RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

It's a Jungle Out There: The Security State of CMS Platforms

SESSION ID: STU-W03A

Maty Siman

Founder & CTO, CISSP
Checkmarx

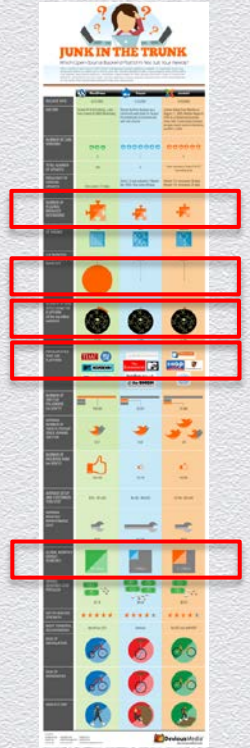
@checkmarx

CMS

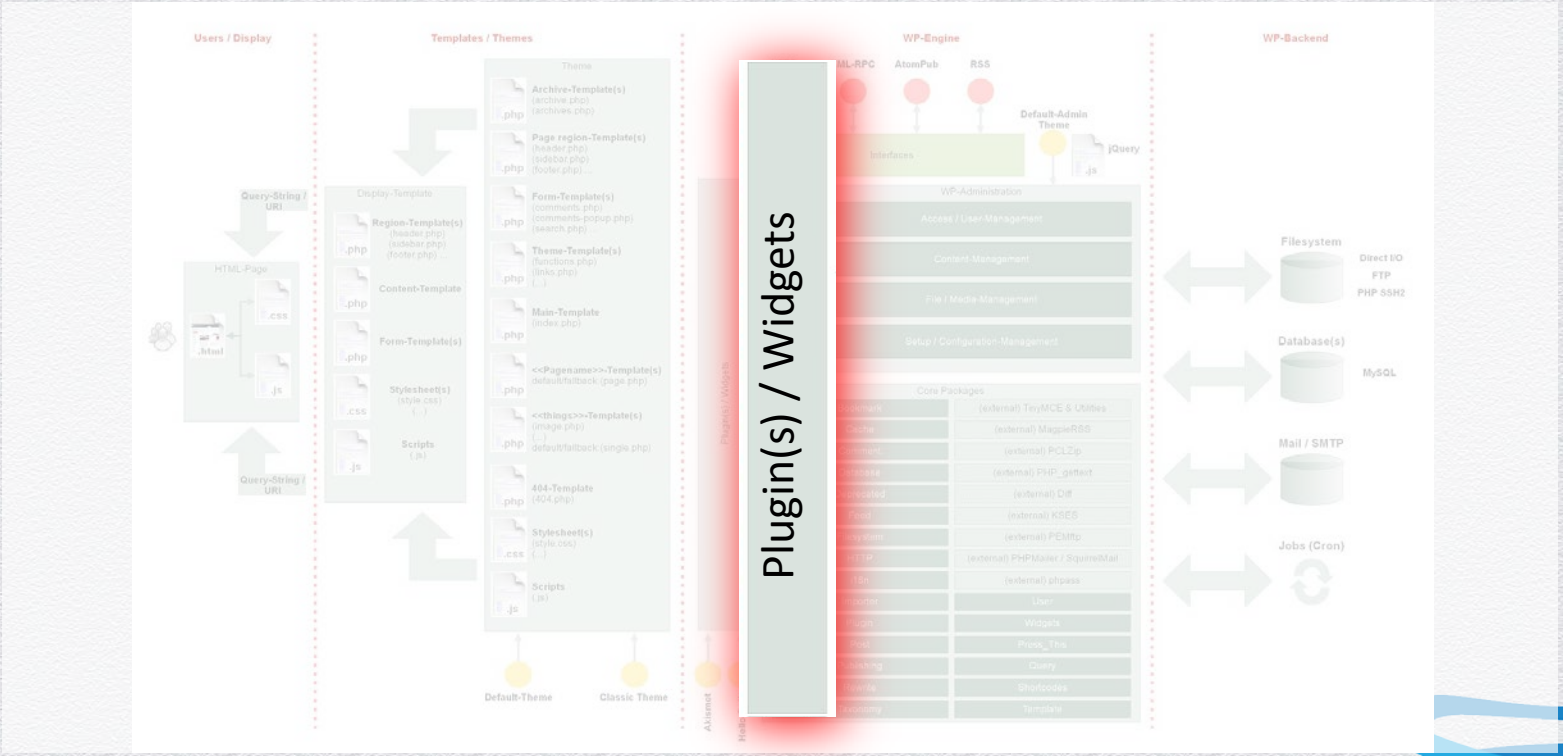
“A Content Management System (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.” (Wikipedia)

Infographics

(http://www.webnethosting.net/wordpress-vs-joomla-vs-drupal-cms-popularity-war/)



Drupal Architecture

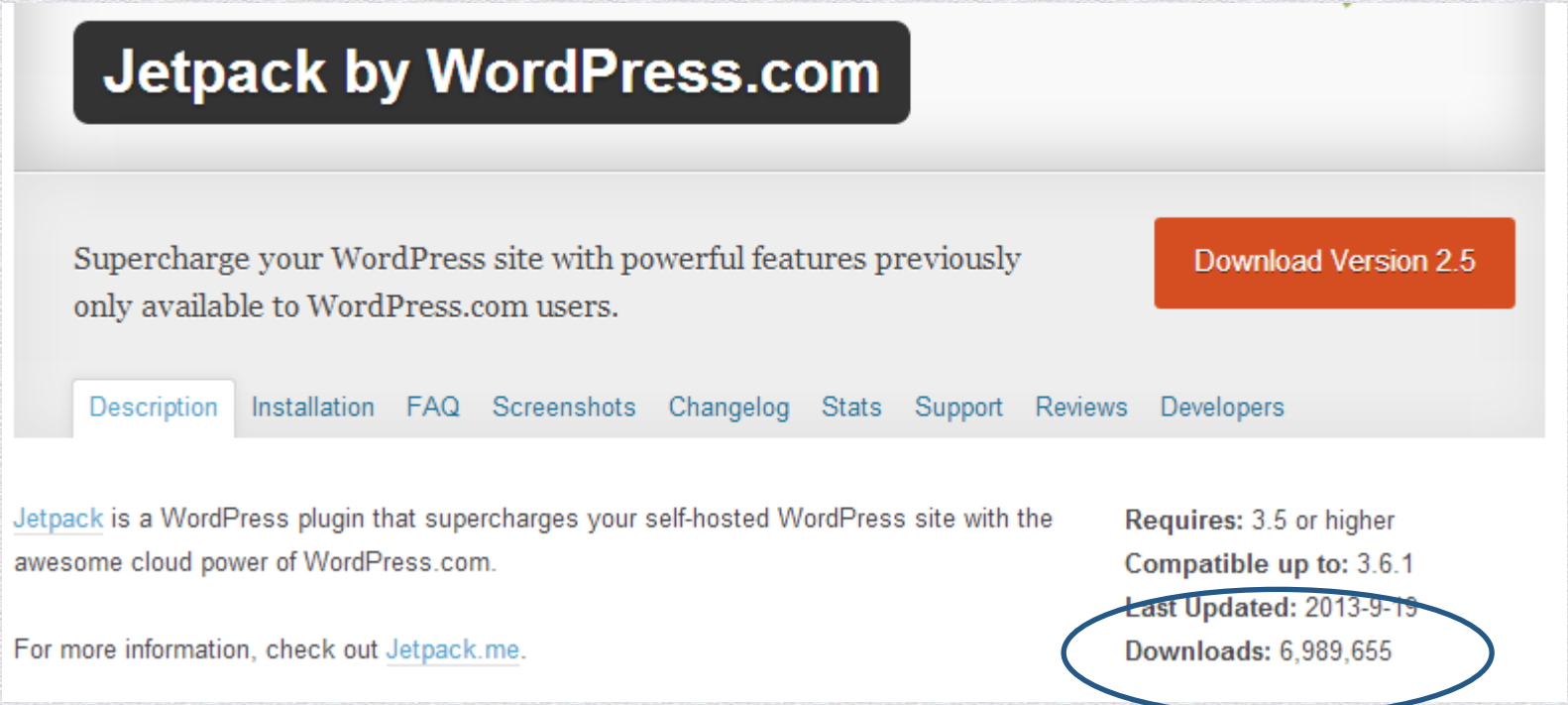


CMS Plugins

Barriers to entry are very low:

- No publishing fees
- No publishing checks
- Simple API
- PHP

Significant Exposure



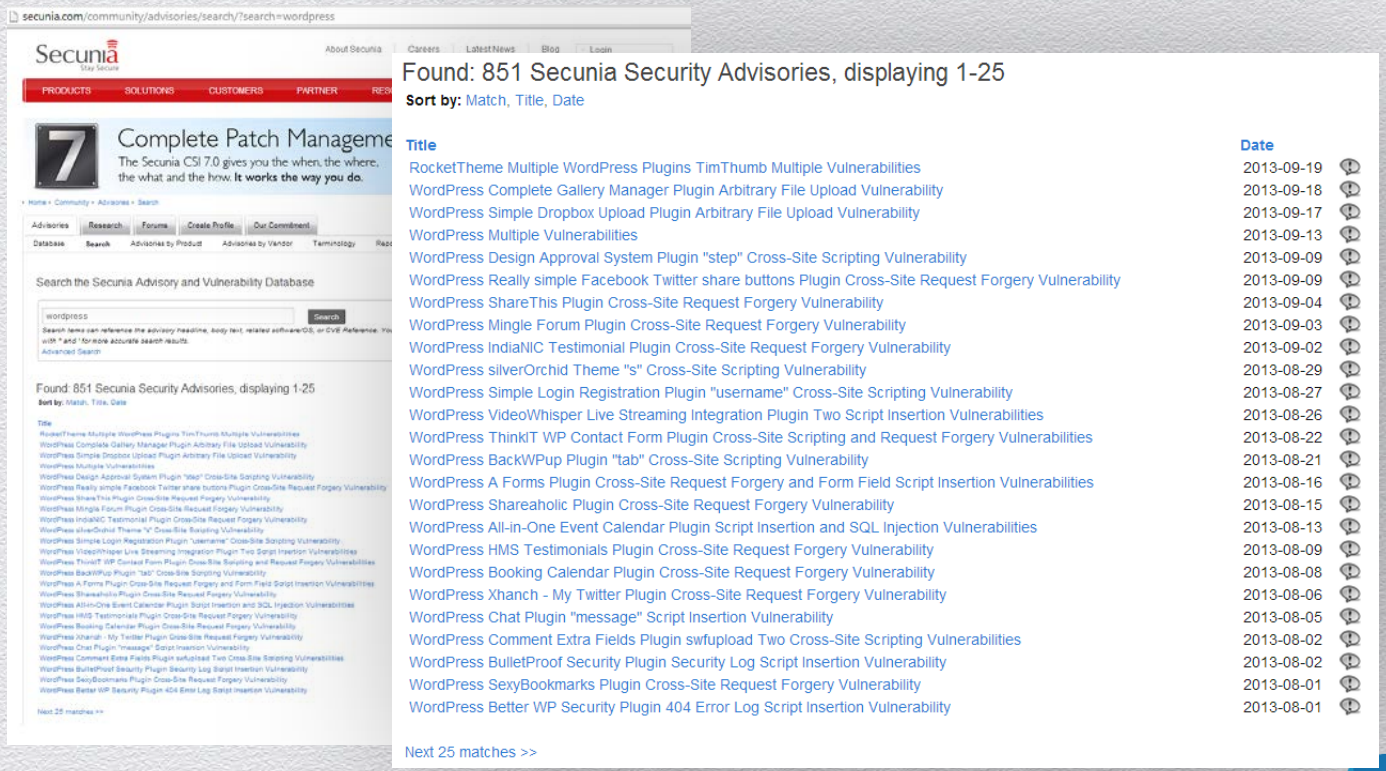
Significant Exposure

Anyone in your company can set a new WordPress instance. No need for IT personnel or R&D assistance.

1+1=?

Low Barrier + Exposure = Security Concern

Some Stats


secunia.com/community/advisories/search/?search=wordpress
Secunia
PRODUCTS
SOLUTIONS
CUSTOMERS
PARTNER
Complete Patch Manageme
The Secunia CSI 7.0 gives you the when, the where, the what and the how. It works the way you do.
Search the Secunia Advisory and Vulnerability Database
wordpress
Search
Found: 851 Secunia Security Advisories, displaying 1-25
Sort by: Match, Title, Date
Found: 851 Secunia Security Advisories, displaying 1-25
Sort by: Match, Title, Date
Title
Date
RocketTheme Multiple WordPress Plugins TimThumb Multiple Vulnerabilities 2013-09-19
WordPress Complete Gallery Manager Plugin Arbitrary File Upload Vulnerability 2013-09-18
WordPress Simple Dropbox Upload Plugin Arbitrary File Upload Vulnerability 2013-09-17
WordPress Multiple Vulnerabilities 2013-09-13
WordPress Design Approval System Plugin "step" Cross-Site Scripting Vulnerability 2013-09-09
WordPress Really simple Facebook Twitter share buttons Plugin Cross-Site Request Forgery Vulnerability 2013-09-09
WordPress ShareThis Plugin Cross-Site Request Forgery Vulnerability 2013-09-04
WordPress Mingle Forum Plugin Cross-Site Request Forgery Vulnerability 2013-09-03
WordPress IndiaNIC Testimonial Plugin Cross-Site Request Forgery Vulnerability 2013-09-02
WordPress silverOrchid Theme "s" Cross-Site Scripting Vulnerability 2013-08-29
WordPress Simple Login Registration Plugin "username" Cross-Site Scripting Vulnerability 2013-08-27
WordPress VideoWhisper Live Streaming Integration Plugin Two Script Insertion Vulnerabilities 2013-08-26
WordPress ThinkIT WP Contact Form Plugin Cross-Site Scripting and Request Forgery Vulnerabilities 2013-08-22
WordPress BackWPup Plugin "tab" Cross-Site Scripting Vulnerability 2013-08-21
WordPress A Forms Plugin Cross-Site Request Forgery and Form Field Script Insertion Vulnerabilities 2013-08-16
WordPress Shareaholic Plugin Cross-Site Request Forgery Vulnerability 2013-08-15
WordPress All-in-One Event Calendar Plugin Script Insertion and SQL Injection Vulnerabilities 2013-08-13
WordPress HMS Testimonials Plugin Cross-Site Request Forgery Vulnerability 2013-08-09
WordPress Booking Calendar Plugin Cross-Site Request Forgery Vulnerability 2013-08-08
WordPress Xhanch - My Twitter Plugin Cross-Site Request Forgery Vulnerability 2013-08-06
WordPress Chat Plugin "message" Script Insertion Vulnerability 2013-08-05
WordPress Comment Extra Fields Plugin swfupload Two Cross-Site Scripting Vulnerabilities 2013-08-02
WordPress BulletProof Security Plugin Security Log Script Insertion Vulnerability 2013-08-02
WordPress SexyBookmarks Plugin Cross-Site Request Forgery Vulnerability 2013-08-01
WordPress Better WP Security Plugin 404 Error Log Script Insertion Vulnerability 2013-08-01
Next 25 matches >>

Our report

Jan . 2013 – 30% of top 50

Feb. – Apr. – Notified 3 vendors (Automatic)

Jun. – 20% of top 50

– 7 out of 10 e-commerce

Recommendations

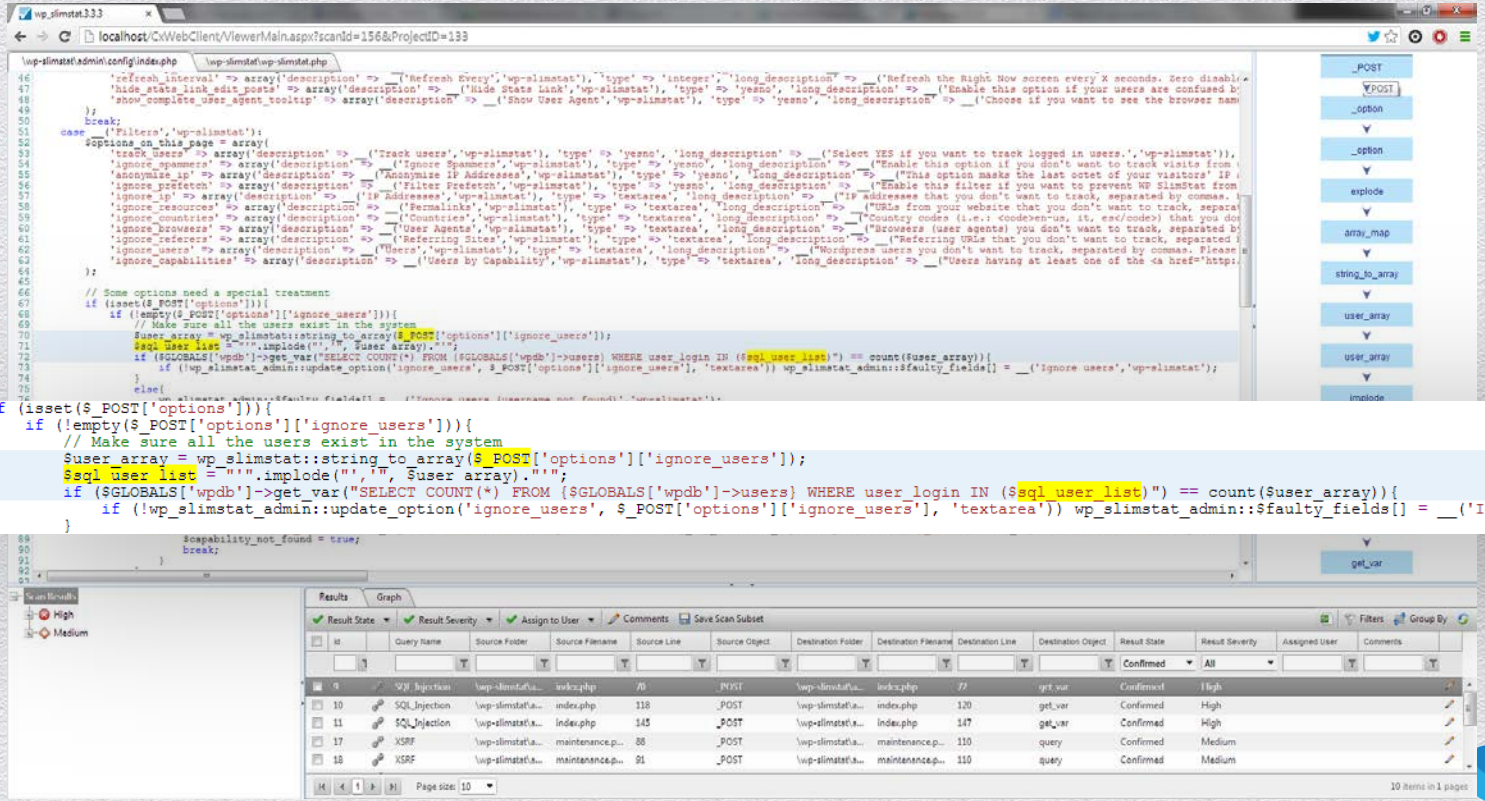
Plugin	LOC	# Downloads	SQLi	XSS	CSRF	PT
[redacted] Lists related entries	4,682	2,093,718	■			
[redacted] Tests the site for broken links and missing images	20,636	1,493,609			■	
[redacted] Add links to Facebook	8,857	1,029,626		■		
[redacted] A review system for comments	26,326	1,002,808	■	■	■	
[redacted] An RSS aggregator	15,481	622,894	■	■		
[redacted] Site backup	247,816	464,212		■		■
[redacted] Embeds Flash and HTML5 video	13,676	380,551		■		■
[redacted] Saves contact from data	22,591	372,150	■	■	■	
[redacted] An alternative WordPress editor	11,395	263,171		■		■
[redacted] Management of site statistics	3,593	152,467	■	■	■	■
[redacted] Transforms WordPress sites to mobile apps	3,820	84,863		■		

Table 1: A summary of the vulnerabilities found in the top 50 most popular general plugins (June 2013)

Plugin	LOC	# Downloads	SQLi	XSS	CSRF	PT	RFI/ LFI
[redacted] Shopping cart	22,277	519,462					
[redacted] Online store setup	39,950	380,800					
[redacted] Paypal shopping cart	1,302	274,273					
[redacted] Store management and performance	42,587	234,134					
[redacted] Store management	56,162	104,420					
[redacted] Shopping cart	42,073	98,521					
[redacted] Shopping cart	19,885	93,537					

Table 2: A summary of the vulnerabilities found in the top 10 most popular e-commerce plugins (June 2013)

SlimStat SQLi



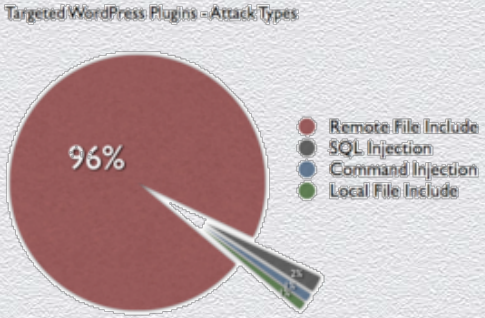
```
if (isset($_POST['options'])){
    if (!empty($_POST['options']['ignore_users'])){
        // Make sure all the users exist in the system
        $user_array = wp_slimstat::string_to_array($_POST['options']['ignore_users']);
        $sql_user_list = "'".implode("','", $user_array)."'";
        if ($GLOBALS['wpdb']->get_var("SELECT COUNT(*) FROM {$GLOBALS['wpdb']->users} WHERE user_login IN ($sql_user_list)") == count($user_array)){
            if (!wp_slimstat_admin::update_option('ignore_users', $_POST['options']['ignore_users'], 'textarea')) wp_slimstat_admin::$faulty_fields[] = __('Ignore users','wp-slimstat');
        }
```

Akamai report (Jan. 8, 2014)

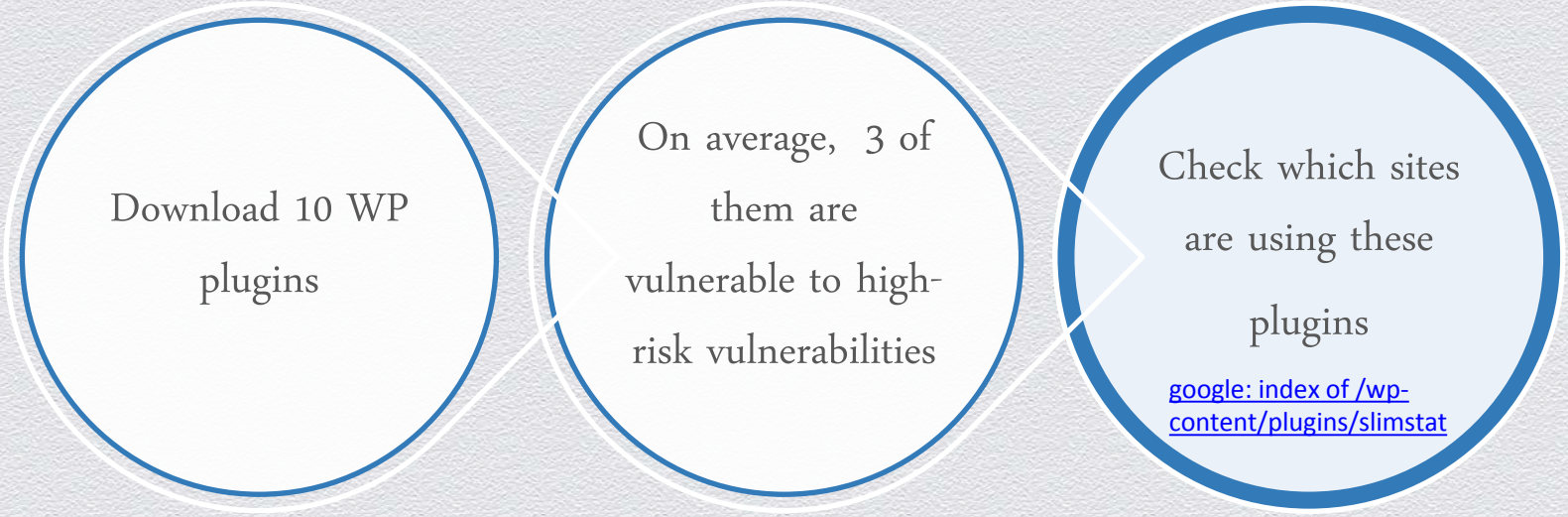
Ory Segal - https://blogs.akamai.com/2014/01/wordpress-plugins-exploitation-through-the-big-data-prism.html

- Are web hackers really targeting WordPress plugins?
- Which WordPress plugins are the most sought after by hackers?
- What types of vulnerabilities are the most coveted by hackers?

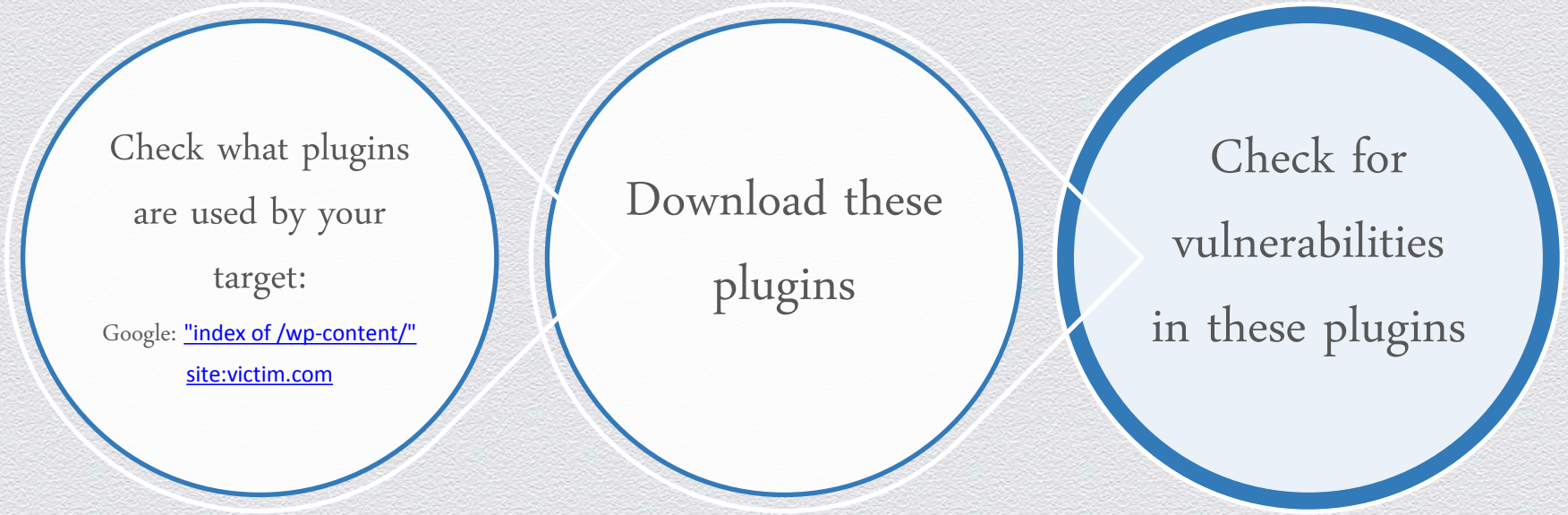
- Approximately 43,000 attacks specifically targeted WordPress plugins during a single week
- A total of 66 different WordPress plugins were targeted, out of which 8 received the lions share of attacks (see chart below)
- The "TimThumb" plugin: http://www.binarymoon.co.uk/projects/timthumb/ received a whopping 73% of all attacks



Anatomy of an attack- Widespread



Anatomy of an attack- Targeted



What should I do?

1. Ask your plugin-market owner what security measures it takes to ensure the security level of the hosted plugins
2. We found that “you get what you pay for” – commercial markets are more secure than free ones (wordpress.com VS. wordpress.org)
3. Upgrade your plugins to their latest version
4. Educate your team regarding the security risks of setting up new CMS instances

Thank you

Maty Siman

Founder & CTO at Checkmarx