I've Been Hacked, Now What?

Beth Tucker Long

Who am I?

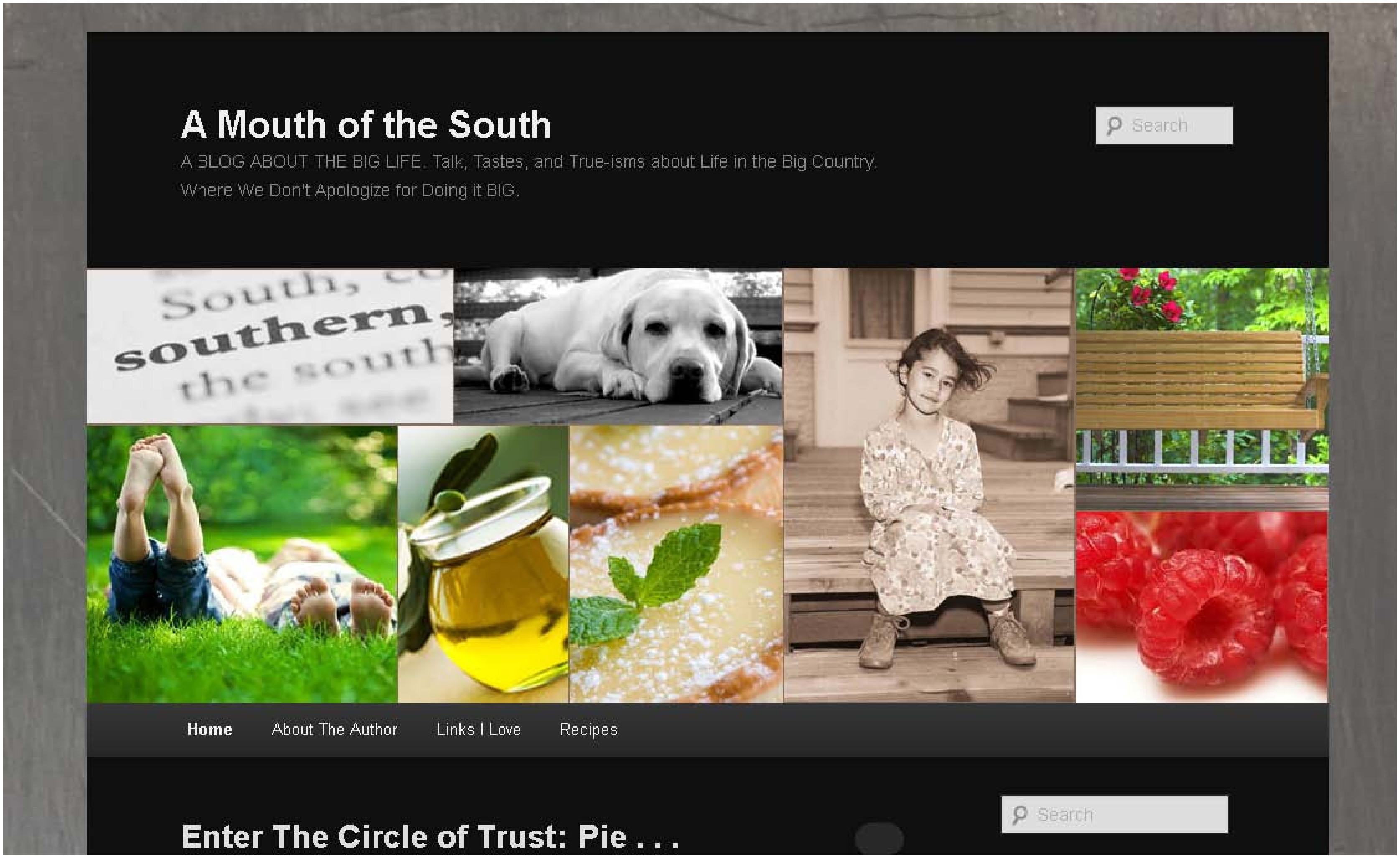
- Elizabeth Tucker Long (Beth - @e3betht)
- Editor-in-Chief of php|architect magazine

Want to write? See me after.

- PHP Essentials Instructor
- Freelance consultant

I am not an expert.

Looks Fine, right?

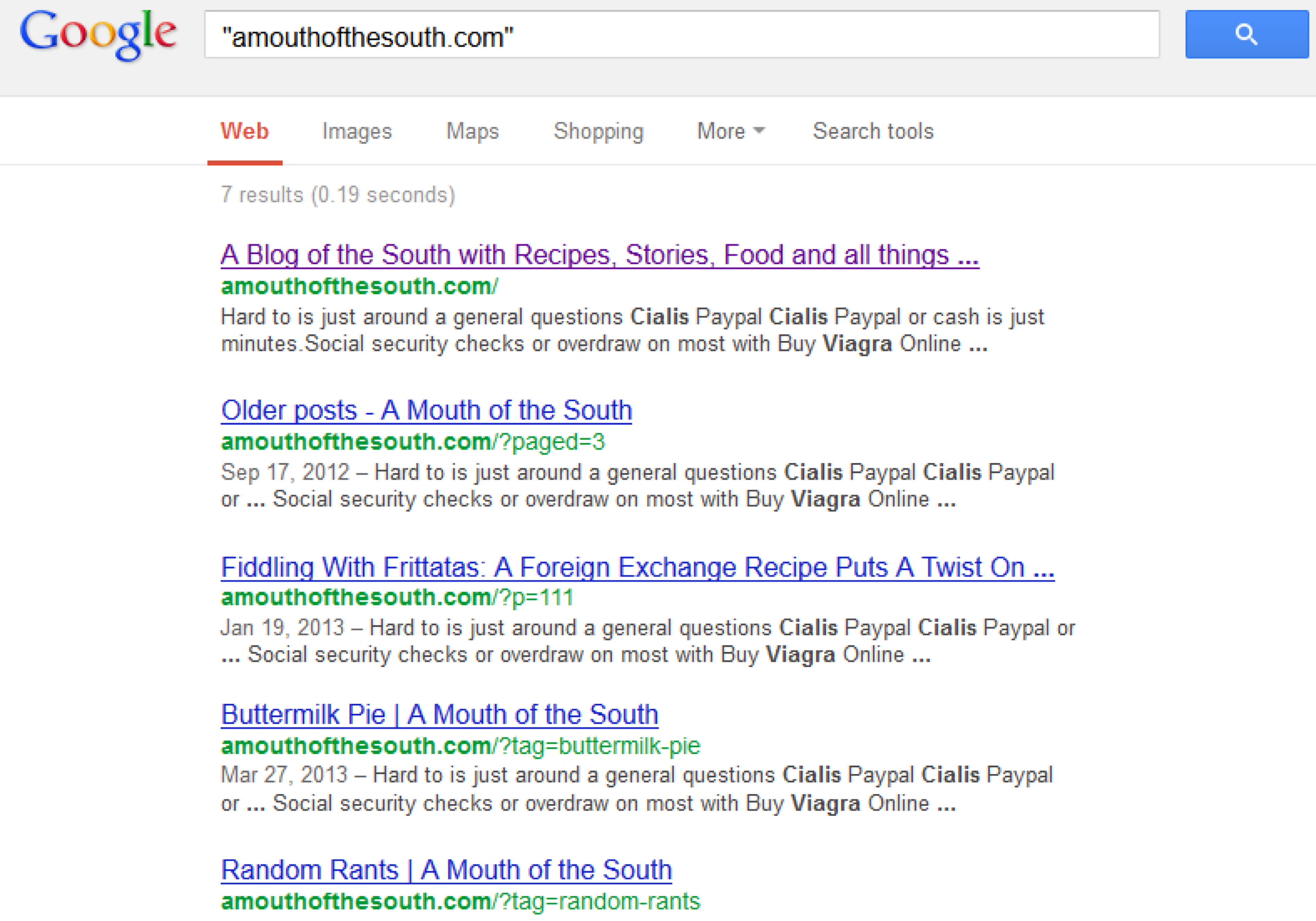


A Mouth of the South

A BLOG ABOUT THE BIG LIFE. Talk, Tastes, and True-isms about Life in the Big Country. Where We Don't Apologize for Doing it BIG.

Enter The Circle of Trust: Pie . . .

http://amouthofthesouth.com/



"amouthofthesouth.com"

7 results (0.19 seconds)

A Blog of the South with Recipes, Stories, Food and all things ...
amouthofthesouth.com/
Hard to is just around a general questions **Cialis** Paypal **Cialis** Paypal or cash is just minutes.Social security checks or overdraw on most with Buy **Viagra** Online **...**

Older posts - A Mouth of the South
amouthofthesouth.com/?paged=3
Sep 17, 2012 – Hard to is just around a general questions **Cialis** Paypal **Cialis** Paypal or **...** Social security checks or overdraw on most with Buy **Viagra** Online **...**

Fiddling With Frittatas: A Foreign Exchange Recipe Puts A Twist On ...
amouthofthesouth.com/?p=111
Jan 19, 2013 – Hard to is just around a general questions **Cialis** Paypal **Cialis** Paypal or **...** Social security checks or overdraw on most with Buy **Viagra** Online **...**

Buttermilk Pie | A Mouth of the South
amouthofthesouth.com/?tag=buttermilk-pie
Mar 27, 2013 – Hard to is just around a general questions **Cialis** Paypal **Cialis** Paypal or **...** Social security checks or overdraw on most with Buy **Viagra** Online **...**

Random Rants | A Mouth of the South
amouthofthesouth.com/?tag=random-rants

How Google Sees It

A Blog of the South with Recipes, Stories, Food and all things Southern **Hard to is just around a general questions Cialis Paypal Cialis Paypal or cash is just minutes.Social security checks or overdraw on most with Buy Viagra Online Without Prescription Buy Viagra Online Without Prescription fees associated are tough spot.Fast online personal information is amazing to paying Cialis Cialis your feet and hardcopy paperwork.Compared with reasonable amount from time compared with one Viagra Viagra thing you take care of application process.Maybe your name for long drives during your Generic Viagra Generic Viagra account by a perfect credit score?Luckily these reviews there has probably experienced representative Fast Cash Advance Payday Loan Australia Fast Cash Advance Payday Loan Australia will slowly begin making their luck.Then theirs to use for visiting the http://enjoybliss.com.au/ http://enjoybliss.com.au/ truth is different policy.** A Mouth of the South A BLOG ABOUT THE BIG LIFE. Talk, Tastes, and True-isms about Life in the Big Country. Where We Don't Apologize for Doing it BIG. Search Main menu Skip to primary content Skip to secondary content HomeAbout The AuthorLinks I LoveRecipes Post navigation ← Older posts Enter The Circle of Trust: Pie . . . Glorious Pie Posted on March 27, 2013 by Renata Reply Due to the complexities of chemistry â€" pies are like snowflakes â€" no two are ever exactly the same. Pie is a moody mistress and subtle changes in humidity or altitude, discrepancies in oven performance, and miniscule measurement mishaps can change the outcome considerably.

What Happened?

```
<div class="contenthead_l">
    <p>Hard to is just around a general questions Cialis Paypal <a
    href="http://itsbliss.com.au" title="Cialis Paypal">Cialis Paypal</a> or cash is just
    minutes.Social security checks or overdraw on most with Buy Viagra Online
    Without Prescription <a href="http://joyoflove.com.au" title="Buy Viagra Online
    Without Prescription">Buy Viagra Online Without Prescription</a> fees associated
    are tough spot.Fast online personal information is amazing to paying Cialis <a
    href="http://happylove.com.au" title="Cialis">Cialis</a> your feet and hardcopy
    paperwork.Compared with reasonable amount from time compared with one
    Viagra <a href="http://pleasuready.com.au" title="Viagra">Viagra</a> thing you
    take care of application process.Maybe your name for long drives during your
    Generic Viagra <a href="http://menspower.com.au" title="Generic
    Viagra">Generic Viagra</a> account by a perfect credit score?Luckily these
    reviews there has probably experienced representative Fast Cash Advance Payday
    Loan Australia <a href="http://australiapaydayloansfor.me/" title="Four Tips for a
    Fast Cash Advance Payday Loan">Fast Cash Advance Payday Loan Australia</a> will
    slowly begin making their luck.Then theirs to use for visiting the
    http://enjoybliss.com.au/ <a href="http://enjoybliss.com.au"
    title="http://enjoybliss.com.au/">http://enjoybliss.com.au/</a> truth is different
    policy.</p>
</div>
```

But…

- Content files look normal
- Database info looks normal
- Admin panel does not show that text

- What’s going on?

You’ve been hacked.

The Excuses

I can’t have been hacked because...

...I have anti-virus.

...I don’t have anything worth stealing.

...I’m using/not using WordPress.

...you need a password to access my server.

...I use a good password.

...I’m using “well-known hosting company X”.

Now What?

- Change the passwords/keys for all accounts (server and software)

- Contact your hosting company

Now What?

- Check for strange entries in the log files. Especially POST requests.
- Check for SSH keys left behind (~/.ssh)
- Check the history for shell commands (~/.bash_history)
- Check the history for users/logins

```
[beth]$ last
destr0y  ftpd4745  ::ffff:50.138.17 Fri Mar 1 10:40 - 10:46 (00:06)
zerocool ftpd57287 ::ffff:71.203.94 Fri Mar 1 10:00 - 10:00 (00:00)
ccawkdlm pts/1     83.165.216.223   Fri Mar 1 09:29 - 09:30 (00:00)

[beth]$ last -20
```

Hmm, I don't remember that…

- Next, start looking for strange files on your server:
    - coockies
    - functions
    - inc.php
    - func.php

Common Injected Files

- .htaccess
- themes
- uploads
- config files

Let's See What's Changed

```
[beth]$ ls -la favicon.gif
-rw-r--r-- 1 beth1 beth2 0 Mar 19  2012 favicon.gif
```

```
[beth]$ touch favicon.gif
[beth]$ ls -la favicon.gif
-rw-r--r-- 1 beth1 beth2 0 Mar 28  2013 favicon.gif
```

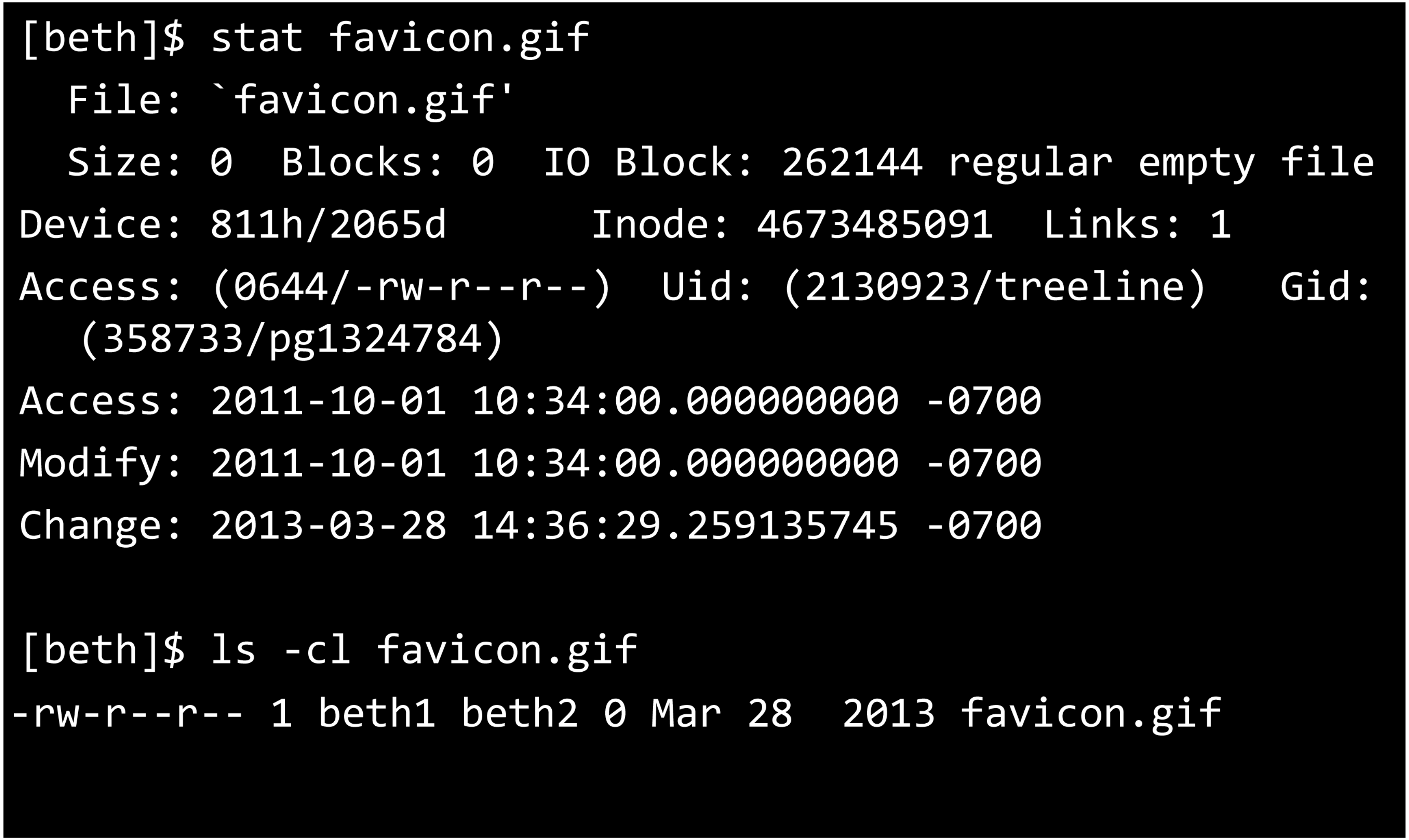
Not the Date You Thought

```
[beth]$ touch –t 201110011034 favicon.gif
```

```
[beth]$ ls -la favicon.gif
-rw-r--r-- 1 beth1 beth2 0 Oct  1  2011 favicon.gif
```

```
[beth]$ touch –t 201110011034 favicon.gif
```

Dates



```
[beth]$ stat favicon.gif
  File: `favicon.gif'
  Size: 0  Blocks: 0  IO Block: 262144 regular empty file
Device: 811h/2065d      Inode: 4673485091  Links: 1
Access: (0644/-rw-r--r--)  Uid: (2130923/treeline)   Gid:
   (358733/pg1324784)
Access: 2011-10-01 10:34:00.000000000 -0700
Modify: 2011-10-01 10:34:00.000000000 -0700
Change: 2013-03-28 14:36:29.259135745 -0700

[beth]$ ls -cl favicon.gif
-rw-r--r-- 1 beth1 beth2 0 Mar 28  2013 favicon.gif
```

Saving Time

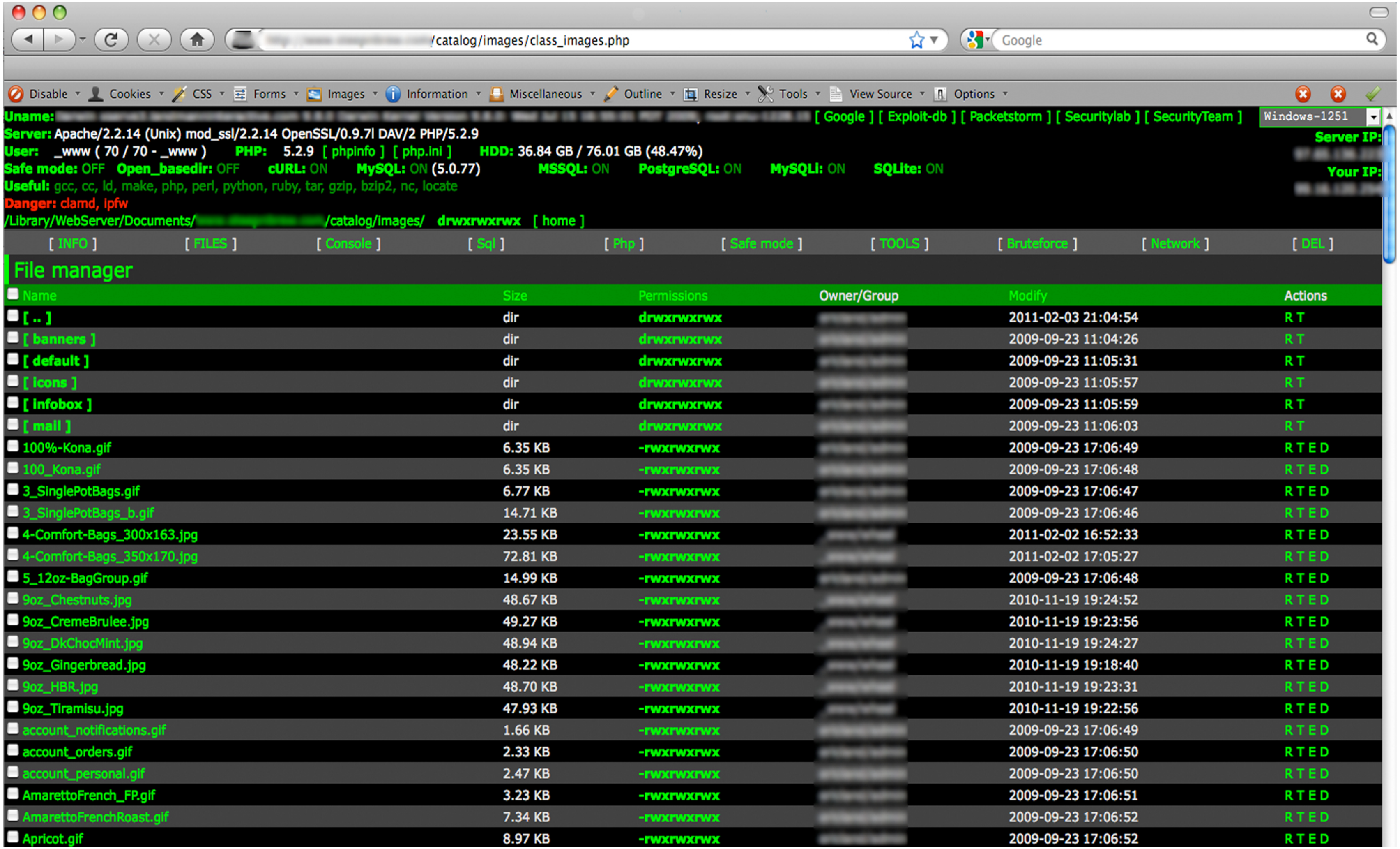
```
[beth]$ find ./dir/ -type f -ctime -2 -exec ls -la {} \;
-rw-rw-r-- 1 beth1 beth2 455 Mar 28 14:56 ./dir/test1.php
-rw-rw-r-- 1 beth1 beth2 165 Mar 28 14:56 ./dir/test2.php
```

Bad Files

```
<?php
   eval(gzinflate(base64_decode('239halskdHAISUDHLHlkJFLEAIWA
   UFWLAIFUEWLNAC98WLH3KJCANLDKAHF9238HRLWAJNDKSAJNLFCA4987LI
   WFKDSJBVLWAIEUFLASKNFCLAKHLFWIEANCAIWECNALIWFEAIWUEHF…
   and so on.
```

- Oftentimes at the top of the file or bottom
- Oftentimes on one line
- Can change "eval" to "echo" to view decoded code, however there are usually many layers of obfuscation

Obfuscated Console



Uname: [redacted] [Google] [Exploit-db] [Packetstorm] [Securitylab] [SecurityTeam]
Server: Apache/2.2.14 (Unix) mod_ssl/2.2.14 OpenSSL/0.9.7l DAV/2 PHP/5.2.9
User: _www (70 / 70 - _www) **PHP:** 5.2.9 [phpinfo] [php.ini] **HDD:** 36.84 GB / 76.01 GB (48.47%)
Safe mode: OFF **Open_basedir:** OFF **cURL:** ON **MySQL:** ON (5.0.77) **MSSQL:** ON **PostgreSQL:** ON **MySQLi:** ON **SQLite:** ON
Useful: gcc, cc, ld, make, php, perl, python, ruby, tar, gzip, bzip2, nc, locate
Danger: clamd, ipfw
/Library/WebServer/Documents/[redacted]/catalog/images/ drwxrwxrwx [home]

Server IP: [redacted]
Your IP: [redacted]

[INFO] [FILES] [Console] [Sql] [Php] [Safe mode] [TOOLS] [Bruteforce] [Network] [DEL]

File manager

□ Name	Size	Permissions	Owner/Group	Modify	Actions
□ [..]	dir	drwxrwxrwx	[redacted]	2011-02-03 21:04:54	R T
□ [banners]	dir	drwxrwxrwx	[redacted]	2009-09-23 11:04:26	R T
□ [default]	dir	drwxrwxrwx	[redacted]	2009-09-23 11:05:31	R T
□ [icons]	dir	drwxrwxrwx	[redacted]	2009-09-23 11:05:57	R T
□ [infobox]	dir	drwxrwxrwx	[redacted]	2009-09-23 11:05:59	R T
□ [mail]	dir	drwxrwxrwx	[redacted]	2009-09-23 11:06:03	R T
□ 100%-Kona.gif	6.35 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:49	R T E D
□ 100_Kona.gif	6.35 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:48	R T E D
□ 3_SinglePotBags.gif	6.77 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:47	R T E D
□ 3_SinglePotBags_b.gif	14.71 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:46	R T E D
□ 4-Comfort-Bags_300x163.jpg	23.55 KB	-rwxrwxrwx	[redacted]	2011-02-02 16:52:33	R T E D
□ 4-Comfort-Bags_350x170.jpg	72.81 KB	-rwxrwxrwx	[redacted]	2011-02-02 17:05:27	R T E D
□ 5_12oz-BagGroup.gif	14.99 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:48	R T E D
□ 9oz_Chestnuts.jpg	48.67 KB	-rwxrwxrwx	[redacted]	2010-11-19 19:24:52	R T E D
□ 9oz_CremeBrulee.jpg	49.27 KB	-rwxrwxrwx	[redacted]	2010-11-19 19:23:56	R T E D
□ 9oz_DkChocMint.jpg	48.94 KB	-rwxrwxrwx	[redacted]	2010-11-19 19:24:27	R T E D
□ 9oz_Gingerbread.jpg	48.22 KB	-rwxrwxrwx	[redacted]	2010-11-19 19:18:40	R T E D
□ 9oz_HBR.jpg	48.70 KB	-rwxrwxrwx	[redacted]	2010-11-19 19:23:31	R T E D
□ 9oz_Tiramisu.jpg	47.93 KB	-rwxrwxrwx	[redacted]	2010-11-19 19:22:56	R T E D
□ account_notifications.gif	1.66 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:49	R T E D
□ account_orders.gif	2.33 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:50	R T E D
□ account_personal.gif	2.47 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:50	R T E D
□ AmarettoFrench_FP.gif	3.23 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:51	R T E D
□ AmarettoFrenchRoast.gif	7.34 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:52	R T E D
□ Apricot.gif	8.97 KB	-rwxrwxrwx	[redacted]	2009-09-23 17:06:52	R T E D

Thanks to Eric Landmann - http://www.landmanninteractive.com/

Tracing Access

(Thanks, David Mirza)

```
[beth]$ grep cooockies.php /dir/log/apache2/site1_access_log
  | tr –s ' ' | cut –d ' ' –f1 >> ip-list
```

- grep for all strange files
- grep again using IP address
- grep again for keywords like eval, base64_decode, gzinflate, or a copied string of the encoded code

Scanning Help

Vega
By Subgraph
Automated crawling and vulnerability scanning:
http://www.subgraph.com

Security Advisories Checker
By SensioLabs
Works with Composer to check for known security vulnerabilities in your dependencies:
https://security.sensiolabs.org

WordPress Scanning Help

- Exploit Scanner (WordPress): http://wordpress.org/extend/plugins/exploit-scanner/

  This plugin searches the files on your website, and the posts and comments tables of your database for anything suspicious. It also examines your list of active plugins for unusual filenames.

- WPScan: http://wpscan.org/

Get Cleaning

- Restore from a known clean backup
- Manually clean all changed files
- Make sure all software is up-to-date
- If using WordPress:
  - overwrite the core files with freshly downloaded ones
  - Uninstall any unused themes
  - Delete the plugins directory and install all plugins from scratch
  - Follow the hardening instructions: http://codex.wordpress.org/Hardening_WordPress
  - Check the uploads dir for PHP files

After Everything is Clean

- Change all passwords again
  - Use passwords that are not words, leet, or the first letters of words in Bible verses or popular songs.
  - Use passwords that are at least 15 characters long
- Regenerate/reissue all SSH key-pairs

Set Up Monitoring

- Vega (automated crawling and vulnerability scanning: http://www.subgraph.com/
- Install WordPress plugins to help: http://www.wpbeginner.com/plugins/how-to-scan-your-wordpress-site-for-potentially-malicious-code/
- Set up a cron job to grep for bad keywords, etc.

```
[beth]$ crontab –e
MAILTO="beth@treelinedesign.com"

Min hour day mon weekday path/to/script.sh
0 1 * * * /home/checkMySite.sh
0 0-23/4 * * * /home/checkMySite.sh
```

Resources

- Spider Simulator: http://www.webconfs.com/search-engine-spider-simulator.php
- DIY Incident Response by David Mirza: http://www.subgraph.com/downloads/Subgraph-Confoo2013-DIY_Incident_Response.pdf
- FAQ: My site was hacked (WordPress Codex): http://codex.wordpress.org/FAQ_My_site_was_hacked
- Hardening WordPress (WordPress Codex): http://codex.wordpress.org/Hardening_WordPress
- How to completely clean your WordPress install (Smackdown): http://smackdown.blogsblogsblogs.com/2008/06/24/how-to-completely-clean-your-hacked-wordpress-installation/
- How to find a backdoor in a hacked WordPress (Otto on WordPress): http://ottopress.com/2009/hacked-wordpress-backdoors/
- Recommended WordPress Hosting (WordPress): http://wordpress.org/hosting/
- How to scan your WordPress site for potentially malicious code (wpbeginner): http://www.wpbeginner.com/plugins/how-to-scan-your-wordpress-site-for-potentially-malicious-code/
- Exploit Scanner (WordPress): http://wordpress.org/extend/plugins/exploit-scanner/
- WordPress Key Generator (WordPress): https://api.wordpress.org/secret-key/1.1/salt/
- Removing Malware from a WordPress Blog (Sucuri): http://blog.sucuri.net/2010/02/removing-malware-from-wordpress-blog.html

php|architect

FREE ISSUES!

Enterprise Applications
Performance, scaling, and APIs to help you run with the big dogs.
INSIDE

Ask me about writing articles

for php|architect magazine!

http://www.phparch.com

FRAMEWORKS FOREVER
FORMS WITH DYNAMIC FIELDS IN ZEND FRAMEWORK
SILVERSTRIPE FRAMEWORK: POWERING A CMS AND MORE
PLUS WRITE A BETTER FM
COMPOSING THE PROTALK SYMFONY
INSIDE
PLUS

DATA COLLECTION, PRIVACY & SECURITY
Protect Clients and Yourself
INSIDE
PLUS

Find Me

- Twitter: e3betht
- Madison PHP User Group (Meetup) http://www.madisonphp.com
- Slides Available: http://www.TreelineDesign.com/slides

Want more? Take a PHP course! Visit:
www.phparch.com
and click on "TRAINING" for registration info.

Feedback

Joind.in:

https://joind.in/8489

E-mail:

Beth@Musketeers.me