



Tek Kullanımlık Şifre

QuiPass ile Tek Kullanımlık Şifre Gönderimi Örnek Uygulama
ve Entegrasyon Kılavuzu

www.quipass.com

Ekim - 2010

QuiPass ile internet siteniz veya uygulamalarınız üzerinden tek kullanımlık şifre gönderimi için başlangıç ve entegrasyon kılavuzu ile örnek uygulama incelemesi.

İÇİNDEKİLER

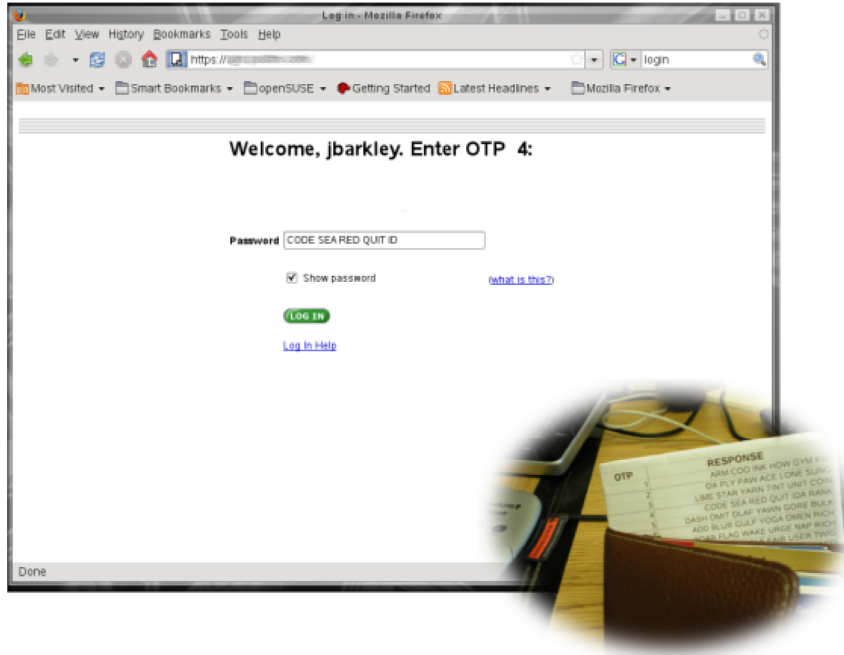
QuiPass ile Tek Kullanımlık Şifre Gönderimi	2
Tek Kullanımlık Şifre Nedir?	2
QuiPass ile Tek Kullanımlık Şifre	3
QuiPass Şifre Gönderim İlkeleri	3
QuiPass Tek Kullanımlık Şifre Uygulamaları Nasıl Eklenir?	3
Tek Kullanımlık Şifre Uygulaması Oluşturma Sonuç Ekranı.....	4
Örnek Tek Kullanımlık Şifre ile Giriş Uygulaması: İŞ UYGULAMASI	6
Genel Bakış ve Tasarlanan Senaryo	6
Tek Kullanımlık Şifre Gönderimi, Yetkilendirme ve Girişi.....	6
Tek Kullanımlık Şifre PHP Demo Uygulaması Dosya ve Açıklamaları	8
Entegrasyon	10
HTTP Protokolü İçin Örnek Entegrasyon.....	11
HTTPS Protokolü İçin Örnek Entegrasyon	12
Hata Kodları	13
QuiPass İstem Yetkilendirme Bilgileri	14
Servis Erişim Adresleri.....	14
Gönderilmesi Zorunlu Olan Bilgiler	14

QUIPASS İLE TEK KULLANIMLIK ŞİFRE GÖNDERİMİ

TEK KULLANIMLIK ŞİFRE NEDİR?

Tek Kullanımlık Şifre (veya İngilizce adıyla: One Time Password – OTP) yalnızca bir oturum süresince veya tek bir yetkilendirme (uygulama veya internet sitesine giriş) için kullanılmak üzere belirli algoritma veya kurallarla üretilen şifrelerdir. Geleneksel sabit şifrelerin aksine tahmin edilmesi veya çeşitli yöntemlerle (örneğin, deneme-yanılma) aşılması neredeyse mümkün olmayan bir güvenlik çemberi sağlamaktadır. Bunun en önemli nedeni sabit bir şifrenin yeterli süre ve yeterli deneme imkanı olduğunda aşılabilmesidir. Ancak; tek kullanımlık şifre bir defaya mahsus olmak üzere, rastgele ve belirli bir geçerlilik süresinde kullanım amacıyla üretildiği için kötü niyetli kişilerin bu şifreleri kırmasına yeterli zaman yeterli deneme imkanını sağlamamaktadır.

Geçmişten günümüze tek kullanımlık şifreler bir çok yöntemle üretilerek sistemlerce doğrulanması sağlanmaktadır.



Kağıt üzerinde önceden üretilmiş ve sistem tarafından istenen sıradakinin girildiği tek kullanımlık şifreler.

(Kaynak: Wikipedia)

Zaman Senkronizeli, Talep Anında veya Matematiksel Algoritmalarla Tek Kullanımlık Şifre Üreticileri



Her bir kullanıcı için tahsis edilmesi gereken şifre üretici cihazlar (yaygın adıyla, Token) belirlenen periyotlara, matematiksel algoritmalarla veya kullanıcı talebine göre ilgili sisteme girişi mümkün kılan şifreler üreterek ekranında göstermektedir ve kullanıcının ekranda gördüğü şifreyi sisteme girmesiyle yetkilendirme sağlanmaktadır. Token'lar zaman senkronizeli, kullanıcı talebi üzerine veya bir matematiksel algoritmalarla şifre üretimi yapmak üzere farklı özelliklere sahip olarak üretilmektedir. Token'ların en büyük olumsuz yanı ise her bir kullanıcı için tahsis edilme zorunluluğu sebebiyle maliyetleridir.

(Görsel Kaynak: Wikipedia)

QUIPASS İLE TEK KULLANIMLIK ŞİFRE

QuiPass tek kullanımlık şifre uygulamasını kullanıcılarına başka hiçbir ek ödeme, masraf veya donanım maliyetleri olmaksızın SMS üzerinden sağlamaktadır. Yaygın şifre üretim yöntemlerinin aksine QuiPass kullanıcılarına şifre üretim kurallarını belirleme imkanı sağlamaktadır. Böylece, her defasında rastgele üretilecek olan şifrelerin hani karakterleri içereceği, kaç karakterden oluşacağı gibi kuralları belirleyerek mümkün olan en üst düzeyde güvenliği sağlamayı kullanıcıların yönetim, gereksinim ve kararlarına bırakmaktadır.

QUIPASS ŞİFRE GÖNDERİM İLKELERİ

QuiPass, kullanıcılarının; mümkün olan en güvenli şifreyi, mümkün olan en kısa sürede ve sağlayabileceği en yüksek güvenlik düzeyinde üreterek göndermelerini sağlamaktadır.

- Şifreler belirlenen kurallara göre, anlık ve rastgele üretilir.
- Şifre üretim kuralları içerisindeki karakter listeleri, karmaşaya yol açacak karakterleri içermez. *Örneğin*, O harfi, 0 rakamı, l (büyük l) harfi, l (küçük L) harfi gibi..
- Şifre SMS içerikleri anlık olarak üretilir ve öncelikli kanaldan anında gönderilir.
- Şifre SMS'leri tek sefer gönderilir.
- Şifre SMS'leri, alıcıya ulaşmaz ise gönderim tekrarlanmaz.
- Gönderilen SMS'ler pazarlama mesaj filtresine takılmaz.
- Her bir alıcı, 3 dakika içerisinde yalnızca tek şifre talebinde bulunabilir.
- QuiPass, hesabınız üzerinden gönderilen Şifre SMS'lerinin anlık olarak iletim durumlarını gösterir.
- Gönderilen SMS maliyetleri kullanıcıya anlık olarak yansıtılır ve açıkça raporlandırılır.

QUIPASS TEK KULLANIMLIK ŞİFRE UYGULAMALARI NASIL EKLENİR?

QuiPass kullanıcı panelindeki Uygulama Yönetimi menüsünde bulunan Uygulama Ekle öğesine tıklayarak veya Uygulama İşlemleri sayfasında bulunan Yeni Bir Uygulama Ekle kısayolunu kullanarak yeni bir tek kullanımlık şifre uygulaması oluşturabilirsiniz.

Uygulama Bilgileri

Temel Bilgiler

Uygulama Türü: 1

Alan Adı: (Öm: *example.com/musteriPaneli*) 2

Şifre Oluşturma Kuralları

Karakter Grupları:

- ABCDEFGHJKLMNPQRSTUVWXYZ 3
- 23456789
- abcdefghijklmnopqrstuvwxyz
- 23456789ABCDEFGHIJKLMNPQRSUWXYZ

Karakter Sayısı: 4 5 6 8 4

1 2 3 5

(Uygulama Ekleme Ekranı, Açıklamalar bir sonraki sayfada mevcuttur.)

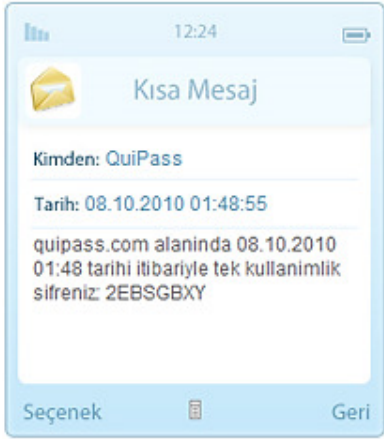
1	Uygulama Türü: Şifre gönderim türünün belirleyicisi olan opsiyonu Tek Kullanımlık Şifre olarak belirleyin.
2	Alan Adı: Bu alana, gönderilecek olan şifrelerin hangi alan veya uygulama için geçerli olduğunu girin. (Bu, kullanıcının talep ettiği şifrenin hangi alana ait olduğunu belirtmek amacıyla şifre SMS'inde gösterilir.)
3	Karakter Grupları: Oluşturulacak olan tek kullanımlık şifrenin hangi karakter grupları kullanılarak üretileceğini seçin.
4	Karakter Sayısı: Üretilecek olan tek kullanımlık şifrenin, kaç karakterden oluşacağını belirleyin. (Tek kullanımlık şifre için, üretilecek olan şifrelerin 8 karakterden oluşması önerilmektedir.)
5	İşlem Butonları
1	Önizleme: Belirlenen opsiyonlar doğrultusunda kullanıcı cihazlarına gönderilecek olan tek kullanımlık şifre iletilerinin bire bir örnek önizlemesini gösterir.
2	Uygulama Kaydet: Girilen değerler ve belirlenen seçenekleri kaydederek yeni bir uygulama oluşturmanızı sağlar.
3	Vazgeç: İşlemi iptal eder.

UYGULAMA OLUŞTURMA SONUÇ EKRANI

[Yeni Bir Uygulama Ekle](#) [Uygulama İşlemleri Sayfasına Git](#) 1

Tebrikler!
Yeni uygulama başarıyla eklendi.

Uygulama Önizlemesi 2



Seçenek 3 Geri

(Kaydedilen Yeni Uygulama Ekranı)

Tek kullanımlık şifre uygulamanıza ait bilgileri girmeniz ve seçenekleri belirlemenizin ardından size uygulama oluşturma sonucunu gösteren ve uygulamanız üzerinden gönderilecek olan şifre iletilerinin birebir örneği şeklinde oluşturulmuş bir önizlemeyi içeren bir sonuç ekranı göstereceğiz.

- 1 Kısayollar:** Uygulamanızı oluşturmanızın ardından kullanabileceğiniz sayfalara ait kısayollar.
- 2 Önizleme Görüntüsü:** Oluşturduğunuz uygulama üzerinden gönderilecek olan şifre iletilerinin birebir kopyasıyla oluşturulmuş önizleme görüntüsü.

(Örnek Tek Kullanımlık Şifre Uygulaması sonraki sayfadan devam etmektedir.)

PHP İLE ÖRNEK TEK KULLANIMLIK ŞİFRE İLE GİRİŞ UYGULAMASI: İŞ UYGULAMASI

GENEL BAKIŞ VE TASARLANAN SENARYO

QuiPass ile Tek Kullanımlık Şifre güvenliğinin nasıl sağlanabileceğini genel şekliyle göstermek ve örnek kodlar ile kolayca kullanabilmenizi sağlamak üzere PHP geliştirme dili ile, **İşUygulaması** adlı örnek bir çalışma hazırlandı.

Hazırlanan senaryoya göre, example.com organizasyonuna ait, web tabanlı bir yönetim uygulaması olan İşUygulaması'na kullanıcı girişi tek kullanımlık şifre ve standart kullanıcı adı – şifre doğrulamasıyla sağlanmaktadır.

Kullanıcı bilgileri, demo uygulamanın veritabanından bağımsız olarak çalışabilmesi için **include/kullanicilar.php** adlı dosyada saklanmaktadır. Örnek uygulama üzerinde kullanıcı bilgileri yalnızca; kullanıcı adı, şifre, parola ve cep telefonu numarasından oluşmaktadır.

Tek kullanımlık şifre ile giriş sağlamak istediğiniz alanlarda kötü amaçlı kullanım ihtimalini ortadan kaldırmak için, QuiPass iki aşamalı bir giriş ekranı kullanmanızı önermektedir.

İşUygulaması'nda da yukarıdaki paragrafta belirtildiği üzere, iki aşamalı bir yetkilendirme mekanizması tasarlanmıştır.

TEK KULLANIMLIK ŞİFRE GÖNDERİMİ, YETKİLENDİRME VE GİRİŞİ

Kullanıcı tek kullanımlık şifre ile giriş yapmak istediğinde ilk olarak, kullanıcı adı ve parola ikilisinden oluşan bir doğrulama yapıp, ardından kullanıcı bilgilerini bu iki veriyle doğrularak; tek kullanımlık şifre gönderilecek olan kullanıcıya ait cep telefonu numarasını kullanıcı bilgilerinden çekmektedir.

Bu anda ./otpGiris.php dosyası,

```
// EĞER KONTROLLERDE HATA YOKSA, QuiPass'e alıcı bilgisi ile birlikte şifre gönderim talebinde bulunulur.
$talepBilgileri = 'u='.$quipassKullaniciAdi.'sp='.$quipaseSifre.'sapp='.$quipassUygulamaKodu.'cr='.$alici;
$tekKullanimlikSifre = istemGonder($quipassApiUrl,$talepBilgileri); // Talep QuiPass'e gönderiliyor.
```

- Eğer ilk aşamadaki yetkilendirme başarılıysa, sistem QuiPass'e tek kullanımlık şifre talebini iletir
- QuiPass, iletilen talebin içerdiği bilgiler doğrultusunda şifreyi üreterek alıcıya gönderir.

- Eğer gönderim başarılıysa alıcıya gönderilen şifrenin MD5 hash'i \$tekKullanimlikSifre değişkenine QuiPass tarafından çıktı olarak metin şeklinde aktarılır.
- Bu aşamada QuiPass tarafından, MD5 hash yerine (dökümanda açıklama ve tanımlayıcı kodları mevcut olan) hatalardan biri çıktı olarak gönderildiyse veya talebi ileten fonksiyon herhangi bir hata oluşturduysa, İşUygulaması hata açıklamasını sistem yöneticisine e-posta ile iletir. (Bu işlemi gerçekleştiren kodların ekran görüntüsü aşağıdadır.)

```

13 if(!$tekKullanimlikSifre)
14 {
15     // istemGonder fonksiyonunun herhangi bir hata yürütmesi halinde hata mesajı göster.
16     echo '<div class="hataDiv"><strong>HATA: </strong> Şu anda cep telefonunuza şifre gönderilemediği için işleminizi tamamlayamıyoruz. Lütfen kısa bir süre sonra tekrar deneyin veya sorunun devam etmesi halinde sistem yöneticinizle iletişime geçin.</div><hr /><a href="index.php?giris=otp">Geri Dön</a>';
17 }
18 elseif(strstr($tekKullanimlikSifre, "HATA"))
19 {
20     // QuiPass'e iletilen talebin hata döndürmesi halinde kullanıcıya hata mesajı göster ve, QuiPass hata açıklamasını çeşitli diğer bilgilerle birlikte yöneticiye e-posta olarak gönder.
21     echo '<div class="hataDiv"><strong>HATA: </strong> Şu anda cep telefonunuza şifre gönderilemediği için işleminizi tamamlayamıyoruz. Lütfen kısa bir süre sonra tekrar deneyin veya sorunun devam etmesi halinde sistem yöneticinizle iletişime geçin.</div><hr /><a href="index.php?giris=otp">Geri Dön</a>';
22     mail($yoneticiEPosta, 'Tek Kullanımlık Şifre Gönderim Hata Açıklaması', $tekKullanimlikSifre . "\n\nALICI: " . $alici . "\n\nUGULAMA KODU: " . $quipassUygulamaKodu);
23 }

```

- Eğer kullanıcı yetkilendirmesi, talebin QuiPass'e iletilmesi veya QuiPass tarafından üretilen şifrenin alıcıya iletilmesi işlemlerinde herhangi bir sorunla karşılaşmadıysa, şifrenin alıcıya iletiildiği ve üretilen şifrenin MD5 hash'inin QuiPass tarafından çıktı olarak uygulamaya aktarıldığı anlaşılır. Bu durumda İşUygulaması QuiPass'in çıktısını oturum değişkenlerine kaydeder.

```

28 $_SESSION['tekKullanimlikSifre'] = $tekKullanimlikSifre;

```

- **GÜVENLİK UYARISI:** Bu aşamada önemli bir nokta, QuiPass çıktısının olası tüm açıkların önüne geçebilmek amacıyla oturum değişkenlerine değil veritabanındaki geçici bilgileri tutan bir tabloya kaydedilmesi önerilmektedir. İşUygulaması gerçek bir uygulama olmadığından yalnızca işleyişin sunulabilmesi amacıyla, QuiPass çıktısı oturum değişkenlerine kaydedilmiştir.
- Kullanıcıya gönderilen şifrenin ve geçici doğrulama tablosuna veya oturum değişkenlerine aktarılan QuiPass çıktısının saklanması için kullanıcıya tek kullanımlık şifre giriş ekranı gösterilir.

iş uygulaması

examplecom

HESAP BİLGİLERİM
Giriş Bilgilerimi Hatırlat

SORUNLARINIZ MI VAR?
Giriş Yapamıyorsanız Tıklayın

GÜVENLİK PROTOKOLLERİ
Güvenlik Uygulamalarını Öğrenin

✓
Tek Kullanımlık Şifre ile Giriş

UYARI: Lütfen cep telefonunuza gönderilen tek kullanımlık şifreyi giriniz.

Tek Kullanımlık Şifreniz:

✓ Giriş Yap

Uyarı: Bu, gerçek bir uygulamaya veya servis değildir. Finansal veya kişisel bilgileriniz istenmez, işlenmez ve toplanmaz.

QuiPass - Tek Kullanımlık Şifre ve Mobil Onay Kodu Gönderim Servisi
(C) 2010 QuiPass - Tek Kullanımlık Şifre - Demo

- Kullanıcı, QuiPass tarafından iletilen tek kullanımlık şifreyi ilgili alana girer.
- **GÜVENLİK UYARISI:** QuiPass çıktısı ile kullanıcı tek kullanımlık şifre girdisini kıyaslamadan veya herhangi bir işlem yapmadan önce, herhangi bir anahtar kullanarak tüm girdilerin veya sisteme aktarılan verilerin güvenliğini arttırıcı önlemler almanız QuiPass tarafından tavsiye edilir. Örneğin, QuiPass çıktısının “ac812175fbeatdb0550899be0d571eec” olduğunu varsayalım. Bu çıktının **md5('ac812175fbeatdb0550899be0d571eec'.Şahtarim);** şeklinde ikinci kez md5 hash'ini alın ve ardından kullanıcı girdisinin “12345678” olduğunu varsayarsak; **ŞkullaniciGirdisi = md5('12345678');** **ŞkullaniciGirdisiKiyaslamaKodu = md5(ŞkullaniciGirdisi.Şahtarim);** şeklinde belirlediğiniz bir anahtar kodla tekrar hash'ini alarak bunu sağlayabilirsiniz.
- ./otpOturum.php dosyasındaki kodların, kullanıcı girdisiyle QuiPass çıktısını karşılaştırmasının ardından, herhangi bir hata veya yanlış giriş durumu oluşmadığı takdirde, sistem tarafından oturum açılır ve kullanıcı yetkilendirmesi tamamlanır.

Giriş başarılı!
Uygulamaya yönlendiriliyorsunuz...

- **GÜVENLİK UYARISI:** Kullanıcı yetkilendirmesinin ardından, kullanıcı üzerine kayıtlı olduğunuz tek kullanımlık şifreyi kullanıcı çıkışı yaptığında veya belirli bir oturum zaman aşımı süresi sonrasında boşaltarak, üretilen şifrenin yalnızca tek sefer kullanıldığından emin olmanız QuiPass tarafından önemle tavsiye edilir.

TEK KULLANIMLIK ŞİFRE PHP DEMO UYGULAMASI DOSYA VE AÇIKLAMALARI

İşUygulaması adlı örnek tek kullanımlık şifre uygulaması dosya listesi ve dosya açıklamaları tablosu.

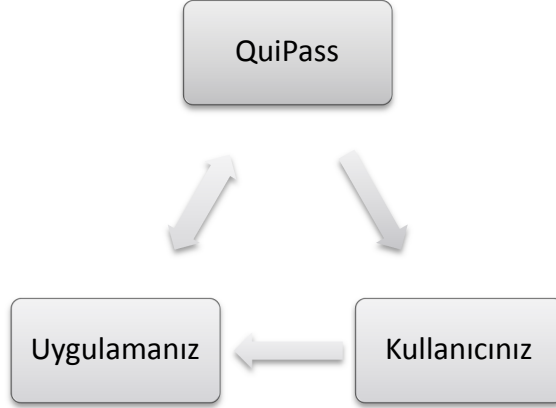
Ana Klasör	
index.php	Kullanıcı giriş ekranını ve Standart Giriş ve Tek Kullanımlık Şifre ile Giriş formlarını gösterir.
otpGiris.php	Kullanıcının, Tek Kullanımlık Şifre ile Giriş yapması için birinci aşamada istenen kullanıcı adı - parola ikilisinin kontrolünün yapılarak kullanıcı bilgilerine ulaşılması, şifre gönderim talebinin QuiPass'e iletilmesini, QuiPass çıktısının saklanması ve hata raporlamasını sağlar ve başarılı şifre iletiminin ardından Tek Kullanımlık Şifre giriş formunu gösterir.
otpOturum.php	Kullanıcının Tek Kullanımlık Şifre alanına girdiği şifreyle, QuiPass tarafından sisteme aktarılan şifre imzasını (orijinal şifrenin MD5 hash'ini) kıyaslayarak yetkilendirmeyi sonuçlandırır.

(Alt klasörlere ait açıklamalar sonraki sayfada bulunmaktadır.)

include/ klasörü	
alt.php	Örnek uygulama tasarımı alt kısmını içerir.
ayarlar.php	Tek Kullanımlık Şifre talebinin QuiPass'e iletilmesi için gerekli olan API erişim bilgilerini (QuiPass hesabınıza ait kullanıcı adı ve şifre) ile kullanacak olduğunuz QuiPass uygulamasına ait Uygulama Kodu ve demo üzerinde hata rapor gönderimi için kullanılacak olan yönetici e-posta adresi gibi bilgileri barındırır.
fonksiyonlar.php	Tek Kullanımlık Şifre talebinin QuiPass'e iletilmesi için kullanılacak olan istemGonder() fonksiyonunu içerir.
Kullanıcılar.php	İşUygulaması kullanıcı erişim bilgilerini (kullanıcı adı, parola, şifre, cep telefonu numarası) içerir. Bu bilgiler Tek Kullanımlık Şifre ile giriş yapacak olan örnek kullanıcıya aittir. İstedığınız herhangi şekilde düzenleyebilirsiniz.
Ust.php	Örnek uygulama tasarımı üst kısmını içerir.
css/ Klasörü	Örnek uygulama stil bilgilerini içeren global.css dosyasını içerir.
r/ Klasörü	Örnek uygulama görsellerini içerir.
js/ Klasörü	Jquery, javascript kütüphanesini içerir.

ENTEGRASYON

QuiPass tek kullanımlık şifre uygulamanızı oluşturmanızın ardından şifre SMS gönderimlerini yapmaya başlayabilmeniz için geriye kalan tek adım uygulama veya internet siteniz üzerindeki ilgili alana servis erişim kodlarını entegre etmektir. Yapılması gereken işlemleri ve süreci özetlemek gerekirse:



- 1 Kullanıcınız, uygulama, yönetim paneli veya internet siteniz üzerinde giriş yapmak ister.
- 2 Uygulamanız veya internet siteniz, kullanıcının yapmak istediği işlem doğrultusunda QuiPass hesabınıza ait yetkilendirme bilgileri ve kullanıcının cihazına ait numara ile talepte bulunur.
- 3 Uygulama veya internet sitenizin QuiPass'e ilettiği talep doğrultusunda oluşturulan şifre kullanıcı cihazına ve oluşturulan şifrenin imzası (md5 hash) talebinize cevap çıktısı olarak tarafınıza iletilir.
- 4 Son olarak kullanıcı girdisiyle, web siteniz veya uygulamanıza QuiPass tarafından iletilen şifre imzasını kıyaslayarak doğrulama işlemi tarafınızca gerçekleştirilir.

Aşağıda başlangıç kılavuzunda da mevcut olan örnek entegrasyon kodları verilmiştir.

(Örnek entegrasyon kodları sonraki sayfada bulunmaktadır.)

HTTP PROTOKOLÜ İÇİN ÖRNEK PHP ENTEGRASYONU

Aşağıdaki **istemGonder()** adlı PHP fonksiyonu, uygulamanız üzerinden uzak sunucularla POST metodu ile veri alışverişi yapmanızı sağlamaktadır. Fonksiyonun çalışması için sunucunuz üzerinde CURL eklentisi kurulu olmalıdır. Eğer CURL kurulu değilse fsockopen() PHP fonksiyonunu kullanarak aynı işlemi gerçekleştirebilirsiniz.

```
<?php
function istemGonder($url,$istem)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER,1);
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $istem);
    curl_setopt($ch, CURLOPT_TIMEOUT, 10);
    $cevap = curl_exec($ch);
    curl_close($ch);
    return $cevap;
}
?>
```

istemGonder() fonksiyonu çalışmak için iki argümana ihtiyaç duymaktadır:

- 1- **\$url:** İstem yapılacak olan uzak sunucu adresi. (örn: <http://www.quipass.com/api/>)
- 2- **\$istem:** Uzak sunucuya gönderilecek olan veriler. (örn: [u=johndoe&p=123456&app=102448](#))

İstem uzak sunucuya ulaşması ve uzak sunucuda işlenmesinin ardından, **istemGonder()** fonksiyonu uzak sunucunun cevap çıktısını tutacaktır.

Gönderim sırasında herhangi bir hata oluşmamışsa bu çıktı, kullanıcı cihazına gönderilen şifreye ait imza olacaktır. Aksi takdirde HATA ibaresiyle birlikte hata kodu ve kısa açıklaması bu çıktıda yer alacaktır.

```
<?php

$url = 'http://www.quipass.com/api/';
$istem = 'u=kullaniciAdiniz&p=sifreniz&app=uygulamaKodu&r=aliciTelefonu';

$sonuc = istemGonder($url, $istem);

?>
```

Yukarıdaki kodla basit bir şekilde, gönderilen şifrenin imzasını alabilir ve **\$sonuc** değişkenini kullanarak kullanıcı girdisini kıyaslayabilirsiniz.

DİKKAT: Güvenli ve sorunsuz çalışan bir sistem için lütfen gerekli hata kontrollerini sağlayarak şifre gönderim taleplerinizi oluşturun ve çıktıları yine kontrol ederek işleyin.

HTTPS PROTOKOLÜ İÇİN ÖRNEK PHP ENTEGRASYONU

HTTPS protokolü üzerinden servis erişimini sağlamak ve çıktıları kabul etmek, sisteminize; üçüncü kişilerce verilerinizin ağ üzerinde taşınması sırasında erişimi tamamen engelleyecek bir güvenlik sağlayacaktır. Aşağıda HTTPS protokolü üzerinden GET methodu ile iletişim sağlayan basit bir PHP fonksiyonu ve fonksiyonun kullanımı ile ilgili bilgiler yer almaktadır.

Önceki bölümde mevcut olan *istemGonder()* fonksiyonunda olduğu gibi aşağıdaki **istemSSL()** fonksiyonu da yine sunucunuz üzerinde CURL eklentisi bulunmasını gerektirmektedir.

```
<?php
function istemSSL($url,$istem)
{
    $ch = curl_init($url.'?'.$istem);

    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 2);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
    curl_setopt($ch, CURLOPT_TIMEOUT, 10);

    $cevap = curl_exec($ch);
    curl_close($ch);
    return $cevap;
}
?>
```

istemSSL() fonksiyonu çalışmak için iki argümana ihtiyaç duymaktadır:

- 1- **\$url:** İstem yapılacak olan uzak sunucu adresi. (örn: <https://secure.quipass.com/api/>)
- 2- **\$istem:** Uzak sunucuya gönderilecek olan veriler. (örn: [u=johndoe&p=123456&app=102448](https://secure.quipass.com/api/?u=johndoe&p=123456&app=102448))

İstem uzak sunucuya ulaşması ve uzak sunucuda işlenmesinin ardından, **istemSSL()** fonksiyonu uzak sunucunun cevap çıktısını tutacaktır.

Gönderim sırasında herhangi bir hata oluşmamışsa bu çıktı, kullanıcı cihazına gönderilen şifreye ait imza olacaktır. Aksi takdirde HATA ibaresiyle birlikte hata kodu ve kısa açıklaması bu çıktıda yer alacaktır.

```
<?php

$url = 'https://secure.quipass.com/api/';
$istem = 'u=kullaniciAdiniz&p=sifreniz&app=uygulamaKodu&r=aliciTelefonu';

$sonuc = istemSSL($url, $istem);

?>
```

Yukarıdaki kodla basit bir şekilde, gönderilen şifrenin imzasını alabilir ve **\$sonuc** değişkenini kullanarak kullanıcı girdisini kıyaslayabilirsiniz.

DİKKAT: Güvenli ve sorunsuz çalışan bir sistem için lütfen gerekli hata kontrollerini sağlayarak şifre gönderim taleplerinizi oluşturun ve çıktıları yine kontrol ederek işleyin.

HATA KODLARI

QuiPass herhangi bir sebeple şifre iletimini tamamlayamadığında aşağıdaki hata kodlarını sonuç olarak döndürür.

001	QuiPass sunucu hatası.
002	QuiPass sunucu hatası.
003	Eksik veya geçersiz bilgi kümesi. Servise gönderilen talep eksik yetkilendirme bilgisi içeriyor.
004	Yetkilendirme başarısız. QuiPass hesap bilgileri ile gönderilen bilgiler uyuşmuyor.
005	Yetersiz bakiye. QuiPass hesabınızda gönderim yapabilmek için yeterli kredi bakiyesi bulunmuyor.
006	Kullanıcı son 3 dakika içerisinde zaten şifre almış. QuiPass hesabınız üzerinden yapılması muhtemel kötü niyetli gönderimlerin engellenmesi için her bir kullanıcıya en az 3 dakika periyotla şifre gönderim kontrolü.
007	Şifre oluşturulamadı. Uygulamanıza ait şifre karakter grubu veya karakter sayısındaki hatalı bilgi sebebiyle şifre oluşturulamıyor.
008	Mesaj işlenemedi. Mesajınız QuiPass sunucusu tarafından işlenemiyor.
009	İşlem hatası.
010	Mesaj gönderilemedi.
011	Geçersiz alıcı veya alıcı kapsama alanı dışında.
012	Gönderi, alıcı operatörü belirlenemediği için yapılamadı.

QUIPASS İSTEM YETKİLENDİRME BİLGİLERİ

Şifre gönderimi için QuiPass sunucularına yapacağınız istemlerde; servisin talebinizi işleyebilmesi için aşağıdaki verileri bulundurmanız gerekmektedir.

SERVİS ERİŞİM ADRESLERİ

QuiPass API servis bağlantı adresleri.

HTTPS API Servisi Bağlantı Adresi:

<https://secure.quipass.com/api/>

HTTP API Servisi Bağlantı Adresi:

<http://www.quipass.com/api/>

SERVİSE GÖNDERİLMESİ ZORUNLU OLAN BİLGİLER

QuiPass şifre gönderim talepleri için API servisine iletilmesi gereken bilgiler.

u	Kullanıcı Adı: QuiPass hesabınıza ait kullanıcı adınız.
p	Şifre: QuiPass hesabınıza ait şifreniz.
app	Uygulama Kodu: Şifre gönderimi için oluşturduğunuz QuiPass uygulamasına ait Uygulama Kodu numarası.
r	Alıcı: Şifre gönderimi yapılacak olan alıcıya ait on haneli telefon numarası. (örn: 5321234567)
islem	İşlem: Yapılacak olan doğrulama işlemi hakkında birkaç kelimelik bilgi veren işlem tanımı. (Yalnızca mobil onay kodu için geçerlidir. Örneğin; "kimlik dogrulama")

Detaylı bilgi için QuiPass.com internet sitesini, gizlilik politikalarını ve hizmet sözleşmesini incelemenizi öneririz.