

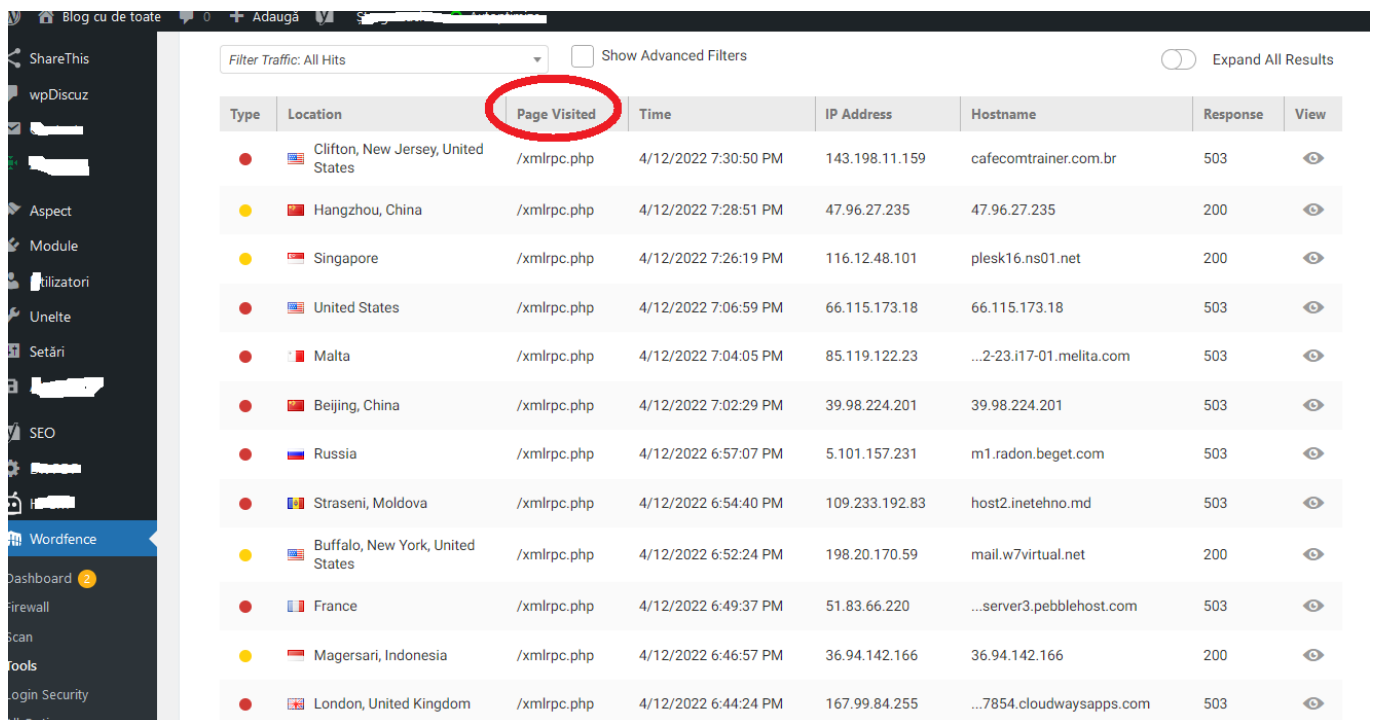
Folosești WordPress? Atenție la fișierul xmlrpc.php

Folosești WordPress pentru blogul tău? Atunci trebuie să fii atent la fișierul *xmlrpc.php*.

Acesta poate fi ținta atacurilor hackerilor care vor să preia controlul asupra blogului tău.

Ce este XLM-RPC?

XLM-RPC este o caracteristică a WordPress care permite postarea de articole direct pe blog, de pe un smartphone precum și alte funcționalități – activitatea unoe module (plug-in), trackback și pinging de pe alte situri. Cu alte cuvinte, deși are utilitatea sa, XLM-RPC este o vulnerabilitate a WordPress care necesită rezolvare.



The screenshot shows a traffic log interface with a table of requests. The 'Page Visited' column is circled in red. The table contains the following data:

Type	Location	Page Visited	Time	IP Address	Hostname	Response	View
●	Clifton, New Jersey, United States	/xmlrpc.php	4/12/2022 7:30:50 PM	143.198.11.159	cafecomtrainer.com.br	503	👁
●	Hangzhou, China	/xmlrpc.php	4/12/2022 7:28:51 PM	47.96.27.235	47.96.27.235	200	👁
●	Singapore	/xmlrpc.php	4/12/2022 7:26:19 PM	116.12.48.101	plesk16.ns01.net	200	👁
●	United States	/xmlrpc.php	4/12/2022 7:06:59 PM	66.115.173.18	66.115.173.18	503	👁
●	Malta	/xmlrpc.php	4/12/2022 7:04:05 PM	85.119.122.23	...2-23.i17-01.melita.com	503	👁
●	Beijing, China	/xmlrpc.php	4/12/2022 7:02:29 PM	39.98.224.201	39.98.224.201	503	👁
●	Russia	/xmlrpc.php	4/12/2022 6:57:07 PM	5.101.157.231	m1.radon.beget.com	503	👁
●	Straseni, Moldova	/xmlrpc.php	4/12/2022 6:54:40 PM	109.233.192.83	host2.inetehno.md	503	👁
●	Buffalo, New York, United States	/xmlrpc.php	4/12/2022 6:52:24 PM	198.20.170.59	mail.w7virtual.net	200	👁
●	France	/xmlrpc.php	4/12/2022 6:49:37 PM	51.83.66.220	...server3.pebblehost.com	503	👁
●	Magersari, Indonesia	/xmlrpc.php	4/12/2022 6:46:57 PM	36.94.142.166	36.94.142.166	200	👁
●	London, United Kingdom	/xmlrpc.php	4/12/2022 6:44:24 PM	167.99.84.255	...7854.cloudwaysapps.com	503	👁

Imagine – atacuri asupra xmlrpc.php – <https://9ro.xzy>

În imaginea de mai sus este un fragment din jurnalul atacurilor executate (fără succes, din fericire) chiar asupra acestui blog.

Atacurile au fost blocate de plug-in-ul de securitate [Wordfence](#).

Dacă însă, din diverse motive, nu vrei să folosești acest plug-in, există o altă soluție de a înlătura vulnerabilitatea XLM-RPC? Da.

Există două mari slăbiciuni ale fișierului *xlmrpx.php*, care au fost exploatare în decursul timpului.

Prima slăbiciune este posibilitatea unor atacuri de tip „brute force” ([forță brută](#)), deoarece un hacker poate folosi o singură comandă pentru a testa un număr foarte mare de combinații *utilizator/parolă*, în speranța de a „nimeri” combinația corectă.

A doua slăbiciune este posibilitatea hackerilor de a face blogul nefuncțional prin atacuri de tip DDos (Distributed Denial of Service) – [mai multe detalii aici](#).

Ambele tipuri de atac se pot contracara dezactivând funcția *xlmrpx.php*. Acest lucru se poate face fie manual, editând fișierul **.htaccess** (ne-recomandat dacă ești începător) sau, mai simplu, folosind unele plug-in-uri special concepute pentru acest scop ([Stop XLM-RPC Attack](#) sau [Control XLM-RPC Publishing](#) sau sus-menționatul [Wordfence](#), care oferă o protecție mai complexă, rezolvând și alte tipuri de amenințări).

NOTĂ: Ștergerea fișierului *xlmrpx.php* poate părea o soluție mai simplă, dar nu este eficientă,

Folosești WordPress? Atenție la fișierul xlmrpc.php

WordPress va reinstala fișierul la fiecare actualizare.

Vrei să fii notificat când postez un nou articol?

Adresa ta de email:

Vreau să fiu notificat!

Livrat de [FeedBurner](#)