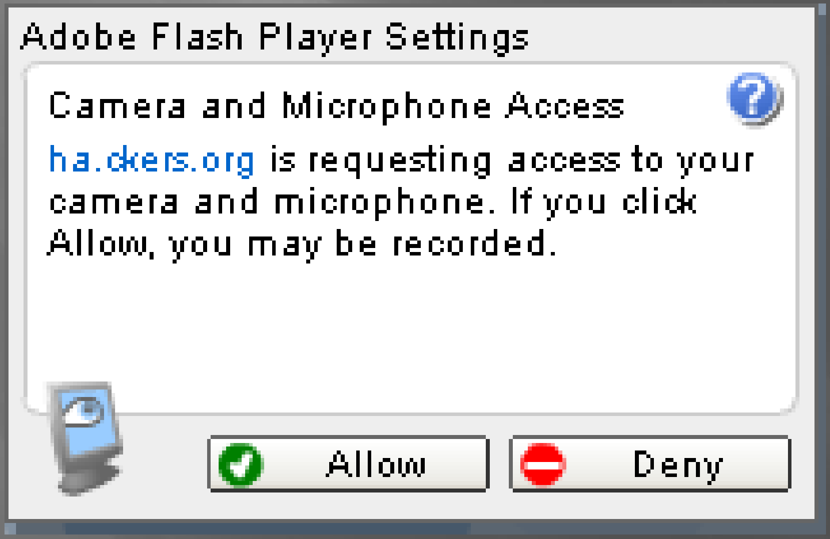
username: test

password:

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

Clickjacking 101

- Typical security dialog…



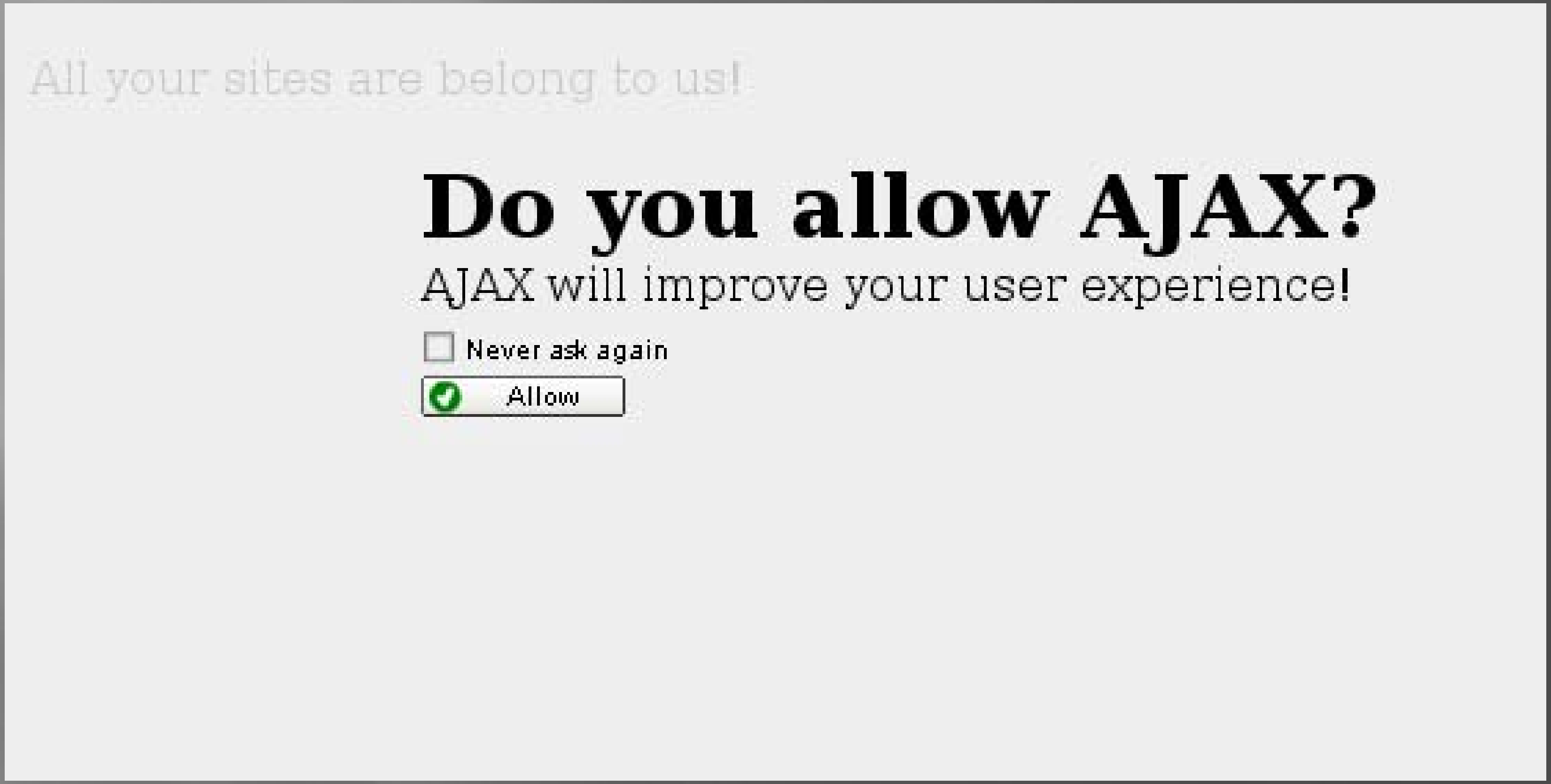
Adobe Flash Player Settings

Camera and Microphone Access

ha.ckers.org is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Clickjacking 101

- PDP's version…



All your sites are belong to us!

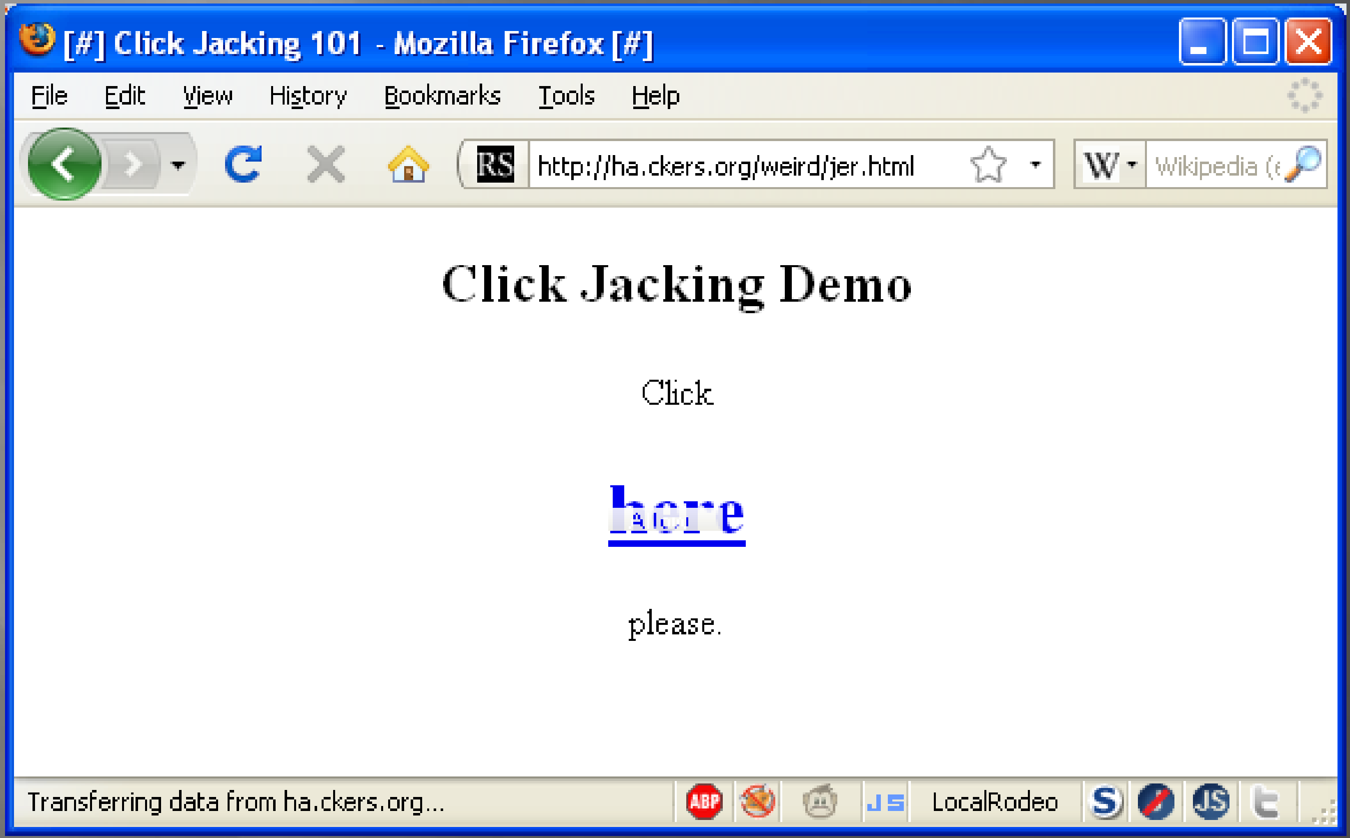
Do you allow AJAX?

AJAX will improve your user experience!

□ Never ask again

Clickjacking 101

- Demo time…



[#] Click Jacking 101 - Mozilla Firefox [#]

http://ha.ckers.org/weird/jer.html

Click Jacking Demo

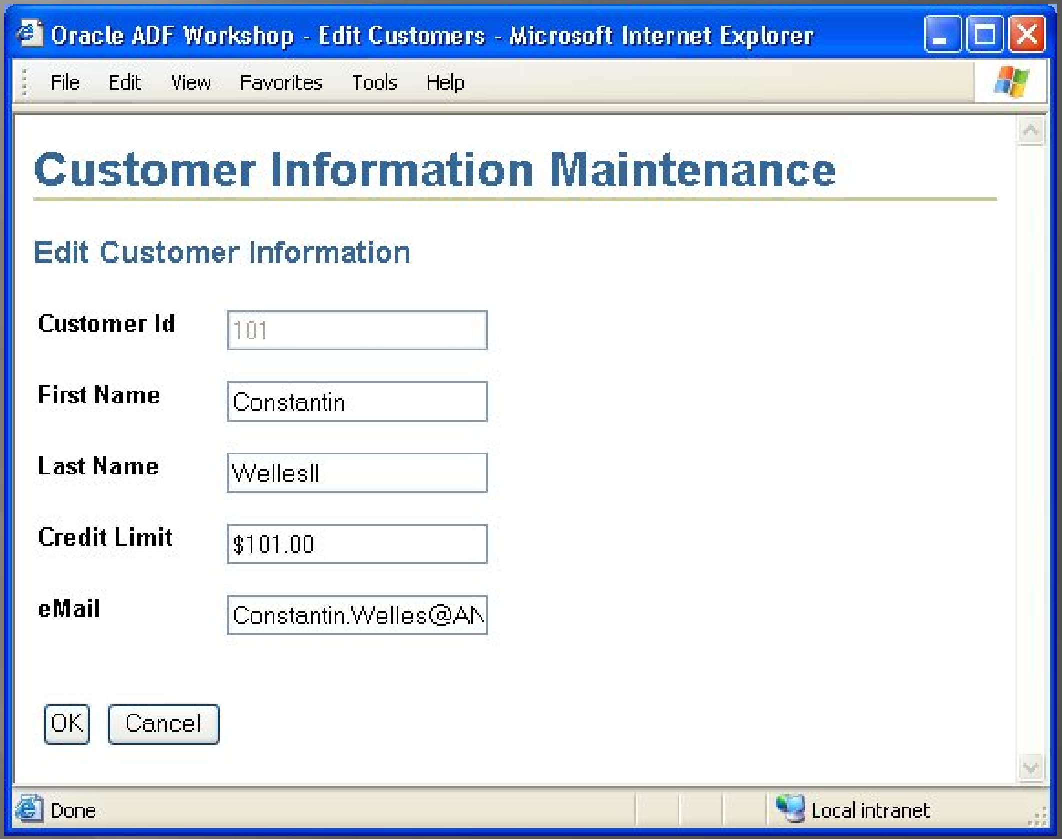
Click

here

please.

Transferring data from ha.ckers.org...

Oracle Webforms



Oracle ADF Workshop - Edit Customers - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help

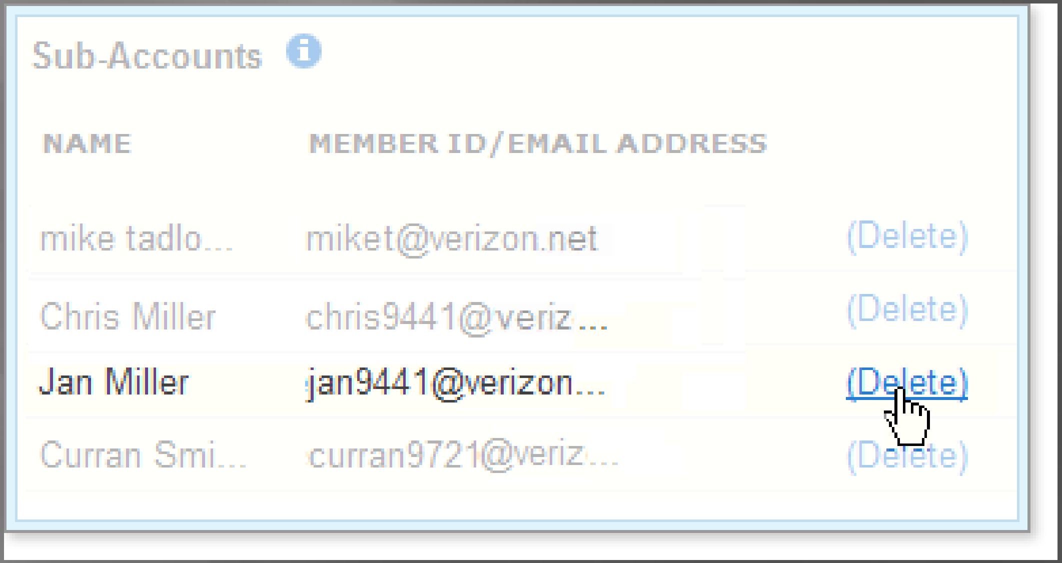
Customer Information Maintenance

Edit Customer Information

Customer Id	101
First Name	Constantin
Last Name	WellesII
Credit Limit	$101.00
eMail	Constantin.Welles@AN

OK
Cancel
Done
Local intranet

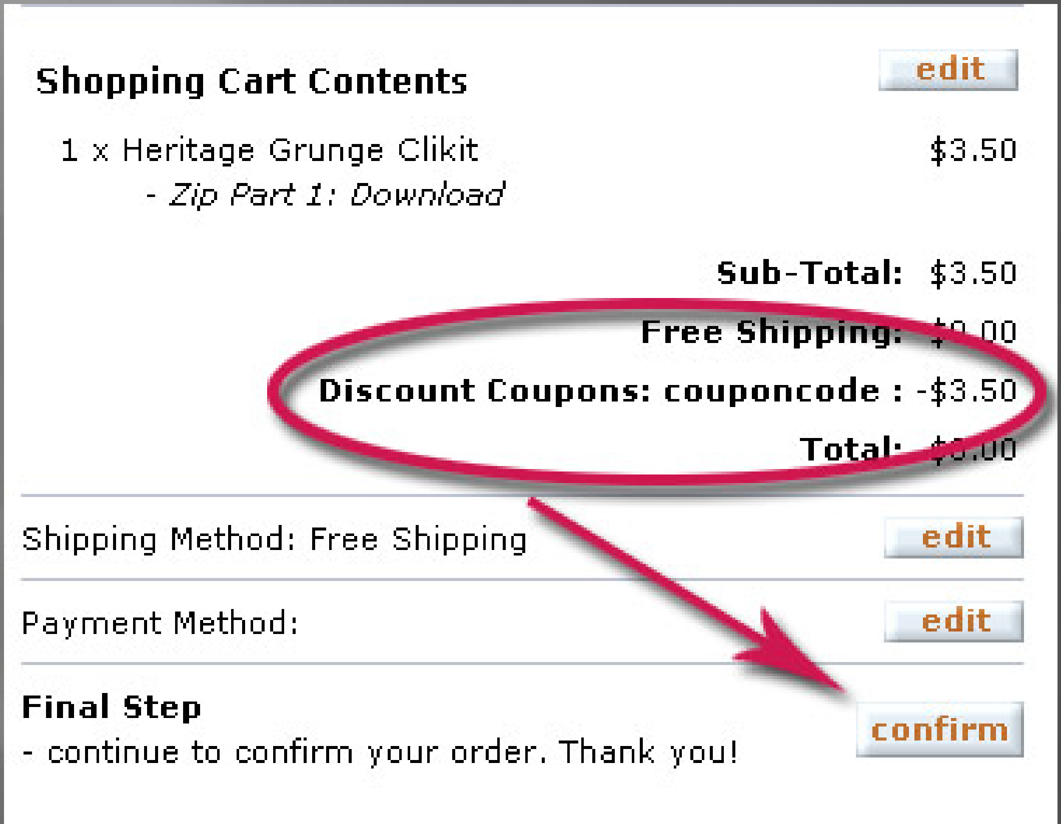
Delete User Accounts



Sub-Accounts

NAME	MEMBER ID/EMAIL ADDRESS	
mike tadlo...	miket@verizon.net	(Delete)
Chris Miller	chris9441@veriz...	(Delete)
Jan Miller	jan9441@verizon...	(Delete)
Curran Smi...	curran9721@veriz...	(Delete)

Auto-purchase



Shopping Cart Contents

1 x Heritage Grunge Clikit — $3.50
- Zip Part 1: Download

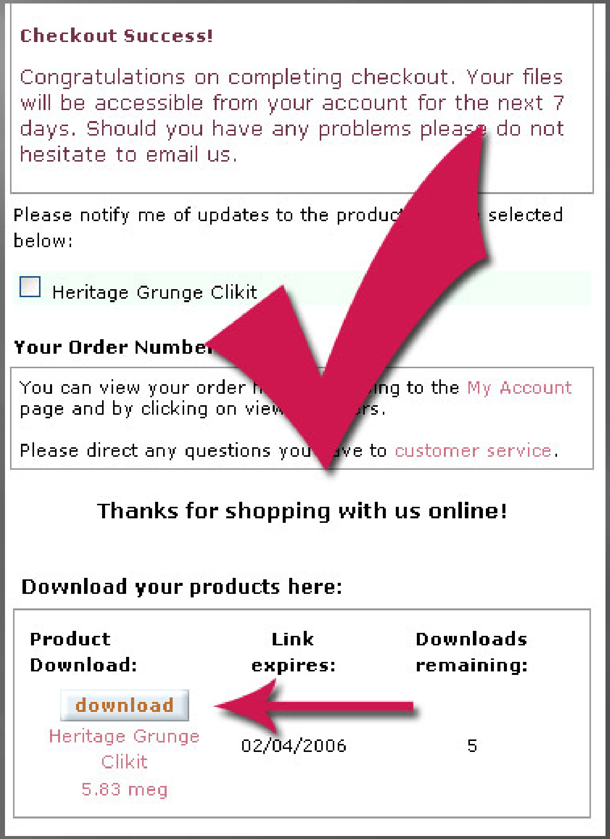
Sub-Total: $3.50
Free Shipping: $0.00
Discount Coupons: couponcode : -$3.50
Total: $0.00

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 produc selected below:

□ Heritage Grunge Clikit

Your Order Numbe

You can view your order h ing to the My Account page and by clicking on view rs.

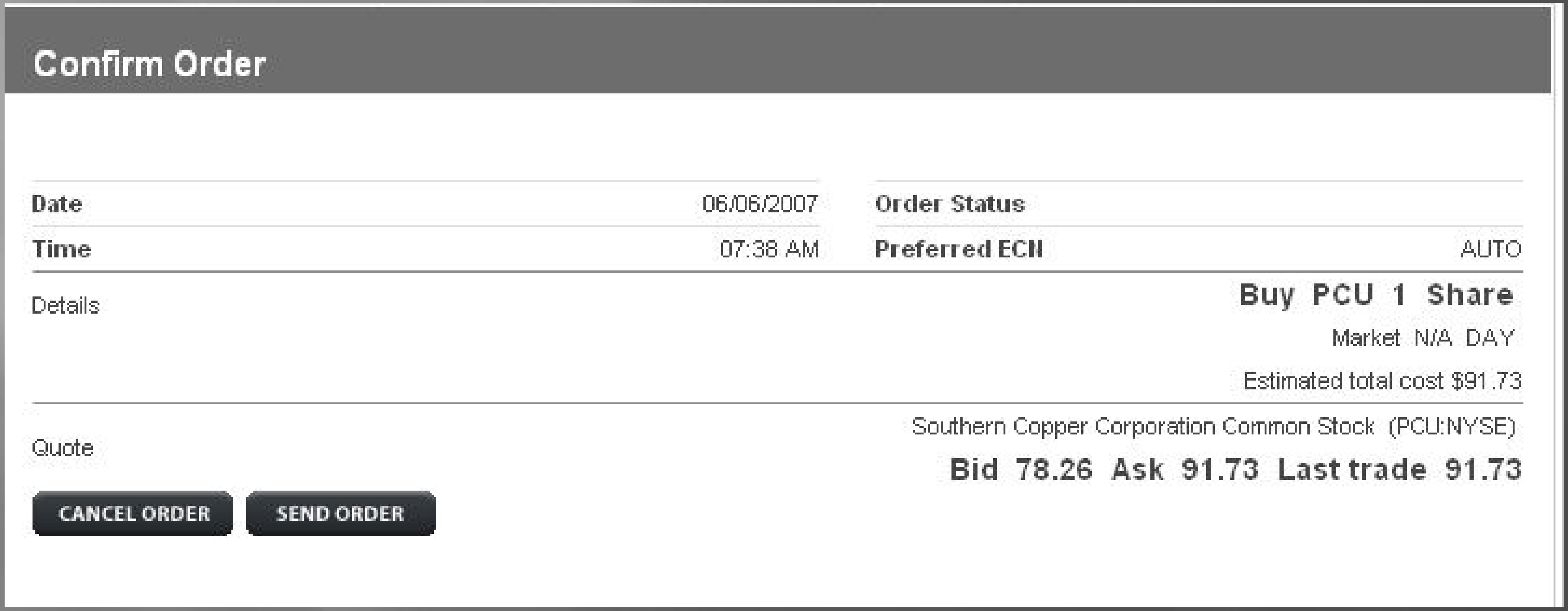
Please direct any questions you ve to customer service.

Thanks for shopping with us online!

Download your products here:

Product Download:	Link expires:	Downloads remaining:
download Heritage Grunge Clikit 5.83 meg	02/04/2006	5

Buy stocks



Confirm Order

Date	06/06/2007	**Order Status**	
Time	07:38 AM	**Preferred ECN**	AUTO

Details

Buy PCU 1 Share

Market N/A DAY

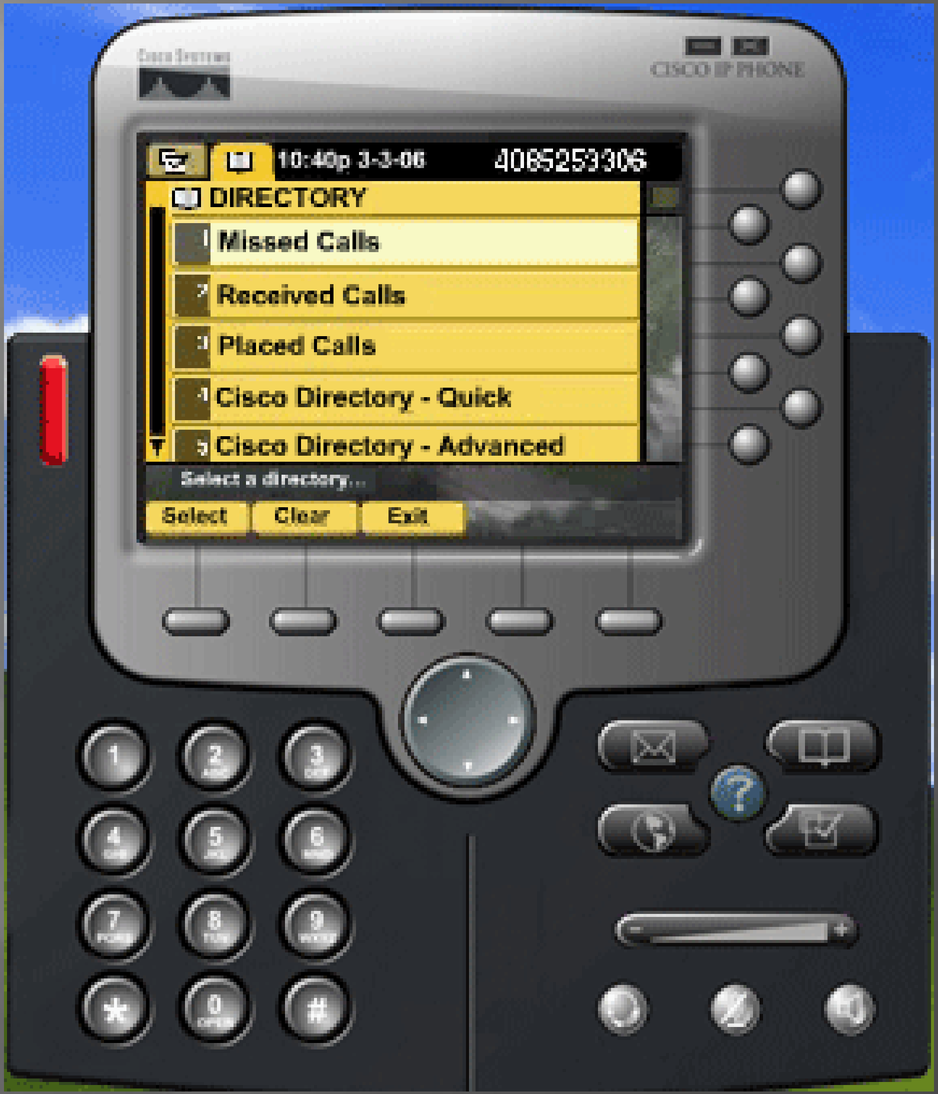
Estimated total cost $91.73

Quote

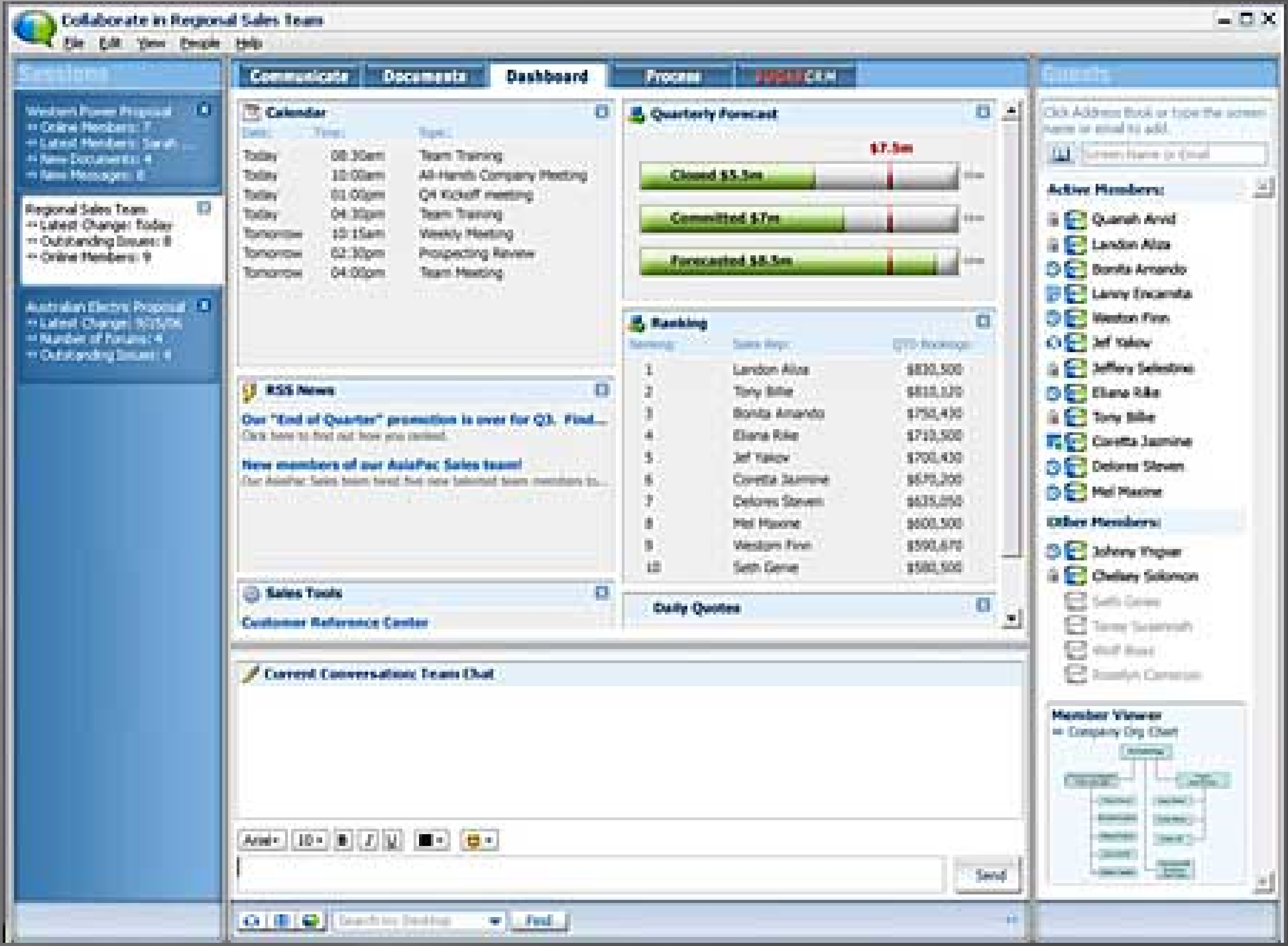
Southern Copper Corporation Common Stock (PCU:NYSE)

Bid 78.26 Ask 91.73 Last trade 91.73

Auto-call


CISCO SYSTEMS
CISCO IP PHONE
10:40p 3-3-06
4085253306
DIRECTORY
1 Missed Calls
2 Received Calls
3 Placed Calls
4 Cisco Directory - Quick
5 Cisco Directory - Advanced
Select a directory...
Select
Clear
Exit

Webex/Meetingplace



Western Power Proposal
-- Online Members: 7
-- Latest Members: Sarah ...
-- New Documents: 4
-- New Messages: 8

Regional Sales Team
-- Latest Change: Today
-- Outstanding Issues: 8
-- Online Members: 9

Australian Electric Proposal
-- Latest Change: 9/15/06
-- Number of Forums: 4
-- Outstanding Issues: 4

Calendar

Date:	Time:	Type:
Today	08:30am	Team Training
Today	10:00am	All-Hands Company Meeting
Today	01:00pm	Q4 Kickoff meeting
Today	04:30pm	Team Training
Tomorrow	10:15am	Weekly Meeting
Tomorrow	02:30pm	Prospecting Review
Tomorrow	04:00pm	Team Meeting

RSS News

Our "End of Quarter" promotion is over for Q3. Find...
Click here to find out how you ranked.

New members of our AsiaPac Sales team!
Our AsiaPac Sales team hired five new talented team members to...

Sales Tools

Customer Reference Center

Quarterly Forecast

$7.5m
Closed $5.5m
Committed $7m
Forecasted $8.5m

Ranking

Ranking	Sales Rep	QTD Bookings
1	Landon Aliza	$830,500
2	Tony Bille	$810,120
3	Bonita Amando	$750,430
4	Eliana Rike	$710,500
5	Jef Yakov	$700,430
6	Coretta Jazmine	$670,200
7	Delores Steven	$625,050
8	Mel Maxine	$600,500
9	Weston Finn	$590,670
10	Seth Gene	$580,500

Daily Quotes

Current Conversation: Team Chat

Click Address Book or type the screen name or email to add.

Screen Name or Email

Active Members:

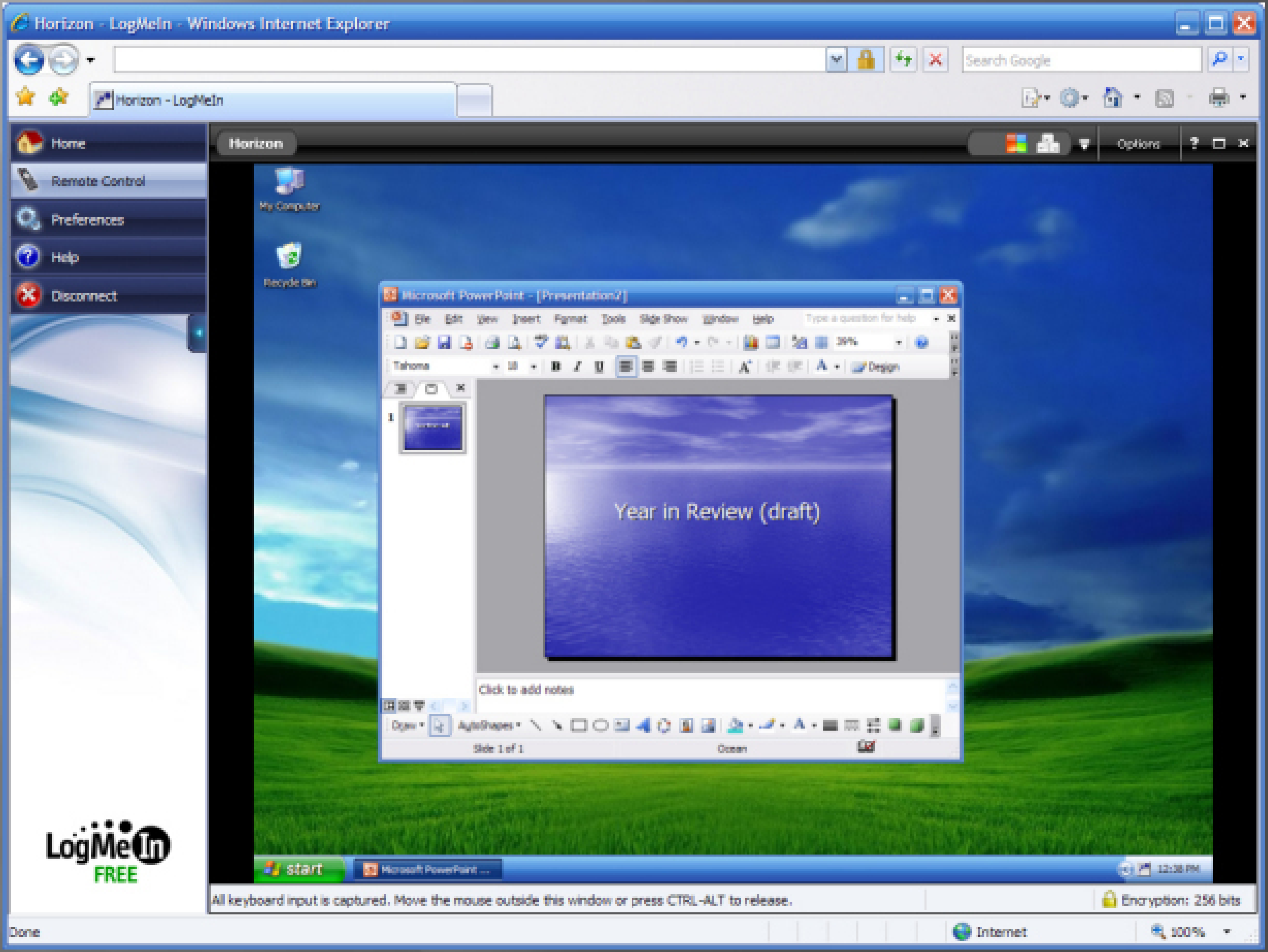
Quanah Arvid
Landon Aliza
Bonita Amando
Lanny Encarnita
Weston Finn
Jef Yakov
Jeffery Selestine
Eliana Rike
Tony Bille
Coretta Jazmine
Delores Steven
Mel Maxine

Other Members:

Johnny Yngvar
Chelsey Solomon
Seth Gene
Toney Susannah
Wolf Russ
Roselyn Cameron

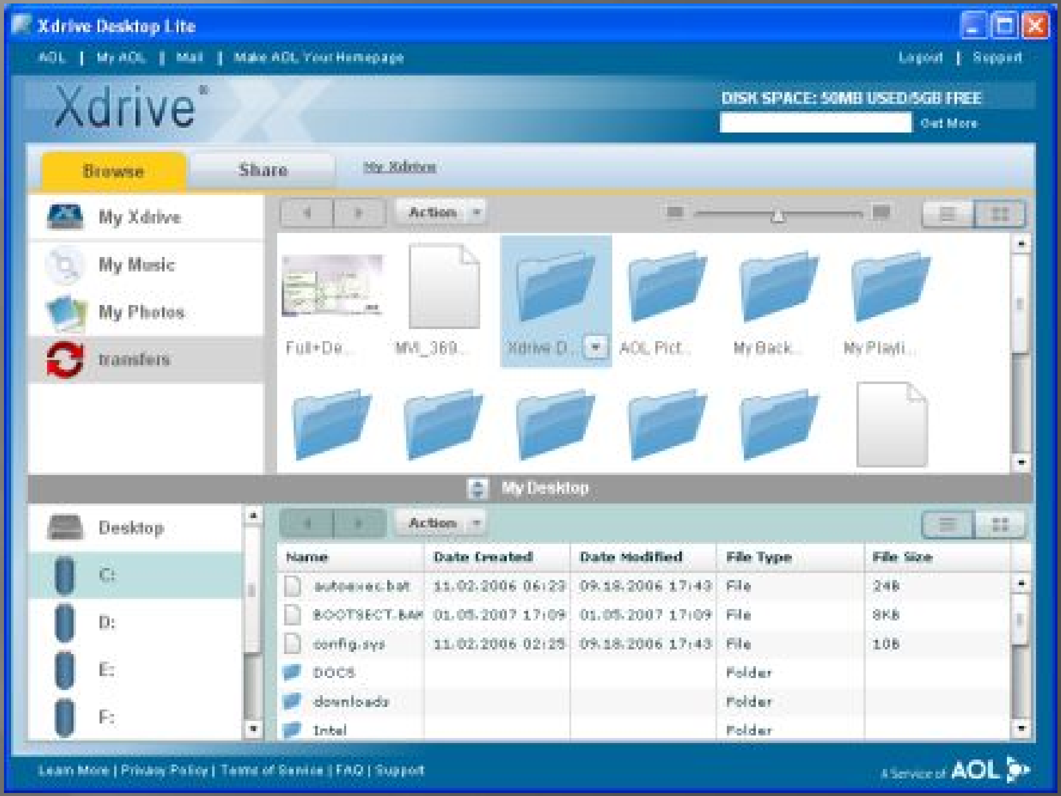
Member Viewer
-- Company Org Chart

Logmein



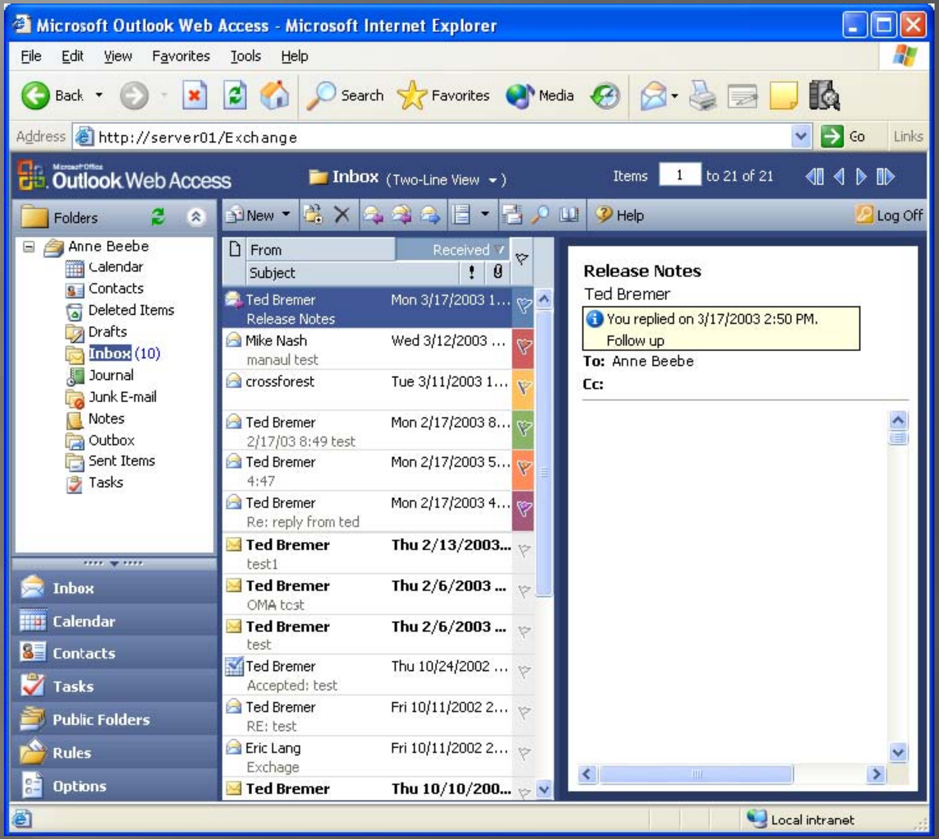
All keyboard input is captured. Move the mouse outside this window or press CTRL-ALT to release.

XDrive



Name	Date Created	Date Modified	File Type	File Size
autoexec.bat	11.02.2006 06:23	09.18.2006 17:43	File	24B
BOOTSECT.BAK	01.05.2007 17:09	01.05.2007 17:09	File	8KB
config.sys	11.02.2006 02:25	09.18.2006 17:43	File	10B
DOCS			Folder	
downloads			Folder	
Intel			Folder	

OWA



Address: http://server01/Exchange

Inbox (Two-Line View) Items 1 to 21 of 21

From Subject	Received
Ted Bremer Release Notes	Mon 3/17/2003 1…
Mike Nash manaul test	Wed 3/12/2003 …
crossforest	Tue 3/11/2003 1…
Ted Bremer 2/17/03 8:49 test	Mon 2/17/2003 8…
Ted Bremer 4:47	Mon 2/17/2003 5…
Ted Bremer Re: reply from ted	Mon 2/17/2003 4…
Ted Bremer test1	**Thu 2/13/2003…**
Ted Bremer OMA test	**Thu 2/6/2003 …**
Ted Bremer test	**Thu 2/6/2003 …**
Ted Bremer Accepted: test	Thu 10/24/2002 …
Ted Bremer RE: test	Fri 10/11/2002 2…
Eric Lang Exchage	Fri 10/11/2002 2…
Ted Bremer	**Thu 10/10/200…**

Release Notes

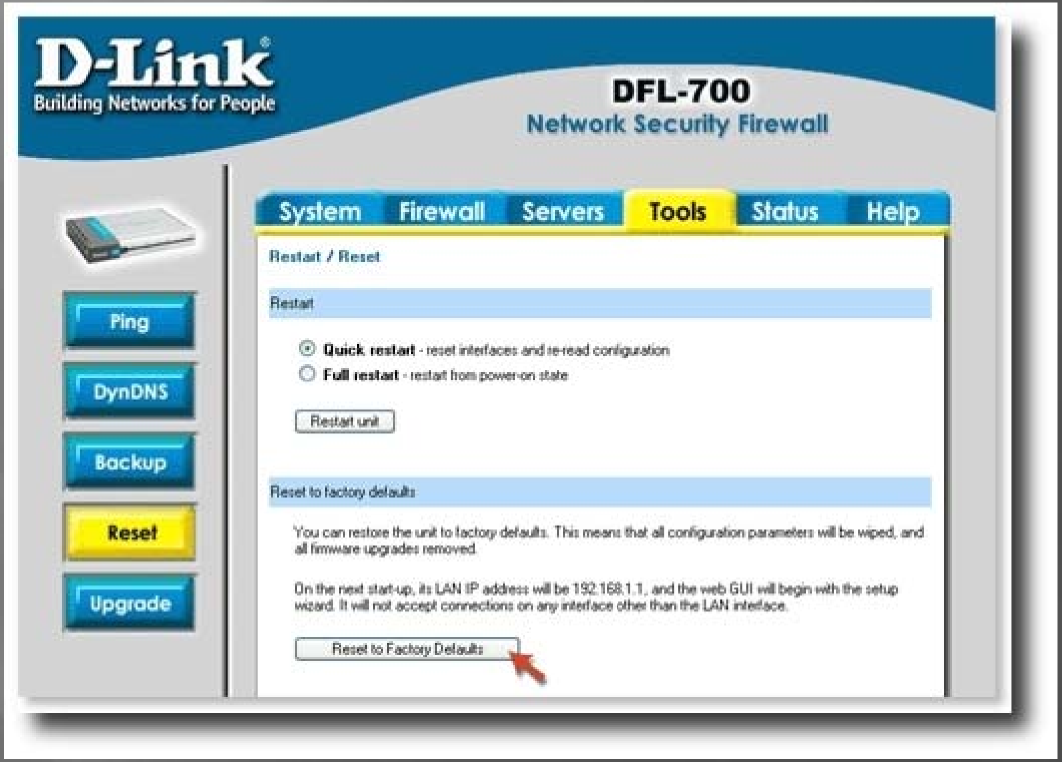
Ted Bremer

You replied on 3/17/2003 2:50 PM.
Follow up

To: Anne Beebe

Cc:

Router Reset



Restart / Reset

Restart

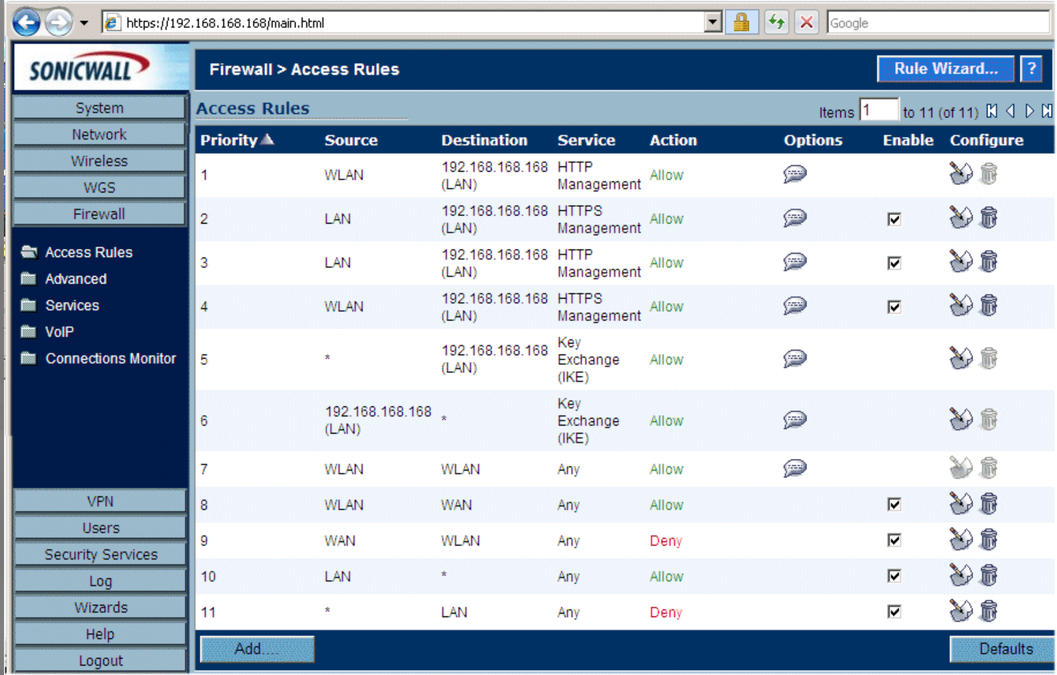
● **Quick restart** - reset interfaces and re-read configuration
○ **Full restart** - restart from power-on state

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 start-up, 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.

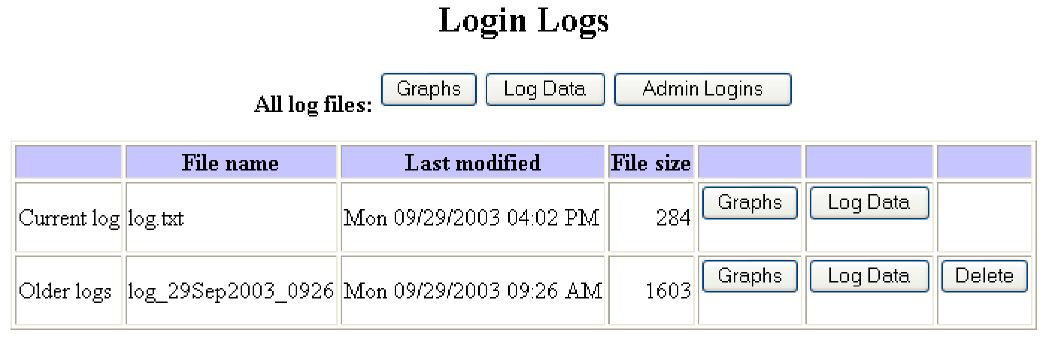
Delete Firewall Rules



Access Rules

Priority ▲	Source	Destination	Service	Action	Options	Enable	Configure
1	WLAN	192.168.168.168 (LAN)	HTTP Management	Allow	💬		
2	LAN	192.168.168.168 (LAN)	HTTPS Management	Allow	💬	☑	
3	LAN	192.168.168.168 (LAN)	HTTP Management	Allow	💬	☑	
4	WLAN	192.168.168.168 (LAN)	HTTPS Management	Allow	💬	☑	
5	*	192.168.168.168 (LAN)	Key Exchange (IKE)	Allow	💬		
6	192.168.168.168 (LAN)	*	Key Exchange (IKE)	Allow	💬		
7	WLAN	WLAN	Any	Allow	💬		
8	WLAN	WAN	Any	Allow		☑	
9	WAN	WLAN	Any	Deny		☑	
10	LAN	*	Any	Allow		☑	
11	*	LAN	Any	Deny		☑	

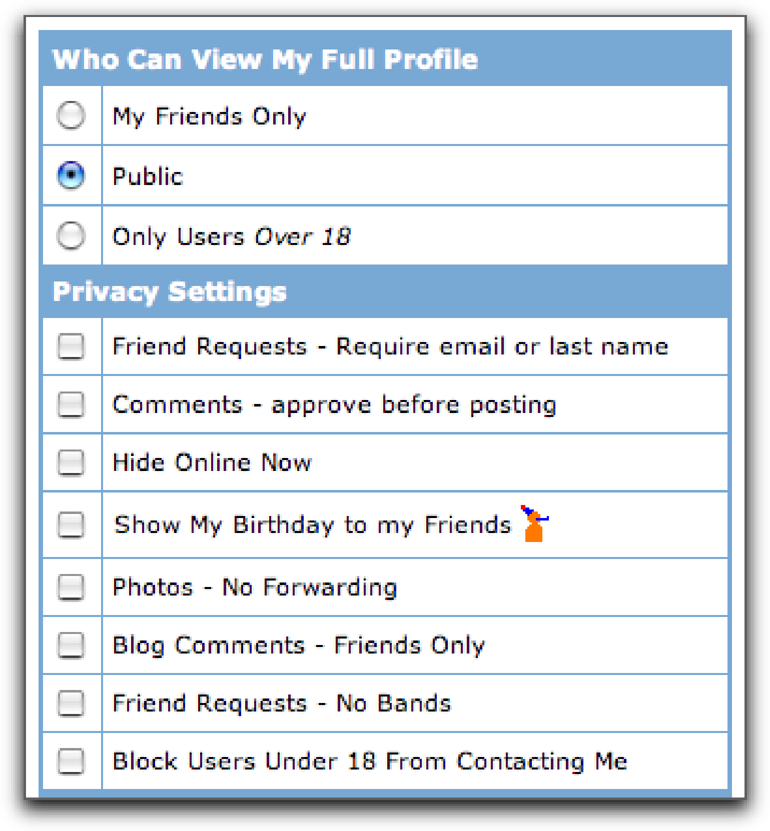
Delete Logs



Login Logs

	File name	Last modified	File size			
Current log	log.txt	Mon 09/29/2003 04:02 PM	284	Graphs	Log Data	
Older logs	log_29Sep2003_0926	Mon 09/29/2003 09:26 AM	1603	Graphs	Log Data	Delete

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

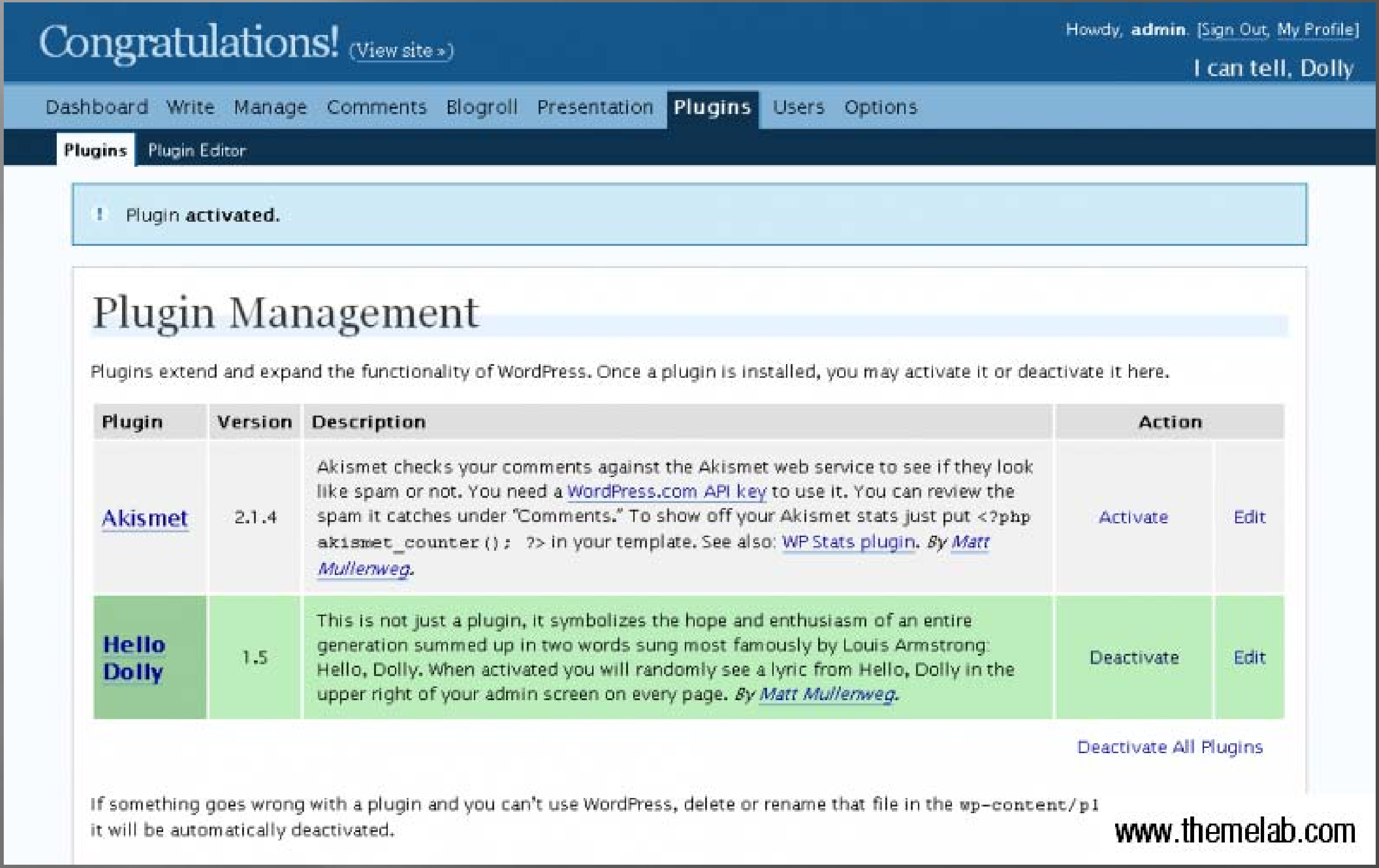
□ Photos - No Forwarding

□ Blog Comments - Friends Only

□ Friend Requests - No Bands

□ Block Users Under 18 From Contacting Me

Deactivate Wordpress Plugins


Congratulations! (View site »)
Howdy, admin. [Sign Out, My Profile]
I can tell, Dolly
Dashboard Write Manage Comments Blogroll Presentation Plugins Users Options
Plugins Plugin Editor

Plugin **activated.**

Plugin Management

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

Plugin	Version	Description	Action	
Akismet	2.1.4	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 `<?php akismet_counter(); ?>` in your template. See also: WP Stats plugin. *By Matt Mullenweg.*	Activate	Edit
Hello Dolly	1.5	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.*	Deactivate	Edit

Deactivate All Plugins

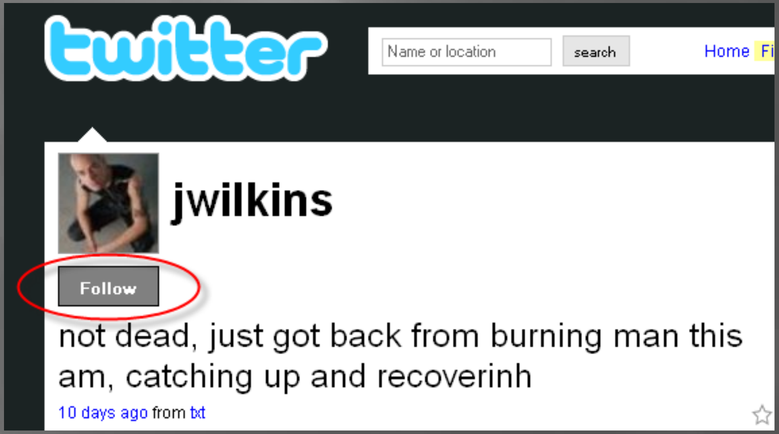
If something goes wrong with a plugin and you can't use WordPress, delete or rename that file in the `wp-content/pl`
it will be automatically deactivated.

www.themelab.com

Digg

- Demo time…

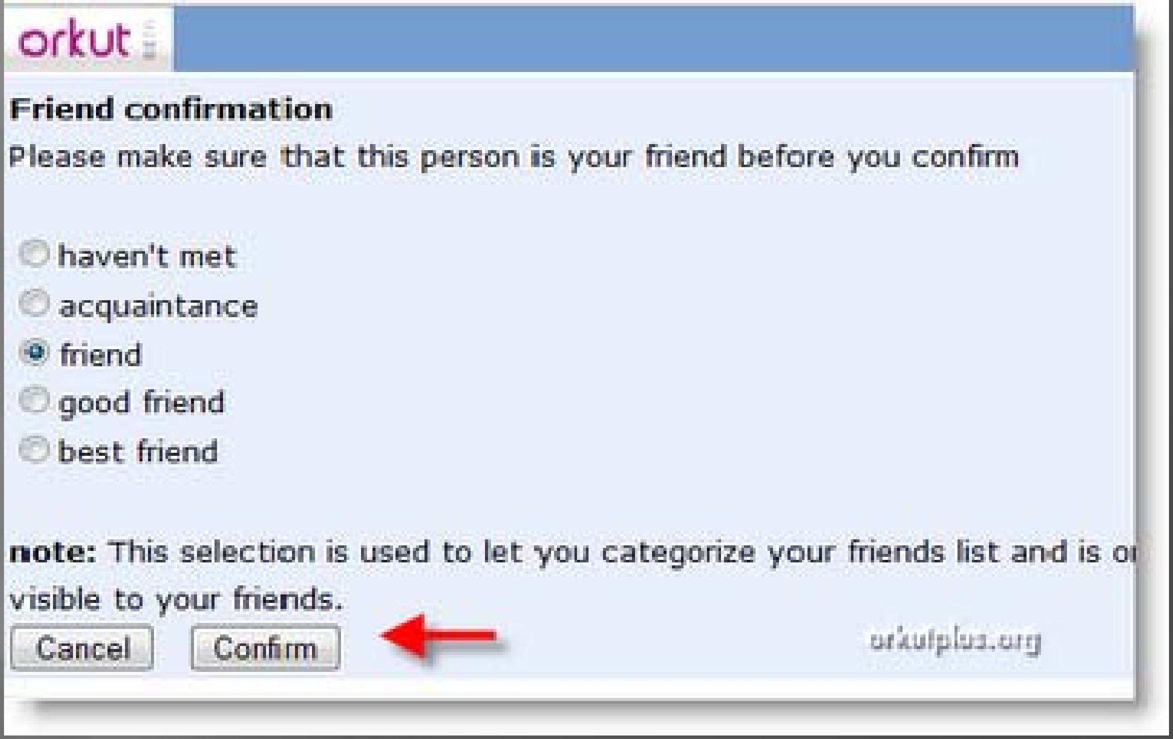
Twitter



not dead, just got back from burning man this am, catching up and recoverinh

10 days ago from txt

Add Friends on Orkut



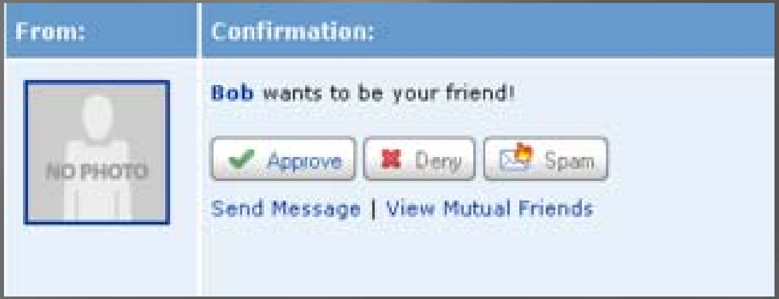
Friend confirmation

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

○ haven't met
○ acquaintance
● friend
○ good friend
○ best friend

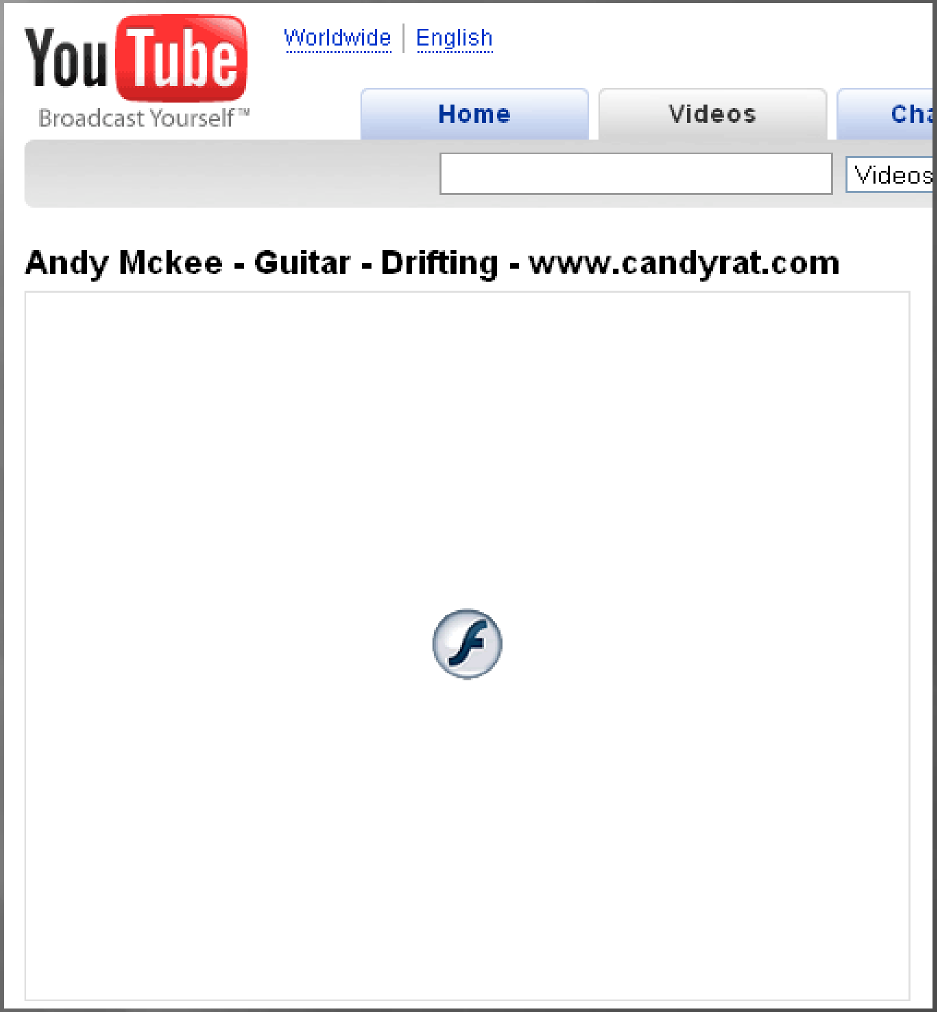
note: This selection is used to let you categorize your friends list and is o visible to your friends.

MySpace



Bob wants to be your friend!

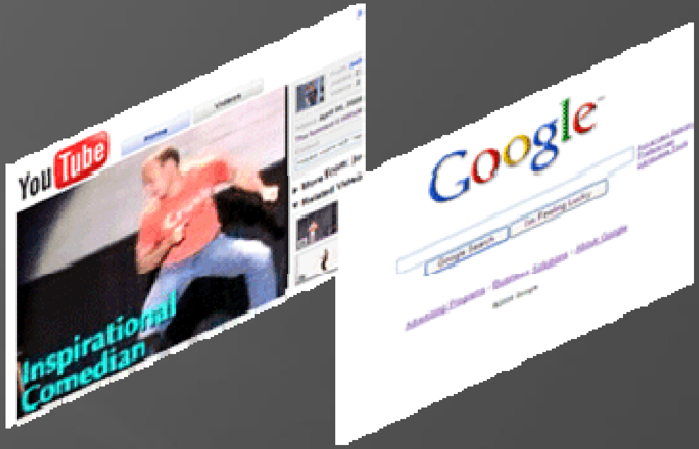
Flashblock

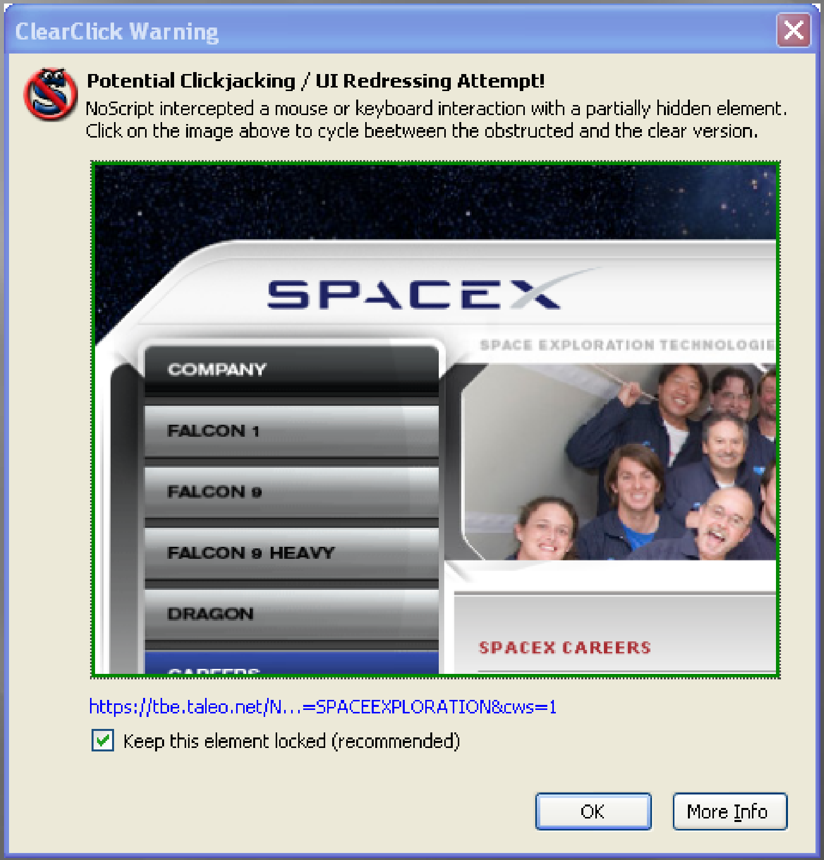


Andy Mckee - Guitar - Drifting - www.candyrat.com

Clickjacking 101

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





ClearClick Warning

Potential Clickjacking / UI Redressing Attempt!

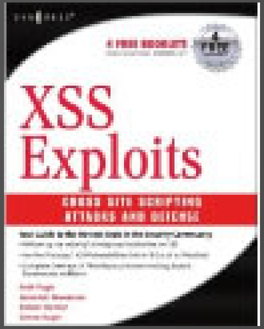
NoScript intercepted a mouse or keyboard interaction with a partially hidden element. Click on the image above to cycle beetween the obstructed and the clear version.

https://tbe.taleo.net/N...=SPACEEXPLORATION&cws=1

☑ Keep this element locked (recommended)

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



XSS Exploits

CROSS SITE SCRIPTING ATTACKS AND DEFENSE