CyberTestify

Otomatik Güvenlik Tarama Raporu

ornek.com · Uyum Paketi

CyberTestify Güvenlik Taraması — Tamamlandı

Rapor No: **CT-ÖRNEK-E5E4**

Doğrulama Kodu: **E336-FB0A**

Bu rapor resmi sızma testi / sertifikasyon değildir.

İçindekiler

1. Yönetici Özeti

GENEL DEĞERLENDİRME

Yüksek Risk

En yüksek hazırlık eksiği KVKK Ön Uyum Kontrolü alanında (rıza mekanizması gözlemlenmeden izleyici çerez/servis kullanımı dikkat çekiyor.); öncelikli ele alınması önerilir. Bu rapor dışarıdan gözlemlenebilir göstergeleri ilgili ilke/madde ile eşler; resmî bir uyum denetimi/sertifikasyon beyanı DEĞİLDİR. Aşağıda her çerçeve ayrı ayrı raporlanmıştır.

> **⚠ Önemli — Bu rapor resmî bir uyum beyanı DEĞİLDİR**
>
> Bu rapor bir **KVKK denetimi**, **PCI DSS sertifikasyonu** veya **ISO 27001 belgelendirmesi DEĞİLDİR.** Yalnızca **dışarıdan gözlemlenebilir** hazırlık eksiklerini ilgili çerçevelerle (KVKK / PCI-DSS / ISO 27001) eşler. Resmî uyum denetimi/beyanı yerine **GEÇMEZ**; nihai değerlendirme için yetkili uzman (KVKK danışmanı / PCI QSA / ISO belgelendirme kuruluşu) gereklidir.

- **Genel risk seviyesi: Yüksek** — 3 çerçeve incelendi; en yüksek hazırlık eksiği **KVKK Ön Uyum Kontrolü** alanında (rıza mekanizması gözlemlenmeden izleyici çerez/servis kullanımı dikkat çekiyor.).
- **KVKK Ön Uyum Kontrolü:** Yüksek
- **PCI-DSS Hazırlık Ön-Değerlendirmesi:** Orta
- **ISO 27001 Hazırlık Kontrol Listesi:** Orta
- **Önerilen ilk adım:** En yüksek eksikli çerçeveden başlayın; hazır adımlar "AI Çözüm Önerileri" bölümünde. Bu rapor resmî bir uyum/sertifikasyon beyanı değildir.

ÖNCELİKLİ AKSİYONLAR

Dışarıdan gözlemlenen boşluklar, uygulama eforuna göre iki grupta önceliklendirildi:

⚡ Hızlı Kazanımlar (genellikle sunucu/yapılandırma — 1-2 gün)

1. **[Orta]** KVKK — Veri sorumlusu ve iletişim bilgisini sitede erişilebilir kılın. → *Düşük eforlu; VERBIS/şeffaflık için gerekli*
2. **[Orta]** PCI-DSS (Req 6.4) — Eksik güvenlik başlıklarını ekleyin. → *XSS/clickjacking yüzeyini kapatır*
3. **[Orta]** ISO 27001 (A.5.7) — /.well-known/security.txt ile zafiyet bildirim kanalı yayınlayın. → *Hızlı ve düşük eforlu kazanım*

🗓 Orta Vadeli (içerik/süreç/entegrasyon gerektirir)

1. **[Yüksek]** KVKK — Çerez açık rızası ekleyin ve rıza öncesi izleyici çerezleri durdurun. → *KVKK m.5 (açık rıza) ihlali göstergesi — Kurul'un uygulamada en sık idari para cezası uyguladığı eksiklik*
2. **[Orta]** KVKK — Erişilebilir aydınlatma metni / gizlilik politikası yayınlayın. → *Şeffaflık yükümlülüğünü karşılar (m.10)*
3. **[Orta]** ISO 27001 (A.5.1) — Erişilebilir bir güvenlik/gizlilik politikası yayınlayın. → *Politika kontrolü için görünür kanıt*
4. **[Orta]** ISO 27001 (A.15) — Görünen üçüncü taraf bağımlılıklarını envanterleyip değerlendirin. → *Tedarik zinciri riskini yönetir*

2. Kontrol Özeti ve Metodoloji

KVKK Ön Uyum Kontrolü

DEĞERLENDİRME (Ne gördük / Ne görmedik)

En dikkat çeken gözlem: üçüncü taraf izleyiciler (Google Tag Manager, Google Analytics, Facebook Pixel, Microsoft Clarity) açık rıza mekanizması görülmeden yükleniyor. Bu, KVKK m.5 (açık rıza) açısından uygulamada en sık idari yaptırıma konu olan eksikliklerden biridir. Ayrıca erişilebilir bir aydınlatma metni gözlemlenmedi; veri sorumlusu/iletişim bilgisi de kontrol edilen sayfalarda bulunamadı.

KVKK GÖZLEM TABLOSU

KVKK İlkesi/Konu	Gözlem	Durum	Öneri
Aydınlatma yükümlülüğü (m.10)	Kontrol edilen sayfalarda (ana sayfa + yaygın yollar) gözlemlenmedi	Gözlemlenmedi	Erişilebilir bir aydınlatma metni/gizlilik politikası yayınlayın
Açık rıza — çerezler (m.5)	Çerez rıza banner'ı gözlemlenmedi	İnceleme gerekli	Rıza öncesi izleyici çerez bırakmayın; açık rıza banner'ı ekleyin
Üçüncü taraf aktarım/izleyiciler (m.8-9)	Gözlemlenen: Google Tag Manager, Google Analytics, Facebook Pixel, Microsoft Clarity	İnceleme gerekli	İzleyicileri açık rızaya bağlayın; aydınlatmada açıkça belirtin
Veri sorumlusu / VERBIS (m.16)	Kontrol edilen sayfalarda gözlemlenmedi	Gözlemlenmedi	Veri sorumlusu kimliği ve iletişim/VERBIS bilgisini yayınlayın
Veri güvenliği tedbirleri (m.12)	Site HTTPS üzerinden sunuluyor (HSTS mevcut), HTTP→HTTPS yönlendirmesi var	Gözlemlendi	Taşıma güvenliğini (HTTPS/HSTS) sürdürün

İZLEYİCİ DETAYI

- **Google Tag Manager** — muhtemel toplanan veri: etiket/olay yönetimi — diğer izleyicileri tetikler.
- **Google Analytics** — muhtemel toplanan veri: kullanım, cihaz, yaklaşık konum ve davranış verisi.
- **Facebook Pixel** — muhtemel toplanan veri: dönüşüm ve kimlik eşleme (Meta hesabıyla ilişkilendirme).
- **Microsoft Clarity** — muhtemel toplanan veri: oturum kaydı, tıklama/kaydırma ısı haritası.

> Bu izleyiciler, gözlemlenebilir bir açık rıza mekanizması OLMADAN yükleniyor görünüyor; KVKK m.5 açısından açık rıza öncesi işleme dikkat gerektirir.

FORM GÖZLEMİ

- Ana sayfada kişisel veri toplayan form gözlemlenmedi.

> **Kapsam:** Yalnızca dışarıdan gözlemlenebilir göstergeler (sayfa/çerez/izleyici/form) değerlendirildi; veri envanteri, saklama-imha politikası, açık rıza metinlerinin içeriği ve veri işleme sözleşmeleri iç değerlendirme gerektirir.

PCI-DSS Hazırlık Ön-Değerlendirmesi

DEĞERLENDİRME (Ne gördük / Ne görmedik)

Kart verisi işleyen bir ortamda en dikkat çeken dış gözlem: **eksik tarayıcı güvenlik başlıkları**. Güvenlik başlıkları, tarayıcı seviyesindeki savunmayı doğrudan etkiler (Req 6.4). Aktarım güvenliği TLSv1.3, sertifika 82 gün geçerli; HTTPS zorunluluğu HSTS ile bildiriliyor.

PCI-DSS GÖZLEM TABLOSU

Gereksinim	Gözlem	Gözlemlenebilir kontrol	Öneri
Req 4.2.1 — Aktarımda güçlü şifreleme	TLS TLSv1.3, sertifika 82 gün	Mevcut	TLS 1.2+ zorunlu; sertifikayı geçerli tutun
Req 4.1 — HTTPS zorunluluğu	HSTS: var; HTTP→HTTPS yönlendirme: var	Mevcut	HSTS ekleyin + tüm HTTP'yi HTTPS'e yönlendirin
Req 6.4 — Güvenlik başlıkları	Eksik: CSP, X-Frame-Options, X-Content-Type-Options	Eksik	Eksik güvenlik başlıklarını ekleyin
Req 8 — Oturum/çerez + otomatik doldurma	Taranan 1 sayfada Set-Cookie gözlemlenmedi	Mevcut	Çerez bayrakları + parola alanında autocomplete="off"
Req 2.2 — Güvenli yapılandırma (sürüm ifşası)	Belirgin sürüm ifşası gözlemlenmedi	Mevcut	Sürüm/teknoloji banner'larını gizleyin
Req 6.5 — Test/staging izleri	Belirgin test/staging/debug izi gözlemlenmedi	Mevcut	Debug/kaynak-haritası/test izlerini üretimden kaldırın
Req 3 — Veri ifşası (açıkta dosya)	Yaygın hassas yollar erişilebilir değil	Mevcut	Açıkta kalan dosyalara erişimi engelleyin

GÜVENLİK BAŞLIKLARI DETAYI (Req 6.4)

Başlık	Durum	Değer/Not
HSTS	Var	max-age=31556926
CSP	Yok	—
X-Frame-Options	Yok	—
X-Content-Type-Options	Yok	—
Referrer-Policy	Yok	—
Permissions-Policy	Yok	—

> **Kapsam:** Dış yüzey (TLS, güvenlik başlıkları, çerez, sürüm ifşası, açıkta dosya, test izleri) değerlendirildi; iç ağ/CDE, ağ segmentasyonu, loglama-izleme (Req 10) ve resmî ASV taraması bu ön-değerlendirmenin dışındadır.

ISO 27001 Hazırlık Kontrol Listesi

DEĞERLENDİRME (Ne gördük / Ne görmedik)

Annex A açısından en dikkat çeken dış gözlem: **erişilebilir politika sayfası eksikliği**. Dışarıdan bakıldığında 3 temel güvenlik başlığı eksik (A.8.23), TLS TLSv1.3 (A.8.24) ve 9 dış servis bağımlılığı (A.15) gözlemlendi. Bunlar teknik kontrolün bir kısmıdır; ISMS kapsamı ve dokümantasyon iç denetim gerektirir.

ISO 27001 ANNEX A GÖZLEM TABLOSU

Madde	Gözlem	Gözlemlenebilir kontrol	Öneri
A.8.24 — Kriptografi	TLS TLSv1.3	Mevcut	TLS 1.2+ ve geçerli sertifika sürdürün
A.8.23/A.8.9 — Güvenlik başlıkları	Eksik: CSP, X-Frame-Options, X-Content-Type-Options	Eksik	Eksik başlıkları ekleyin
A.8.9 — Güvenli yapılandırma (sürüm ifşası)	banner gözlemlenmedi	Mevcut	Sürüm bilgisini gizleyin
A.8.12 — Veri sızıntısı	Belirgin sızıntı göstergesi gözlemlenmedi	Mevcut	Açık dosya/bilgi sızıntısı göstergelerini giderin
A.5.1 — Politikalar	Gizlilik/güvenlik politikası sayfası gözlemlenmedi	Eksik	Erişilebilir bir politika sayfası yayınlayın
A.5.7/A.6 — Zafiyet bildirim kanalı	security.txt: gözlemlenmedi	Eksik	/.well-known/security.txt ile bildirim kanalı tanımlayın
A.15 — Üçüncü taraf bağımlılıkları	9 dış alan adı gözlemlendi	Bilgilendirme	Dış bağımlılıkları envanterleyin/değerlendirin

ÜÇÜNCÜ TARAF BAĞIMLILIKLARI (görünür)

Sayfada yüklenen dış alan adları (tedarikçi/veri işleyen envanteri için):

- googletagmanager.com
- connect.facebook.net
- clarity.ms
- schema.org
- instagram.com
- ornek-app.firebaseapp.com
- firestore.googleapis.com
- firebasestorage.googleapis.com
- facebook.com

> Her dış bağımlılık bir tedarik zinciri/veri işleyen riski taşır (A.15); envanterlenip değerlendirilmelidir.

> **Kapsam:** Dışarıdan gözlemlenebilir teknik kontroller değerlendirildi; ISMS kapsamı, politika-prosedür dokümantasyonu, erişim yönetimi ve iç süreçler ayrı bir uygunluk denetimi gerektirir.

POZİTİF GÜVENCE — İNCELENEN ÇERÇEVELER

Bu ön-değerlendirme, ana sayfa dâhil **1 benzersiz sayfada** dışarıdan gözlemlenebilir hazırlık göstergelerini üç çerçeveyle eşledi. "Eksik bulunamadı" sonuçları da şeffaf gösterilir:

Çerçeve	Sonuç
KVKK Ön Uyum Kontrolü	⚠ Hazırlık eksiği var (Yüksek — yukarıda ayrıntılı)
PCI-DSS Hazırlık Ön-Değerlendirmesi	⚠ Hazırlık eksiği var (Orta — yukarıda ayrıntılı)

Çerçeve	Sonuç
ISO 27001 Hazırlık Kontrol Listesi	⚠ **Hazırlık eksiği var (Orta — yukarıda ayrıntılı)**

Üç-durum ayrımı (dürüstlük): ✓ *Belirgin eksik yok* = kontrol çalıştı, temiz · ⚠ *Eksik var* = yukarıda ayrıntılı · ⚠ *İncelenemedi* = veri toplanamadı (uyumlu anlamına GELMEZ).

Bu paket NE değerlendirir, NE değerlendirmez

DEĞERLENDİRİR (pasif — yalnız GET ile dış gözlem): aydınlatma/gizlilik metni varlığı, çerez rıza banner'ı, izleyiciler + rıza ilişkisi, kişisel-veri formları, HTTPS/taşıma güvenliği, çerez bayrakları, veri sorumlusu/iletişim bilgisi — keşfedilen 1 sayfada, ilgili KVKK/PCI/ISO maddeleriyle eşlenerek.

DEĞERLENDİRMEZ: iç veri envanteri, saklama/imha politikası, veri işleme sözleşmeleri, ağ segmentasyonu/CDE (PCI), ISMS dokümantasyonu, resmî ASV/QSA taraması, aktif zafiyet testi. Bunlar iç denetim + yetkili uzman gerektirir. Bir çerçevede "eksik bulunamadı" ifadesi, **uyumlu olduğunuzu KANITLAMAZ** — yalnız dışarıdan gözlemlenen göstergelerin temiz olduğunu gösterir.

3. AI Çözüm Önerileri

Bu bölüm, uyum ön-değerlendirmenizde dışarıdan gözlemlenen eksikler için çerçeve çerçeve düzeltme adımları içerir (resmî uyum beyanı değildir).

KVKK Ön Uyum Kontrolü

Aşağıdaki adımlar dışarıdan gözlemlenen KVKK hazırlık eksiklerini gidermeye yöneliktir (resmî uyum beyanı değildir).

Aydınlatma metni / Gizlilik politikası

KVKK m.10 kapsamında; hangi kişisel verilerin, hangi amaçla ve hukuki sebeple işlendiğini + veri sorumlusu/VERBIS bilgisini içeren erişilebilir bir metin yayınlayın (footer'dan linkleyin).

Çerez açık rızası

İzleyici/analitik çerezleri **rıza alınmadan ÖNCE bırakmayın** (gözlemlenen izleyiciler: Google Tag Manager, Google Analytics, Facebook Pixel, Microsoft Clarity). Kategorili (zorunlu/analitik/pazarlama) bir çerez rıza banner'ı ekleyin; yalnızca onaylanan kategoriler yüklensin (Cookiebot/OneTrust/iubenda/Klaro vb.).

Veri sorumlusu / iletişim

Veri sorumlusu kimliğini, iletişim bilgisini ve (varsa) VERBIS kaydını sitede erişilebilir kılın.

Not

Bu öneriler dışarıdan gözlemlenebilir teknik göstergelere dayanır; tam uyum için veri envanteri, saklama/imha politikası ve gerekli sözleşmeler dâhil kapsamlı bir hukuki değerlendirme gereklidir.

PCI-DSS Hazırlık Ön-Değerlendirmesi

Aşağıdaki adımlar PCI-DSS ile ilişkili, dışarıdan gözlemlenen eksiklikleri gidermeye yöneliktir.

Güvenlik başlıkları

```
add_header Content-Security-Policy "default-src 'self'; frame-ancestors 'self'" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-Content-Type-Options "nosniff" always;
```

ISO 27001 Hazırlık Kontrol Listesi

Aşağıdaki adımlar ISO 27001 ile ilişkili, dışarıdan gözlemlenen eksiklikleri gidermeye yöneliktir.

Güvenlik başlıkları


```
add_header Content-Security-Policy "default-src 'self'; frame-ancestors 'self'" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-Content-Type-Options "nosniff" always;
```


Politika sayfası

Erişilebilir bir gizlilik/güvenlik politikası sayfası yayınlayın.

Ek öneriler

- `/.well-known/security.txt` ile bir zafiyet bildirim kanalı yayınlayın (A.5.7).
- Görünen dış bağımlılıkları (üçüncü taraf servisler) envanterleyip veri-işleyen değerlendirmesine dâhil edin (A.15).

4. Ek — Sözlük

XSS	Cross-Site Scripting — sayfaya kötü amaçlı betik enjekte edilebilmesi.
TLS	Taşıma katmanı şifrelemesi (HTTPS'in temeli).
HSTS	Tarayıcıyı yalnız HTTPS kullanmaya zorlayan güvenlik başlığı.
CSP	İçerik Güvenlik Politikası — XSS/enjeksiyon azaltma başlığı.
KVKK	Kişisel Verilerin Korunması Kanunu (Türkiye).
VERBİS	Veri Sorumluları Sicil Bilgi Sistemi (KVKK kayıt sistemi).
Clickjacking	Sayfanın görünmez iframe içine alınıp kullanıcı tıklamalarının kandırılması.