

RSA[®]CONFERENCE2014

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

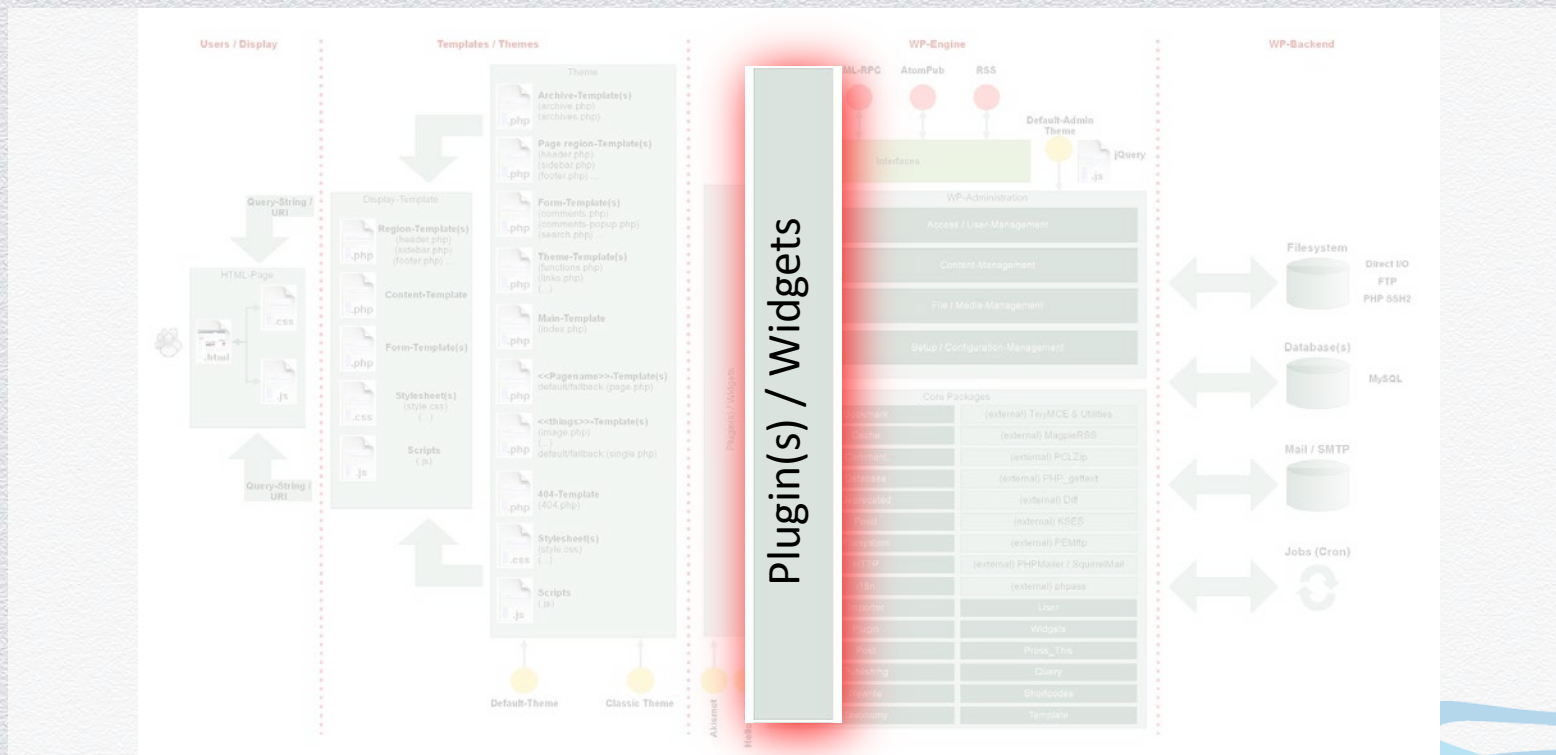
“A Content Management System (CMS) is a computer program that allows publishing, editing and modifying content as well as maintenance from a central interface.” (Wikipedia)

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

Jetpack by WordPress.com

Supercharge your WordPress site with powerful features previously only available to WordPress.com users.

[Download Version 2.5](#)

[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

[Jetpack](#) is a WordPress plugin that supercharges your self-hosted WordPress site with the awesome cloud power of WordPress.com.

For more information, check out [Jetpack.me](#).

Requires: 3.5 or higher
Compatible up to: 3.6.1
Last Updated: 2013-9-19
Downloads: 6,989,655

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
Stay Secure

PRODUCTS SOLUTIONS CUSTOMERS PARTNER RES

Complete Patch Management
The Secunia CSI 7.0 gives you the when, the where, the what and the how. It works the way you do.

Home Community Advisories Search

Advisories Research Forums Create Profile Our Community

Database Search Advisories by Product Advisories by Vendor Terminology RSS

Search the Secunia Advisory and Vulnerability Database

wordpress
Search terms can reference the advisory headline, body text, related software(CVE, or CVE Reference. You with * and / for more accurate search results.
Advanced Search

Found: 851 Secunia Security Advisories, displaying 1-25
Sort by: Match, Title, Date

Title

RocketTheme Multiple WordPress Plugins TimThumb Multiple Vulnerabilities
WordPress Complete Gallery Manager Plugin Arbitrary File Upload Vulnerability
WordPress Simple Dropbox Upload Plugin Arbitrary File Upload Vulnerability
WordPress Multiple Vulnerabilities
WordPress Design Approval System Plugin "step" Cross-Site Scripting Vulnerability
WordPress Really simple Facebook Twitter share buttons Plugin Cross-Site Request Forgery Vulnerability
WordPress ShareThis Plugin Cross-Site Request Forgery Vulnerability
WordPress Mingle Forum Plugin Cross-Site Request Forgery Vulnerability
WordPress IndiaNIC Testimonial Plugin Cross-Site Request Forgery Vulnerability
WordPress silverOrchid Theme "s" Cross-Site Scripting Vulnerability
WordPress Simple Login Registration Plugin "username" Cross-Site Scripting Vulnerability
WordPress VideoWhisper Live Streaming Integration Plugin Two Script Insertion Vulnerabilities
WordPress ThinkIT WP Contact Form Plugin Cross-Site Scripting and Request Forgery Vulnerabilities
WordPress BackWPup Plugin "tab" Cross-Site Scripting Vulnerability
WordPress A Forms Plugin Cross-Site Request Forgery and Form Field Script Insertion Vulnerabilities
WordPress Shareaholic Plugin Cross-Site Request Forgery Vulnerability
WordPress All-in-One Event Calendar Plugin Script Insertion and SQL Injection Vulnerabilities
WordPress HMS Testimonials Plugin Cross-Site Request Forgery Vulnerability
WordPress Booking Calendar Plugin Cross-Site Request Forgery Vulnerability
WordPress Xhanch - My Twitter Plugin Cross-Site Request Forgery Vulnerability
WordPress Chat Plugin "message" Script Insertion Vulnerability
WordPress Comment Extra Fields Plugin swfupload Two Cross-Site Scripting Vulnerabilities
WordPress BulletProof Security Plugin Security Log Script Insertion Vulnerability
WordPress SexyBookmarks Plugin Cross-Site Request Forgery Vulnerability
WordPress Better WP Security Plugin 404 Error Log Script Insertion Vulnerability

Next 25 matches >>

Found: 851 Secunia Security Advisories, displaying 1-25

Sort by: Match, Title, Date

Title

RocketTheme Multiple WordPress Plugins TimThumb Multiple Vulnerabilities
WordPress Complete Gallery Manager Plugin Arbitrary File Upload Vulnerability
WordPress Simple Dropbox Upload Plugin Arbitrary File Upload Vulnerability
WordPress Multiple Vulnerabilities
WordPress Design Approval System Plugin "step" Cross-Site Scripting Vulnerability
WordPress Really simple Facebook Twitter share buttons Plugin Cross-Site Request Forgery Vulnerability
WordPress ShareThis Plugin Cross-Site Request Forgery Vulnerability
WordPress Mingle Forum Plugin Cross-Site Request Forgery Vulnerability
WordPress IndiaNIC Testimonial Plugin Cross-Site Request Forgery Vulnerability
WordPress silverOrchid Theme "s" Cross-Site Scripting Vulnerability
WordPress Simple Login Registration Plugin "username" Cross-Site Scripting Vulnerability
WordPress VideoWhisper Live Streaming Integration Plugin Two Script Insertion Vulnerabilities
WordPress ThinkIT WP Contact Form Plugin Cross-Site Scripting and Request Forgery Vulnerabilities
WordPress BackWPup Plugin "tab" Cross-Site Scripting Vulnerability
WordPress A Forms Plugin Cross-Site Request Forgery and Form Field Script Insertion Vulnerabilities
WordPress Shareaholic Plugin Cross-Site Request Forgery Vulnerability
WordPress All-in-One Event Calendar Plugin Script Insertion and SQL Injection Vulnerabilities
WordPress HMS Testimonials Plugin Cross-Site Request Forgery Vulnerability
WordPress Booking Calendar Plugin Cross-Site Request Forgery Vulnerability
WordPress Xhanch - My Twitter Plugin Cross-Site Request Forgery Vulnerability
WordPress Chat Plugin "message" Script Insertion Vulnerability
WordPress Comment Extra Fields Plugin swfupload Two Cross-Site Scripting Vulnerabilities
WordPress BulletProof Security Plugin Security Log Script Insertion Vulnerability
WordPress SexyBookmarks Plugin Cross-Site Request Forgery Vulnerability
WordPress Better WP Security Plugin 404 Error Log Script Insertion Vulnerability

Date

2013-09-19
2013-09-18
2013-09-17
2013-09-17
2013-09-13
2013-09-09
2013-09-09
2013-09-09
2013-09-04
2013-09-03
2013-09-02
2013-08-29
2013-08-27
2013-08-26
2013-08-22
2013-08-21
2013-08-16
2013-08-15
2013-08-13
2013-08-09
2013-08-08
2013-08-06
2013-08-05
2013-08-02
2013-08-02
2013-08-01
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

The screenshot displays the SlimStat SQLi exploit interface. The top section shows the exploit code in a text editor, which includes configuration options for the exploit, such as the refresh interval, hide stats link, and show complete user agent tooltip. The code also includes a function to update the 'ignore_users' option in the SlimStat database. The right side of the interface features a control panel with buttons for various actions: _POST, _POST, _option, _option, explode, array_map, string_to_array, user_array, user_array, and implode. The bottom section shows the results of the exploit, including a table with columns for ID, Query Name, Source Folder, Source Filename, Source Line, Source Object, Destination Folder, Destination Filename, Destination Line, Destination Object, Result State, Result Severity, Assigned User, and Comments. The table lists several successful SQLi attacks, including SQL Injection, SQLi Injection, and XSSF, with their respective source and destination files and lines.

```
wp-slimstat.admin.config/index.php wp-slimstat/wp-slimstat.php
46 'refresh_interval' => array('description' => __('Refresh Every','wp-slimstat'), 'type' => 'integer', 'long_description' => __('Refresh the Right Now screen every X seconds. Zero disables'),
47 'hide_stats_link_edit_posts' => array('description' => __('Hide Stats Link','wp-slimstat'), 'type' => 'yesno', 'long_description' => __('Enable this option if your users are confused by'),
48 'show_complete_user_agent_tooltip' => array('description' => __('Show User Agent','wp-slimstat'), 'type' => 'yesno', 'long_description' => __('Choose if you want to see the browser name'));
49 break;
50 case 'filters': 'wp-slimstat':
51     $options_on_this_page = array(
52         'track_users' => array('description' => __('Track users','wp-slimstat'), 'type' => 'yesno', 'long_description' => __('Select YES if you want to track logged in users.','wp-slimstat')),
53         'ignore_spammers' => array('description' => __('Ignore Spammers','wp-slimstat'), 'type' => 'yesno', 'long_description' => __('Enable this option if you don't want to track visits from IP addresses that you don't want to track, separated by comma.')),
54         'anonymous_ip' => array('description' => __('Anonymous IP Addresses','wp-slimstat'), 'type' => 'yesno', 'long_description' => __('This option marks the last octet of your visitors' IP.')),
55         'ignore_prefetch' => array('description' => __('Filter Prefetch','wp-slimstat'), 'type' => 'yesno', 'long_description' => __('Enable this filter if you want to prevent WP SlimStat from tracking prefetch requests.')),
56         'ignore_ip' => array('description' => __('IP Addresses','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('IP addresses that you don't want to track, separated by comma.')),
57         'ignore_resources' => array('description' => __('Permalinks','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('URLs from your website that you don't want to track, separated by comma.')),
58         'ignore_countries' => array('description' => __('Countries','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('Country codes (i.e.: <code>en-us, it, es</code>) that you don't want to track, separated by comma.')),
59         'ignore_browsers' => array('description' => __('User Agents','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('Browsers (user agents) you don't want to track, separated by comma.')),
60         'ignore_referrals' => array('description' => __('Referring Sites','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('Referring URLs that you don't want to track, separated by comma.')),
61         'ignore_users' => array('description' => __('Users','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('WordPress users you don't want to track, separated by comma. Please use the format: <code>user@example.com</code>.')),
62         'ignore_capabilities' => array('description' => __('Users by Capability','wp-slimstat'), 'type' => 'textarea', 'long_description' => __('Users having at least one of the <a href="http://codex.wordpress.org/Role-Based-Access-Control">capabilities</a> that you don't want to track, separated by comma.'));
63     };
64 // Some options need a special treatment
65 if (isset($POST['options'])) {
66     if (isset($POST['options']['ignore_users'])) {
67         // Make sure all the users exist in the system
68         $user_array = wp_slimstat::string_to_array($POST['options']['ignore_users']);
69         $sql_user_list = implode("','", $user_array);
70         if ($GLOBALS['wpdb']->get_var("SELECT COUNT(*) FROM ($GLOBALS['wpdb']->users) WHERE user_login IN ($sql_user_list)") == count($user_array)) {
71             if (!wp_slimstat_admin::update_option('ignore_users', $POST['options']['ignore_users'], 'textarea')) wp_slimstat_admin::$faulty_fields[] = __('Ignore users','wp-slimstat');
72         } else {
73             wp_slimstat_admin::$faulty_fields[] = __('Ignore users (usernames not found)','wp-slimstat');
74         }
75     }
76 }
77 if (isset($POST['options'])) {
78     if (isset($POST['options']['ignore_users'])) {
79         // Make sure all the users exist in the system
80         $user_array = wp_slimstat::string_to_array($POST['options']['ignore_users']);
81         $sql_user_list = implode("','", $user_array);
82         if ($GLOBALS['wpdb']->get_var("SELECT COUNT(*) FROM ($GLOBALS['wpdb']->users) WHERE user_login IN ($sql_user_list)") == count($user_array)) {
83             if (!wp_slimstat_admin::update_option('ignore_users', $POST['options']['ignore_users'], 'textarea')) wp_slimstat_admin::$faulty_fields[] = __('Ignore users','wp-slimstat');
84         }
85     }
86 }
87 $capability_not_found = true;
88 break;
89 }
90 }
91 }
92 }
93 }
94 }
95 }
96 }
97 }
98 }
99 }
100 }
101 }
102 }
103 }
104 }
105 }
106 }
107 }
108 }
109 }
110 }
111 }
112 }
113 }
114 }
115 }
116 }
117 }
118 }
119 }
120 }
121 }
122 }
123 }
124 }
125 }
126 }
127 }
128 }
129 }
130 }
131 }
132 }
133 }
134 }
135 }
136 }
137 }
138 }
139 }
140 }
141 }
142 }
143 }
144 }
145 }
146 }
147 }
148 }
149 }
150 }
151 }
152 }
153 }
154 }
155 }
156 }
157 }
158 }
159 }
160 }
161 }
162 }
163 }
164 }
165 }
166 }
167 }
168 }
169 }
170 }
171 }
172 }
173 }
174 }
175 }
176 }
177 }
178 }
179 }
180 }
181 }
182 }
183 }
184 }
185 }
186 }
187 }
188 }
189 }
190 }
191 }
192 }
193 }
194 }
195 }
196 }
197 }
198 }
199 }
200 }
201 }
202 }
203 }
204 }
205 }
206 }
207 }
208 }
209 }
210 }
211 }
212 }
213 }
214 }
215 }
216 }
217 }
218 }
219 }
220 }
221 }
222 }
223 }
224 }
225 }
226 }
227 }
228 }
229 }
230 }
231 }
232 }
233 }
234 }
235 }
236 }
237 }
238 }
239 }
240 }
241 }
242 }
243 }
244 }
245 }
246 }
247 }
248 }
249 }
250 }
251 }
252 }
253 }
254 }
255 }
256 }
257 }
258 }
259 }
260 }
261 }
262 }
263 }
264 }
265 }
266 }
267 }
268 }
269 }
270 }
271 }
272 }
273 }
274 }
275 }
276 }
277 }
278 }
279 }
280 }
281 }
282 }
283 }
284 }
285 }
286 }
287 }
288 }
289 }
290 }
291 }
292 }
293 }
294 }
295 }
296 }
297 }
298 }
299 }
300 }
301 }
302 }
303 }
304 }
305 }
306 }
307 }
308 }
309 }
310 }
311 }
312 }
313 }
314 }
315 }
316 }
317 }
318 }
319 }
320 }
321 }
322 }
323 }
324 }
325 }
326 }
327 }
328 }
329 }
330 }
331 }
332 }
333 }
334 }
335 }
336 }
337 }
338 }
339 }
340 }
341 }
342 }
343 }
344 }
345 }
346 }
347 }
348 }
349 }
350 }
351 }
352 }
353 }
354 }
355 }
356 }
357 }
358 }
359 }
360 }
361 }
362 }
363 }
364 }
365 }
366 }
367 }
368 }
369 }
370 }
371 }
372 }
373 }
374 }
375 }
376 }
377 }
378 }
379 }
380 }
381 }
382 }
383 }
384 }
385 }
386 }
387 }
388 }
389 }
390 }
391 }
392 }
393 }
394 }
395 }
396 }
397 }
398 }
399 }
400 }
401 }
402 }
403 }
404 }
405 }
406 }
407 }
408 }
409 }
410 }
411 }
412 }
413 }
414 }
415 }
416 }
417 }
418 }
419 }
420 }
421 }
422 }
423 }
424 }
425 }
426 }
427 }
428 }
429 }
430 }
431 }
432 }
433 }
434 }
435 }
436 }
437 }
438 }
439 }
440 }
441 }
442 }
443 }
444 }
445 }
446 }
447 }
448 }
449 }
450 }
451 }
452 }
453 }
454 }
455 }
456 }
457 }
458 }
459 }
460 }
461 }
462 }
463 }
464 }
465 }
466 }
467 }
468 }
469 }
470 }
471 }
472 }
473 }
474 }
475 }
476 }
477 }
478 }
479 }
480 }
481 }
482 }
483 }
484 }
485 }
486 }
487 }
488 }
489 }
490 }
491 }
492 }
493 }
494 }
495 }
496 }
497 }
498 }
499 }
500 }
501 }
502 }
503 }
504 }
505 }
506 }
507 }
508 }
509 }
510 }
511 }
512 }
513 }
514 }
515 }
516 }
517 }
518 }
519 }
520 }
521 }
522 }
523 }
524 }
525 }
526 }
527 }
528 }
529 }
530 }
531 }
532 }
533 }
534 }
535 }
536 }
537 }
538 }
539 }
540 }
541 }
542 }
543 }
544 }
545 }
546 }
547 }
548 }
549 }
550 }
551 }
552 }
553 }
554 }
555 }
556 }
557 }
558 }
559 }
560 }
561 }
562 }
563 }
564 }
565 }
566 }
567 }
568 }
569 }
570 }
571 }
572 }
573 }
574 }
575 }
576 }
577 }
578 }
579 }
580 }
581 }
582 }
583 }
584 }
585 }
586 }
587 }
588 }
589 }
590 }
591 }
592 }
593 }
594 }
595 }
596 }
597 }
598 }
599 }
600 }
601 }
602 }
603 }
604 }
605 }
606 }
607 }
608 }
609 }
610 }
611 }
612 }
613 }
614 }
615 }
616 }
617 }
618 }
619 }
620 }
621 }
622 }
623 }
624 }
625 }
626 }
627 }
628 }
629 }
630 }
631 }
632 }
633 }
634 }
635 }
636 }
637 }
638 }
639 }
640 }
641 }
642 }
643 }
644 }
645 }
646 }
647 }
648 }
649 }
650 }
651 }
652 }
653 }
654 }
655 }
656 }
657 }
658 }
659 }
660 }
661 }
662 }
663 }
664 }
665 }
666 }
667 }
668 }
669 }
670 }
671 }
672 }
673 }
674 }
675 }
676 }
677 }
678 }
679 }
680 }
681 }
682 }
683 }
684 }
685 }
686 }
687 }
688 }
689 }
690 }
691 }
692 }
693 }
694 }
695 }
696 }
697 }
698 }
699 }
700 }
701 }
702 }
703 }
704 }
705 }
706 }
707 }
708 }
709 }
710 }
711 }
712 }
713 }
714 }
715 }
716 }
717 }
718 }
719 }
720 }
721 }
722 }
723 }
724 }
725 }
726 }
727 }
728 }
729 }
730 }
731 }
732 }
733 }
734 }
735 }
736 }
737 }
738 }
739 }
740 }
741 }
742 }
743 }
744 }
745 }
746 }
747 }
748 }
749 }
750 }
751 }
752 }
753 }
754 }
755 }
756 }
757 }
758 }
759 }
760 }
761 }
762 }
763 }
764 }
765 }
766 }
767 }
768 }
769 }
770 }
771 }
772 }
773 }
774 }
775 }
776 }
777 }
778 }
779 }
780 }
781 }
782 }
783 }
784 }
785 }
786 }
787 }
788 }
789 }
790 }
791 }
792 }
793 }
794 }
795 }
796 }
797 }
798 }
799 }
800 }
801 }
802 }
803 }
804 }
805 }
806 }
807 }
808 }
809 }
810 }
811 }
812 }
813 }
814 }
815 }
816 }
817 }
818 }
819 }
820 }
821 }
822 }
823 }
824 }
825 }
826 }
827 }
828 }
829 }
830 }
831 }
832 }
833 }
834 }
835 }
836 }
837 }
838 }
839 }
840 }
841 }
842 }
843 }
844 }
845 }
846 }
847 }
848 }
849 }
850 }
851 }
852 }
853 }
854 }
855 }
856 }
857 }
858 }
859 }
860 }
861 }
862 }
863 }
864 }
865 }
866 }
867 }
868 }
869 }
870 }
871 }
872 }
873 }
874 }
875 }
876 }
877 }
878 }
879 }
880 }
881 }
882 }
883 }
884 }
885 }
886 }
887 }
888 }
889 }
890 }
891 }
892 }
893 }
894 }
895 }
896 }
897 }
898 }
899 }
900 }
901 }
902 }
903 }
904 }
905 }
906 }
907 }
908 }
909 }
910 }
911 }
912 }
913 }
914 }
915 }
916 }
917 }
918 }
919 }
920 }
921 }
922 }
923 }
924 }
925 }
926 }
927 }
928 }
929 }
930 }
931 }
932 }
933 }
934 }
935 }
936 }
937 }
938 }
939 }
940 }
941 }
942 }
943 }
944 }
945 }
946 }
947 }
948 }
949 }
950 }
951 }
952 }
953 }
954 }
955 }
956 }
957 }
958 }
959 }
960 }
961 }
962 }
963 }
964 }
965 }
966 }
967 }
968 }
969 }
970 }
971 }
972 }
973 }
974 }
975 }
976 }
977 }
978 }
979 }
980 }
981 }
982 }
983 }
984 }
985 }
986 }
987 }
988 }
989 }
990 }
991 }
992 }
993 }
994 }
995 }
996 }
997 }
998 }
999 }
```

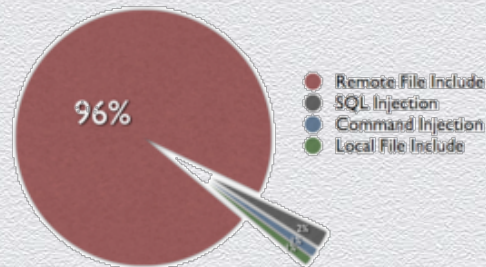
ID	Query Name	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination Filename	Destination Line	Destination Object	Result State	Result Severity	Assigned User	Comments
9	SQL Injection	wp-slimstat...	index.php	118	_POST	wp-slimstat...	index.php	118	get_var	Confirmed	High		
10	SQL Injection	wp-slimstat...	index.php	138	_POST	wp-slimstat...	index.php	120	get_var	Confirmed	High		
11	SQL Injection	wp-slimstat...	index.php	143	_POST	wp-slimstat...	index.php	147	get_var	Confirmed	High		
17	XSRF	wp-slimstat...	maintenance.p...	88	_POST	wp-slimstat...	maintenance.p...	110	query	Confirmed	Medium		
18	XSRF	wp-slimstat...	maintenance.p...	91	_POST	wp-slimstat...	maintenance.p...	110	query	Confirmed	Medium		

Akamai report (Jan. 8, 2014)

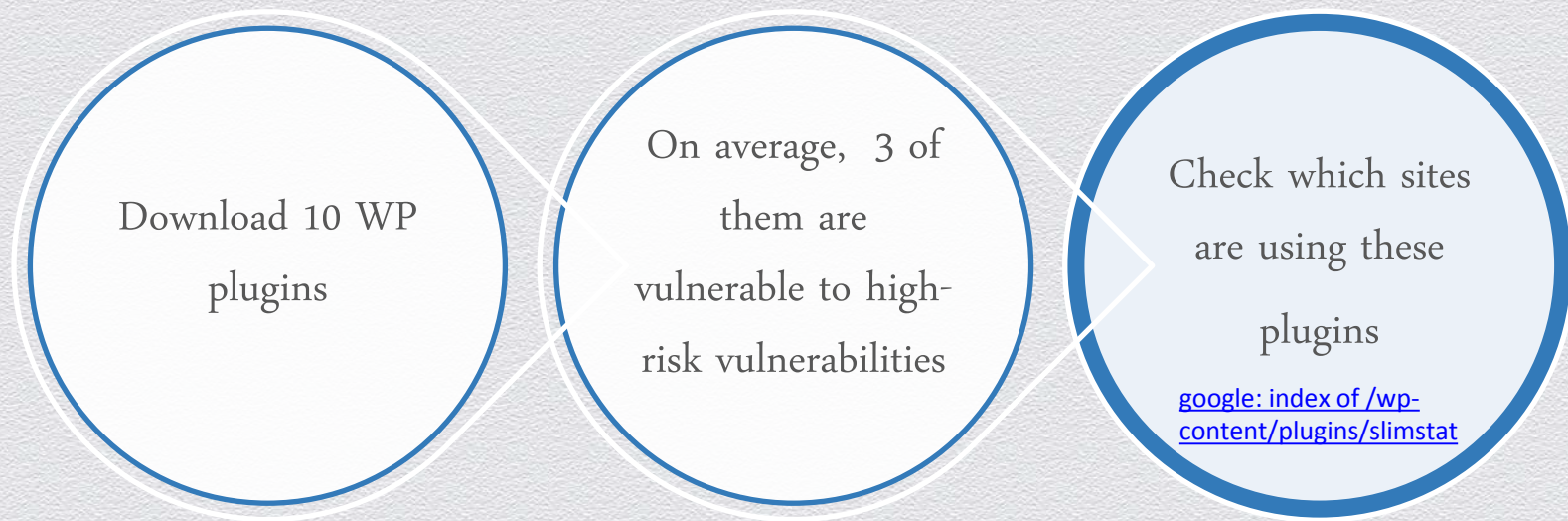
Ory Segal - <https://blogs.akamai.com/2014/01/wordpress-plugins-exploitation-through-the-big-data-prism.html>

- 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

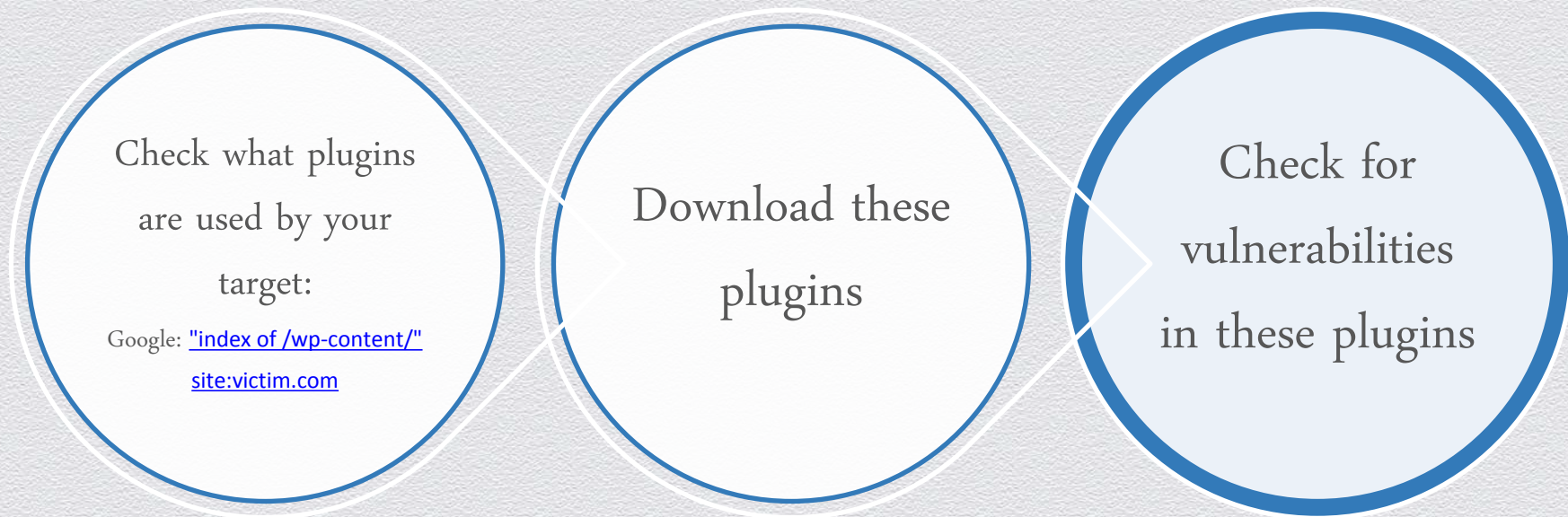
Targeted WordPress Plugins - Attack Types



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



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank you

Maty Siman

Founder & CTO at Checkmarx