NOTICE: You Do NOT Have the Right
to Reprint or Resell this Report!

You Also MAY NOT Give it Away,
Sell or Share the Content Herein.

If you obtained this report from anywhere other than the official site you have a pirated copy.


Local
LEADBOSS
PageOne

Published By:
PageOneTraffic Ltd.

Disclaimer

This report has been diligently researched and compiled with the intent to provide information for those wishing to learn about Wordpress security.

Throughout the making of this consumer report, every effort has been made to ensure the highest amount of accuracy and effectiveness for the techniques suggested by the author. The report may contain contextual, as well as, typographical mistakes.

No information provided in this report constitutes a warranty of any kind; nor shall readers of this report rely solely on any such information or advice. All content, products, and services are not to be considered as legal, medical, or professional advice and are to be used for personal use and information purposes only.

This report makes no warranties or guarantees express or implied, as to the results provided by the strategies, techniques, and advice presented in this report. The publishers of this report expressly disclaim any liability arising from any strategies, techniques, and advice presented in this report.

The purpose of this consumer report is to educate and guide. Neither the publisher nor the author warrant that the information contained within this consumer report is free of omissions or errors and is fully complete. Furthermore, neither the publisher nor the author shall have responsibility or liability to any entity or person as a result of any damage or loss alleged to be caused or caused indirectly or directly by this report.

Even if all steps mentioned are followed correctly and exactly as specified and stipulated in this guide and the accompanying videos, it is reasonable to assume that there is inherent risk in anything to do related to the topic covered.

You are advised to do your own due diligence before following any of the tasks mentioned in the guide and take proper precautions, such as: implementing recovery measures and creating backups before trying anything from this guide.

Introduction

This guide has been divided into two distinct parts:

Part 1: Offline Lead Generation

Part 2: The 'HOW TO' Manual for Running 8 Security Tests and providing easy solutions.

I have deliberately left out all of the fluff and lengthy explanations so that you can easily and quickly master the techniques.

Its important to understand that this system is geared to tackle the easy to solve problems so that you can approach a prospect without needing to be a security expert.

Let's face it, we all know how crucial security is to our business. One hacked site can cost thousands of dollars to fix. With the knowledge you are about to learn here you will be saving your clients valuable time and money.

I am confident that this is the best security course you will ever buy. You will know exactly how to run the tests, fix the issues and bring this knowledge to your offline businesses. And even more important you will be a 'Super Hero' in their eyes and earn lots of money in the process.

Upgrade to LocalLeadBoss Software here

PART ONE: OFFLINE LEAD GENERATION

The Approach

In this section, I am going to show you how you can use the knowledge of Wordpress security to find clients, both in local markets and online.

Did you know that most internet marketers know very little about Wordpress security (even the ones who teach Wordpress). So you will be leap years ahead of them and in turn you will be getting paid for this knowledge.

Local business owners are in the worst position of all. Many assume that security measures are taken into consideration by their web designers or webmasters, and even worse, most do not understand the consequences of a security breech. They simply don't have a clue that their sites are vulnerable and this is where you come in. IT IS YOUR DUTY to protect them and earn a nice paycheck as a side-effect.

There are 6 easy steps to follow:

1. Identify a business category or niche to go after
2. Search for vulnerable sites
3. Run simple tests
4. Send them an e-mail or a direct mail
5. Cash check and fix their site
6. Upsell to more value added services

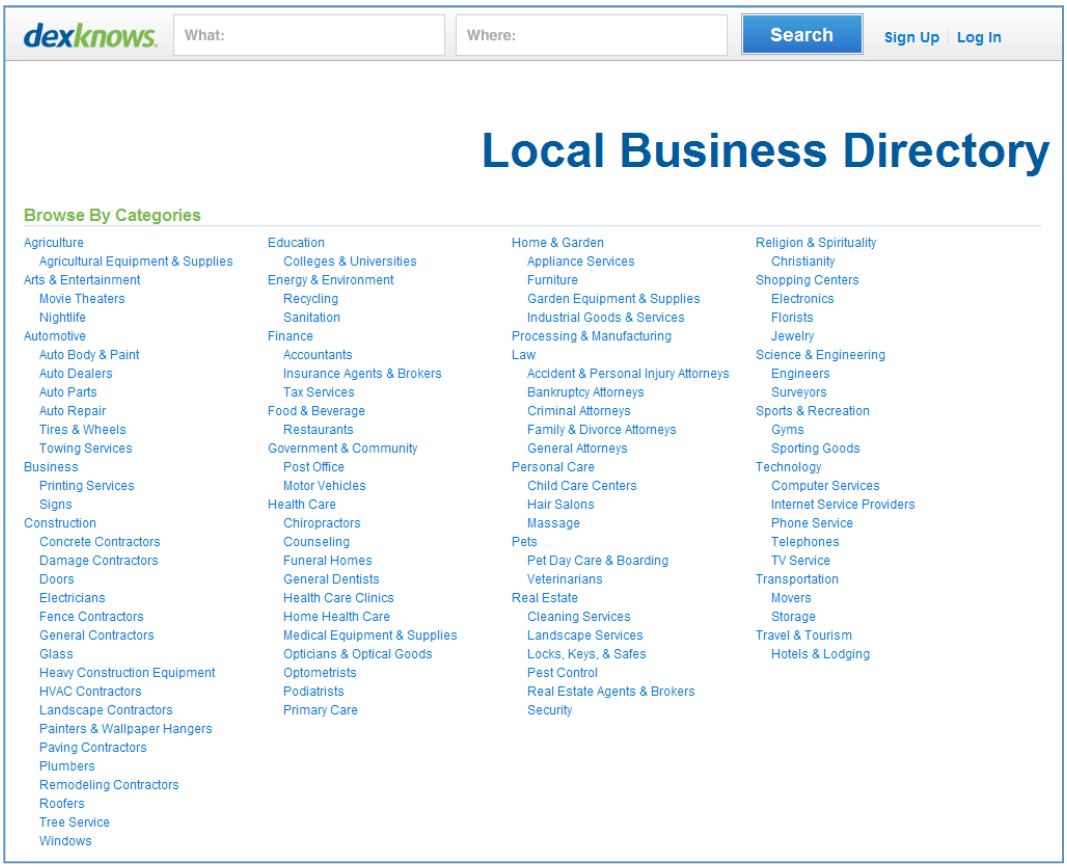
It's a fairly simple approach and SIMPLE works best.

So, let's go through the steps.

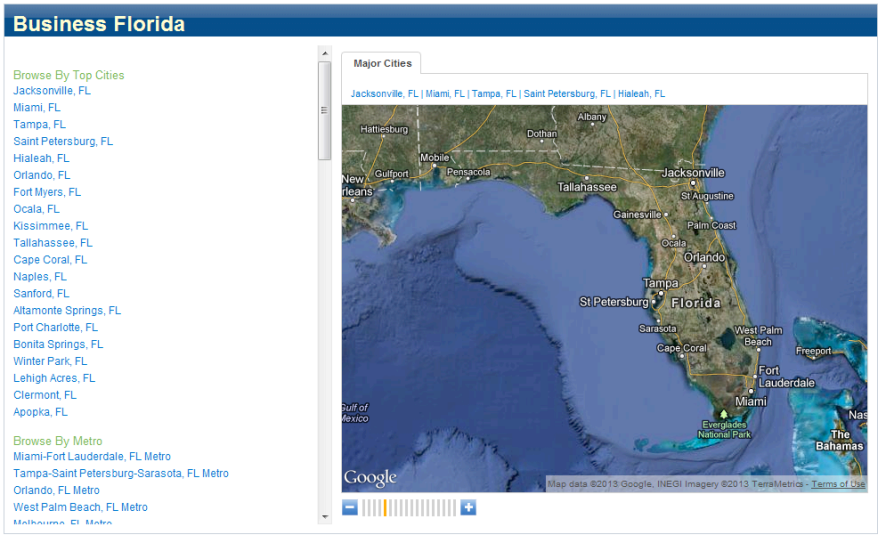
Step 1: Identify Business Category

Now, here's the deal. The business category doesn't even matter. No diamonds in your backyard! Just go to one of the following sites.

Go to www.dexknows.com/browse-directory.asp



If you click on any one of the categories it takes you to a page that lets you select a specific region for that category. For example, click on 'construction' and then 'Florida' and you will get a map (as seen below). Click any of the cities and it returns the businesses for that category.



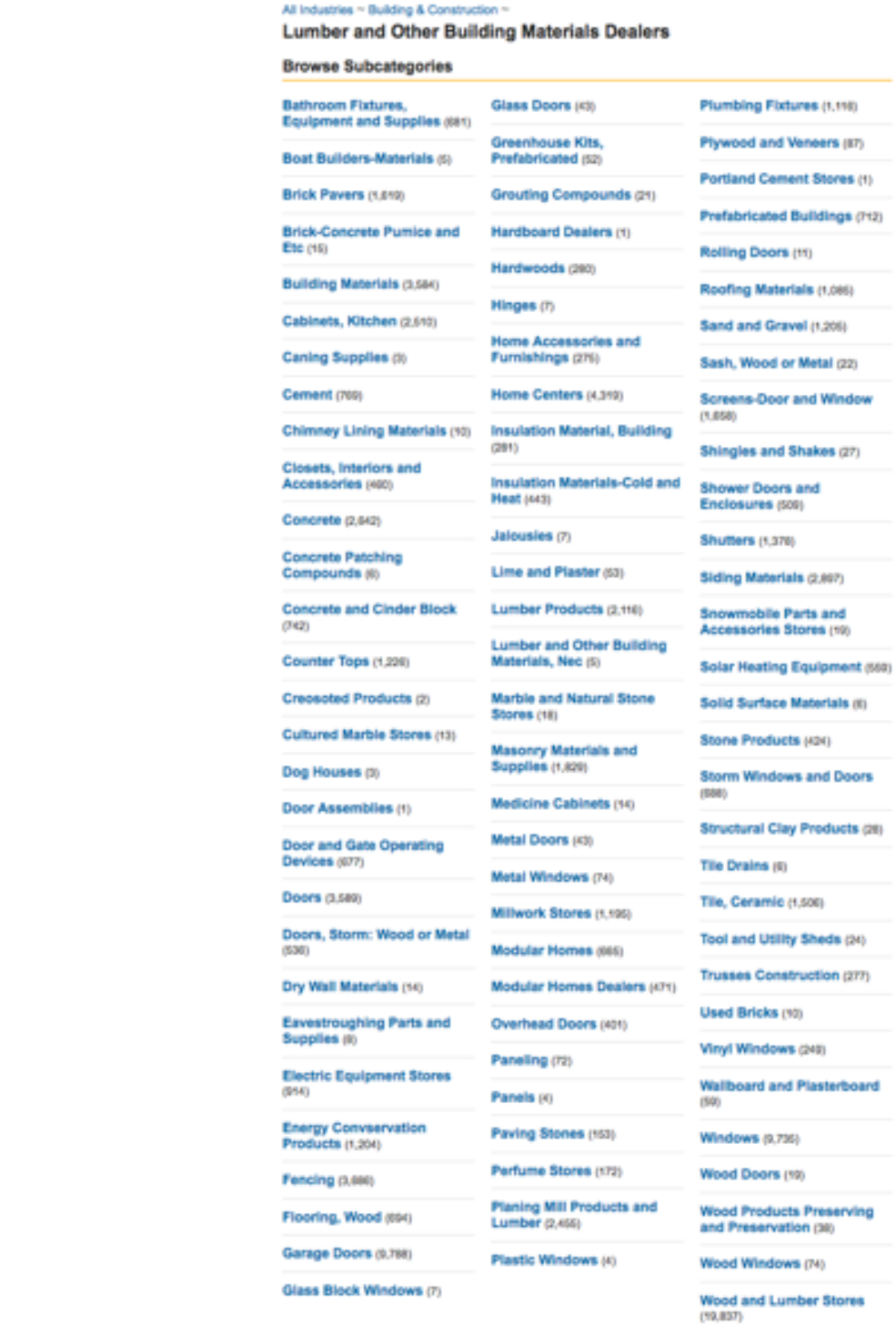
This is one of my favorite resources and I highly recommend it. Remember, any of these categories will work. However, if there is a market that you have worked in before then start there and work your way through. Most of these categories will have websites - some smaller, some larger. Work within your comfort zone to start. Obviously, some websites will be easier to make contact with than others.

The next website is I recommend is http://www.manta.com

They have different portals for different countries that you can use. Scroll to the bottom till you see this:

These are TOP level listings and most will have sub-categories.

As an example look at the number of sub-categories in “Building Materials”



All Industries ~ Building & Construction ~

Lumber and Other Building Materials Dealers

Browse Subcategories

- Bathroom Fixtures, Equipment and Supplies (681)
- Boat Builders-Materials (5)
- Brick Pavers (1,619)
- Brick-Concrete Pumice and Etc (15)
- Building Materials (3,584)
- Cabinets, Kitchen (2,510)
- Caning Supplies (3)
- Cement (709)
- Chimney Lining Materials (10)
- Closets, Interiors and Accessories (480)
- Concrete (2,642)
- Concrete Patching Compounds (6)
- Concrete and Cinder Block (742)
- Counter Tops (1,226)
- Creosoted Products (2)
- Cultured Marble Stores (13)
- Dog Houses (3)
- Door Assemblies (1)
- Door and Gate Operating Devices (677)
- Doors (3,589)
- Doors, Storm: Wood or Metal (536)
- Dry Wall Materials (14)
- Eavestroughing Parts and Supplies (8)
- Electric Equipment Stores (914)
- Energy Convservation Products (1,204)
- Fencing (3,886)
- Flooring, Wood (694)
- Garage Doors (9,788)
- Glass Block Windows (7)
- Glass Doors (43)
- Greenhouse Kits, Prefabricated (52)
- Grouting Compounds (21)
- Hardboard Dealers (1)
- Hardwoods (280)
- Hinges (7)
- Home Accessories and Furnishings (275)
- Home Centers (4,319)
- Insulation Material, Building (281)
- Insulation Materials-Cold and Heat (443)
- Jalousies (7)
- Lime and Plaster (53)
- Lumber Products (2,116)
- Lumber and Other Building Materials, Nec (5)
- Marble and Natural Stone Stores (18)
- Masonry Materials and Supplies (1,829)
- Medicine Cabinets (14)
- Metal Doors (43)
- Metal Windows (74)
- Millwork Stores (1,195)
- Modular Homes (665)
- Modular Homes Dealers (471)
- Overhead Doors (401)
- Paneling (72)
- Panels (4)
- Paving Stones (153)
- Perfume Stores (172)
- Planing Mill Products and Lumber (2,456)
- Plastic Windows (4)
- Plumbing Fixtures (1,116)
- Plywood and Veneers (87)
- Portland Cement Stores (1)
- Prefabricated Buildings (712)
- Rolling Doors (11)
- Roofing Materials (1,085)
- Sand and Gravel (1,205)
- Sash, Wood or Metal (22)
- Screens-Door and Window (1,858)
- Shingles and Shakes (27)
- Shower Doors and Enclosures (509)
- Shutters (1,378)
- Siding Materials (2,897)
- Snowmobile Parts and Accessories Stores (19)
- Solar Heating Equipment (569)
- Solid Surface Materials (8)
- Stone Products (424)
- Storm Windows and Doors (888)
- Structural Clay Products (28)
- Tile Drains (6)
- Tile, Ceramic (1,506)
- Tool and Utility Sheds (24)
- Trusses Construction (277)
- Used Bricks (10)
- Vinyl Windows (249)
- Wallboard and Plasterboard (59)
- Windows (9,735)
- Wood Doors (19)
- Wood Products Preserving and Preservation (36)
- Wood Windows (74)
- Wood and Lumber Stores (19,837)

3 Hot Tips To Find Buyers

1. **Make sure they are already spending money on marketing.**
2. **High revenue per customers. (Then they will spend more on getting them)**
3. **Already a high demand for their services.**

Examples: Dentists, Chiropracters, Electricians, Roofers. (High revenue per customer)

Bad Examples: Restaurants, Flower shops. (Low revenue per customer)

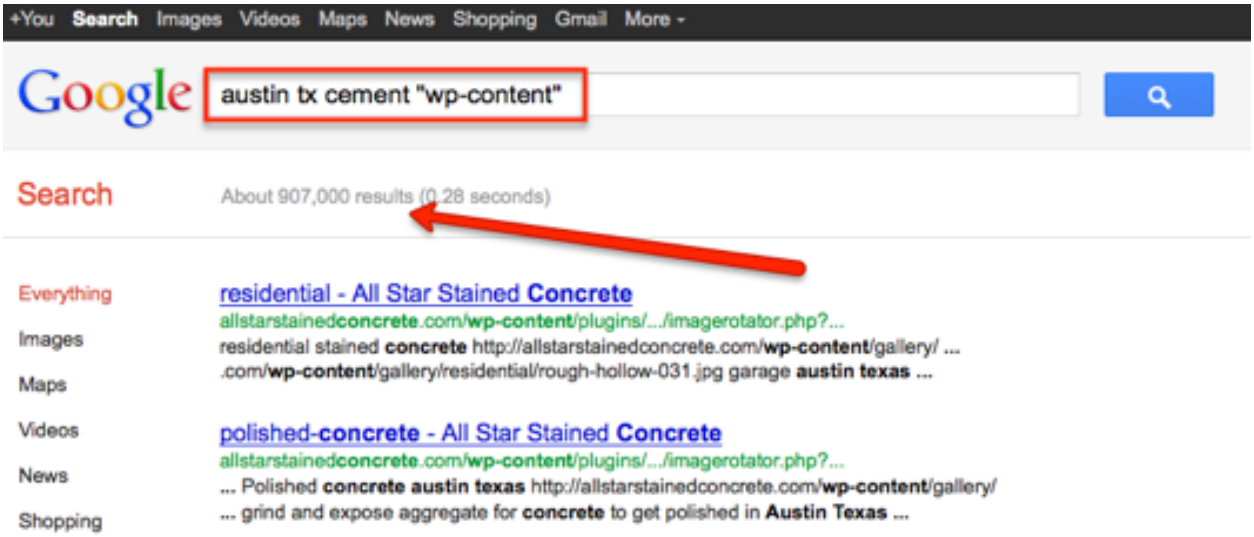
Step 2: Search For Vulnerable Sites

In this instance, think of Google as your best friend. It is a highly evolved search machine that will index everything a normal human would not. So, when you use search strings, you get everything you need.

Watch me try an obscure category that most people would probably ignore.

"Cement" or "Concrete"

Now let's add in a location - Austin, TX. Look at the search results. There is big money in this (and many others).



907,000 results!

Granted, many of these will be pages and other stuff, but this is a category you wouldn't normally venture into.

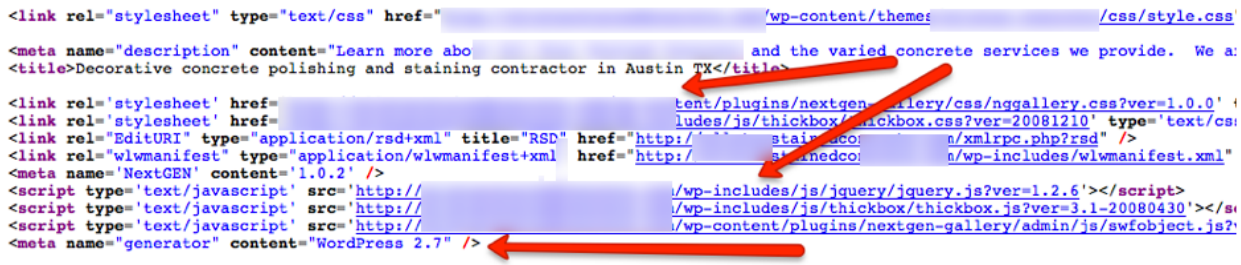
Now, it's time to check for vulnerabilities.

Believe it or not, with local businesses, you'll pretty much be at a close to 100% accuracy rate each time. Now let's look at the first website and run 4 simple tests.

The first result is actually a feed page, so I'll have to go to the root domain. I'm doing this on the fly, while typing this report to show you real life proof and I can bet I'll find vulnerabilities here.

Here's the homepage.

The next thing we need to do is identify whether or not the site is Wordpress. Just go to "view" then "source" in your browser. Below you see the source using Firefox.



Notice the wp-content and wp-includes. This confirms that it is a Wordpress site.

Next check the version that they are using. In this example they are using Wordpress 2.7. The most current version is 3.5.1. This is your first indicator that they are not up-to-date with security.

Ok, let's run some tests ...

All of the checks can be automated using the LocalLeadBoss software App which runs on Mac and PC. You can watch a demo here.

Step 3: Run Simple Tests

For this example, I am only going to run 4 tests. However, you will learn 8 different easy tests to run.

Now, it's time to test this site for basic security. This step is so easy, a child could do it ...

Test 1 - Is the wp-config.php file readable?

The wp-config.php file does not need to be publicly readable or even executable. This is a common mistake made by most Wordpress users. By default Wordpress installs this configuration file in the root directory, which is NOT secure.

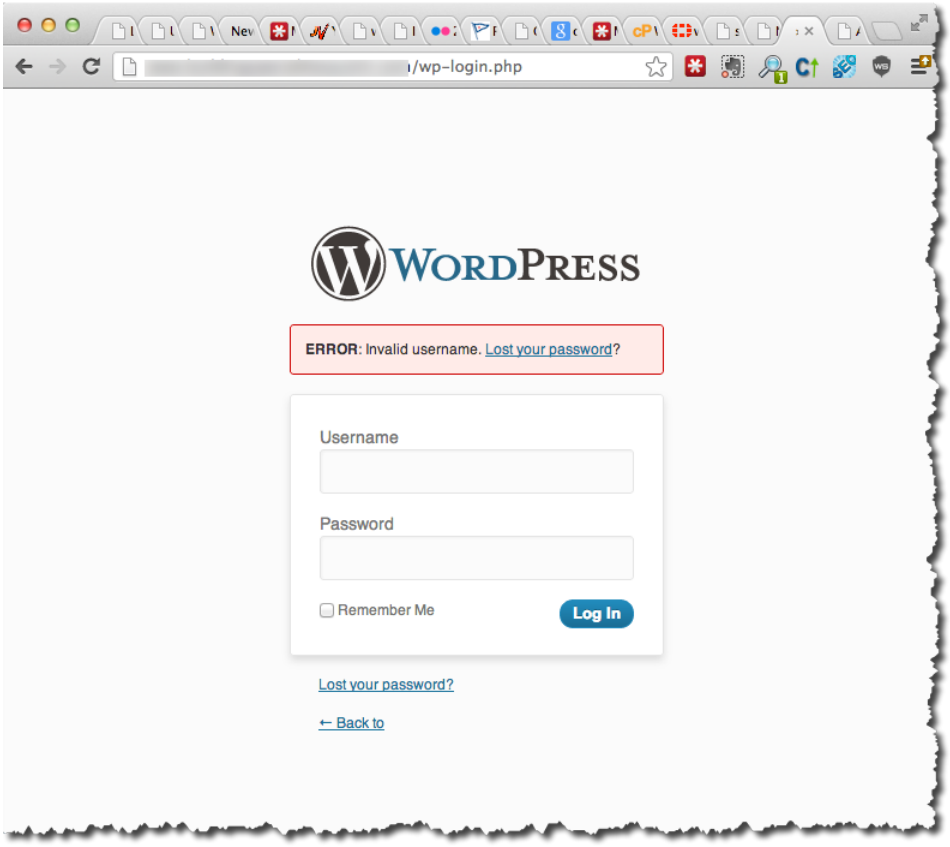
To correct this, it is recommended that you move the wp-config.php file one directory above public_html (or www.root), which is where your index.html or index.php are located.

Once you have done this try and access the wp-config.php file. If you get a 404 error, CONGRATULATIONS you have done a great job. If you get a blank page, then the site is still NOT secure. So let's see how our friends did in the example...

Let's move on to test 2...

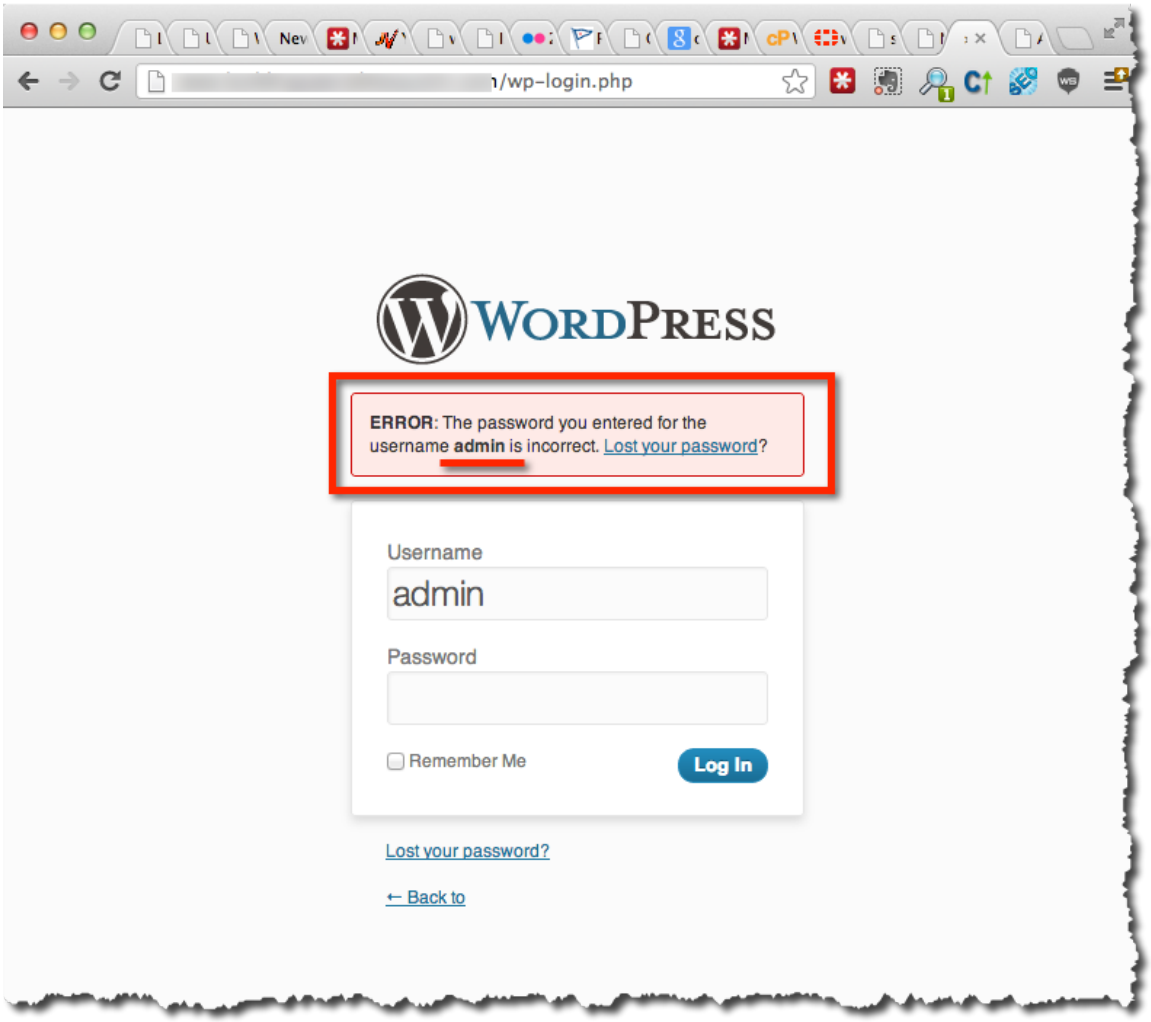
Test 2 - Is the ADMIN username changed?

Let's go a step further and try to login. I entered the username “abcd” and password “efgh”. What I am looking for is an error message. And just as I thought it returns the following error.



Now, chances are they just have an "admin" login.

So, I’ll take my chances and try and login with that.



I proceed to type "admin" in the username field and "blah in the password field.

Ok, clearly these guys HAVE NO CLUE about even basic security.

FAILED (Miserably)

Test 3 - Is the readme.html file still available?

This file lets you see the wp version and therefore makes it easy for accessing “known” exploits. We already know they are using version 2.7 by looking at the code but its revealed really easily right here:

Once again they have...

FAILED

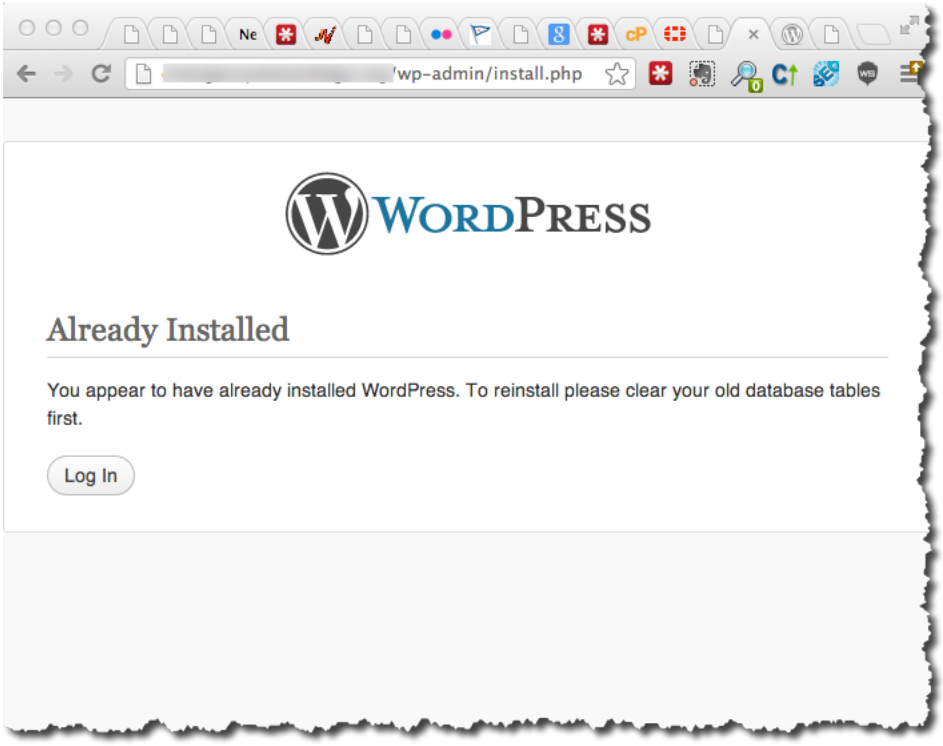
Time to move on to the 4th and final test...

Test 4 - Is the installation script still available?

Leaving the install script behind is the most common error you'll see in Wordpress websites.

Here's the bad news...

Every time you update a theme or a wp version, your security has to be re-checked again as the new version replaces almost everything that was secured, which includes the install files. The good news is that it is another opportunity for you to provide a service to your client.



So let's check. As you can see the install script is still available.

FAILED

Our test website scored a 4/4 failure rate. They are at a high level of risk with serious vulnerabilities.

You can stop at this stage and help them out. But we have also detailed later in the guide 8 tests that you can run together with how to fix them without having to be a security expert.

Now, it is time to help them out.

Step 4: Send Them A Warning

This step can either be done via email or direct mail depending on the contact information you are able to obtain.

But first I really want you to think about this. What would you do if this was a friend of yours? How quickly would you want to communicate with them? Would you not want to call them right away and tell them what you have discovered? And stress the importance of getting the problem fixed immediately?

You business clients deserve the same level of urgency. They ought to have a similar response to your friends.

Sometimes it will be difficult to find the contact information for the owner or key decision maker. Here are some things that have worked for me...

I have found the best place to find the person I am looking for is either through the Better Business Bureau at www.bbb.org or www.manta.com or lastly look up the domain contact details in domain tools: domaintools.com

But first try going to their “Contact Us” or “About Us” page. Often this will give you the actual business name, which in many cases may be different from the domain name.
Using these methods you should be able to find an e-mail, as well as, a snail mail address. I actually recommend snail mailing (it seems to ignite a higher level of importance), but you can try e-mail instead if you wish.

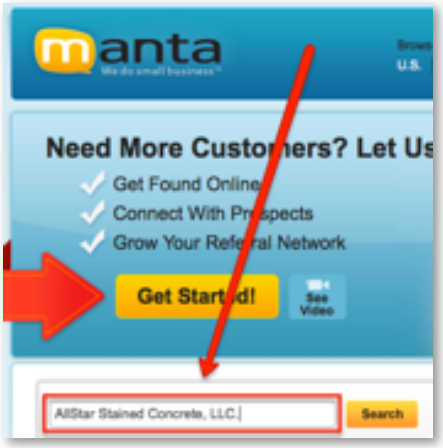
Now, it’s time to find the owner's name of our test website.
Let’s go to www.bbb.org.

Click on the button that says “Checkout A Business Or a Charity”.

This should bring you to the search page for that city. Now enter the business name and click search.

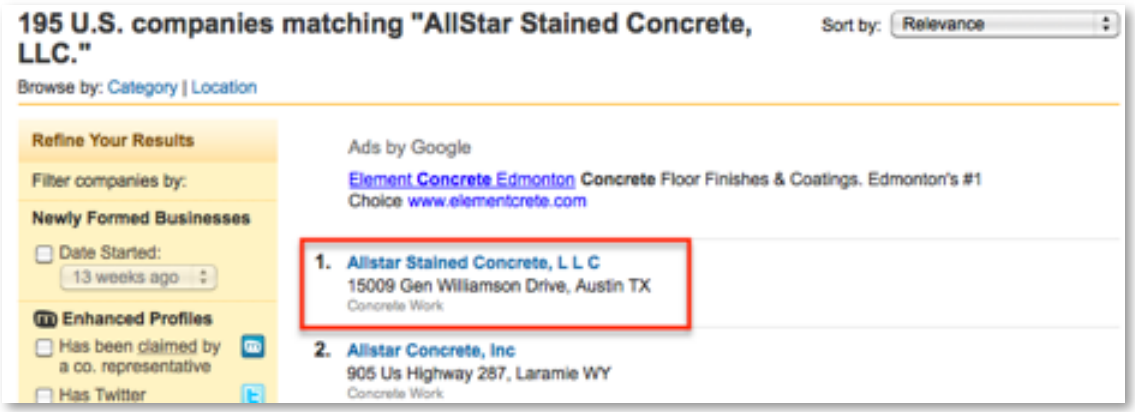
In this particular example it returned no results. This is common and can happen. However, it is a good practice to do this with every business you want to send a letter to anyway.

The next step is to go to www.manta.com and search for the same business.



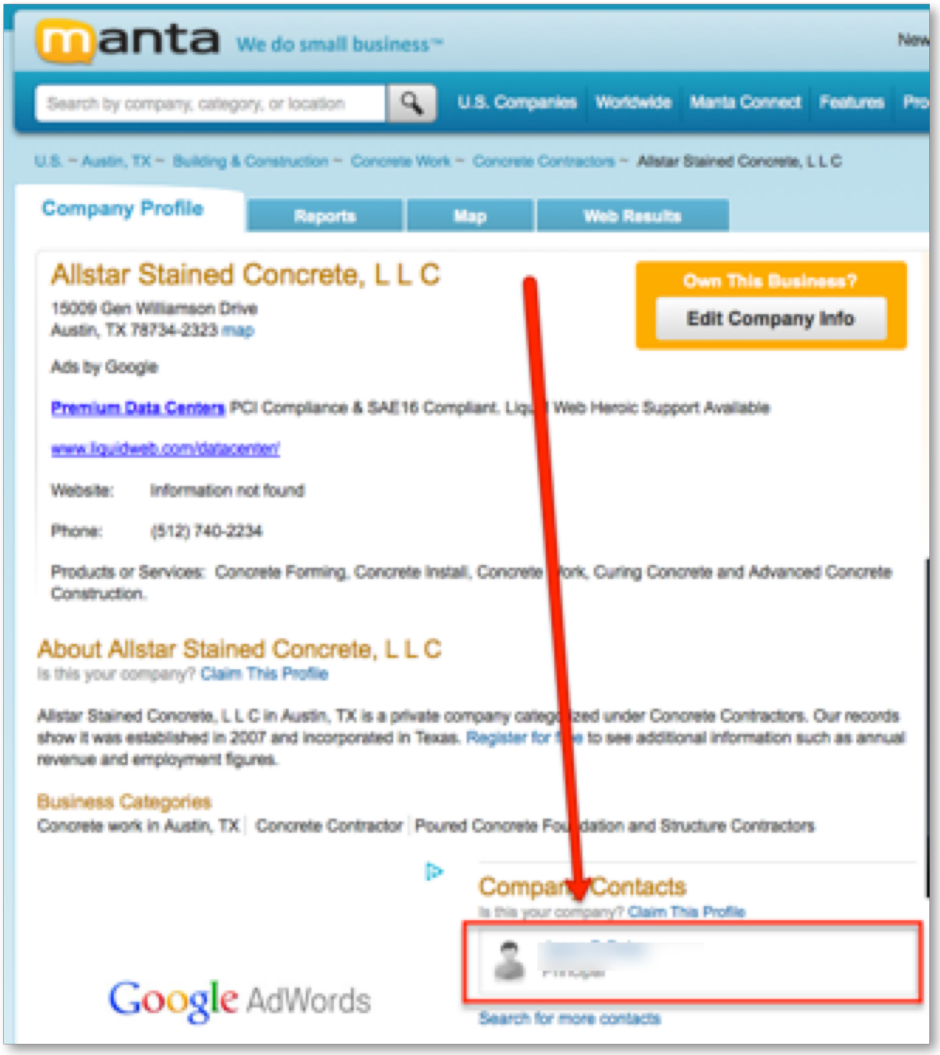
As you can see below, the search was successful.

Let's take a look... We are able to see that the address matches the one on the website contact page. Therefore, we can confirm that we have found the correct mailing address.



Now click on the listing to get the details.

You're looking for the name of the owner, CEO, Principal, etc., which will be in the "Company Contacts" section on the right side as seen below.



Lets assume our "Principal" here as: James Bean.

Now we can proceed with writing a letter addressed to him directly.

Make sure to make it personal. Use "Dear James" vs. "Dear James Bean" or "Dear Mr. Bean".

Tip: Check multiple places for the name spelling. This is important because business owners sometimes use misspellings deliberately to identify commercial mail.

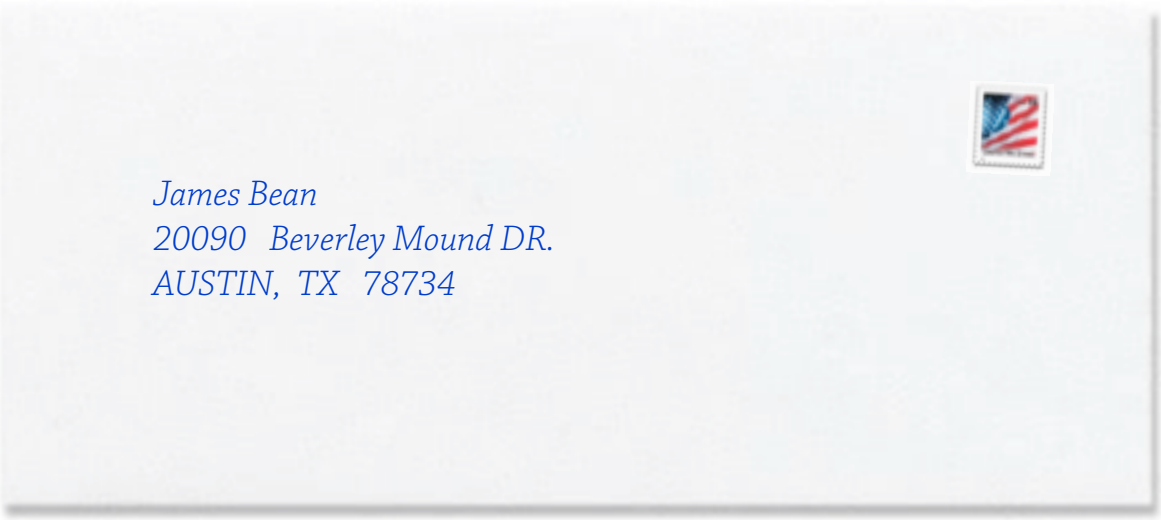
I strongly recommend you use direct mail as your first choice. Business owners are always inundated by e-mails so they have put in place various measures to deal with this. Some have set up spam filters, while others have e-mails read and deleted by gatekeepers. More important the success rate is usually much lower. Although, test both options as some niches may do better with e-mail.

The other advantage you will have is that you will set yourself apart from your competitors. These days with e-mail, text messaging, FaceBook, Twitter, etc. very few people even bother to use direct mail. Make your direct mail piece look professional and you will definitely stand out.

Do not use FedEx. It's way too expensive and doesn't have the return rate that most people claim. Nothing beats a simple white envelope! As a matter of fact, find the cheapest envelope you can buy. Now keep in mind, I'm using the example here for North America, so you may have to adapt to your region.

Use the same type of envelope you would send to your mother, grandmother, father, uncle, etc. - personal! Below is a picture of what I use.

Notice how I have made everything on the envelope look very personal.



Most important, I did not use any company names. The probability of this getting to the right person is extremely high, which is exactly what you want. That is my free direct mail tip for you that you can use forever.

The biggest problem with direct mail is reach and opt-in rate and by using the handwritten envelope and a real stamp you will address this issue. Feel confident that the direct mail will be read by the right person!

Next I have included the exact words that you want to use. Feel free to modify it to make it more personal, but this should be your starting ground. Why re-invent the wheel when we have already done all the work for you and this letter has been tested numerous times with great results.

Download Client Letter Template

Don't forget to customize this with the personalization of the prospect's first name and their website URL.

Remember to keep it as simple as possible.

You can send the same content in an e-mail if you wish.

Step 5: Fix Site & Cash Check

Security can be difficult to sell. Often people don't think about it, but wish they had if they have a break-in. Sometimes we have to use a little bit of fear to move them into an action mindset. This is not intended to scare them off, but to provide valuable information that can potentially save their company thousands of dollars. There are lots of publicly available statistics on break-ins and hacks so use these to your benefit. Share them with your prospective client to move them towards a decision.

Now, I recommend charging at least $100 per hour for this service and giving an estimate of 2 to 4 hours.

So how do you actually get all of this taken care of.

It's quite simple – review the steps in the next section of this document. It will take you less than 30 minutes to make the changes.

- Setup a backup tool for automated backups to Amazon.

- Show the client how to use LastPass (lastpass.com) – and then they will never need to remember passwords again. (This free tip will change their life and they won't stop thanking you)

Part two of this course gives you eight tests that you can do in under 30 minutes. Each test provides an easy to fix solution. As well, I have included over-the-shoulder videos that show you exactly how to do all of this.

PART TWO: THE 'HOW TO' MANUAL
- RUNNING 8 SECURITY TESTS -

Introduction

This part of the course is literally a 'How To' manual. It is designed in a way that you can learn the tests quickly and implement the solutions just as fast. Whenever you are putting the security steps into action on a website speed is very important, but so is accuracy. You want to make sure that you are clear about what you are doing.

BUT you don't need to be a security expert – and that's beauty of the training. To focus on the simple solutions that have the highest impact.

I recommend that once you have gone through the material try out the steps on one of your own websites. **Don't forget to take a backup of both the website and database**. This is just good practice and you should do this with your client sites as well. Once you feel comfortable in what you are doing you are ready to go search your leads and make some money.

Remember there are also videos for you to follow. They walk you through the process screen by screen. I have not expanded on some things as I am assuming that you have some familiarity with Wordpress. If not, inside of cpanel there are usually video tutorials that you can refer to. Use those instead of YouTube videos to ensure accuracy.

The Tests

All of the tests are broken down into 3 categories: 1. Problem - which explains why it is a concern, 2. Solution - this tells you exactly what you need to do to fix the problem, and 3. Communication With Client - this is for you to copy/paste directly into the client email or direct mail.

The video training for this section is here

Test 1: Check the Wordpress Version

PROBLEM: An out of date Wordpress version puts your website at risk. Keeping the Wordpress core up to date is one of the most important aspects of keeping your site secure. If vulnerabilities are discovered in Wordpress and a new version is released to address the issue, the information required to exploit the vulnerability is almost certainly in the public domain. This makes old versions more open to attacks and is one of the primary reasons you should always keep Wordpress up to date.

This is probably the most effective solution to put in place.

SOLUTION: Thanks to automatic updates updating is very easy. Just go to Dashboard - Updates and click "Upgrade". Remember; always backup your files and database before upgrading!

COMMUNICATION WITH CLIENT: Your Wordpress Version is out of date. Hackers deliberately look for out of date versions because they know how easy it is to exploit an issue on an old version.

Test 2: Check if the wp-config.php file is present in the default location

PROBLEM: The wp-config.php file by default in Wordpress is installed in the root directory, which is not secure. It does not need to be publicly accessible. A very common mistake made by Wordpress users. Keeping the website wp-config.php file hidden from outside of your network makes it harder for hackers to compromise your database. The reason is this is where your database password is stored. So it's the first place a hacker will look.

Check http://www.clientdomain.com/wp-config.php

SOLUTION: In order to fix this issue you have to move the **wp-config.php** file one level up in the folder structure in cpanel.
If the original location was:
/home/www/wp-config.php then move the file to: /home/wp-config.php.

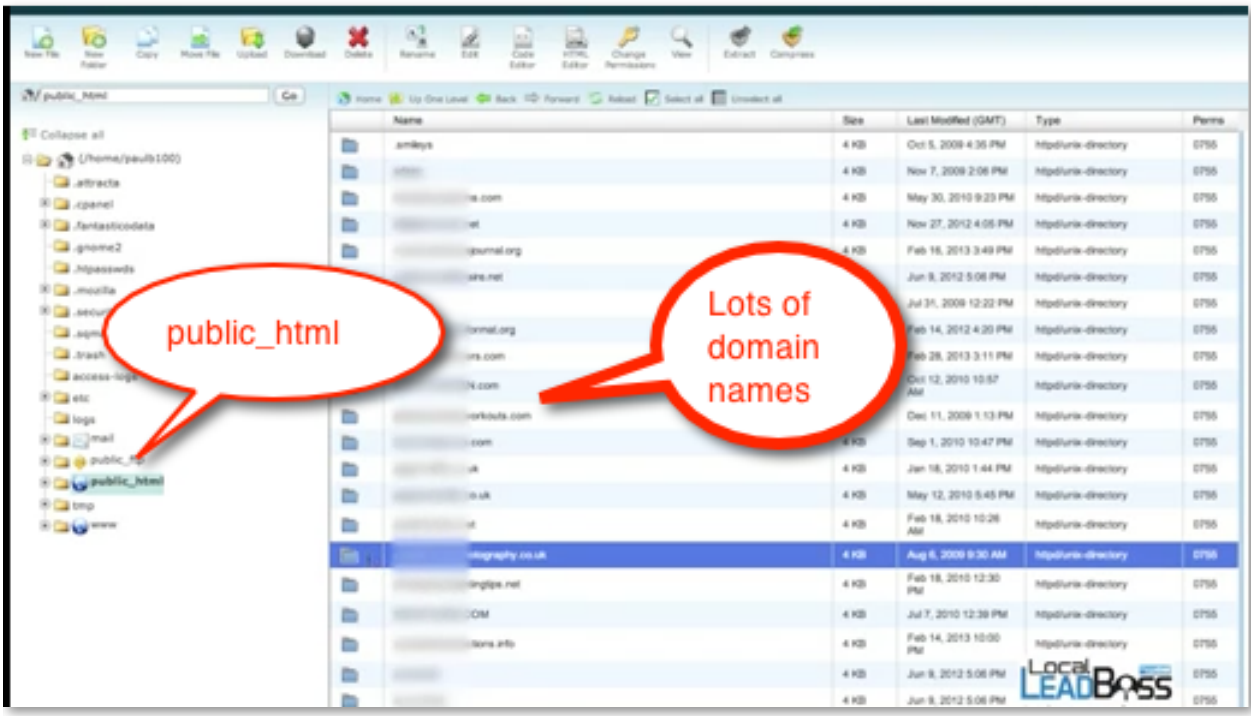
Or for instance from
/home/www/my-blog/wp-config.php to: /home/www/wp-config.php.

This can be done as a drag and drop in cpanel - watch the video.

IMPORTANT

When you login to the client's cpanel - there is a small possibility they are using shared hosting and are using an addon domain instead of normal reseller account.

When you log in you may a list of domains like this:



If this is the case then **don't** move the wp-config file. Instead simply add these 5 lines to the end of a file called .htaccess.

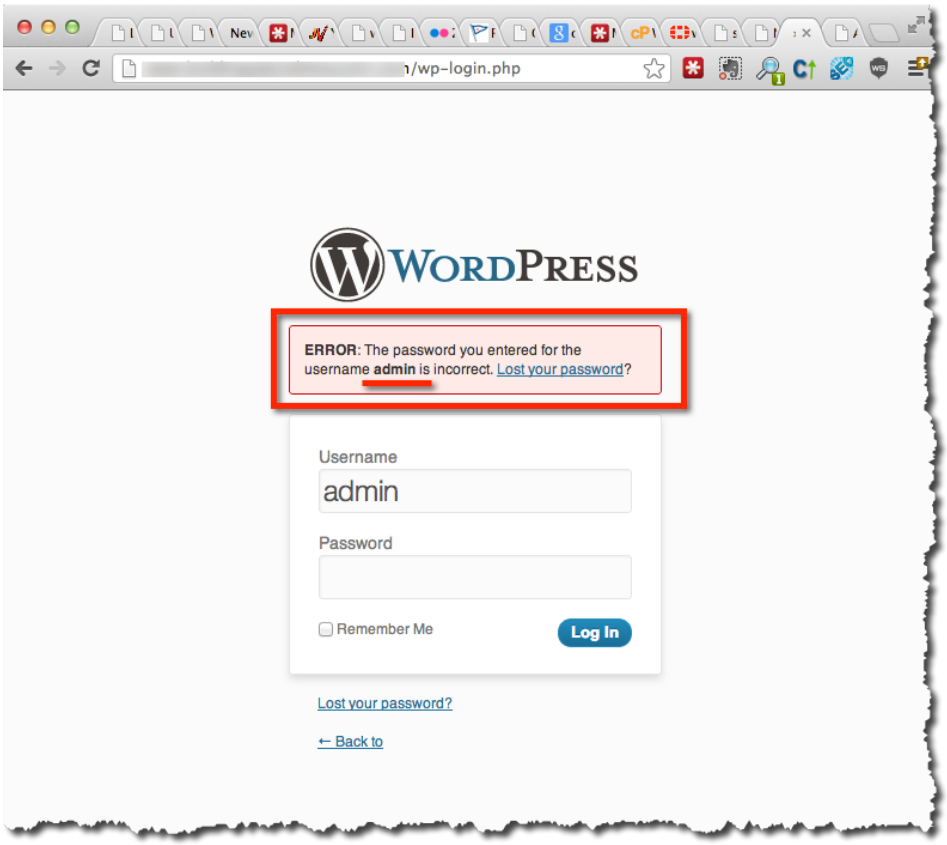
```
# protect wpconfig.php
<files wp-config.php>
order allow,deny
deny from all
</files>
```

COMMUNICATION WITH CLIENT: Your Wordpress configuration file is accessible from the Internet. What this means is that any hacker can get access to your database password if they got access to this file. This is high risk and the first place a hacker will go, so we move it out of the way.

Test 3: Check if the Username is still 'Admin'

PROBLEM: It's important to change the Wordpress username from its default setting of 'Admin'. Leaving it as 'Admin' means that potential hackers have only to guess the password. **They are already half way in.**

By default on failed login attempts Wordpress will tell you whether the username or password is wrong. An attacker can use that to find out which usernames are active on your system and then use brute-force methods to hack the password.



SOLUTION: The solution to this problem is simple. Simply create a new username and give it administrator permissions. When creating the new password make it's a complex password. (Tip: Use Lastpass.com)

Once the change has been made, simply logout and then log back in with the new username and delete the admin user account.

COMMUNICATION WITH CLIENT: Your Wordpress default username 'Admin' has NOT been changed. This makes it twice as easy for a hacker to get in.

Test 4: Is the install.php file accessible and in its default location?

PROBLEM: There have been several cases where attackers have used the install file to create access to the database. It's important to remove or move this file. Once you install WP this file becomes useless and there's no reason to keep it in the default location and accessible via HTTP.

Check http://www.clientdomain.com/wp-admin/install.php

SOLUTION: This is a very easy problem to solve. Delete or rename the *install.php* file (you'll find it in the *wp-admin* folder) to something more unique like "install-876.php"

COMMUNICATION WITH CLIENT: The Wordpress install file is still in its default location which should normally be removed as it makes it easy for the attacker to gain access to your database.

Test 5: Check if the 'Upgrade.php' script still exists

PROBLEM: There have been several cases where attackers have used the Upgrade file to create access to the database.

Check http://www.clientdomain.com/wp-admin/upgrade.php

SOLUTION: This is another easy fix. Simply remove, rename or move the file.

COMMUNICATION WITH CLIENT: The Wordpress upgrade file is accessible from outside. This file is not needed and can be used by attackers to gain access to your database.

Test 6: Is the readme.html file accessible and in the default location

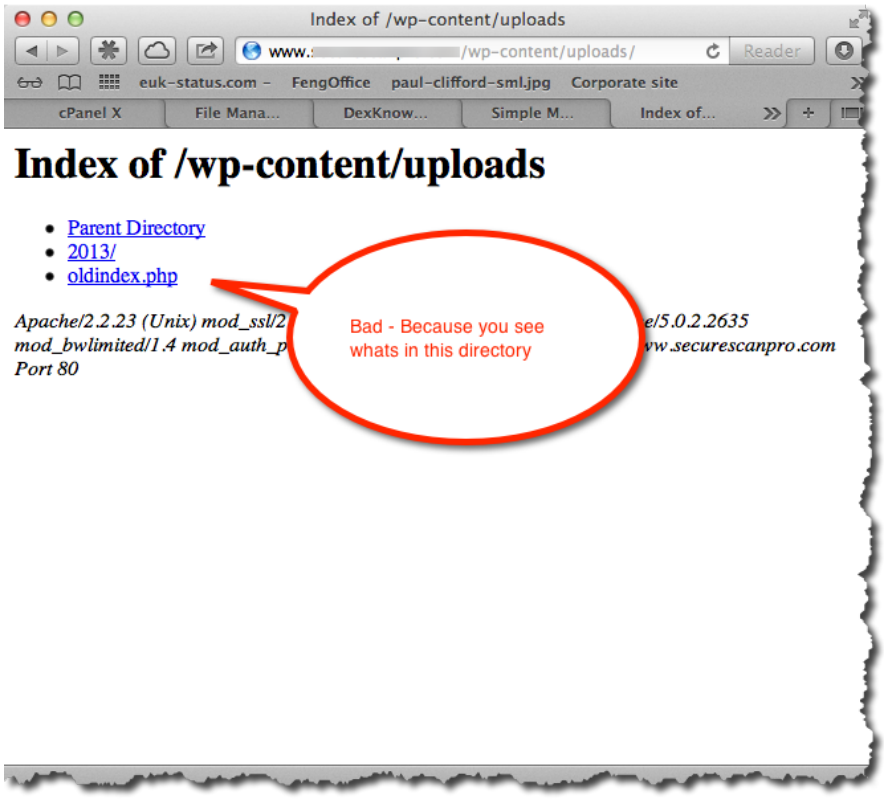
PROBLEM: You should be proud that your site is powered by Wordpress, but remember you should hide the exact version you're using. The *readme.html* file contains the WP version

information and if left on the default location (WP root) attackers can easily find out your WP version. This means it would be easy for them to identify weaknesses in your version and use them to compromise your website.

Check http://www.clientdomain.com/readme.html

SOLUTION: This too is a very easy problem to solve. Rename the file to something more unique like "readme-876.html"; delete it; move it to another location so that it's not accessible via HTTP.

COMMUNICATION WITH CLIENT: The Wordpress Readme file is accessible from the Internet. This provides an attacker with exactly what version you are running. This file is completely unnecessary.



Test 7: Check if the 'Uploads Directory' exists

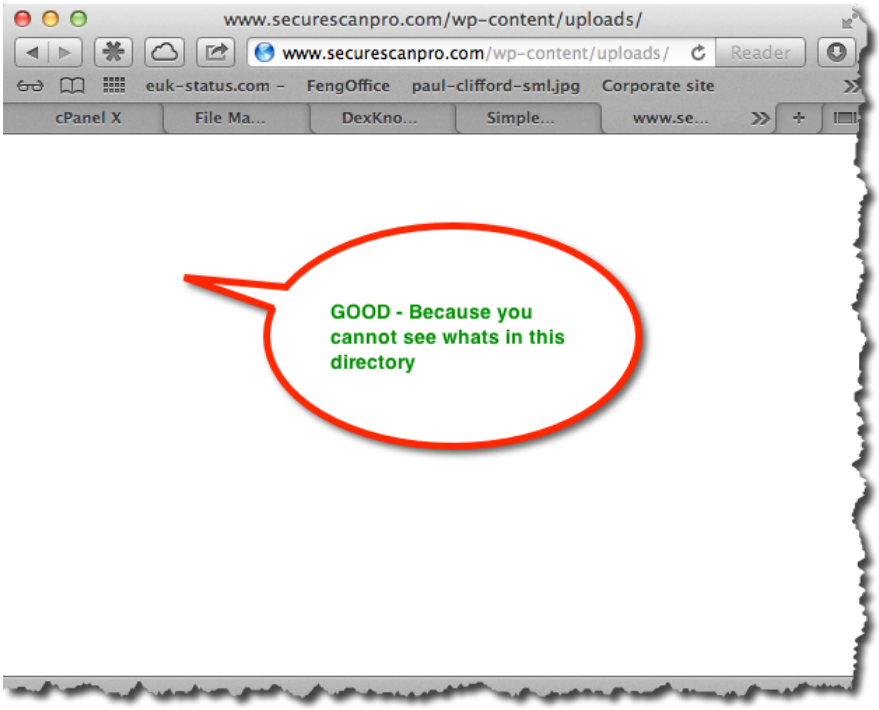
PROBLEM: The uploads directory is where Wordpress puts all user uploaded content. With this unprotected it means that anyone can see any files that have been uploaded there.

Check http://www.clientdomain.com/wp-content/uploads/

SOLUTION: There are 2 solutions. Solution 1: The simplest is to create a file called index.php in that folder. Leave the file empty, it simply needs to exist.

Solution 2: Edit the .htaccess file (found in the public_html) root directory. Simply add this line.

```
Options -Indexes
```



COMMUNICATION WITH CLIENT: The uploads directory is where Wordpress puts all user uploaded content. With this unprotected it means that anyone can see any files that have been uploaded there. This a intellectual property theft risk.

Test 8: Complete a Malware check

PROBLEM: Google maintains a directory of sites that may have been hacked or compromised and are hosting malware or dangerous code used in phishing attacks. It's important to ensure that your site is listed as safe, or it may be removed from Google's search engine.

SOLUTION: You can use the Google Safe Browsing tool to do a quick Malware check. Simply copy this URL into your browser:

http://www.google.com/safebrowsing/diagnostic?site=dailyblogtips.com

and change the blog URL at the end of the string. The results will tell you if there was any malware detected, as well as, the number of pages that were tested over the last 90 days and how many servers are hosting the site.

COMMUNICATION WITH CLIENT: Google runs a safebrowsing tool and if your site is found in it – then Google will remove you from the search engine. Therefore its critical to get your site protected.

As always, thank you for trusting us to bring you the best products in the market. I really appreciate you and want you to be successful. If you like this course leave a comment in the thread.

Remember the goal is to get in the front door and this is an angle that nobody is using. Once you are in you can begin to sell all types of services. Here are some to consider: SEO, Web Design, Mobile, FaceBook, Social Media, and Reputation Management.

All of the above checks can be automated using the LocalLeadBoss software App which runs on Mac and PC. You can watch a demo here.

Your Extra Features and Bonuses.

- ➔ Download Client Letter Template
- ➔ 3 Offline Themes Download (click here)
- ➔ Download GutWrenching Statistics
  (these are unbranded so you can include your own logo)

- ➔ Would you like An Additional 7 Themes

I have arranged with Jason Keith to give you (for free) an additional 7 Offline themes. Click here for free access:

- ➔ 4 Email Templates
- ➔ Advanced Security Training (optional)
- ➔ Register for Live Training

[Upgrade to LocalLeadBoss Software here]