I've Been Hacked, Now What?

Beth Tucker Long

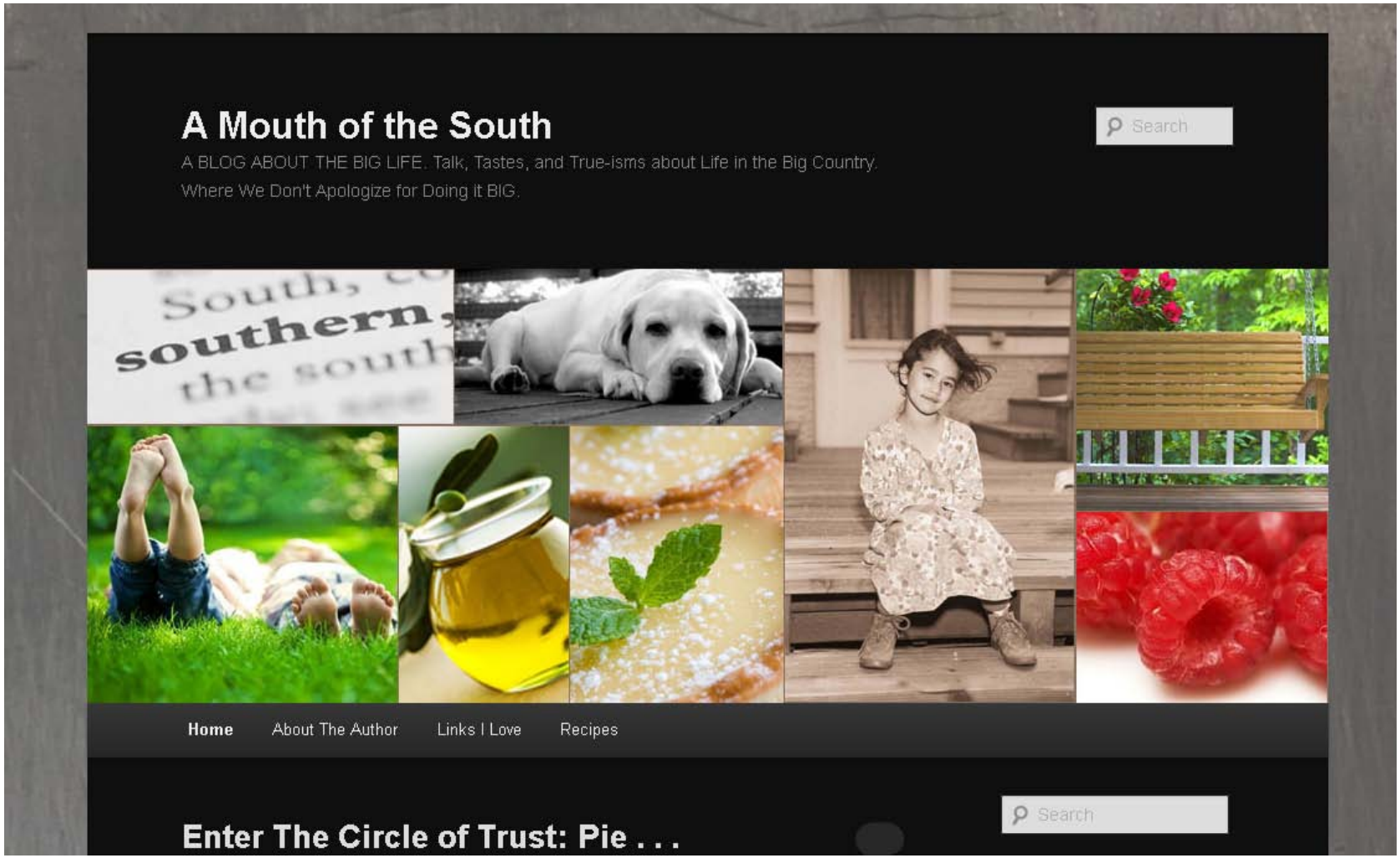
Who am I?

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

Want to write?
See me after.

- PHP Essentials Instructor
- Freelance consultant

Looks Fine, right?



http://amouthofthesouth.com/

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?

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.

But…

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

- Where is it coming from?

Now What?

- Change the passwords/keys for all accounts (server and software)
- Check for SSH keys left behind (~/.ssh)
- Check the history for shell commands (~/.bash_history)
- Check the history for users/logins
- Contact your hosting company

```
[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


[beth]$ touch –t 201110011034 favicon.gif
[beth]$ ls -la favicon.gif
-rw-r--r-- 1 beth1 beth2 0 Oct  1  2011 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 Oct  1  2011 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

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

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!

Ask me about writing articles

for php|architect magazine!

http://www.phparch.com

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:

http://www.madisonphp.com

E-mail:

Beth@Musketeers.me