

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 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);

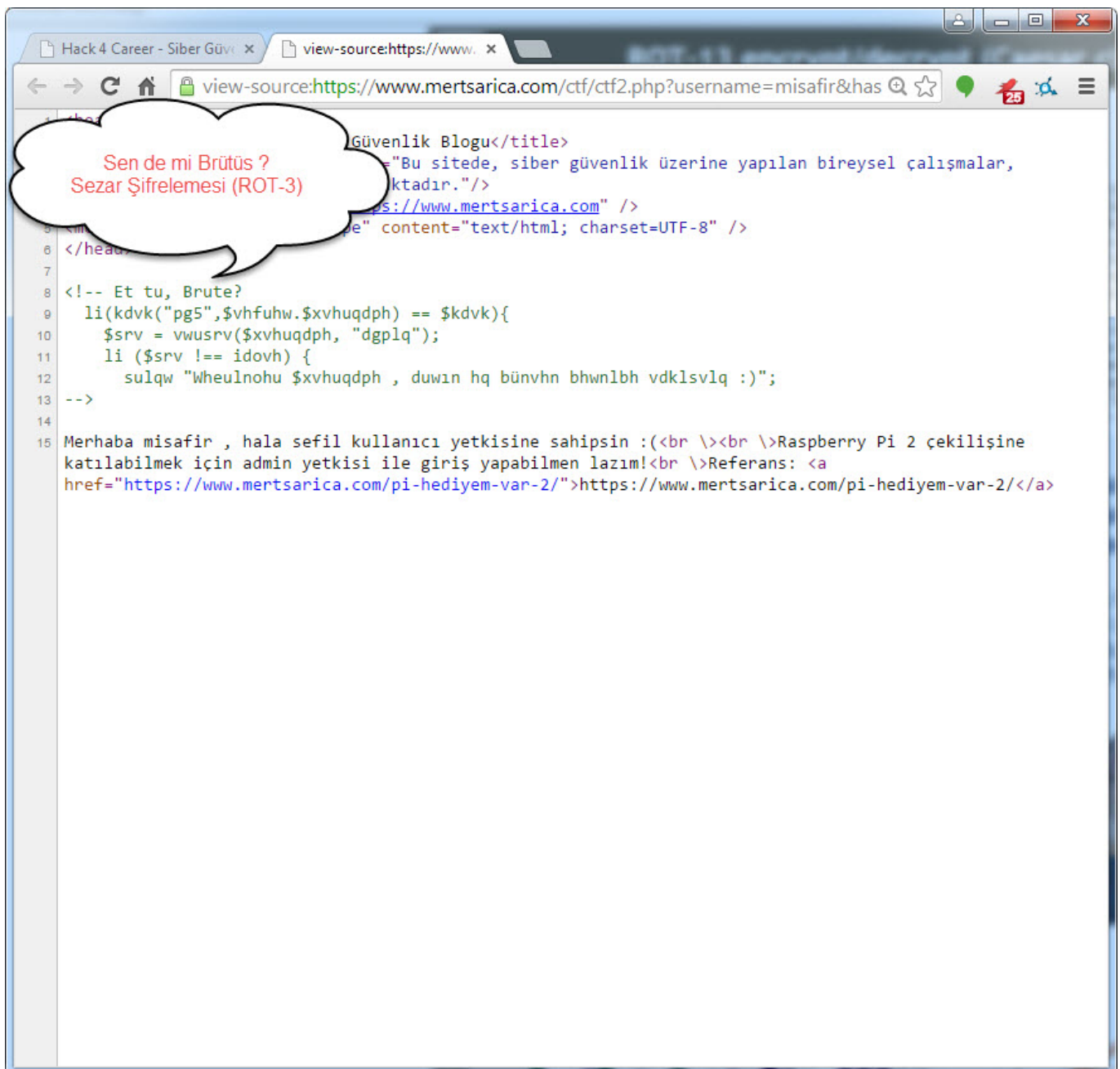
```

```
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.



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");
```

■ ■ ■

[illegible]

```
https://www.mertsarica.com/ctf/ctf2.php?username=misafir%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%90%00%00%00%00%00%00admin&hash=373fb330afbc0b1a568ff4a3ef1b2a6
```

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:

```
cekkilis.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
```



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.