

Pi Hediye m Vardı, Verdim, Gitti #2 :)

written by Mert SARICA | 15 April 2015

Ve 3 Nisan 2015 tarihinde ikincisi düzenlenen Pi Hediye m 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 Hediye 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-hediye-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);

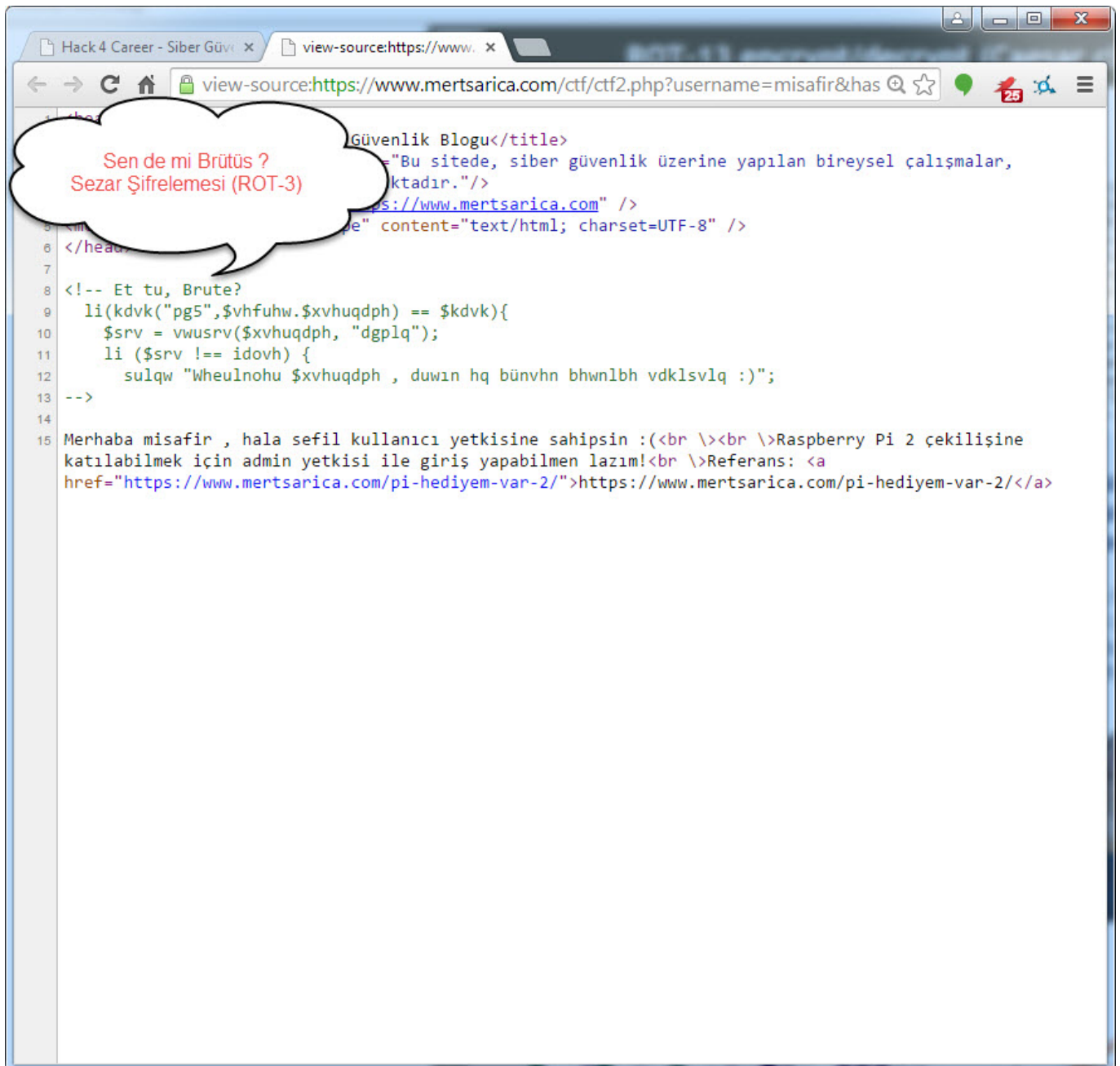
```

```
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.



```
view-source:https://www.mertsarica.com/ctf/ctf2.php?username=misafir&has

Güvenlik Blogu</title>
="Bu sitede, siber güvenlik üzerine yapılan bireysel çalışmalar,
ktadır."/>
ps://www.mertsarica.com" />
e" content="text/html; charset=UTF-8" />
6 </head>
7
8 <!-- Et tu, Brute?
9   li(kdvk("pg5",$vhfuhw.$xvhuqdph) == $kdvk){
10    $srv = vwusrv($xvhuqdph, "dgplq");
11    li ($srv != idovh) {
12      sulqw "Wheulnohu $xvhuqdph , duwın hq bünvhn bhwnlbh vdklsvlq :)";
13    -->
14
15 Merhaba misafir , hala sefil kullanıcı yetkisine sahipsin :(<br \><br \>Raspberry Pi 2 çekilişine
katılabilmek için admin yetkisi ile giriş yapabilmen lazım!<br \>Referans: <a
href="https://www.mertsarica.com/pi-hediyem-var-2/">https://www.mertsarica.com/pi-hediyem-var-2/</a>
```

The screenshot shows the Braingle website's Caesar Cipher page. The page is titled "Codes and Ciphers :: Caesar Cipher" and provides an overview of the cipher method. It includes a sidebar with links to various cipher types such as Monoalphabetic, Polyalphabetic, Polygraphic, Transposition, and Others. The main content area features a "Caesar Encoder / Decoder" tool with a text input field for the number of letters to shift (set to 3), a plaintext input field containing "This is a secret message", and a ciphertext output field showing "wklv lv d vhfuhw phvvdjh". Below the tool are "Encipher" and "Decipher" buttons. The page also contains a "Your Ad Here" placeholder and a "#101" identifier.

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");
```