

## Güvenlik Açığı Bildirim Formu

**Güvenlik Açığı Bildirim Politikası (Vulnerability Disclosure Policy)** kapsamında, WIN platformunda veya platforma bağlı altyapılarda tespit ettiğiniz **teknik güvenlik açıklarının** ve **güvenlik zafiyetlerinin** sorumlu açıklama (responsible disclosure) ilkesiyle bildirilmesi için bu form kullanılır.

Bu form **güvenlik araştırmacıları** ve **teknik ekipler** tarafından doldurulur. Genel müşteri desteği, hesap/şifre talepleri, içerik şikayeti veya resmî makam talepleri için kullanılmaz; bu konularda ilgili kanallara başvurunuz (bkz. [Güvenlik Açığı Bildirim Politikası](#) Bölüm 3.2). Detaylı kurallar, kapsam içi/dışı varlıklar ve rapor gereksinimleri için politikayı okumanız önerilir.

### Platform / Güvenlik İletişim Bilgileri

<b>Unvan</b>	WIN TECH BİLİŞİM VE ORGANİZASYON TİC. A.Ş. ("WIN")
<b>Adres</b>	Acıbadem Mah. Asafbey Sk. İmer Apt. No: 7 A, Kadıköy / İstanbul
<b>Vergi Dairesi</b>	Kadıköy Vergi Dairesi
<b>Vergi Kimlik No</b>	8111599712
<b>Web</b>	<a href="http://whoisnextapp.com">whoisnextapp.com</a>
<b>Güvenlik açığı bildirim e-posta</b>	<a href="mailto:info@whoisnextapp.com">info@whoisnextapp.com</a>

Formu doldurup imzaladıktan sonra **tarayarak** [info@whoisnextapp.com](mailto:info@whoisnextapp.com) adresine gönderebilirsiniz. Hassas bilgiler (token, test hesabı, PoC kodu) mümkünse **ayrı dosyada** ve **şifreli** iletilmeli; parola ayrı kanaldan paylaşılabilir.

### Bu form hangi konular için değildir?

- Hesap erişimi / şifre unutma → Uygulama içi Yardım/Destek
- İçerik şikayeti / taciz / kişisel güvenlik → Uygulama içi "Bildir/Şikayet Et" veya [Şikayet ve İhbar Formu](#)
- Resmî makam talepleri → [Kolluk Kuvvetleri Rehberi](#)

## 1. Bildirici / Arařtırmacı Bilgileri

(Geri dönüş ve koordinasyon için zorunludur. Tercih edilen dil belirtmeniz yanıt süresini kolaylaştırır.)

Alan	Doldurulacak
Ad – Soyad veya takma ad (handle)	_____
E-posta adresi (bildirime esas)	_____
Kurum / bağımsız (isteğe bağlı)	_____
Tercih edilen iletişim dili (Türkçe / İngilizce / diğer)	_____
WIN kullanıcı hesabı (varsa; teşekkür ödülü için)	_____

## 2. Özet Başlık

(Zafiyeti tek cümleyle özetleyin.)

---

---

---

## 3. Etkilenen Varlık

(Politika kapsamındaki varlıklar: whoisnextapp.com, legal.whoisnextapp.com, api.whoisnextapp.com, Firebase endpoint'leri, WIN iOS/Android resmî mağaza sürümleri. Hangi alan/sürüm/endpoint/ekran etkilendi?)

Alan	Doldurulacak
Etkilenen alan (web / mobil / API / diğer)	_____
Domain, uygulama sürümü veya endpoint	_____

Ekran / akış / sayfa (mümkünse)

#### 4. Zafiyet Türü

(İlgili tüm maddeleri işaretleyin. Politika Bölüm 1.2 ile uyumludur.)

- Yetkilendirme (authorization) zafiyeti (IDOR, broken access control)
- Kimlik doğrulama / oturum zafiyeti (session fixation, token sızıntısı, MFA bypass)
- Hesap ele geçirme riski (account takeover; doğrulama akışı zafiyeti vb.)
- Kişisel veri / hassas veri ifşası (KVKK/GDPR riski)
- İş mantığı (business logic) zafiyeti (ödeme, abonelik, güvenlik doğrulama, engelleme vb.)
- Mobil uygulama zafiyeti (insecure storage, certificate validation vb.)
- API zafiyeti (rate-limit bypass, object-level authorization vb.)
- Kriptografi / anahtar yönetimi hatası
- Üçüncü taraf tedarikçi / SDK kaynaklı risk (Platform'a etkisi belirtin)
- Diğer: \_\_\_\_\_

#### 5. Adım Adım Yeniden Üretim (Repro Steps)

(Zafiyetin nasıl tekrarlanabileceğini sırayla yazın. Mümkünse numaralı adımlar.)

---

---

---

---

---

---

---

---

---

---

## 6. Beklenen vs Gerçekleşen Davranış

	Açıklama
<b>Beklenen davranış</b>	_____
	_____
<b>Gerçekleşen davranış</b>	_____
	_____

## 7. Etki ve İstismar Edilebilirlik

(En kötü senaryo, pratik etki ve hangi koşullarda istismar edilebileceği.)

---

---

---

---

---

---

---

## 8. Kanıt (Asgari)

(Ekran görüntüsü, kısa video veya minimal PoC. Veri minimizasyonu ilkesine uygun; kişisel veri/özel içerik içermemeli. Hassas detaylar ayrı/sifreli dosyada iletilebilir.)

- Ek(ler) e-posta ile gönderildi (buraya "Ek: ..." yazın)
- Kanıt metin olarak aşağıda

---

---

---

---

## 9. Önerilen Düzeltme (İsteğe Bağlı)

---

---

---

## 10. Hassas Bilgiler (Varsa)

*(Erişim belirteci, test hesabı bilgisi, log parçası vb. Mümkünse ayrı dosyada, şifreli; parola farklı kanaldan. Bu alanda yalnızca "Ayrı şifreli dosyada iletildi" gibi not bırakabilirsiniz.)*

---

---

---

## 11. İyi Niyet ve Politika Uyumu Beyanı

*(Güvenlik Açığı Bildirim Politikası Bölüm 4 ve 10 uyarınca. İyi niyetli araştırma, zarar vermeme, veri minimizasyonu ve sorumlu açıklama kurallarına uyduğunuzu beyan ediniz.)*

- **İyi niyet:** Bu bildirim **iyi niyetle**, güvenlik iyileştirmesi amacıyla yapıyorum; şantaj, tehdit veya veri sızdırma amacı taşıyorum.
- **Kapsam ve yöntem:** Araştırmamı politika kapsamındaki varlıklarda, **gerekli asgari adımlarla** ve kullanıcı verisine zarar vermeden yürüttüm.
- **Veri:** İstmeden kişisel veriye veya özel içeriğe eriştiysem, veriyi çoğaltmadım/indirmediğim; talebiniz üzerine güvenli şekilde sileceğim.
- **Kamuya açıklama:** Zafiyeti WIN'in yazılı izni olmadan kamuya açıklamayacağım (sosyal medya, blog, CVE, broker paylaşımı vb.).

**Evet**, yukarıdaki beyanları kabul ediyorum ve Güvenlik Açığı Bildirim Politikasına uyduğumu beyan ederim.

---

## 12. Tarih ve İmza

**Tarih:** \_\_\_\_ / \_\_\_\_ / \_\_\_\_\_

**İmza:** \_\_\_\_\_

(Formu doldurup e-posta ile göndermeniz bildirim kayda alınması için yeterlidir; özel olarak talep edilmedikçe ıslak imzalı nüsha zorunlu değildir.)

## İşlem ve Yanıt

- Bildirimler **kayıt altına alınır**; [Güvenlik Açığı Bildirim Politikası](#) çerçevesinde değerlendirilir.
- **Alındı onayı:** hedef 3 iş günü içinde; **ilk teknik değerlendirme:** hedef 7-14 iş günü. Karmaşık zafiyetlerde süre uzayabilir; düzenli güncelleme verilir.
- Eksik veya yeterince spesifik olmayan raporlarda **ek bilgi** talep edilir; kapsam dışı veya politika ihlali durumunda rapor işleme alınmayabilir.
- Geçerli ve benzersiz teknik güvenlik açıkları için politika uyarınca **sembolik teşekkür ödülü** (“+1 Deck”) uygulanabilir; WIN hesabınız varsa ödül hesabınıza tanımlanır.
- Raporla ilgili verileri, doğrulama ve giderim tamamlandıktan sonra **güvenli şekilde silmeniz** talep edilebilir.

*Bu form, WIN (Whoisnextapp) platformu ve WIN TECH BİLİŞİM VE ORGANİZASYON TİC. A.Ş. için hazırlanmıştır. Güncel [Güvenlik Açığı Bildirim Politikası](#), [Kullanım Koşulları](#) ve iletişim kanalları whoisnextapp.com ile uygulama içi "Yasal" bölümünde yayımlanır.*