Forum:Hack Forums

Thread: Finding Php Shell Scripts In Your Website

DarkMethods - *August 9, 2015, 4:34 am*

Here is a simple bash shell script that will search your public_html directories for common file names as well as search all files for common methods used for shell scripts using the fastest possible method with a large number of files. It will dump the results to a file called "php_backdoors" which you can examine to determine what is and what is not a false positive.

To use this shell script just paste this into a file called checker.sh in the directory before your public_html folder, then run it with the following command:
sh checker.sh

Here it's code.
Code #!/bin/bash

cd public_html/

find . -type f \(-iname "1.*" -o -iname "sh.php" \) -print0 >> ../php_backdoors

find . -type f \(-iname "*.php" -o -iname "*.inc" \) -print0 | xargs -0 -r grep -REn \

'(c99|r57|exif_read_data|extract|passthru|shell_ex ec|base64_decode|fopen|fclose|eval|Refresh|refresh |justrulz)' >> ../php_backdoors

find . -type f \(-iname "*.gif" -o -iname "*.jpg" -o -iname "*.jpeg" \) -print0 | xargs -0 -r grep -REn \
'(eval|base64_decode)' >> ../image_backdoors

xorl - *August 9, 2015, 10:15 am*

lol that's shittiest php shell detector i've ever seen

IDK - *August 9, 2015, 1:14 pm*

(Aug 9, 2015 10:15 AM)xorl Wrote: *[CITE]* lol that's shittiest php shell detector i've ever seen
can't agree with you more ??

Th3PonyWizard - *August 9, 2015, 1:18 pm*

(Aug 9, 2015 10:15 AM)xorl Wrote: *[CITE]* lol that's shittiest php shell detector i've ever seenThis is scratching the top when you're scanning your site from outside the PHP system. This is not the correct way to approach this.

ras4sc - *August 9, 2015, 3:59 pm*

This will pick up the most common web shells.. nothing wrong with this

Manipulate - *August 13, 2015, 11:09 pm*

Let me just rename mt file to TO0R.php ok fixed now its undetectable (rofl)

ProblemSolva - *August 14, 2015, 1:36 am*

This will only find skid shells, who doesnt know how to hide a shell.

Th3PonyWizard - *August 14, 2015, 4:01 am*

Quote:justrulz
I don't get this one, halp

Disparity - *August 15, 2015, 3:45 am*

(Aug 9, 2015 04:34 AM)DarkMethods Wrote: [CITE] Here is a simple bash shell script that will search your public_html directories for common file names as well as search all files for common methods used for shell scripts using the fastest possible method with a large number of files.
It's fast because it has nothing to it.