Pi Hediyem Vardı, Verdim, Gitti #2 :)

written by Mert SARICA | 15 April 2015

Ve 3 Nisan 2015 tarihinde ikincisi düzenlenen Pi Hediyem 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 "

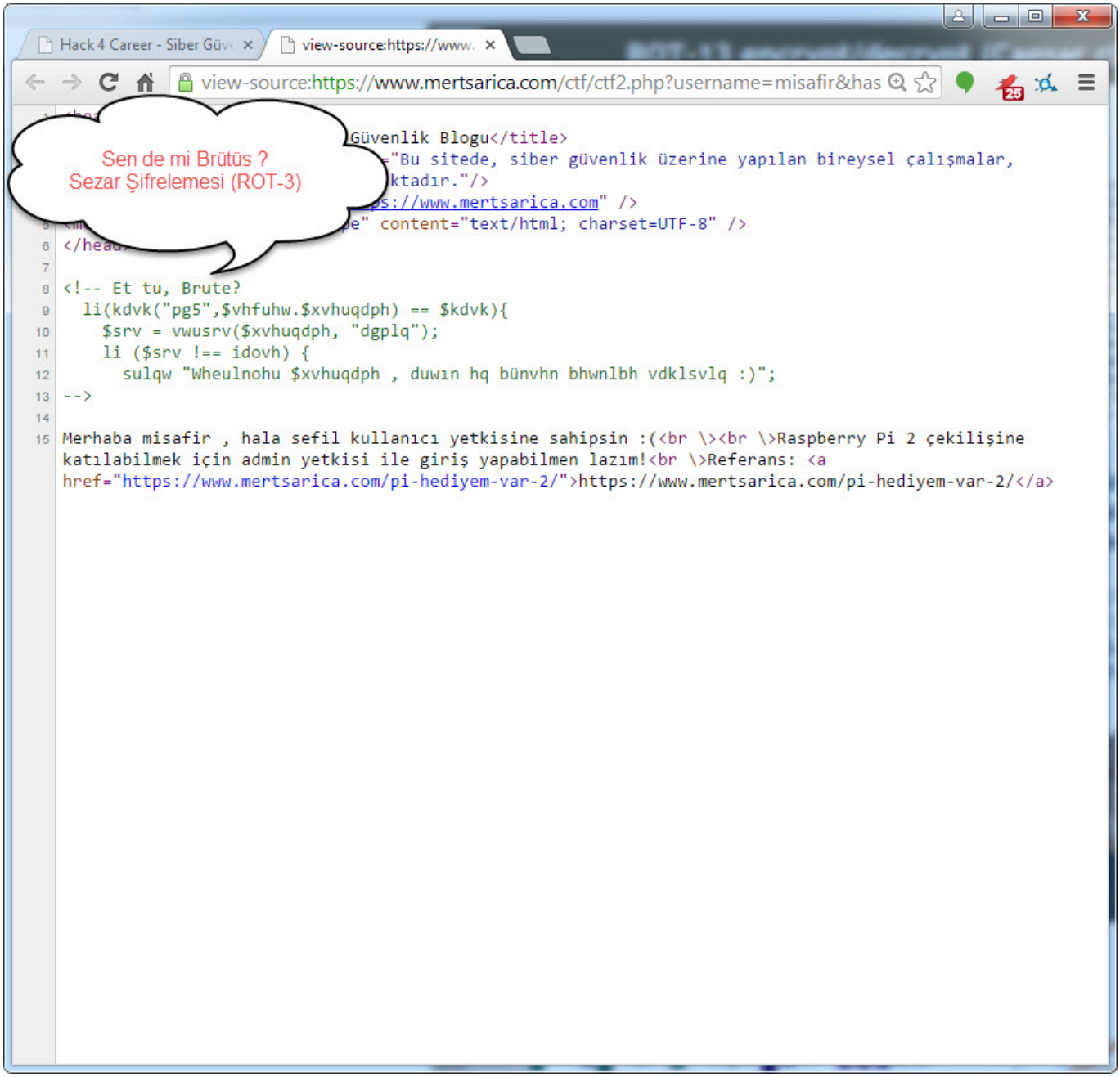
Pi Hediyem Var çekilişine katılmak için bu ekran görüntüsünü ve çözüm yolunu
Mert SARICA ile paylaşabilirsin";
    } else {
      print "Merhaba $username , hala sefil kullanıcı yetkisine sahipsin :(";
      print "

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.



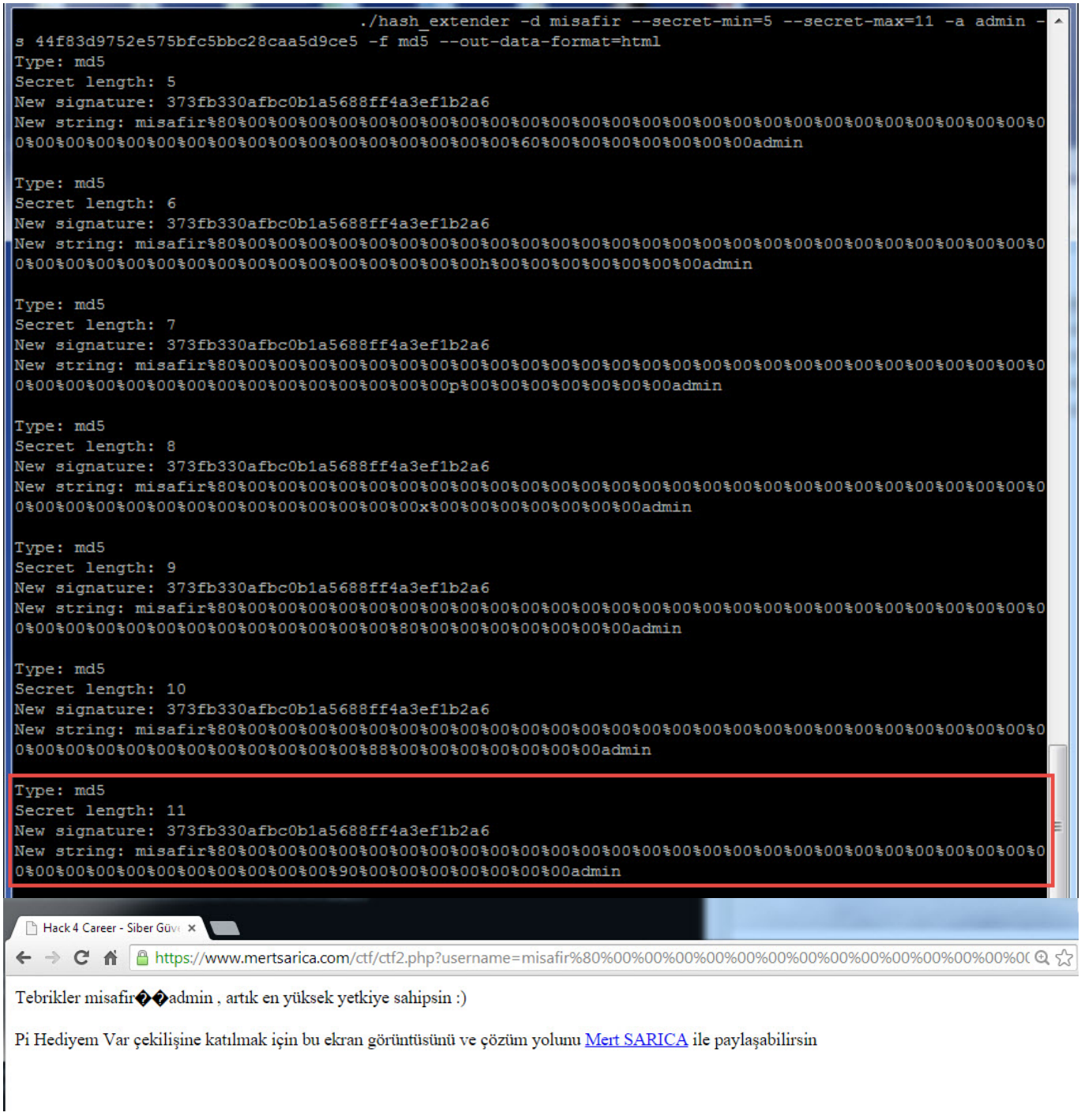


Ortaya çıkan aşağıdaki PHP kodundan, Merkle–Damgård hash fonksiyonunun MAC (mesaj doğrulama kodu) olarak kullanıldığının ve bunun da hash uzunluk genişletme zafiyetine yol açtığını anlayabilirdiniz.

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

```
    if ($pos !== false) {
      print "Tebrikler $username , artık en yüksek yetkiye sahipsin :)";
  ...
```

strpos fonksiyonu ile username parametresinde admin karakter dizisi (string) kullanıldığında, kullanıcıya yönetici yetkisi (admin) verildiği için, hash uzunluk genişletme saldırısından faydalanarak username parametresine admin karakter dizisini manuel olarak veya hash_extender aracı ile (deneme yanılma yöntemi ile secret değişkeninin 11 hane olduğunu bulacaktınız) ekleyebilir, yeni üretilen hash değerini de hash parametresi ile birlikte sunucuya göndererek başarıyla admin yetkisine sahip olabilirdiniz.


./hash_extender -d misafir --secret-min=5 --secret-max=11 -a admin -s 44f83d9752e575bfc5bbc28caa5d9ce5 -f md5 --out-data-format=html
Type: md5
Secret length: 5
New signature: 373fb330afbc0b1a5688ff4a3ef1b2a6
New string: misafir%80%00%00%00

https://www.mertsarica.com/ctf/ctf2.php?username=misafir%80%00%00%00