

Forum:[Hack Forums](#)

Thread: [PHP static code analysis vs ~1000 top WP plugins = 103 vulnerable plugins found](#)

SIM-2902786 - November 24, 2015, 8:27 pm

"???? Introduction

I've been making php static code analysis tool for a while and few months ago I ran it against ~1000 (more or less) top wordpress plugins.

Scanning results were manually verified in my spare time and delivered to official plugins@wordpress.org from 04.07.2015 to 31.08.2015. Most of reported plugins are already patched, some are not. Vulnerable and not patched plugins are already removed from official wordpress plugin repository.

???? Results

103 plugins vulnerable with more than 4.000.000 active installations in total (~30.000.000 downloads)"

To read further, visit:

<http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-plugins.html>

Vellichor - November 24, 2015, 9:12 pm

Extremely impressive. Have you considered implementing more logical attacks such as Race Conditioning?

?Criminal - November 25, 2015, 6:07 am

you copied this from r/netsec/, its pretty funny someone else is subscribed to their feed but anyways race conditions would be hard to check for in static analysis you would have to do it dynamically to spam http requests till an interesting end result occurs. Unless your cinu? if you are big fan of your post its interesting how your custom analyzer found so many vulns it motivated me to work on my own.

Roz225 - November 25, 2015, 6:39 am

Awesome project! don't give up mate :)

Viktory - November 25, 2015, 10:00 am

Great project, if you're the author. I remember seeing similar analysis on rent-a-webdev website's codes. Let me see if I can find it.

(Nov 24, 2015 10:12 PM)Vellichor Wrote: [\[CITE\]](#) Extremely impressive. Have you considered implementing more logical attacks such as Race Conditioning?wuz gud =]