

Pi Hediye Vardı, Verdim, Gitti #2 :)

written by Mert SARICA | 15 April, 2015

Ve 3 Nisan 2015 tarihinde ikincisi düzenlenen [Pi Hediye Var](#) hacking oyununun çözüm yolu ile Raspberry Pi 2'yi kazanan talihli karşınızda!

KAYNAK KODU:

Hack 4 Career - Siber Güvenlik Blogu

```
< ?php
$username = 'misafir';
$secret = 'H4ck4C4r33r';
$pos = '';

if(isset($_GET['username'])){
    $username = $_GET['username'];
    $username = strtolower($username);
}

if(isset($_GET['hash'])){
    if (preg_match('#[0-9a-f]{32}#i', $_GET['hash'])) {
        $hash = $_GET['hash'];
        $hash = strtolower($hash);
    }
}

// Debug
//print "
" . (hash("md5",$secret.$username));
//exit;

if(isset($username) and isset($hash)){
    // print "
" . $username;
    // print "
" . $secret;
    if(hash("md5",$secret.$username) == $hash){
        $pos = strpos($username, "admin");
        if ($pos !== false) {
```

```
print "Tebrikler $username , artık en yüksek yetkiye sahipsin :)";
print "
```

Pi Hediyem Var çekilişine katılmak için bu ekran görüntüsünü ve çözüm yolunu [Mert SARICA](#) ile paylaşabilirsin";

```
} else {
    print "Merhaba $username , hala sefil kullanıcı yetkisine sahipsin :(";
    print "
```

Raspberry Pi 2 çekilişine katılabilmek için admin yetkisi ile giriş yapabilmen lazım!";

```
print "
```

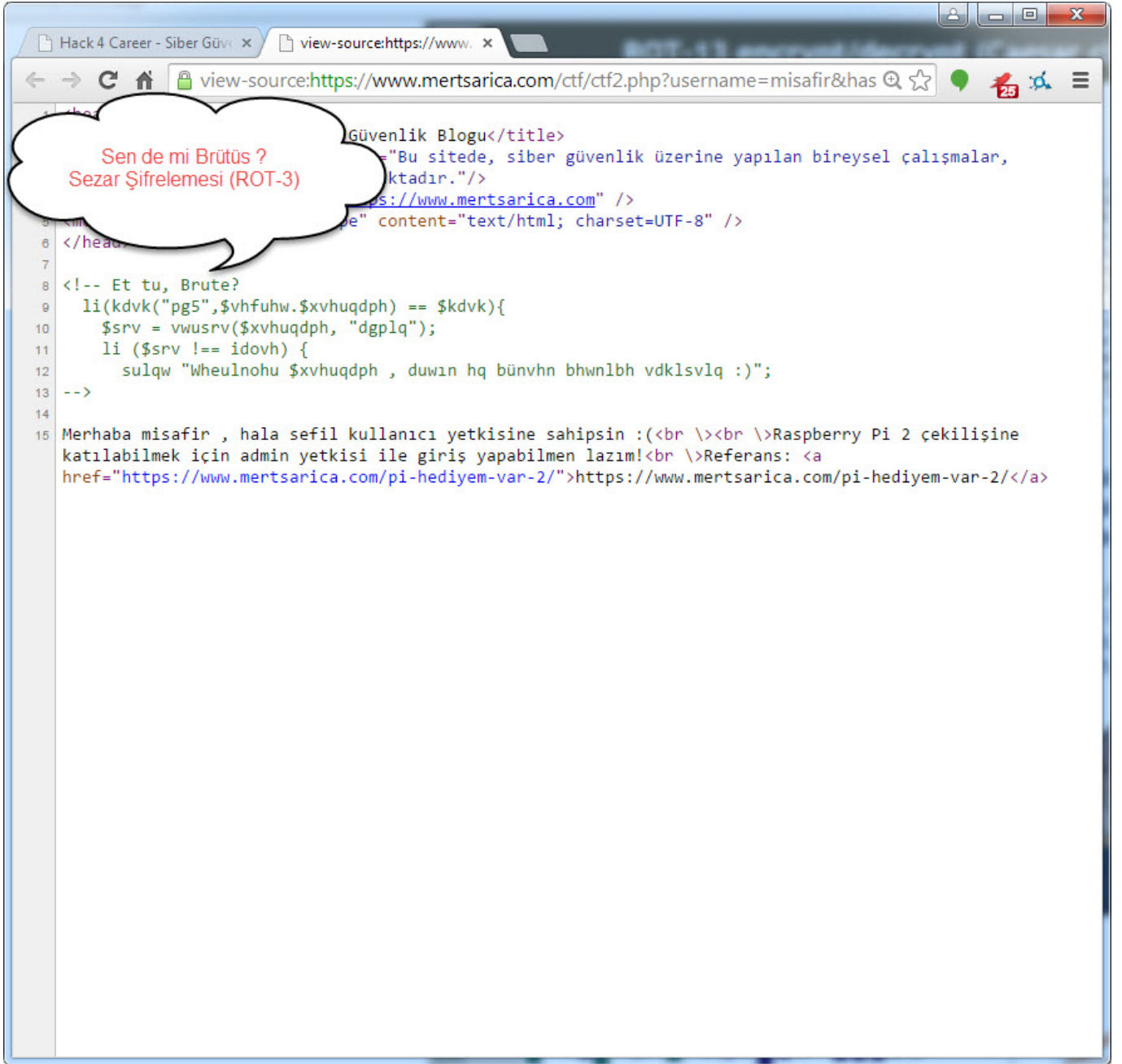
Referans: <https://www.mertsarica.com/pi-hediyem-var-2/>;

```
}
} else {
    $username = 'misafir';
    $loc = "Location: " . "https://www.mertsarica.com/ctf/ctf2.php?" .
"username=" . $username . "&hash=" . hash("md5",$secret.$username);
    header($loc);
    exit;
}
} else {
    $username = 'misafir';
    $loc = "Location: " . "https://www.mertsarica.com/ctf/ctf2.php?" .
"username=" . $username . "&hash=" . hash("md5",$secret.$username);
    header($loc);
    exit;
}
?>
```

ÇÖZÜM:

<https://www.mertsarica.com/ctf/ctf2.php> sayfasının kaynak koduna bakılarak [Et tu, Brute?](#)

[\(Sen de mi Brütüs\)](#) cümlesinden bunun [Sezar](#)'a ait bir söz olduğundan yola çıkarak gizlenmiş mesajın [Sezar'ın Şifrelemesi](#) ile oluşturulduğunu (ROT-3 kullanılmıştır) tahmin edebilirdiniz. Çözmek için ise [Google'dan](#) faydalanabilirdiniz.



The screenshot shows the Braingle website's Caesar Cipher page. The browser address bar displays `www.braingle.com/brainteasers/codes/caesar.php`. The page features a blue header with the Braingle logo and navigation links for [Sign In](#) and [Create a free account](#). Below the header is a green navigation bar with categories: [Brain Teasers](#), [Trivia](#), [Mentalrobics](#), [Games](#), and [Community](#). A secondary bar lists sub-categories: [Brain Teasers](#), [Optical Illusions](#), [Puzzle Hunts](#), and [Codes & Ciphers](#). The main content area is titled "Codes and Ciphers :: Caesar Cipher" and contains a description of the cipher, an example of encoding, and a "Caesar Encoder / Decoder" tool. The tool has a text input field for the number of letters to shift (set to 3), a "Plaintext" box containing PHP code, and a "Ciphertext" box containing the encoded output. Below the code boxes are "Encipher" and "Decipher" buttons. The sidebar on the left lists various cipher types: Monoalphabetic (Caesar, Atbash, Keyword, Pigpen / Masonic, Polybius Square), Polyalphabetic (Vigenère, Beaufort, Autokey, Running Key), Polygraphic (Playfair, Bifid, Trifid, Four-square), Transposition (Rail Fence, Route, Columnar, Transposition), and Others (Book, Beale, Morse Code, Tap Code, One-time Pad, Scytale, Semaphore, ASCII, Steganography). At the bottom of the sidebar are social sharing links for Google and del.icio.us, and an RSS feed icon.

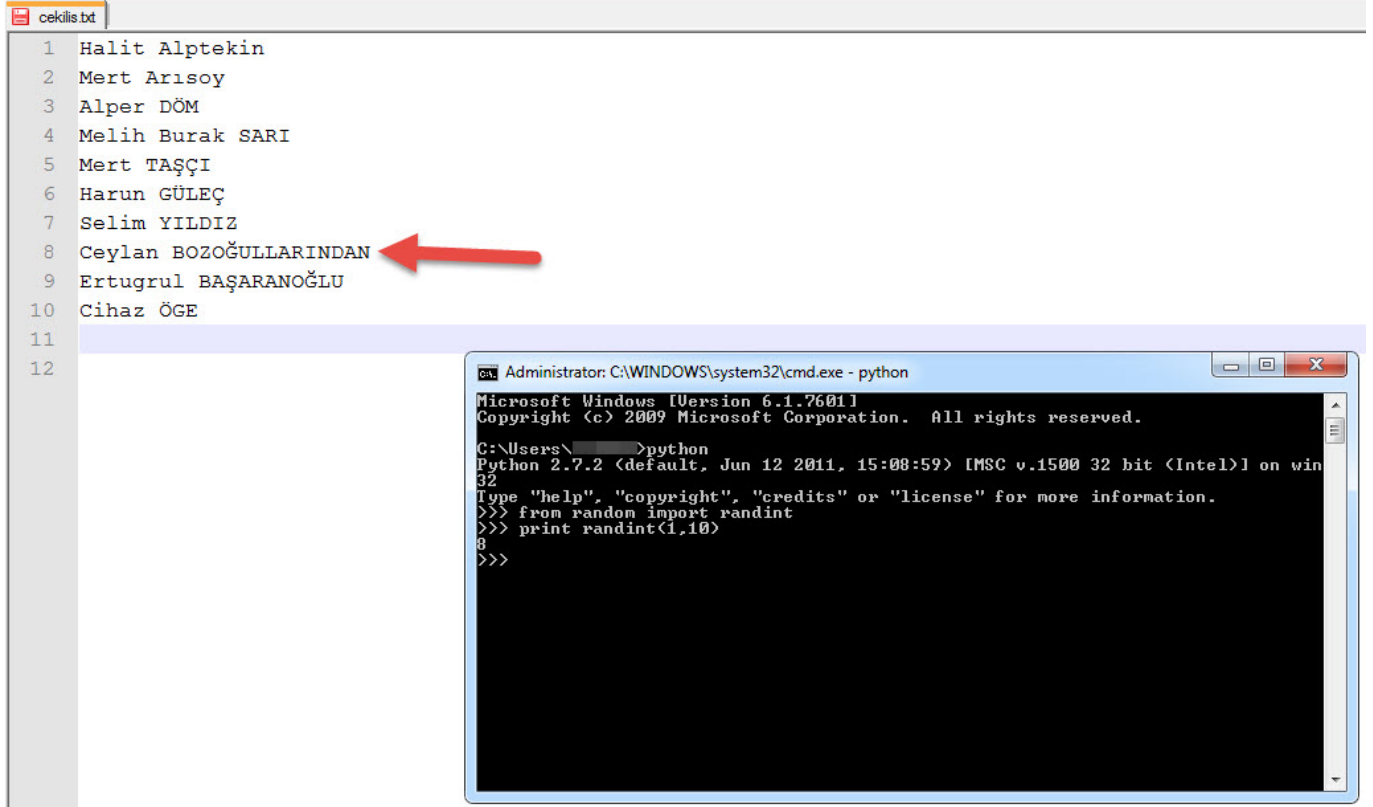
Ortaya çıkan aşağıdaki PHP kodundan, [Merkle–Damgård](#) hash fonksiyonunun [MAC](#) (mesaj doğrulama kodu) olarak kullanıldığının ve bunun da [hash uzunluk genişletme zafiyetine](#) yol açtığını anlayabilirsiniz.

```
...
if(hash("md5",$secret.$username) == $hash){
    $pos = strpos($username, "admin");
    if ($pos !== false) {
```


%00%90%00%00%00%00%00%00%00%00admind&hash=373fb330afbc0b1a5688ff4a3ef1b2a6

OYUNU BAŞARIYLA TAMAMLAYANLAR: Halit Alptekin, Deniz Parlak, Mert Arısoy, Alper DÖM, Melih Burak SARI, Mert TAŞÇI, Harun GÜLEÇ, Ali AĞDENİZ, Selim YILDIZ, Ceylan BOZOĞULLARINDAN, Ertugrul BAŞARANOĞLU, Cihad ÖGE, Kürşat Oğuzhan AKINCI (geç bildirim), Sipke Mellema

ÇEKİLİŞ ve KAZANAN TALİHLİ:



```
cekilis.txt
1 Halit Alptekin
2 Mert Arısoy
3 Alper DÖM
4 Melih Burak SARI
5 Mert TAŞÇI
6 Harun GÜLEÇ
7 Selim YILDIZ
8 Ceylan BOZOĞULLARINDAN
9 Ertugrul BAŞARANOĞLU
10 Cihaz ÖGE
11
12
```

```
Administrator: C:\WINDOWS\system32\cmd.exe - python
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>python
Python 2.7.2 (default, Jun 12 2011, 15:08:59) IMSC v.1500 32 bit (Intel) on win
32
Type "help", "copyright", "credits" or "license" for more information.
>>> from random import randint
>>> print randint(1,10)
8
>>>
```

Başta kazanan talihli **Ceylan BOZOĞULLARINDAN** olmak üzere oyunu başarıyla çözen, katılan, destekleyen, sponsor olan herkese teşekkür eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim.