WordPress Güvenliği

written by Mert SARICA | 2 September 2019
If you are looking for an English version of this article, please visit here.

Neredeyse 10 yıla yakın bir süredir siber güvenlik üzerine araştırmalar yapıp, öğrendiklerimi yazmaya, sizlerle paylaşmaya devam ediyorum. Sizlerden gelen geri bildirimlere baktığımda çoğunluğunuzun yazdıklarımdan faydalandığını görmek beni bir hayli mutlu ediyor. Kimi zaman özünde kötü niyet olmayıp sadece bana mesaj vermek için bloguma ufak çaplı siber saldırı (Örnek: DoS ile Mücadele yazısı) gerçekleştirenler, aşağıdaki gibi yönetici girişi yapmayı deneyenler olsa da bazen tam olarak sebebini ve niyetini anlayamadığım saldırılarla da karşılaşıyorum. Bundan yola çıkarak ben de bu yazımda, bu saldırılardan birini nasıl tespit ettiğime ve benim gibi WordPress CMS kullananların bloglarını nasıl güvenli hale getirebilecekleri ile ilgili ipuçları vermeye karar verdim.

☐	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

Öncelikle WordPress ile ilgili istatistiki bilgilere yer vermek gerekirse, WordPress dünya genelinde en çok kullanılan içerik yönetim sistemidir ve CMS

dünyasının ~%60‘ına hakimdir. Internet genelindeki web sitelerinin ~%33‘ünde yine WordPress kullanılmakta olup ~55.000‘den fazla yakın eklentisi bulunmaktadır. Yıllar içinde WordPress üzerinde tespit edilen zafiyet türleri değişiklik gösterse de bu zamana kadar en çok tespit edilen zafiyet türü Cross-Site Scripting (XSS)‘dir. WordPress zafiyet veritabanına baktığımızda ise WordPress’in kendi kodlarında (core) ve eklentilerinde bu zamana dek 15.000‘den fazla zafiyet tespit edildiğini görebiliyoruz.

WordPressler’in genel olarak nasıl hacklendiğine baktığımızda çoğunlukla güvensiz barındırma firmaları/hizmetleri, zayıf yönetici parolası, güncel olmayan sürüm, eklentiler, temalar ve arka kapı içeren korsan temalar (Örnek: Arka Kapı Avı yazısı) kaynaklı olduğunu görüyoruz.

Benim de zayıf yönetici parolalarını tespit etmek için denenen wp-admin sayfam her ne kadar internete açık olsa da uzun yıllardır Duo Two-Factor Authentication eklentisinden faydalanarak yönetici girişi için iki faktörlü doğrulama kullanıyorum. Ayrıca Wordfence Security eklentisinden de faydalanarak deneme yanılma saldırıları gerçekleştiren ip adreslerinin otomatik olarak engellenmesini, olası güvenlik zafiyetlerin tespit edilip raporlanmasını da sağlıyorum. Arka kapı içeren temalara karşı da ücretli tema kullanmayı tercih ediyorum. Güvensiz barındırma hizmetleri ile uğraşmamak adına da yine uzun yıllardan beri VPS kullanıyorum.

2018 yılının Temmuz ayında günlerden bir gün yine blogumun Wordfence eklentisinin güvenlik ekranını (dashboard) kontrol ederken, yönetici sayfama deneme yanılma saldırısı (brute-force) yapıp en çok bloklanan ip adreslerinin Türkiye’den olması dikkatimi çekti. IP adreslerinin whois bilgilerini kontrol ettiğimde, tamamına yakınının iDealhosting isimli barındırma servisi sağlayan bir firmaya ait olduğunu öğrendim ve güvenlik araştırması adına bu ip adreslerinden bloguma gerçekleştirilen saldırıları yakından izlemeye karar verdim.

Wordfence activity in the past week

Wordfence™

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

Update Blocked IPs

Top 5 Countries Blocked

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

Update Blocked Countries

Top 5 Failed Logins

Username	Login Attempts	Existing User
admin	7	Yes

Update Login Security Options

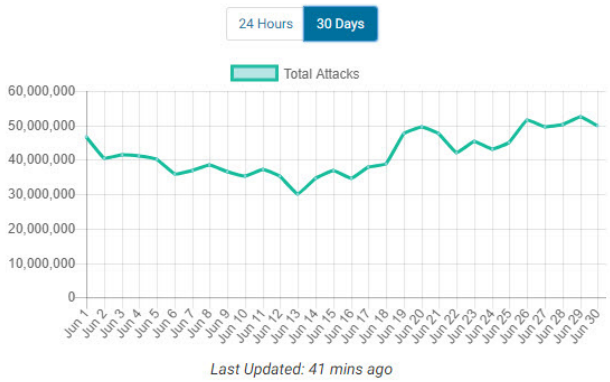
Firewall Summary: Attacks Blocked for www.mertsarica.com

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



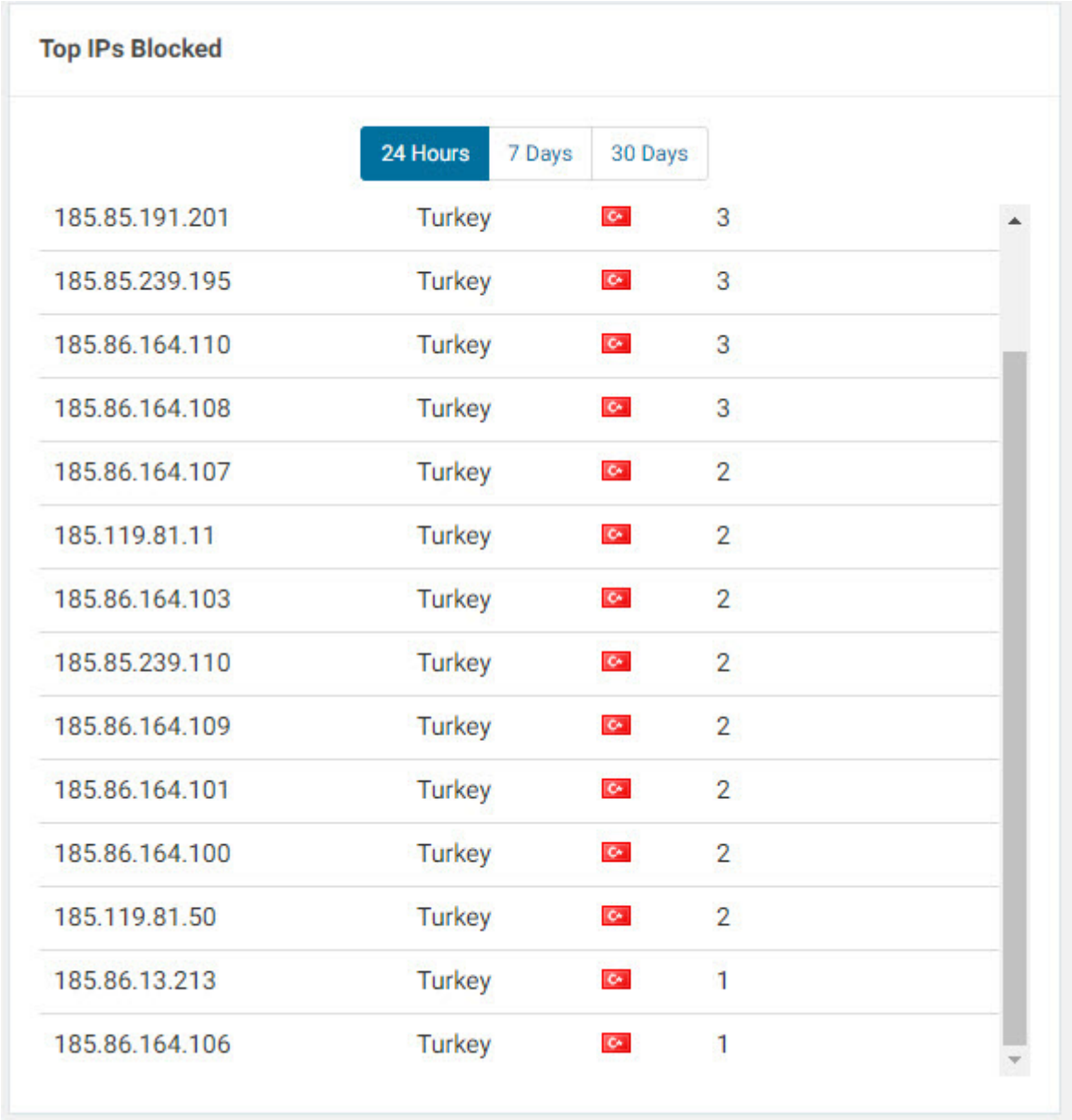
Last Updated: 41 mins ago

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



Ekim ayında güvenlik ekranını tekrar kontrol ettiğimde ise deneme yanılma saldırılarının 22 ip adresinden aralıksız olarak devam ettiğini gördüm. Tabii bir güvenlik araştırmacısı olarak aklıma gelen sorulardan ilki bunun bloguma gerçekleştirilen hedeflenmiş bir saldırı girişimi olup, olmadığıydı. Bunu öğrenmenin en kolay yollarından biri deneme yanılma saldırılarında kullanılan parolaları öğrenmekti dolayısıyla vakit kaybetmeden işe koyuldum.

Top IPs Blocked

24 Hours | 7 Days | 30 Days

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

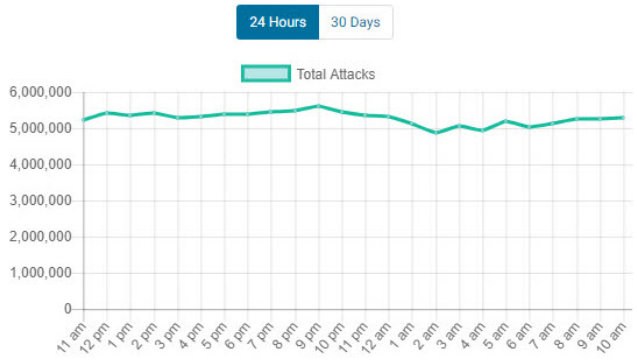
Firewall Summary: Attacks Blocked for www.mertsarica.com

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

Premium

How are these categorized?

Total Attacks Blocked: Wordfence Network



IP Tools

- Decimal IP Calculator
- ASN Information
- CIDR/Netmask
- What's your IP
- IP Geo-location Lookup
- **IPWHOIS Lookup**

Email Share

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 Go »

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

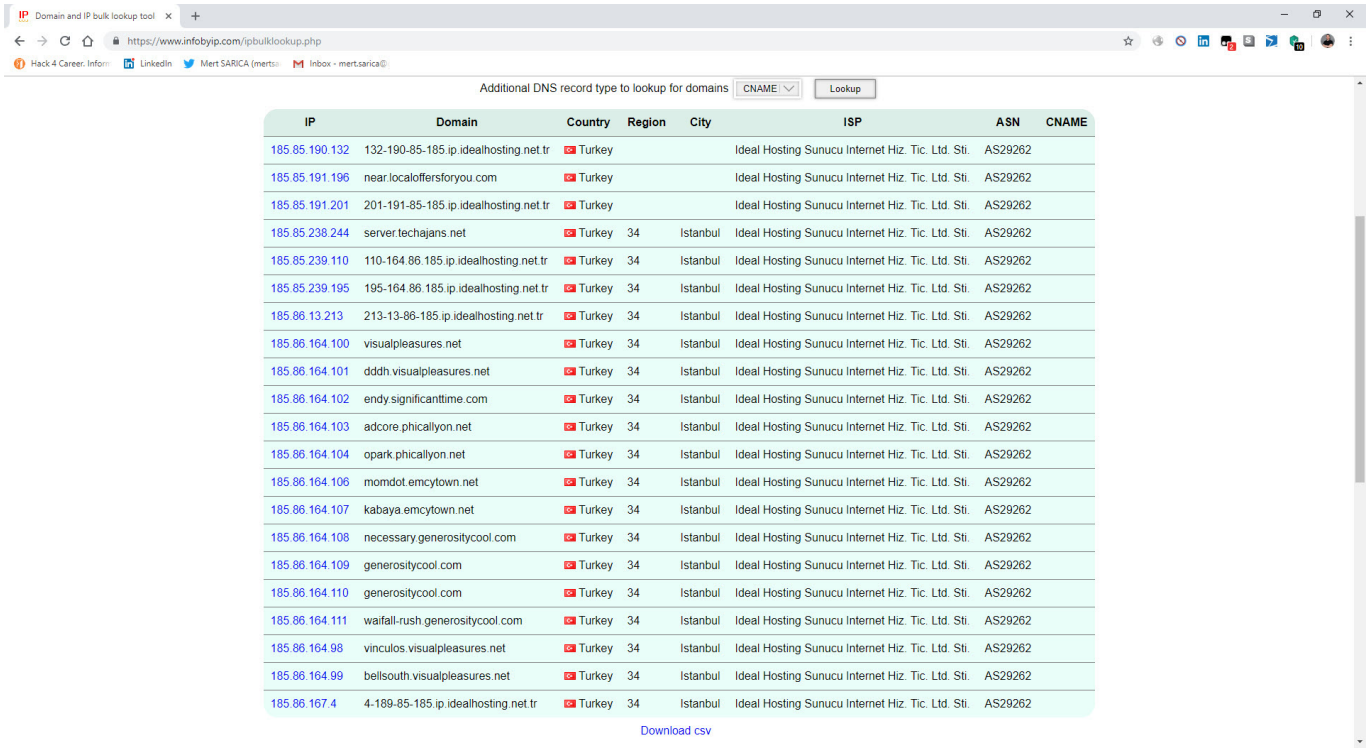
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% 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

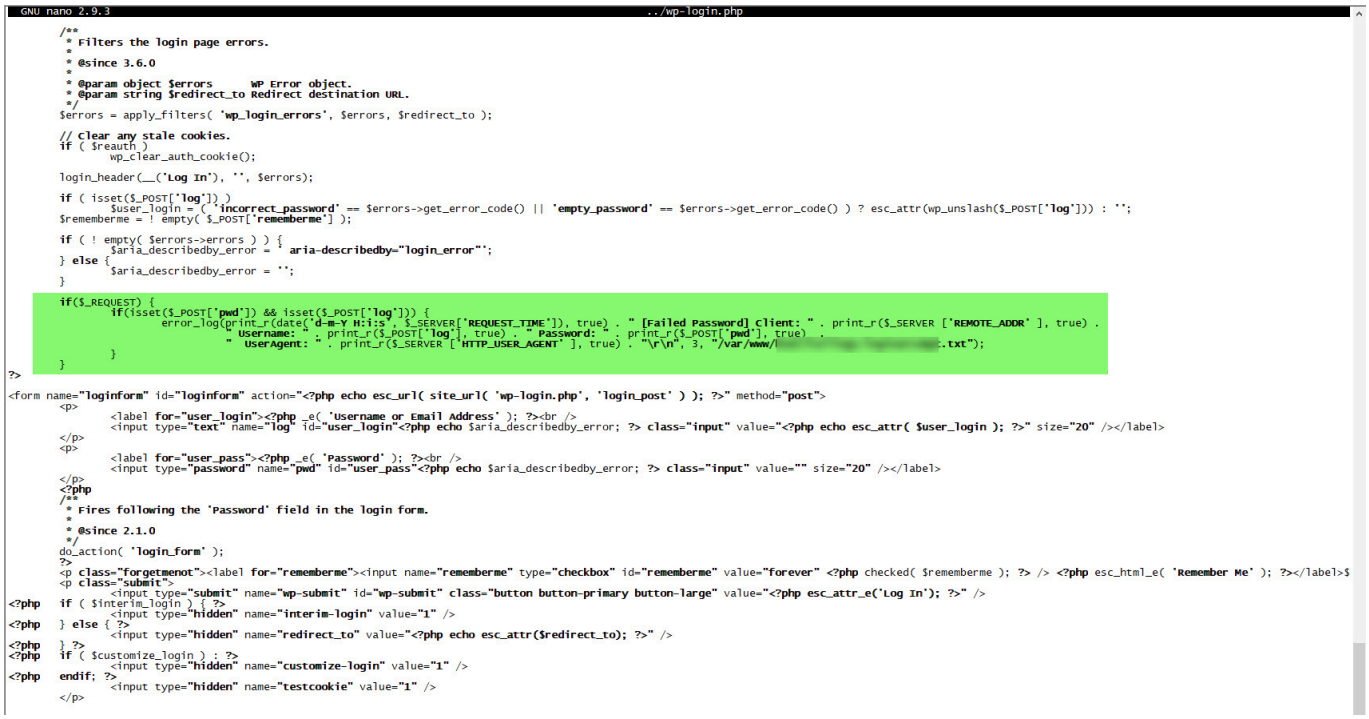
organisation:   ORG-IHSI2-RIPE
org-name:       IDEAL HOSTING SUNUCU INTERNET HIZM. TIC. LTD. STI
org-type:       Other
address:        Agaoglu 212 MyOffice K.19 D.314-315-316 Gunesli, Bagcilar / ?STANBUL
phone:          +902127060300
abuse-c:        IH1624-RIPE
```



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

İlk olarak wp-login.php dosyasına yapılan hatalı giriş denemelerini parola ile birlikte diske kayıt eden bir PHP kodu hazırladım. Ardından bu kayıt edilen dosyadaki değişikliklerden de anlık olarak haberdar olabilmek için OSSEC HIDS üzerinde küçük bir tanım yaptım.




```
        /**
         * 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>

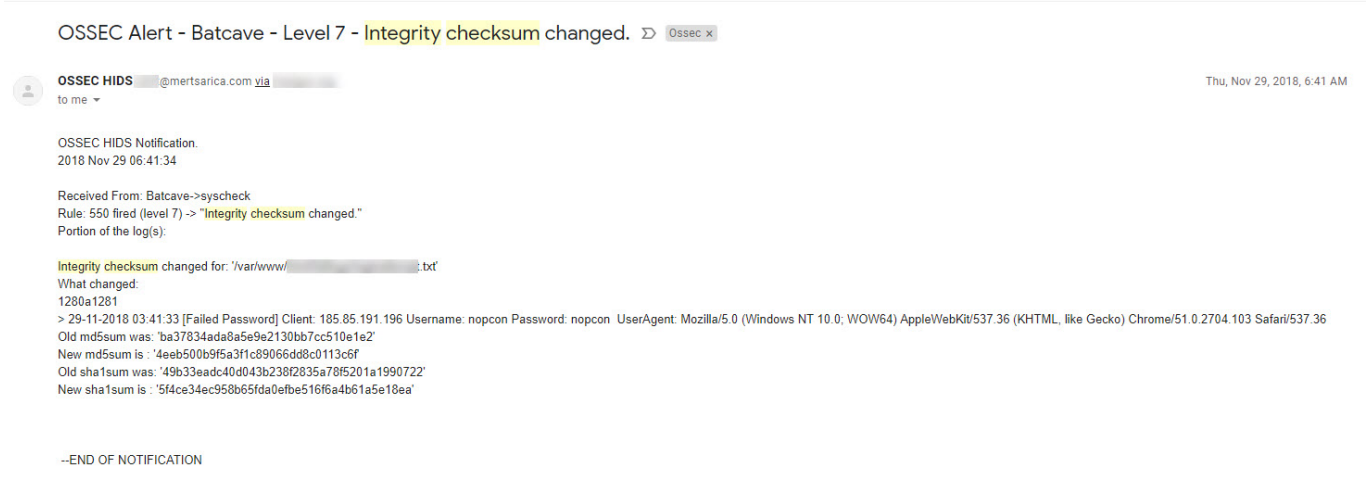
  <!--  .txt -->
  <directories report_changes="yes" realtime="yes" check_all="yes">/root/ </directories>
  <directories report_changes="yes" realtime="yes" check_all="yes">/var/www/ </directories>

  <!-- 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>
```

Ekim ayının sonu ve Kasım ayı boyunca kayıt altına alınan hatalı kullanıcı adı ve parola denemelerine baktığımda, denenen kullanıcı adı ve parolaların sözlükte yer alan sıradan kelimeler yerine blog yazılarımda geçen kelimelerden oluştuğunu öğrendim. Bu bilgi benim için hedeflenmiş bir saldırı girişimi olduğuna işaret ediyordu.



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

OSSEC HIDS @mertsarica.com via
to me

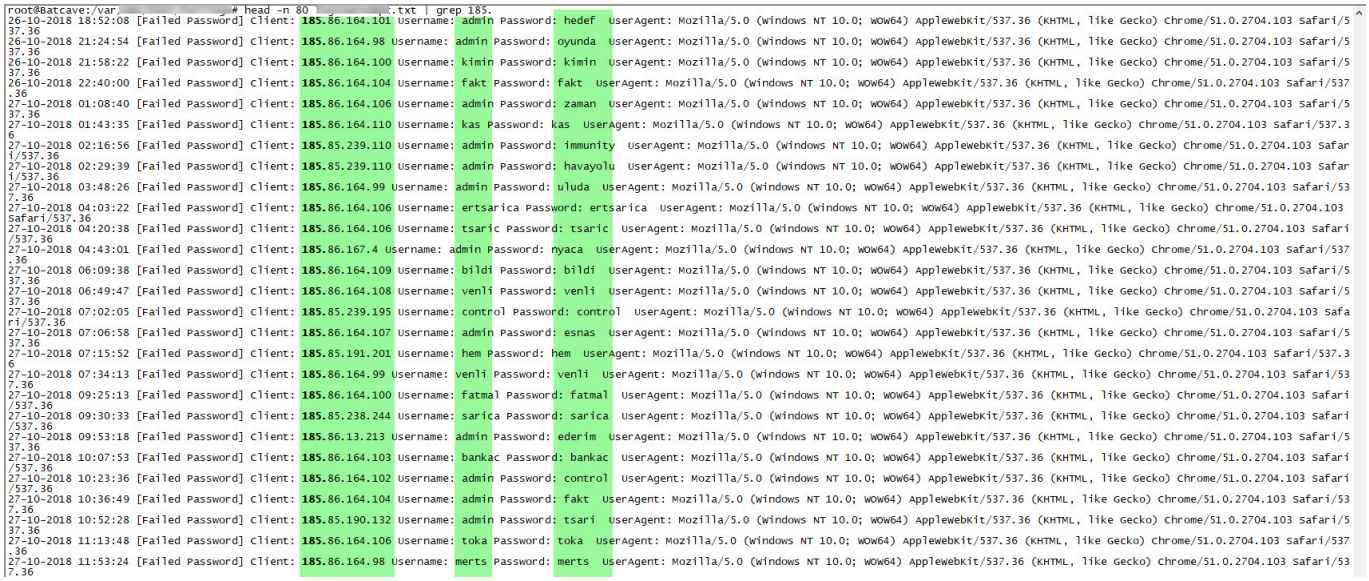
Thu, Nov 29, 2018, 6:41 AM

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

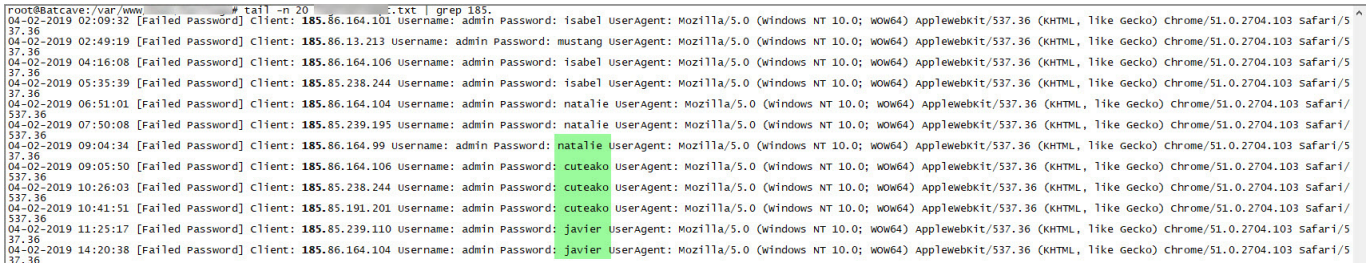
Received From: Batcave->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

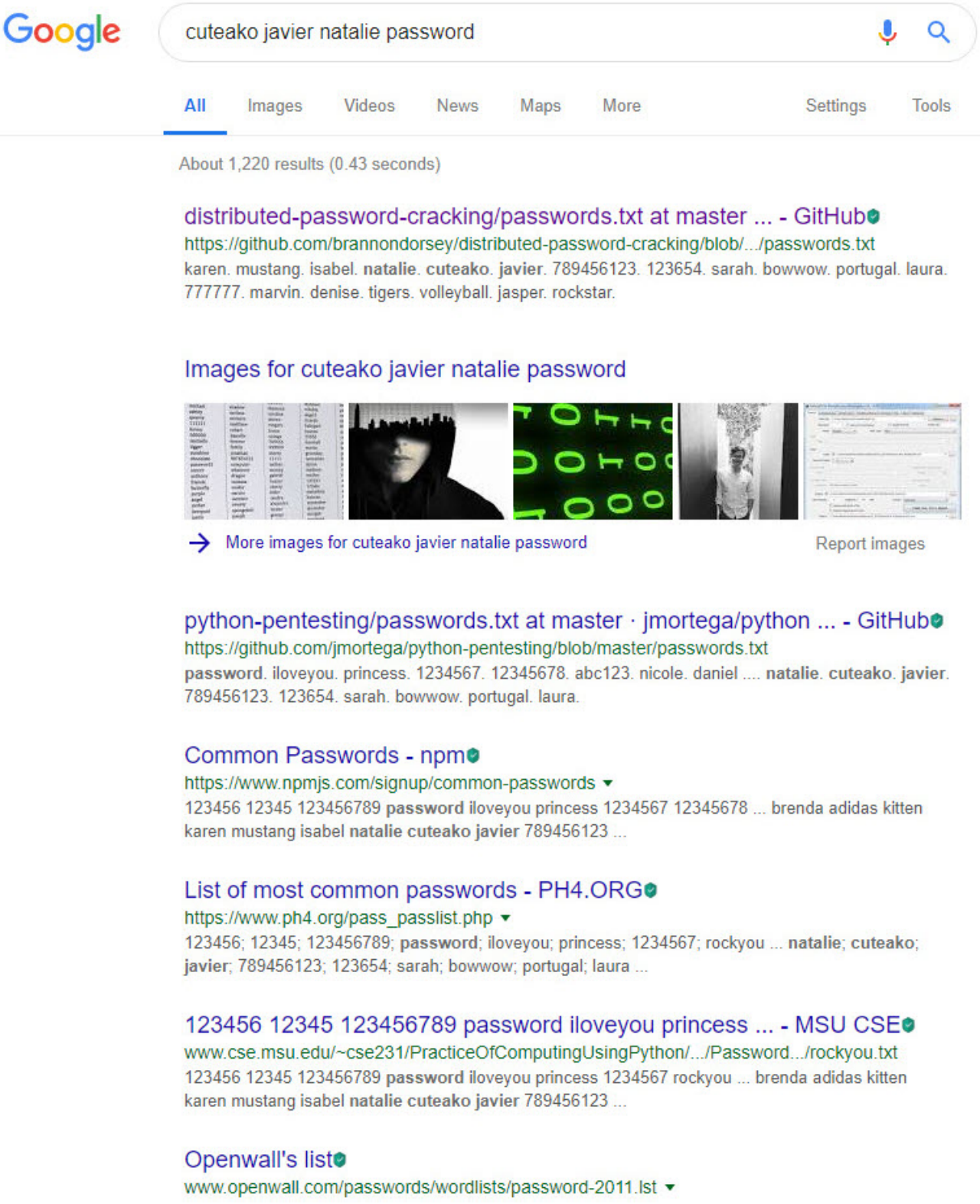
Integrity checksum changed for: '/var/www/ .txt'
What changed:
1280a1281
> 29-11-2018 03:41:33 [Failed Password] Client: 185.85.191.196 Username: nopcon Password: nopcon UserAgent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Old md5sum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

--END OF NOTIFICATION

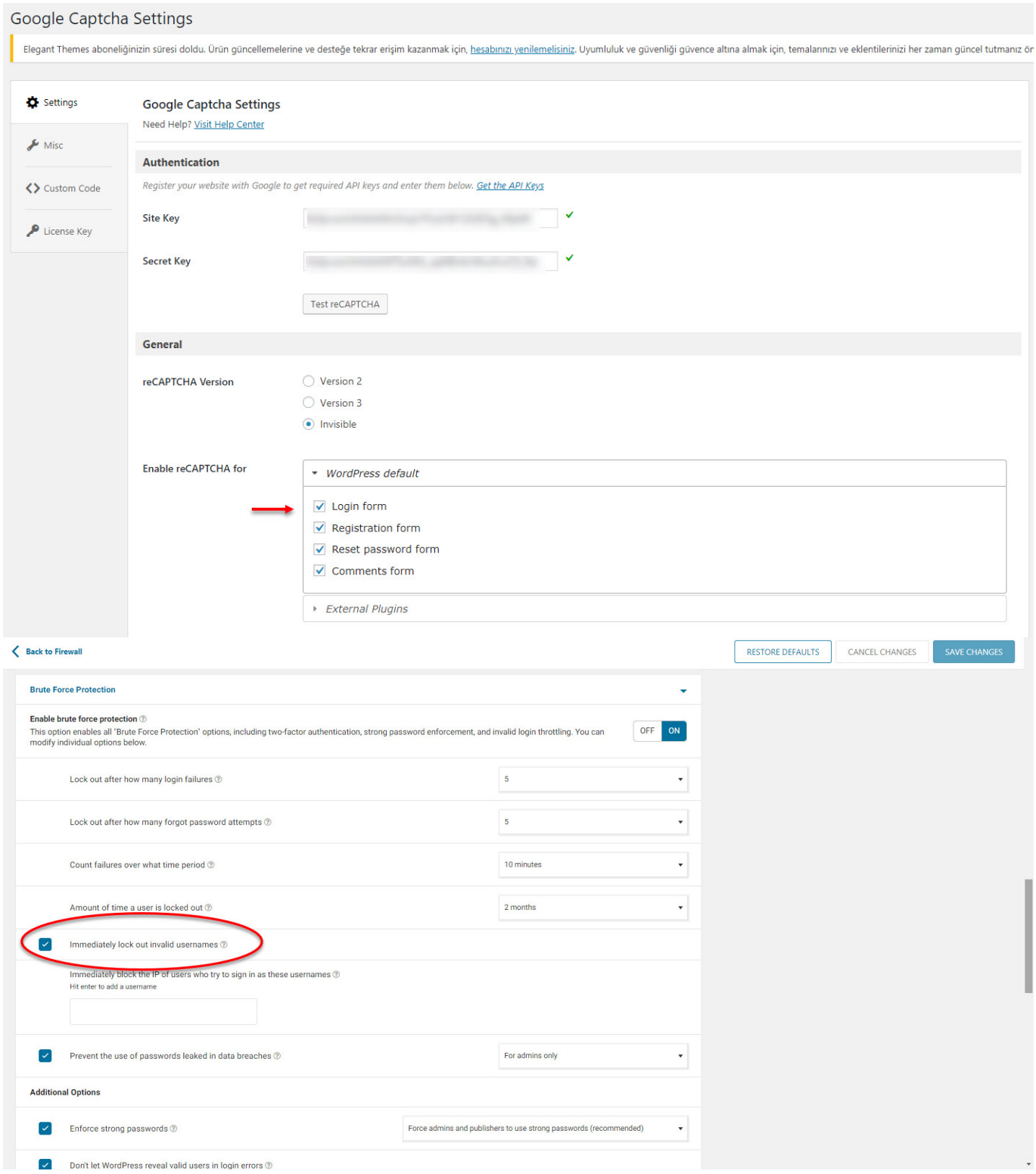


2019 yılının Şubat ayında denenen parolalara tekrar baktığımda ise bu defa 2009 yılında hacklenen Rockyou.com sitesinin veritabanından elde edilen parolaların denenmeye başladığını gördüm.





Araştırmamı tamamladıktan sonra daha önce gevşettiğim güvenlik kontrollerini sıkılaştırmak için öncelikle Google Captcha eklentisini yönetici sayfası için etkin hale getirdim. Ardından da Wordfence'in Firewall ayarları sayfasındaki Brute Force Protection bölümünde hatalı kullanıcı adı denemesi yapan ip adresinin otomatik olarak bloklanmasını sağladım.



Bu araştırma sonucunda aylardır blogumu hacklemek için birilerinin uğraştığını üzülerek öğrenmiş oldum. Benim gibi WordPress CMS kullananların ise Google Captcha, Duo Two-Factor Authentication ve Wordfence Security eklentilerini muhakkak kurup düzgün bir şekilde ayarlarını yapmalarını ve ayrıca OSSEC HIDS ile de şüpheli durumlara karşı sistemlerini yakından izlemelerini şiddetle tavsiye ederim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.