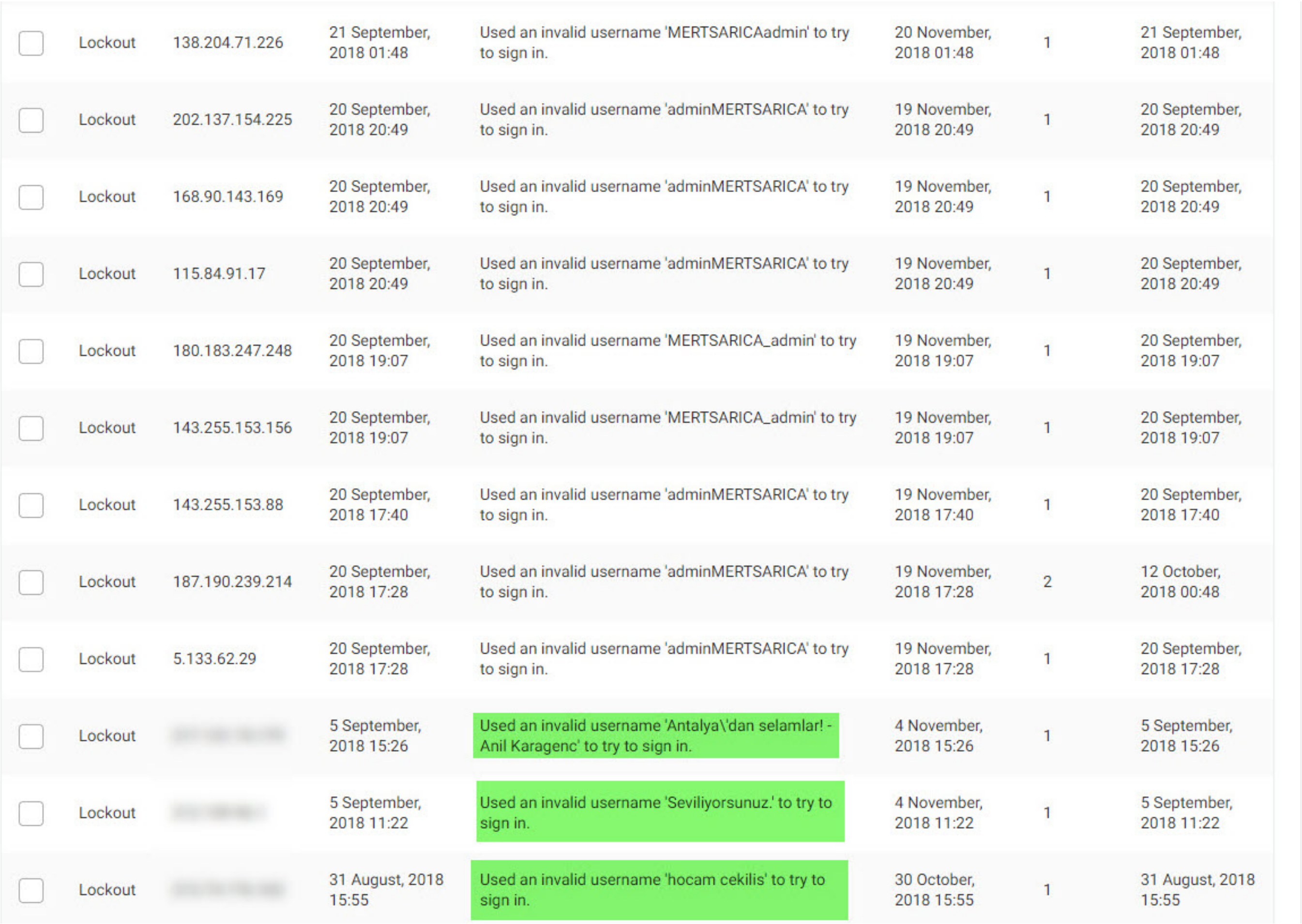
WordPress Security

written by Mert SARICA | 2 September 2019

For nearly a decade, I have been conducting research on cybersecurity and continue to write and share what I have learned with all of you. When I look at the feedback I receive from you, it makes me very happy to see that many of you benefit from what I write. Sometimes, there are those who perform minor cyber attacks to my blog, such as a small-scale DoS attack, not with malicious intent but simply to send me a message. There are also instances where I encounter attacks that I cannot fully understand the reason or intention behind, including attempts to access the administrator page. Based on this, in this article, I have decided to share how I detect one of these attacks and provide tips on how WordPress CMS users like myself can secure their blogs.



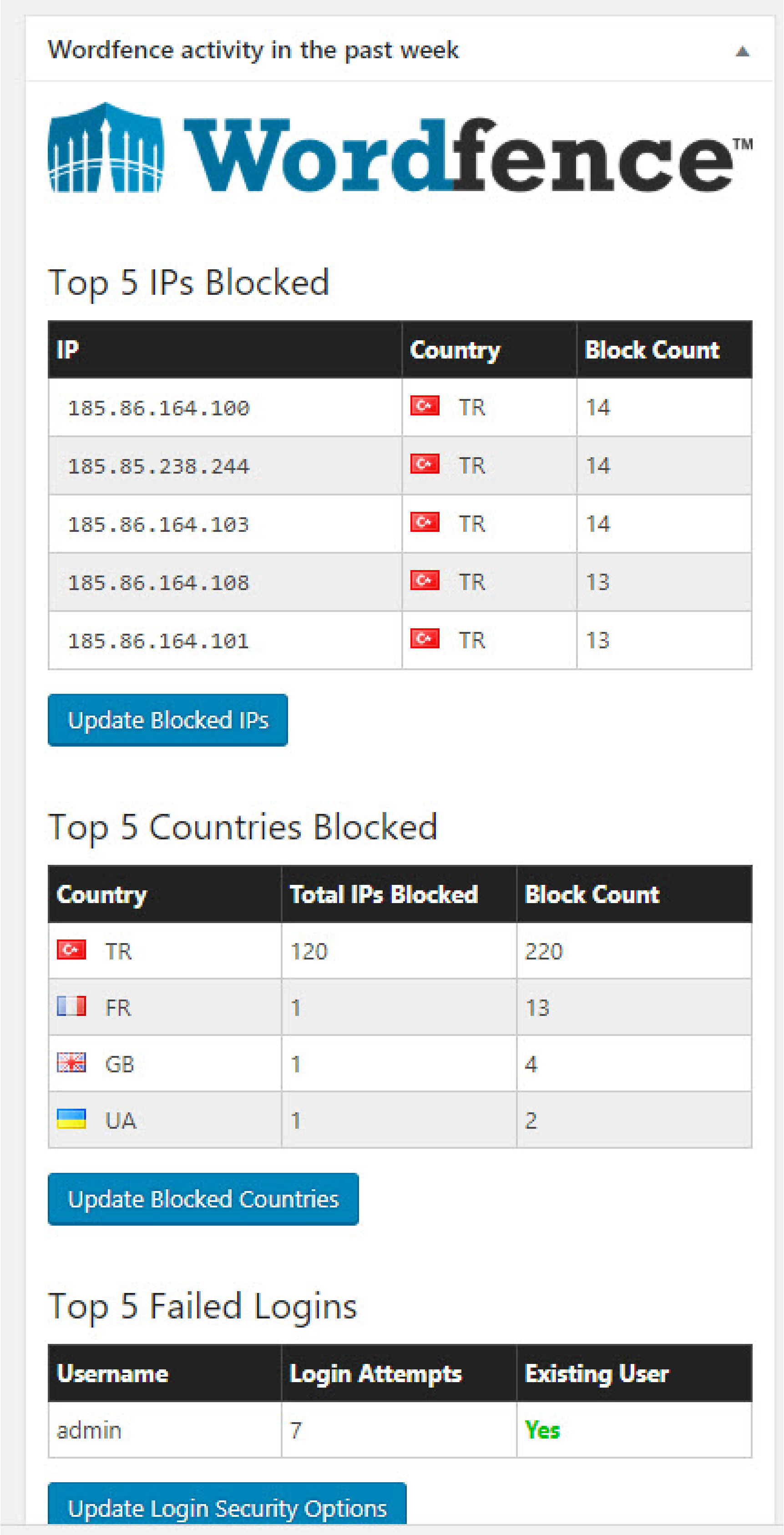
□	Lockout	138.204.71.226	21 September, 2018 01:48	Used an invalid username 'MERTSARICAadmin' to try to sign in.	20 November, 2018 01:48	1	21 September, 2018 01:48
□	Lockout	202.137.154.225	20 September, 2018 20:49	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 20:49	1	20 September, 2018 20:49
□	Lockout	168.90.143.169	20 September, 2018 20:49	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 20:49	1	20 September, 2018 20:49
□	Lockout	115.84.91.17	20 September, 2018 20:49	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 20:49	1	20 September, 2018 20:49
□	Lockout	180.183.247.248	20 September, 2018 19:07	Used an invalid username 'MERTSARICA_admin' to try to sign in.	19 November, 2018 19:07	1	20 September, 2018 19:07
□	Lockout	143.255.153.156	20 September, 2018 19:07	Used an invalid username 'MERTSARICA_admin' to try to sign in.	19 November, 2018 19:07	1	20 September, 2018 19:07
□	Lockout	143.255.153.88	20 September, 2018 17:40	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 17:40	1	20 September, 2018 17:40
□	Lockout	187.190.239.214	20 September, 2018 17:28	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 17:28	2	12 October, 2018 00:48
□	Lockout	5.133.62.29	20 September, 2018 17:28	Used an invalid username 'adminMERTSARICA' to try to sign in.	19 November, 2018 17:28	1	20 September, 2018 17:28
□	Lockout	[redacted]	5 September, 2018 15:26	Used an invalid username 'Antalya\'dan selamlar! - Anil Karagenc' to try to sign in.	4 November, 2018 15:26	1	5 September, 2018 15:26
□	Lockout	[redacted]	5 September, 2018 11:22	Used an invalid username 'Seviliyorsunuz.' to try to sign in.	4 November, 2018 11:22	1	5 September, 2018 11:22
□	Lockout	[redacted]	31 August, 2018 15:55	Used an invalid username 'hocam cekilis' to try to sign in.	30 October, 2018 15:55	1	31 August, 2018 15:55

First, if we look at the statistical information related to WordPress, it is the most widely used content management system globally, accounting for about 60% of the CMS market. Approximately 33% of all websites on the internet use WordPress, with over 55,000 plugins available. Over the years, the types of vulnerabilities detected in WordPress have varied, but the most commonly found vulnerability to date is Cross-Site Scripting (XSS). When we examine the WordPress vulnerability database, we can see that more than 15,000 vulnerabilities have been identified in WordPress core code and plugins.

When we consider how WordPress sites are generally hacked, we often find that it is due to insecure hosting services, weak administrator passwords, outdated versions of WordPress, plugins, themes, and the use of pirated themes (Backdoor Hunting) containing backdoors.

Although my wp-admin page, which is used to detect weak administrator passwords, is publicly accessible, I have been using the Duo Two-Factor Authentication plugin for years to implement multi-factor authentication for administrator login. I also utilize the Wordfence Security plugin to automatically block IP addresses involved in brute-force attacks, as well as to detect and report potential security vulnerabilities. Additionally, I prefer to use premium themes to avoid themes containing backdoors. To avoid dealing with insecure hosting services, I have been using a VPS for many years.

One day in July 2018, while checking the security dashboard of my Wordfence plugin, I noticed that the most blocked IP addresses were from Turkey, indicating attempts of brute-force attacks on my administrator page. When I checked the whois information of these IP addresses, I discovered that the majority of them were associated with a hosting service provider called iDealhosting. Intrigued by this, I decided to closely monitor the attacks originating from these IP addresses on my blog as part of a security investigation.



Wordfence activity in the past week

Top 5 IPs Blocked

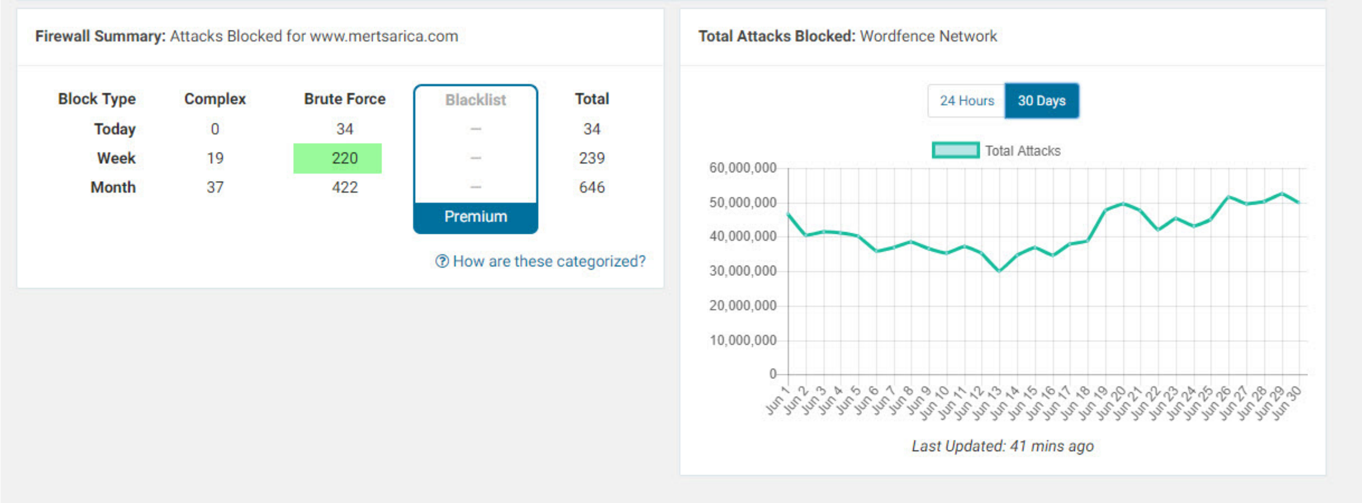
IP	Country	Block Count
185.86.164.100	TR	14
185.85.238.244	TR	14
185.86.164.103	TR	14
185.86.164.108	TR	13
185.86.164.101	TR	13

Top 5 Countries Blocked

Country	Total IPs Blocked	Block Count
TR	120	220
FR	1	13
GB	1	4
UA	1	2

Top 5 Failed Logins

Username	Login Attempts	Existing User
admin	7	Yes



Firewall Summary: Attacks Blocked for www.mertsarica.com

Block Type	Complex	Brute Force	Blacklist	Total
Today	0	34	—	34
Week	19	220	—	239
Month	37	422	—	646

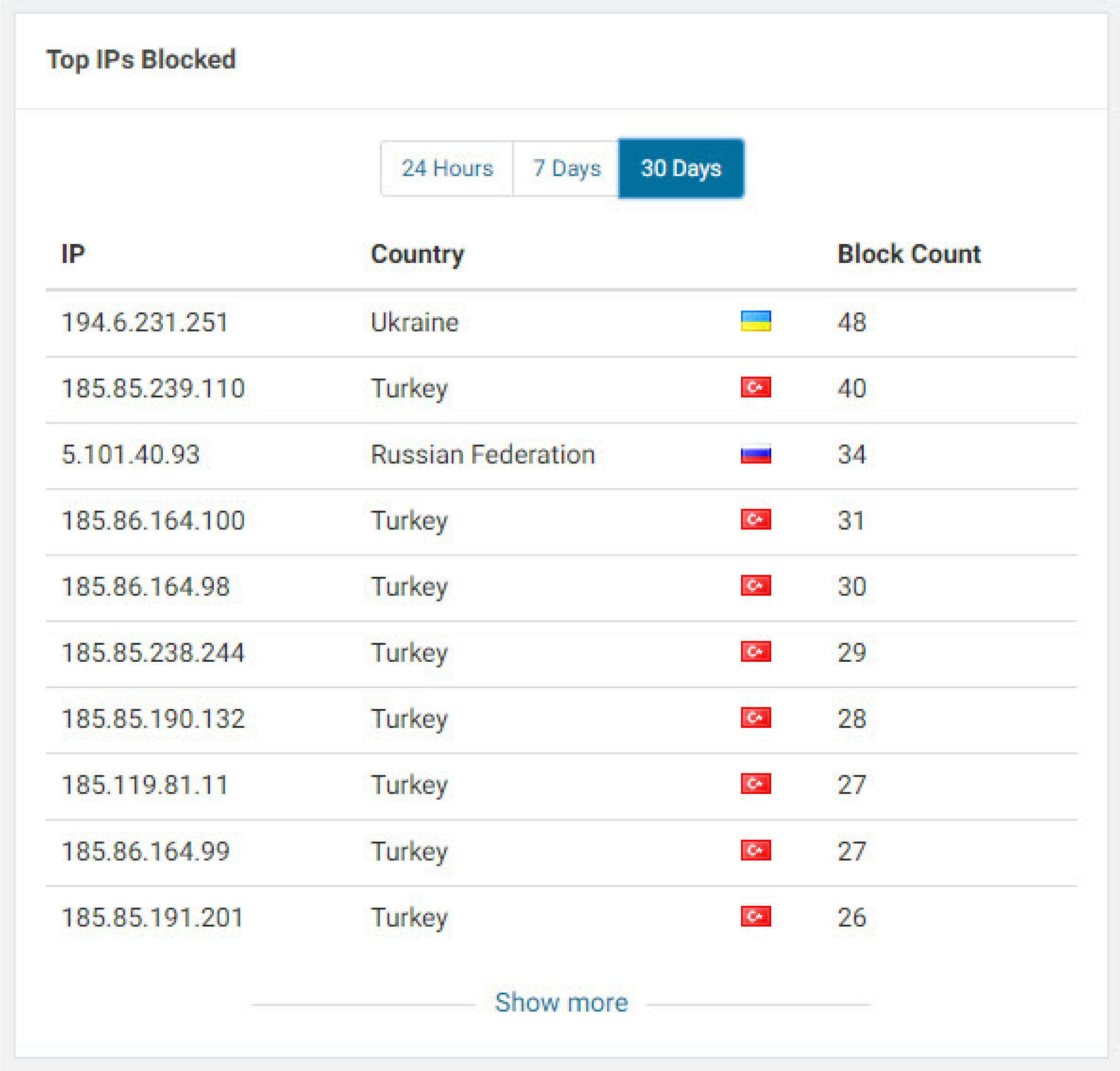
Premium

ⓘ How are these categorized?

Total Attacks Blocked: Wordfence Network

24 Hours | 30 Days

Last Updated: 41 mins ago

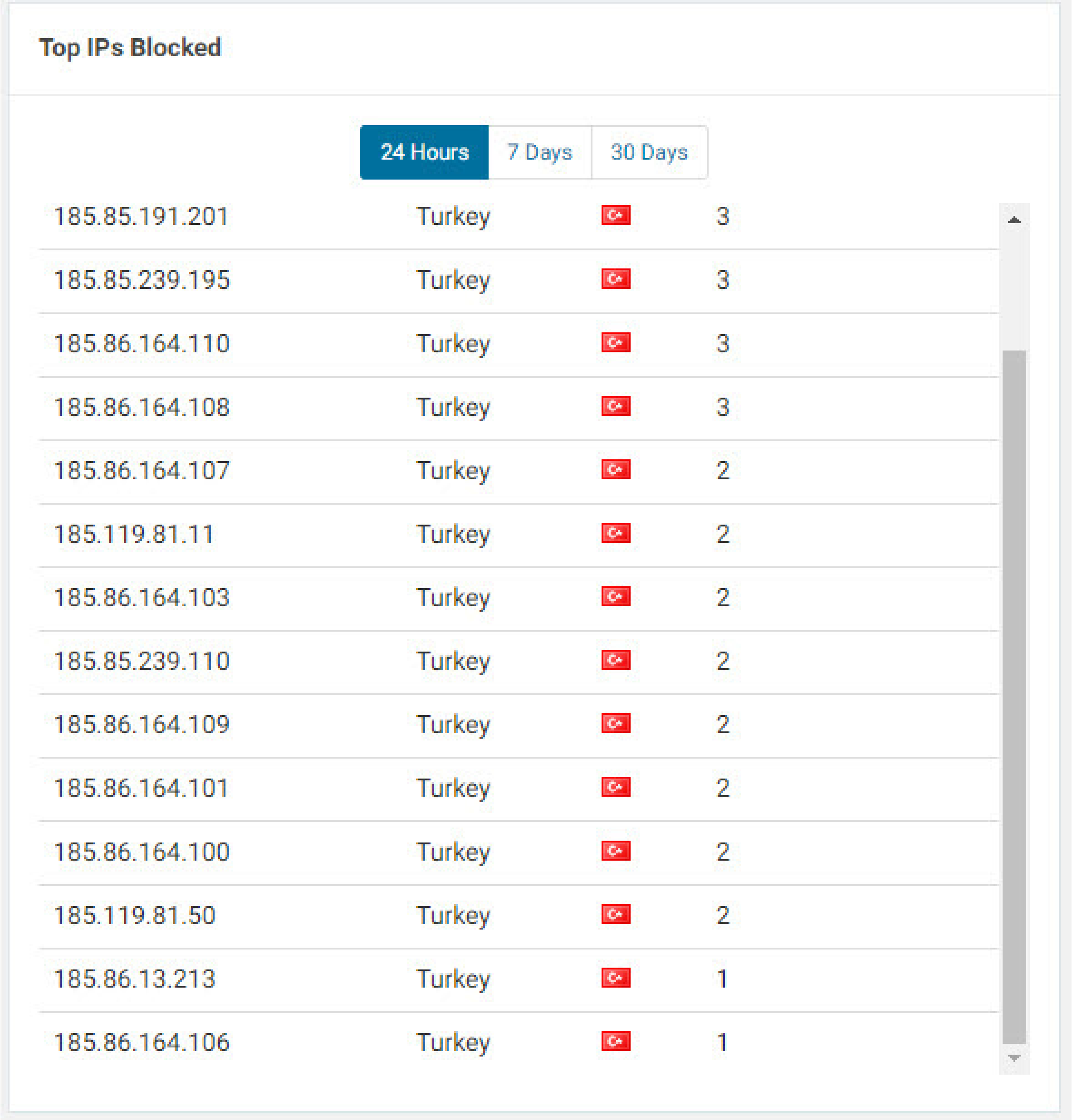


Top IPs Blocked

24 Hours | 7 Days | 30 Days

IP	Country	Block Count
194.6.231.251	Ukraine 🇺🇦	48
185.85.239.110	Turkey 🇹🇷	40
5.101.40.93	Russian Federation 🇷🇺	34
185.86.164.100	Turkey 🇹🇷	31
185.86.164.98	Turkey 🇹🇷	30
185.85.238.244	Turkey 🇹🇷	29
185.85.190.132	Turkey 🇹🇷	28
185.119.81.11	Turkey 🇹🇷	27
185.86.164.99	Turkey 🇹🇷	27
185.85.191.201	Turkey 🇹🇷	26

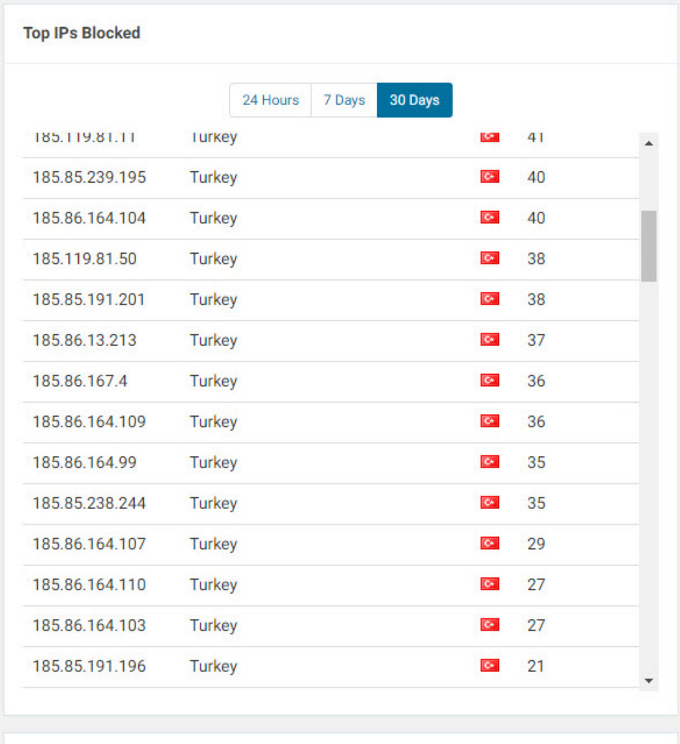
Show more



Top IPs Blocked

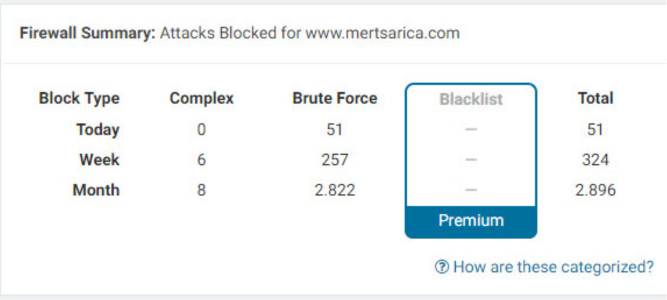
185.85.191.201	Turkey	🇹🇷	3
185.85.239.195	Turkey	🇹🇷	3
185.86.164.110	Turkey	🇹🇷	3
185.86.164.108	Turkey	🇹🇷	3
185.86.164.107	Turkey	🇹🇷	2
185.119.81.11	Turkey	🇹🇷	2
185.86.164.103	Turkey	🇹🇷	2
185.85.239.110	Turkey	🇹🇷	2
185.86.164.109	Turkey	🇹🇷	2
185.86.164.101	Turkey	🇹🇷	2
185.86.164.100	Turkey	🇹🇷	2
185.119.81.50	Turkey	🇹🇷	2
185.86.13.213	Turkey	🇹🇷	1
185.86.164.106	Turkey	🇹🇷	1

When I checked the security dashboard again in October, I noticed that the brute-force attacks were still ongoing from 22 IP addresses. As a security researcher, one of the first questions that came to mind was whether this was a targeted attack attempt on my blog. One of the easiest ways to determine this was to learn the passwords used in the brute-force attacks. Therefore, without wasting any time, I got to work on it.



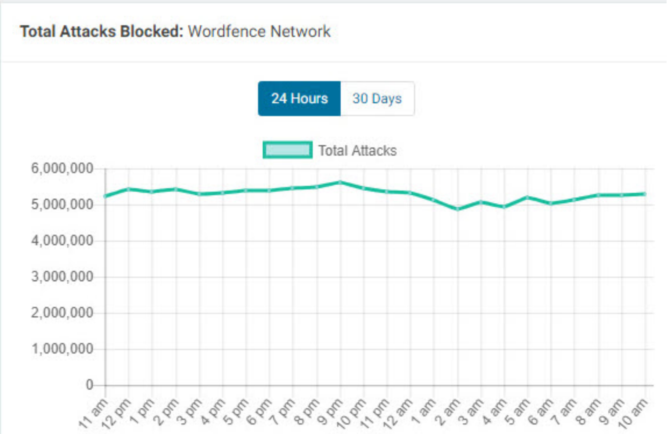
Top IPs Blocked

185.119.81.11	Turkey	41
185.85.239.195	Turkey	40
185.86.164.104	Turkey	40
185.119.81.50	Turkey	38
185.85.191.201	Turkey	38
185.86.13.213	Turkey	37
185.86.167.4	Turkey	36
185.86.164.109	Turkey	36
185.86.164.99	Turkey	35
185.85.238.244	Turkey	35
185.86.164.107	Turkey	29
185.86.164.110	Turkey	27
185.86.164.103	Turkey	27
185.85.191.196	Turkey	21

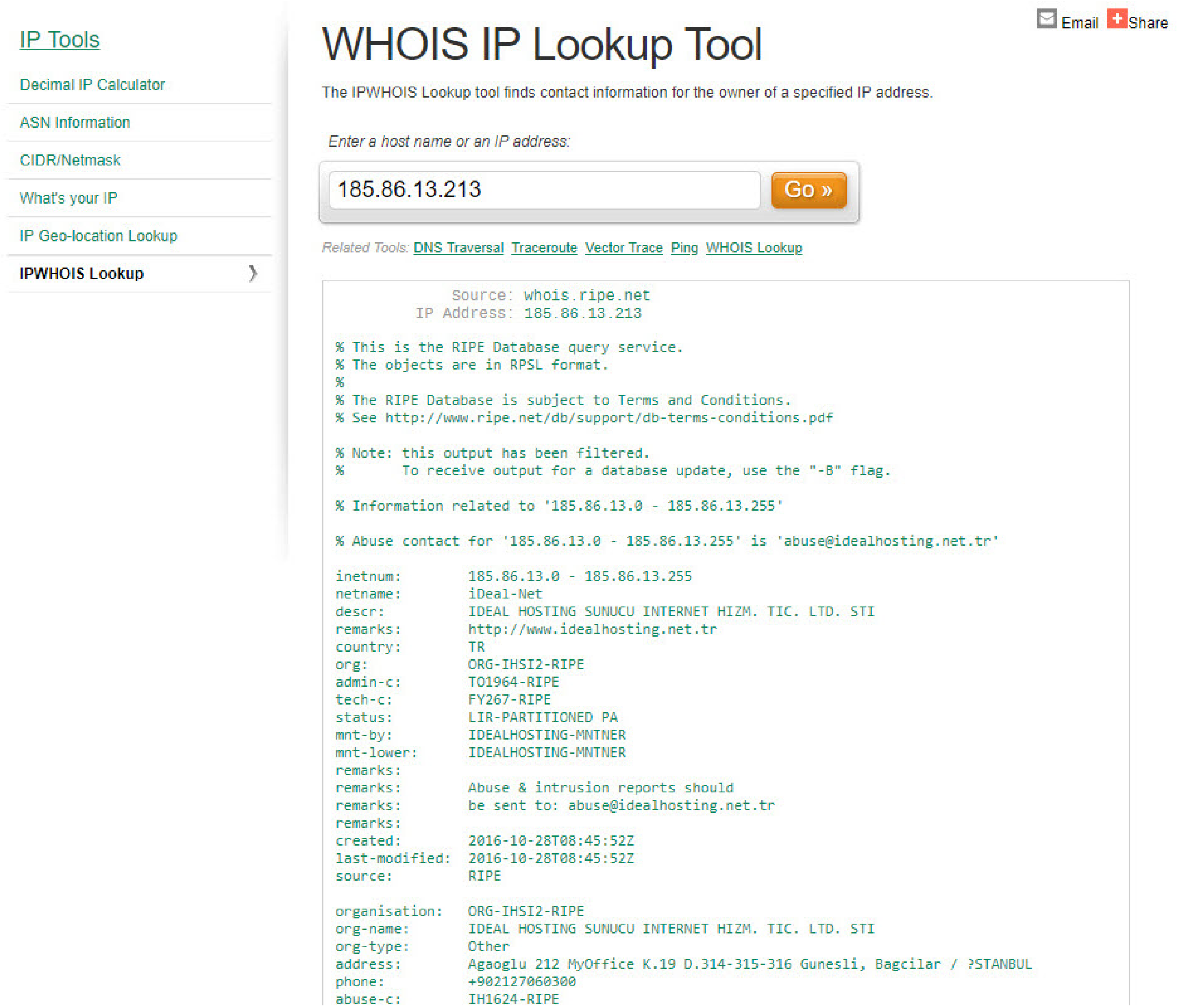


Firewall Summary: Attacks Blocked for www.mertsarica.com

Block Type	Complex	Brute Force	Blacklist	Total
Today	0	51	–	51
Week	6	257	–	324
Month	8	2.822	–	2.896



Total Attacks Blocked: Wordfence Network



WHOIS IP Lookup Tool

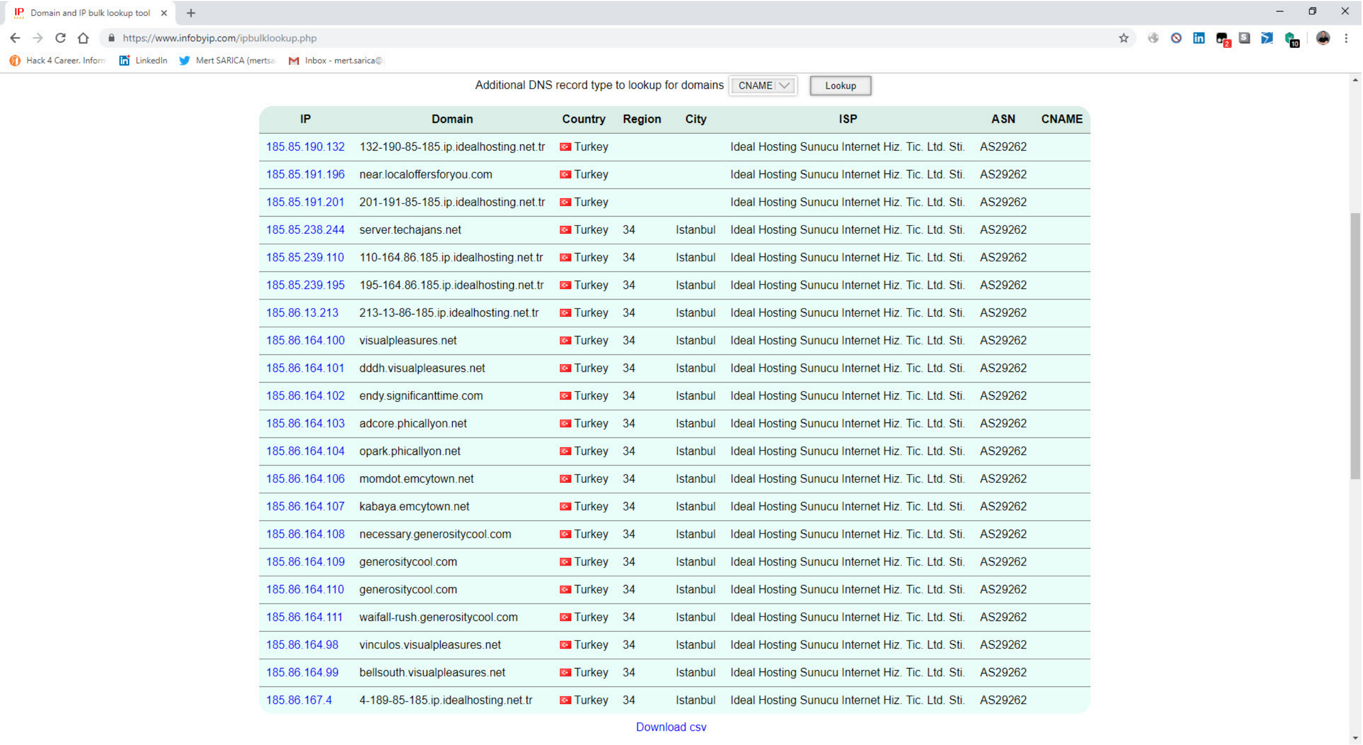
The IPWHOIS Lookup tool finds contact information for the owner of a specified IP address.

Enter a host name or an IP address:

185.86.13.213

Related Tools: DNS Traversal Traceroute Vector Trace Ping WHOIS Lookup

```
             Source:  whois.ripe.net
         IP Address:  185.86.13.213

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '185.86.13.0 - 185.86.13.255'

% Abuse contact for '185.86.13.0 - 185.86.13.255' is 'abuse@idealhosting.net.tr'

inetnum:        185.86.13.0 - 185.86.13.255
netname:        iDeal-Net
descr:          IDEAL HOSTING SUNUCU INTERNET HIZM. TIC. LTD. STI
remarks:        http://www.idealhosting.net.tr
country:        TR
org:            ORG-IHSI2-RIPE
admin-c:        TO1964-RIPE
tech-c:         FY267-RIPE
status:         LIR-PARTITIONED PA
mnt-by:         IDEALHOSTING-MNTNER
mnt-lower:      IDEALHOSTING-MNTNER
remarks:
remarks:        Abuse & intrusion reports should
remarks:        be sent to: abuse@idealhosting.net.tr
remarks:
created:        2016-10-28T08:45:52Z
last-modified:  2016-10-28T08:45:52Z
source:         RIPE

organisation:   ORG-IHSI2-RIPE
org-name:       IDEAL HOSTING SUNUCU INTERNET HIZM. TIC. LTD. STI
org-type:       Other
address:        Agaoglu 212 MyOffice K.19 D.314-315-316 Gunesli, Bagcilar / ?STANBUL
phone:          +902127060300
abuse-c:        IH1624-RIPE
```

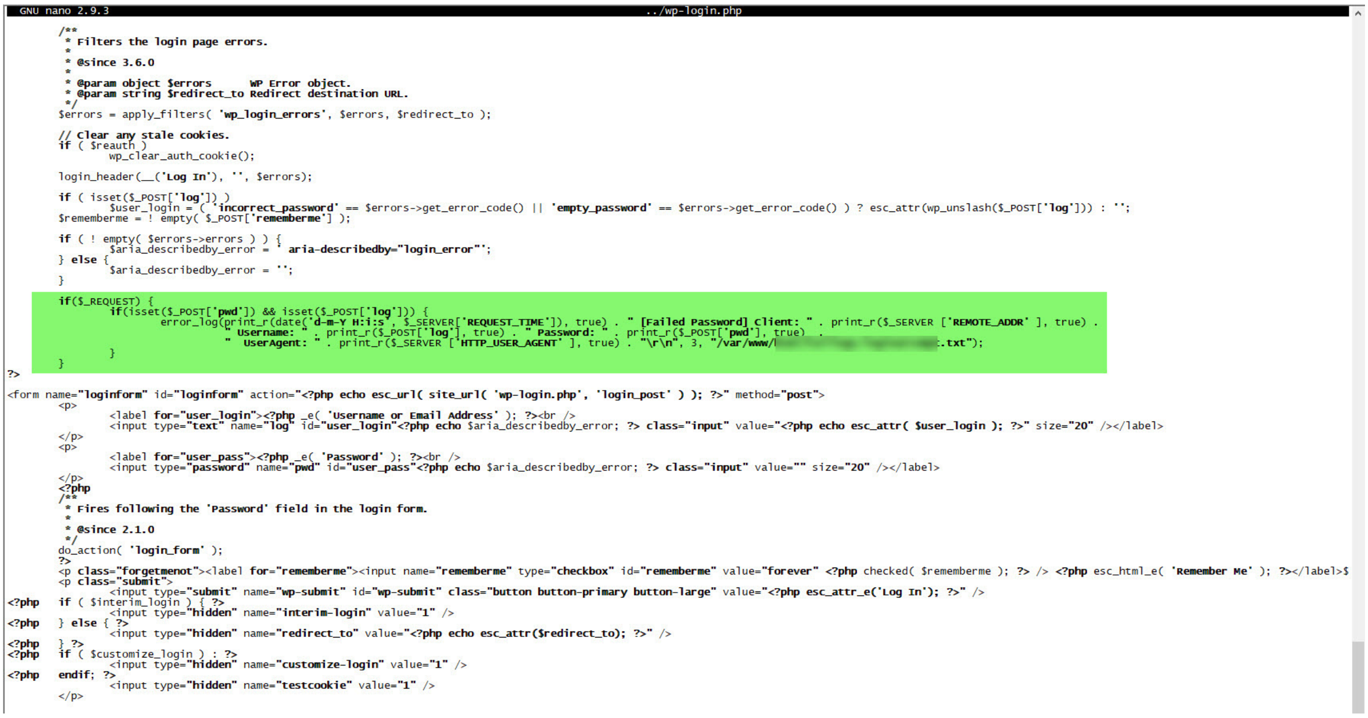

Domain and IP bulk lookup tool
https://www.infobyip.com/ipbulklookup.php
Hack 4 Career. Inform
LinkedIn
Mert SARICA (mertsa
Inbox - mert.sarica@

Additional DNS record type to lookup for domains CNAME Lookup

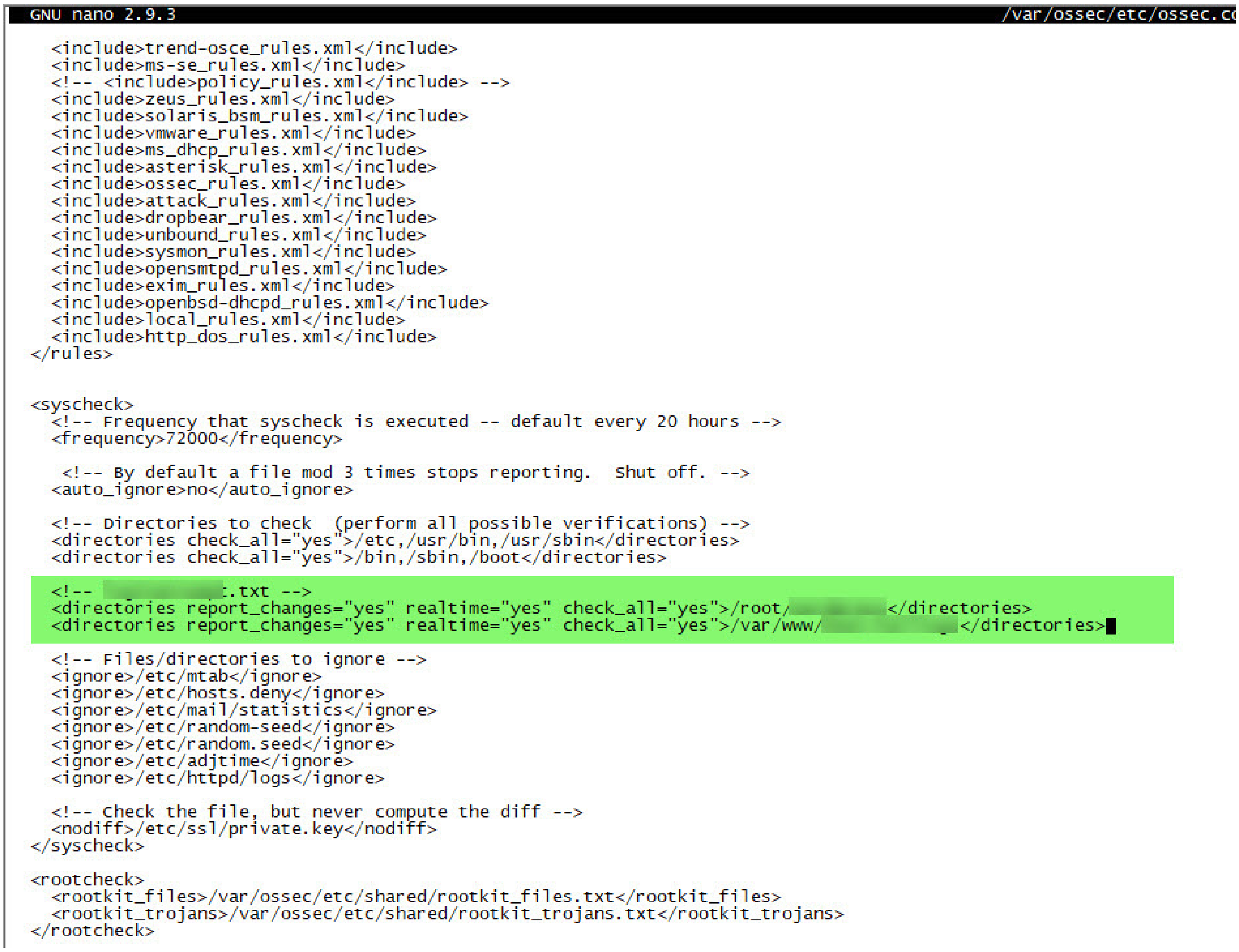
IP	Domain	Country	Region	City	ISP	ASN	CNAME
185.85.190.132	132-190-85-185.ip.idealhosting.net.tr	Turkey			Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.191.196	near.localoffersforyou.com	Turkey			Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.191.201	201-191-85-185.ip.idealhosting.net.tr	Turkey			Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.238.244	server.techajans.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.239.110	110-164.86.185.ip.idealhosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.85.239.195	195-164.86.185.ip.idealhosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.13.213	213-13-86-185.ip.idealhosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.100	visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.101	dddh.visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.102	endy.significanttime.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.103	adcore.phicallyon.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.104	opark.phicallyon.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.106	momdot.emcytown.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.107	kabaya.emcytown.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.108	necessary.generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.109	generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.110	generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.111	waifall-rush.generositycool.com	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.98	vinculos.visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.164.99	bellsouth.visualpleasures.net	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	
185.86.167.4	4-189-85-185.ip.idealhosting.net.tr	Turkey	34	Istanbul	Ideal Hosting Sunucu Internet Hiz. Tic. Ltd. Sti.	AS29262	

Download csv

First, I prepared a PHP code that records failed login attempts to the wp-login.php file, along with the passwords, and saves them to disk. Then, to stay informed about any changes in the recorded file in real-time, I made a small definition in OSSEC HIDS.

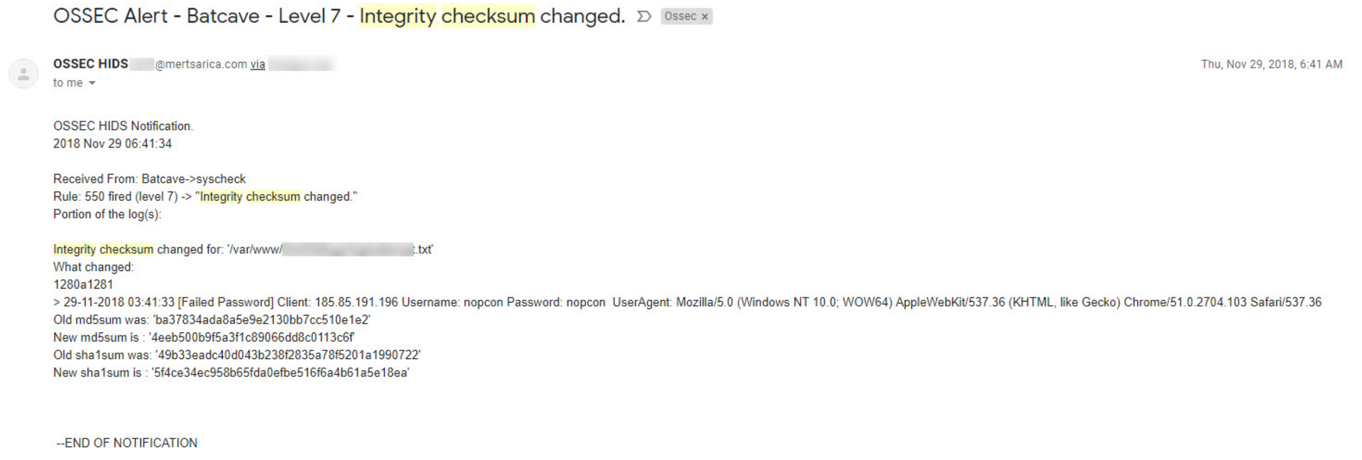


```
  GNU nano 2.9.3                                                    ../wp-login.php

        /**
         * Filters the login page errors.
         *
         * @since 3.6.0
         *
         * @param object $errors      WP Error object.
         * @param string $redirect_to Redirect destination URL.
         */
        $errors = apply_filters( 'wp_login_errors', $errors, $redirect_to );

        // Clear any stale cookies.
        if ( $reauth )
                wp_clear_auth_cookie();

        login_header(__('Log In'), '', $errors);

        if ( isset($_POST['log']) )
                $user_login = ( 'incorrect_password' == $errors->get_error_code() || 'empty_password' == $errors->get_error_code() ) ? esc_attr(wp_unslash($_POST['log'])) : '';
        $rememberme = ! empty( $_POST['rememberme'] );

        if ( ! empty( $errors->errors ) ) {
                $aria_describedby_error = ' aria-describedby="login_error"';
        } else {
                $aria_describedby_error = '';
        }

        if($_REQUEST) {
                if(isset($_POST['pwd']) && isset($_POST['log'])) {
                        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Failed Password] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                  " Username: " . print_r($_POST['log'], true) . " Password: " . print_r($_POST['pwd'], true)  .
                                  "  UserAgent: " . print_r($_SERVER ['HTTP_USER_AGENT' ], true) . "\r\n", 3, "/var/www/[redacted].txt");
                }
        }
?>

<form name="loginform" id="loginform" action="<?php echo esc_url( site_url( 'wp-login.php', 'login_post' ) ); ?>" method="post">
        <p>
                <label for="user_login"><?php _e( 'Username or Email Address' ); ?><br />
                <input type="text" name="log" id="user_login"<?php echo $aria_describedby_error; ?> class="input" value="<?php echo esc_attr( $user_login ); ?>" size="20" /></label>
        </p>
        <p>
                <label for="user_pass"><?php _e( 'Password' ); ?><br />
                <input type="password" name="pwd" id="user_pass"<?php echo $aria_describedby_error; ?> class="input" value="" size="20" /></label>
        </p>
        <?php
        /**
         * Fires following the 'Password' field in the login form.
         *
         * @since 2.1.0
         */
        do_action( 'login_form' );
        ?>
        <p class="forgetmenot"><label for="rememberme"><input name="rememberme" type="checkbox" id="rememberme" value="forever" <?php checked( $rememberme ); ?> /> <?php esc_html_e( 'Remember Me' ); ?></label>$
        <p class="submit">
                <input type="submit" name="wp-submit" id="wp-submit" class="button button-primary button-large" value="<?php esc_attr_e('Log In'); ?>" />
<?php   if ( $interim_login ) { ?>
                <input type="hidden" name="interim-login" value="1" />
<?php   } else { ?>
                <input type="hidden" name="redirect_to" value="<?php echo esc_attr($redirect_to); ?>" />
<?php   } ?>
<?php   if ( $customize_login ) : ?>
                <input type="hidden" name="customize-login" value="1" />
<?php   endif; ?>
                <input type="hidden" name="testcookie" value="1" />
        </p>
```



```
 GNU nano 2.9.3                                                                          /var/ossec/etc/ossec.c
    <include>trend-osce_rules.xml</include>
    <include>ms-se_rules.xml</include>
    <!-- <include>policy_rules.xml</include> -->
    <include>zeus_rules.xml</include>
    <include>solaris_bsm_rules.xml</include>
    <include>vmware_rules.xml</include>
    <include>ms_dhcp_rules.xml</include>
    <include>asterisk_rules.xml</include>
    <include>ossec_rules.xml</include>
    <include>attack_rules.xml</include>
    <include>dropbear_rules.xml</include>
    <include>unbound_rules.xml</include>
    <include>sysmon_rules.xml</include>
    <include>opensmtpd_rules.xml</include>
    <include>exim_rules.xml</include>
    <include>openbsd-dhcpd_rules.xml</include>
    <include>local_rules.xml</include>
    <include>http_dos_rules.xml</include>
  </rules>


  <syscheck>
    <!-- Frequency that syscheck is executed -- default every 20 hours -->
    <frequency>72000</frequency>

     <!-- By default a file mod 3 times stops reporting.  Shut off. -->
     <auto_ignore>no</auto_ignore>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/bin,/sbin,/boot</directories>

    <!-- [redacted].txt -->
    <directories report_changes="yes" realtime="yes" check_all="yes">/root/[redacted]</directories>
    <directories report_changes="yes" realtime="yes" check_all="yes">/var/www/[redacted]</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/random.seed</ignore>
    <ignore>/etc/adjtime</ignore>
    <ignore>/etc/httpd/logs</ignore>

    <!-- Check the file, but never compute the diff -->
    <nodiff>/etc/ssl/private.key</nodiff>
  </syscheck>

  <rootcheck>
    <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
  </rootcheck>
```

When I examined the recorded failed username and password attempts throughout the end of October and the month of November, I discovered that the attempted usernames and passwords consisted of words found in my blog posts rather than ordinary dictionary words. This information indicated to me that it was indeed a targeted attack attempt.



OSSEC Alert - Batcave - Level 7 - Integrity checksum changed. Ossec ×

OSSEC HIDS [redacted]@mertsarica.com via [redacted]
to me

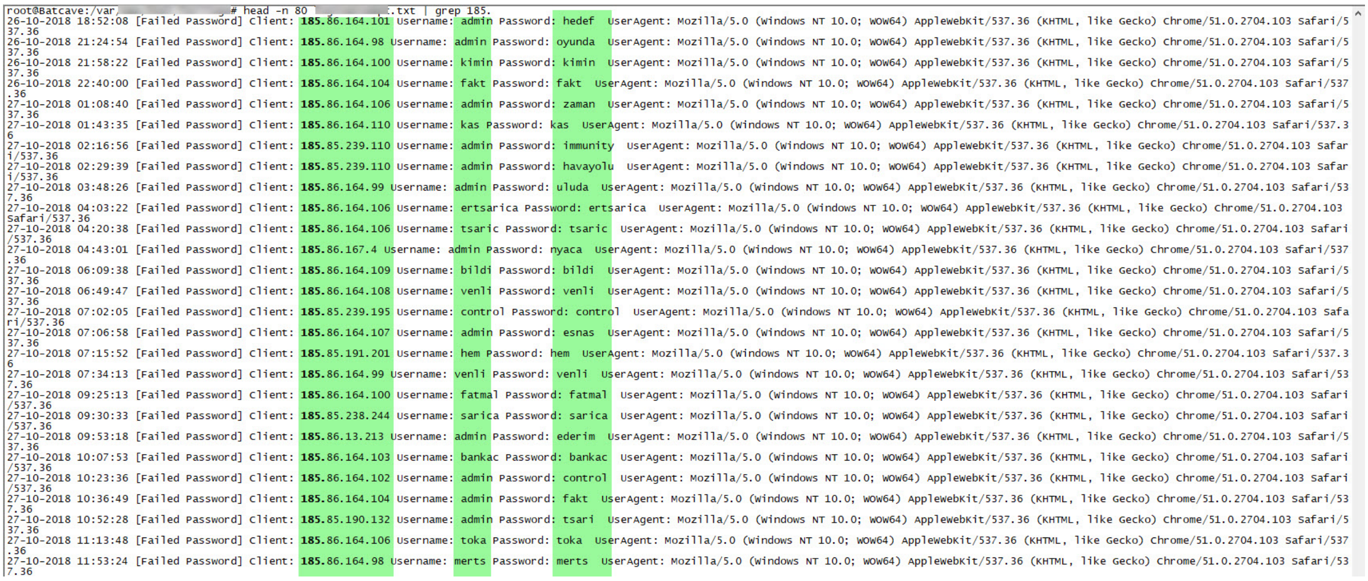
Thu, Nov 29, 2018, 6:41 AM

OSSEC HIDS Notification.
2018 Nov 29 06:41:34

Received From: Batcave->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

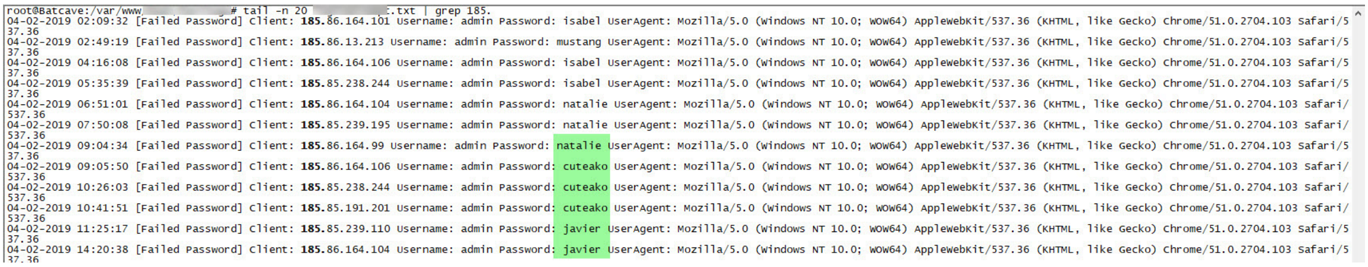
```
Integrity checksum changed for: '/var/www/[redacted].txt'
What changed:
1280a1281
> 29-11-2018 03:41:33 [Failed Password] Client: 185.85.191.196 Username: nopcon Password: nopcon  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Old md5sum was: 'ba37834ada8a5e9e2130bb7cc510e1e2'
New md5sum is : '4eeb500b9f5a3f1c89066dd8c0113c6f'
Old sha1sum was: '49b33eadc40d043b238f2835a78f5201a1990722'
New sha1sum is : '5f4ce34ec958b65fda0efbe516f6a4b61a5e18ea'
```

--END OF NOTIFICATION

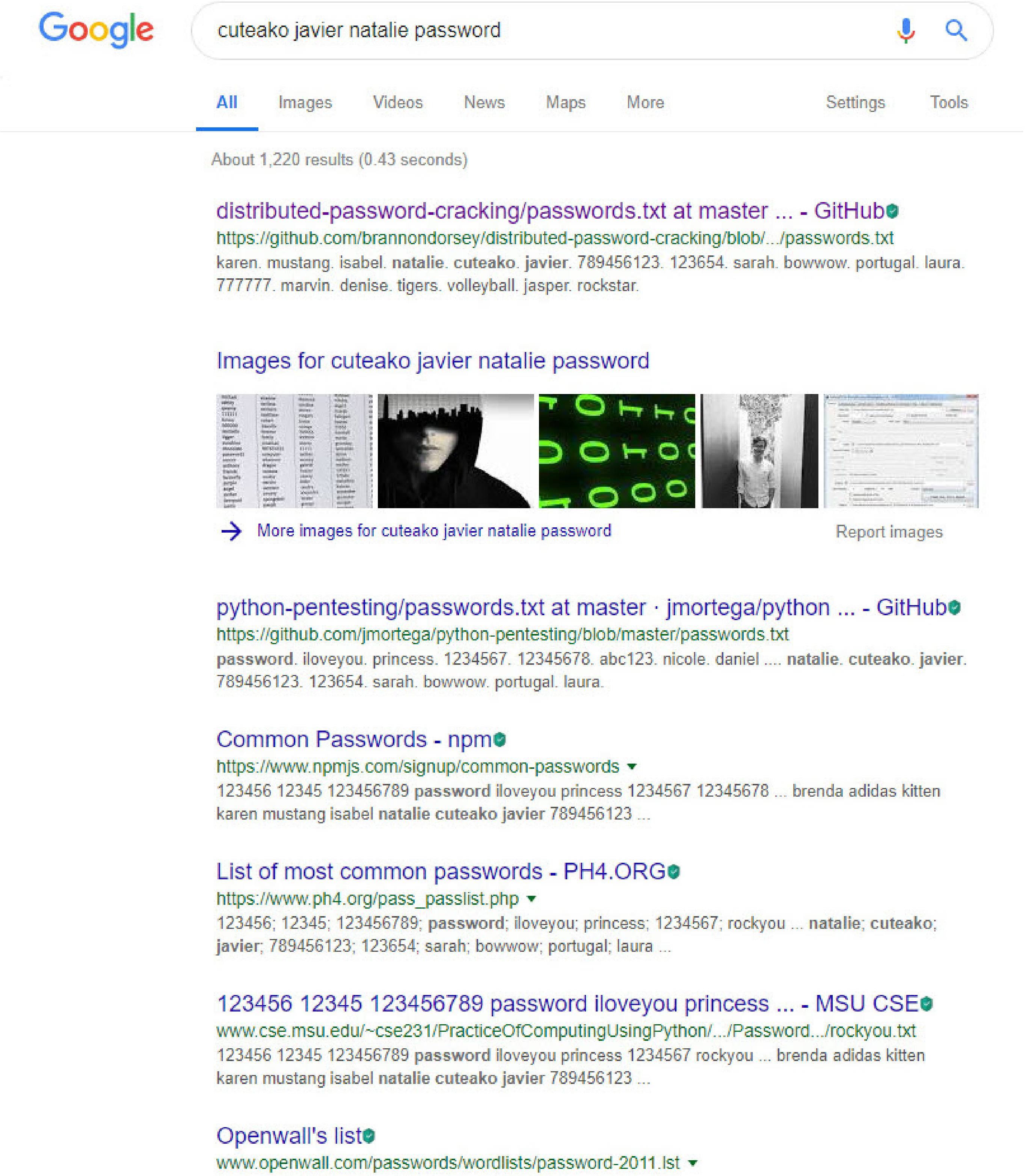


```
root@Batcave:/var/[redacted]# head -n 80 [redacted].txt | grep 185.
26-10-2018 18:52:08 [Failed Password] Client: 185.86.164.101 Username: admin Password: hedef  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
26-10-2018 21:24:54 [Failed Password] Client: 185.86.164.98 Username: admin Password: oyunda  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
26-10-2018 21:58:22 [Failed Password] Client: 185.86.164.100 Username: kimin Password: kimin  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
26-10-2018 22:40:00 [Failed Password] Client: 185.86.164.104 Username: fakt Password: fakt  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537
.36
27-10-2018 01:08:40 [Failed Password] Client: 185.86.164.106 Username: admin Password: zaman  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 01:43:35 [Failed Password] Client: 185.86.164.110 Username: kas Password: kas  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3
6
27-10-2018 02:16:56 [Failed Password] Client: 185.85.239.110 Username: admin Password: immunity  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safar
i/537.36
27-10-2018 02:29:39 [Failed Password] Client: 185.85.239.110 Username: admin Password: havayolu  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safar
i/537.36
27-10-2018 03:48:26 [Failed Password] Client: 185.86.164.99 Username: admin Password: uluda  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
27-10-2018 04:03:22 [Failed Password] Client: 185.86.164.106 Username: ertsarica Password: ertsarica  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103
Safari/537.36
27-10-2018 04:20:38 [Failed Password] Client: 185.86.164.106 Username: tsaric Password: tsaric  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 04:43:01 [Failed Password] Client: 185.86.167.4 Username: admin Password: nyaca  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537
.36
27-10-2018 06:09:38 [Failed Password] Client: 185.86.164.109 Username: bildi Password: bildi  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 06:49:47 [Failed Password] Client: 185.86.164.108 Username: venli Password: venli  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 07:02:05 [Failed Password] Client: 185.85.239.195 Username: control Password: control  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safa
ri/537.36
27-10-2018 07:06:58 [Failed Password] Client: 185.86.164.107 Username: admin Password: esnas  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 07:15:52 [Failed Password] Client: 185.85.191.201 Username: hem Password: hem  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3
6
27-10-2018 07:34:13 [Failed Password] Client: 185.86.164.99 Username: venli Password: venli  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
27-10-2018 09:25:13 [Failed Password] Client: 185.86.164.100 Username: fatmal Password: fatmal  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 09:30:33 [Failed Password] Client: 185.85.238.244 Username: sarica Password: sarica  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 09:53:18 [Failed Password] Client: 185.86.13.213 Username: admin Password: ederim  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 10:07:53 [Failed Password] Client: 185.86.164.103 Username: bankac Password: bankac  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 10:23:36 [Failed Password] Client: 185.86.164.102 Username: admin Password: control  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari
/537.36
27-10-2018 10:36:49 [Failed Password] Client: 185.86.164.104 Username: admin Password: fakt  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
27-10-2018 10:52:28 [Failed Password] Client: 185.85.190.132 Username: admin Password: tsari  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
27-10-2018 11:13:48 [Failed Password] Client: 185.86.164.106 Username: toka Password: toka  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537
.36
27-10-2018 11:53:24 [Failed Password] Client: 185.86.164.98 Username: merts Password: merts  UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/53
7.36
```

When I revisited the attempted passwords in February 2019, I noticed that this time the passwords being tested were obtained from the database of Rockyou.com, which was hacked in 2009.



```
root@Batcave:/var/www[redacted]# tail -n 20 [redacted].txt | grep 185.
04-02-2019 02:09:32 [Failed Password] Client: 185.86.164.101 Username: admin Password: isabel UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 02:49:19 [Failed Password] Client: 185.86.13.213 Username: admin Password: mustang UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 04:16:08 [Failed Password] Client: 185.86.164.106 Username: admin Password: isabel UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 05:35:39 [Failed Password] Client: 185.85.238.244 Username: admin Password: isabel UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 06:51:01 [Failed Password] Client: 185.86.164.104 Username: admin Password: natalie UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 07:50:08 [Failed Password] Client: 185.85.239.195 Username: admin Password: natalie UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 09:04:34 [Failed Password] Client: 185.86.164.99 Username: admin Password: natalie UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 09:05:50 [Failed Password] Client: 185.86.164.106 Username: admin Password: cuteako UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 10:26:03 [Failed Password] Client: 185.85.238.244 Username: admin Password: cuteako UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 10:41:51 [Failed Password] Client: 185.85.191.201 Username: admin Password: cuteako UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36
04-02-2019 11:25:17 [Failed Password] Client: 185.85.239.110 Username: admin Password: javier UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
04-02-2019 14:20:38 [Failed Password] Client: 185.86.164.104 Username: admin Password: javier UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/5
37.36
```



cuteako javier natalie password

About 1,220 results (0.43 seconds)

distributed-password-cracking/passwords.txt at master ... - GitHub
https://github.com/brannondorsey/distributed-password-cracking/blob/.../passwords.txt
karen. mustang. isabel. **natalie**. **cuteako**. **javier**. 789456123. 123654. sarah. bowwow. portugal. laura. 777777. marvin. denise. tigers. volleyball. jasper. rockstar.

Images for cuteako javier natalie password

python-pentesting/passwords.txt at master · jmortega/python ... - GitHub
https://github.com/jmortega/python-pentesting/blob/master/passwords.txt
password. iloveyou. princess. 1234567. 12345678. abc123. nicole. daniel .... **natalie**. **cuteako**. **javier**. 789456123. 123654. sarah. bowwow. portugal. laura.

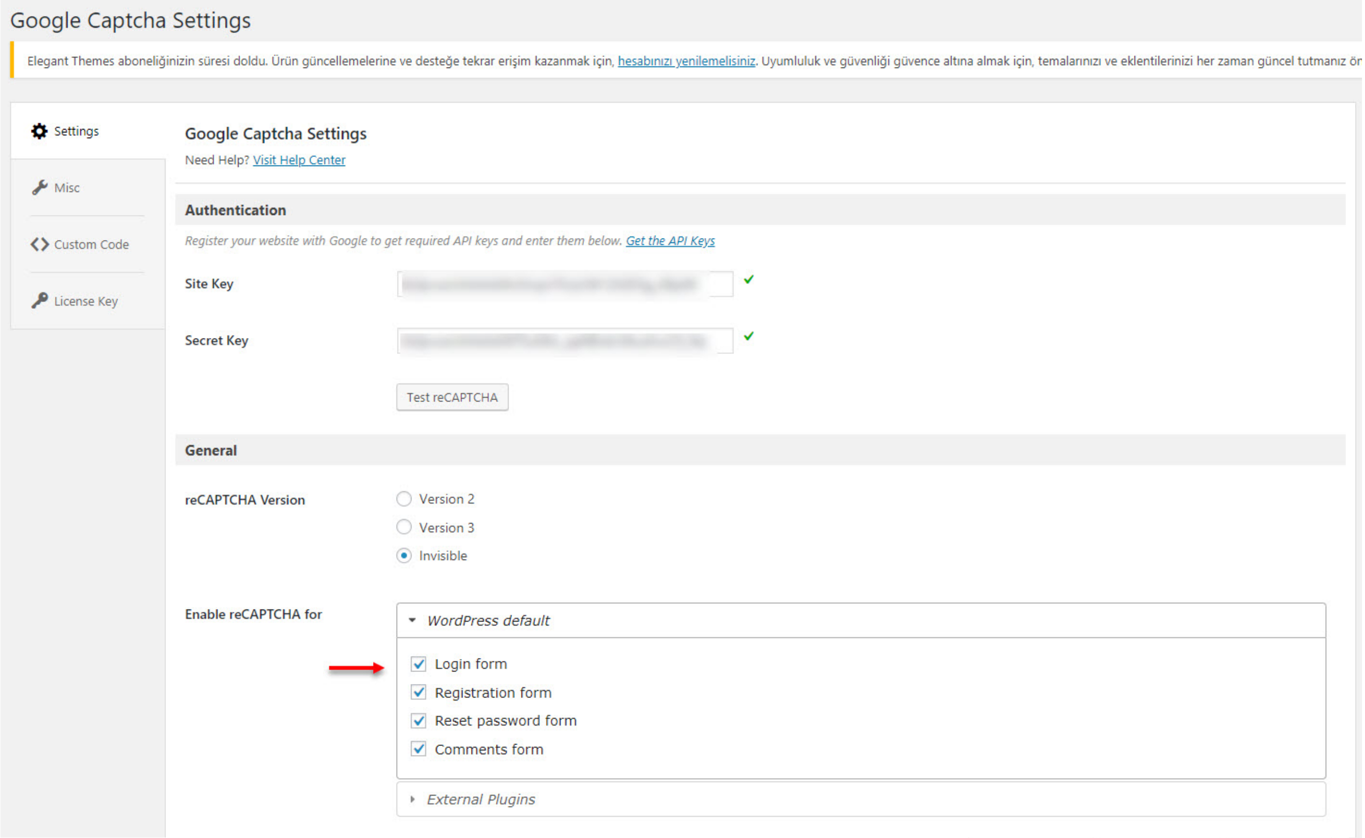
Common Passwords - npm
https://www.npmjs.com/signup/common-passwords
123456 12345 123456789 **password** iloveyou princess 1234567 12345678 ... brenda adidas kitten karen mustang isabel **natalie cuteako javier** 789456123 ...

List of most common passwords - PH4.ORG
https://www.ph4.org/pass_passlist.php
123456; 12345; 123456789; **password**; iloveyou; princess; 1234567; rockyou ... **natalie**; **cuteako**; **javier**; 789456123; 123654; sarah; bowwow; portugal; laura ...

123456 12345 123456789 password iloveyou princess ... - MSU CSE
www.cse.msu.edu/~cse231/PracticeOfComputingUsingPython/.../Password.../rockyou.txt
123456 12345 123456789 **password** iloveyou princess 1234567 rockyou ... brenda adidas kitten karen mustang isabel **natalie cuteako javier** 789456123 ...

Openwall's list
www.openwall.com/passwords/wordlists/password-2011.lst

After completing my research, I decided to tighten the security controls that I had previously relaxed. Firstly, I enabled the Google Captcha plugin for the administrator page. This added an additional layer of protection against automated login attempts. Additionally, in the Brute Force Protection section of Wordfence’s Firewall settings, I configured it to automatically block IP addresses that made failed username attempts. These measures helped strengthen the security of my website.



Google Captcha Settings

Elegant Themes aboneliğinizin süresi doldu. Ürün güncellemelerine ve desteğe tekrar erişim kazanmak için, hesabınızı yenilemelisiniz. Uyumluluk ve güvenliği güvence altına almak için, temalarınızı ve eklentilerinizi her zaman güncel tutmanız ör

Google Captcha Settings

Need Help? Visit Help Center

Authentication

Register your website with Google to get required API keys and enter them below. Get the API Keys

Site Key: [redacted] ✓

Secret Key: [redacted] ✓

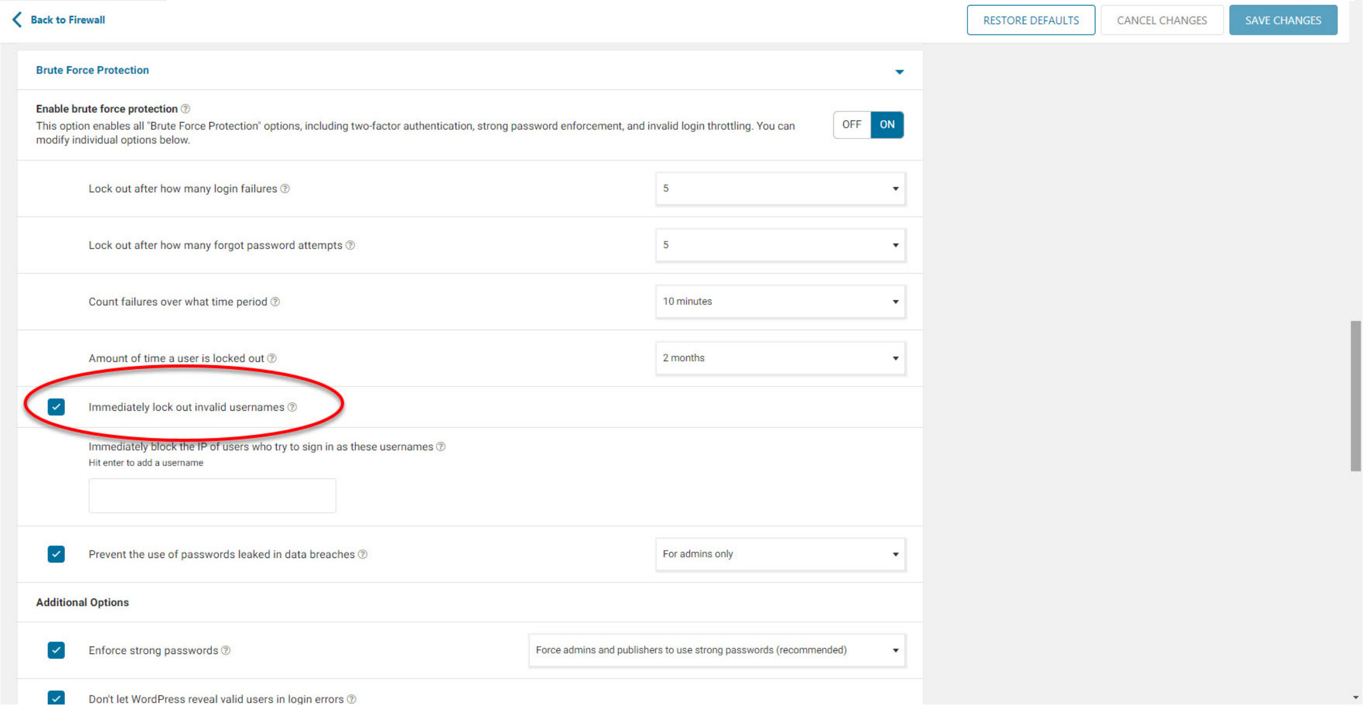
General

reCAPTCHA Version
○ Version 2
○ Version 3
● Invisible

Enable reCAPTCHA for

WordPress default
☑ Login form
☑ Registration form
☑ Reset password form
☑ Comments form

External Plugins



Brute Force Protection

Enable brute force protection
This option enables all "Brute Force Protection" options, including two-factor authentication, strong password enforcement, and invalid login throttling. You can modify individual options below.
OFF [✓ ON]

Lock out after how many login failures: 5

Lock out after how many forgot password attempts: 5

Count failures over what time period: 10 minutes

Amount of time a user is locked out: 2 months

☑ Immediately lock out invalid usernames

Immediately block the IP of users who try to sign in as these usernames
Hit enter to add a username

☑ Prevent the use of passwords leaked in data breaches: For admins only

Additional Options

☑ Enforce strong passwords: Force admins and publishers to use strong passwords (recommended)

☑ Don't let WordPress reveal valid users in login errors

As a result of this research, I sadly learned that someone has been attempting to hack my blog for months. For WordPress CMS users like myself, I strongly recommend installing and properly configuring the Google Captcha, Duo Two-Factor Authentication, and Wordfence Security plugins. Additionally, I highly recommend closely monitoring your systems with OSSEC HIDS to detect any suspicious activities. Taking these precautions is crucial to enhance the security of your WordPress website.

Hope to see you in the following articles.