CyberTestify

Otomatik Güvenlik Tarama Raporu

rest.vulnweb.com · Keşif Paketi

CyberTestify Güvenlik Taraması — Tamamlandı

Rapor No: **CT-ÖRNEK-F82E**

Doğrulama Kodu: **5A53-5E8E**

Bu rapor resmi sızma testi / sertifikasyon değildir.

İçindekiler

HEDEF
rest.vulnweb.com

PAKET
Keşif Paketi

RAPOR NO
CT-ÖRNEK-F82E

1. Yönetici Özeti

GENEL DEĞERLENDİRME

Yüksek Risk

Bu hedef HTTPS üzerinden yanıt vermiyor; iletişim şifresiz taşınıyor (öncelikli olarak HTTPS'e geçilmelidir). En yüksek risk CMS & Bilinen CVE Taraması alanında (Bilinen bir CMS parmak izi tespit edilmedi · sunucu/yazılım sürümünde 21 bilinen CVE) tespit edildi; öncelikli olarak giderilmesi önerilir. Aşağıda her alan ayrı ayrı raporlanmıştır.

⚡ Yönetim Kararı

Öncelikli ele alınması gereken **2** yüksek/kritik seviyeli gösterge tespit edildi; bunlar için acil bir düzeltme planı önerilir. Orta/düşük göstergeler planlı iyileştirmeyle giderilebilir.

- **Genel risk seviyesi: Yüksek** — 3 alan incelendi; en yüksek risk **CMS & Bilinen CVE Taraması** alanında (Bilinen bir CMS parmak izi tespit edilmedi · sunucu/yazılım sürümünde 21 bilinen CVE).
- ⚠ **HTTPS desteklenmiyor:** Hedef HTTPS (443) üzerinden yanıt vermedi; keşif http:// üzerinden yürütüldü. Şifresiz iletişim başlı başına ciddi bir bulgudur (aşağıda).
- **Kapsam (gerçek sayılar):** 0 alt domain envanterlendi · 12 API/Swagger yolu denendi (2 sayfa tarandı) · 6+ pasif CMS/teknoloji sinyali incelendi.
- **Önerilen ilk adım:** En yüksek riskli alandan başlayın; her bulgu için adım adım hazır çözümler "AI Çözüm Önerileri" bölümünde sunulur.

İyileştirme Öncelikleri

⚡ **En Acil / Öncelikli:** HTTPS desteklenmiyor (şifresiz iletişim); Güncel olmayan bileşen (CVE).

2. Bulgular

2.1 Zafiyet Dağılımı

Bu taramada toplam **2** bulgu göstergesi tespit edildi; şiddet dağılımı aşağıdadır.

2.2 Master Bulgu Tablosu

ID	Başlık	Durum	Şiddet
CT-1	HTTPS desteklenmiyor (şifresiz iletişim)	Açık	Yüksek
CT-2	Güncel olmayan bileşen (CVE)	Açık	Yüksek

Ne test edildi, ne çıktı?

✓ TEST EDİLDİ — GÖSTERGE BULUNAMADI

- **Subdomain-Takeover Taraması** 0 alt domain kaydı denendi (siteye bağlı alt adresler — isim isim liste: "Subdomain Takeover Taraması" bölümü); devralma göstergesi bulunamadı (başkasının ele geçirebileceği boşta kayıt yok)
- **API & Swagger Keşfi** 12 yol denendi (12 sabit + 0 site-haritası adayı, 2 sayfadan — denenen yolların TAM listesi: "API & Swagger Keşfi" bölümü); herkese açık API şeması bulunamadı (dışarıdan okunabilen API dokümanı yok)
- **CMS / Framework CVE Eşleşmesi** 6 pasif sinyal kategorisi incelendi (başlıklar, meta generator, HTML izleri, sürüm dosyaları, bilinen CMS yolları, kütüphane ipuçları — tam liste: "CMS & Bilinen CVE Taraması" bölümü); bilinen bir CMS/çatı parmak izi tespit edilmedi
- **Site haritası + robots.txt yol keşfi** Site haritası + robots.txt Disallow'dan türetilen 0 yol denendi (yalnız var/yok kontrolü — aday yolların listesi: "API & Swagger Keşfi" bölümü); hassas/idari uç bulunamadı

⚠ GÖSTERGE BULUNDU — AYRINTISI AŞAĞIDAKİ BÖLÜMLERDE

- **Sunucu/Yazılım Banner → Bilinen CVE** Banner sürümünde 21 bilinen CVE (PHP 7.1.26 — CVE numaraları: "Sunucu/Yazılım Banner Sürümü" bölümü)
- **USOM/SGB Bildirim Eşlemesi** 5 kamuya açık bildirim imzası gözlemlendi (sürüm doğrulanamadı — gösterge; hangi bildirimler: "USOM/SGB Bildirim Eşlemesi" bölümündeki eşleşme tablosu)

2.3 Detaylı Bulgular

[YÜKSEK] CT-1 · HTTPS desteklenmiyor (şifresiz iletişim)

Durum: Açık

Açıklama: Site HTTPS üzerinden yanıt vermiyor; iletişim şifresiz (düz metin) HTTP ile yürüyor.

Nasıl Tespit Edildi: Hedef HTTPS'e yanıt vermiyor; tüm trafik şifresiz (düz metin) taşınıyor — dinlenebilir/değiştirilebilir. Çözüm: geçerli TLS sertifikası + HTTP→HTTPS yönlendirme + HSTS.

İş Etkisi: Site HTTPS üzerinden yanıt vermiyor; sayfaya gelen/giden tüm trafik ŞİFRESİZ (düz metin) taşınıyor. Aynı ağdaki bir saldırgan trafiği dinleyebilir, oturum/şifre çalabilir veya içeriği değiştirebilir; modern tarayıcılar sayfayı "Güvenli değil" olarak işaretler.

ÖNERİLEN DÜZELTME

Geçerli bir TLS sertifikası kurun (ücretsiz: Let's Encrypt), tüm HTTP isteklerini kalıcı olarak (301) HTTPS'e yönlendirin ve HSTS başlığını ekleyin.

Referans: CWE-319 · OWASP A02:2021 Cryptographic Failures

[YÜKSEK] CT-2 · Güncel olmayan bileşen (CVE)

Durum: Açık

Açıklama: Güncel olmayan bir bileşen/CMS parmak izi ve olası bilinen CVE.

Nasıl Tespit Edildi: Ayrıntı aşağıdaki "CMS & Bilinen CVE Taraması" bölümündedir.

İş Etkisi: Güncel olmayan bileşen bilinen CVE'lerle istismara açıktır; hedefli saldırı riski.

ÖNERİLEN DÜZELTME

Bileşen/eklenti/tema sürümlerini güncel tutun; otomatik güncelleme + bağımlılık taraması kurun.

Referans: CWE-1104 · OWASP A06:2021 Vulnerable & Outdated Components

3. Kontrol Özeti ve Metodoloji

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
HTTPS desteklenmiyor (şifresiz iletişim)	Yüksek	Hedef HTTPS'e yanıt vermiyor; tüm trafik şifresiz (düz metin) taşınıyor — dinlenebilir/değiştirilebilir. Çözüm: geçerli TLS sertifikası + HTTP→HTTPS yönlendirme + HSTS.
CMS & Bilinen CVE Taraması — Bilinen bir CMS parmak izi tespit edilmedi · sunucu/yazılım sürümünde 21 bilinen CVE	Yüksek	Ayrıntı aşağıdaki "CMS & Bilinen CVE Taraması" bölümündedir.

KAPSAM VE METODOLOJİ

Bu rapor, üç keşif alanında **pasif** (istismar içermeyen) tekniklerle, dışarıdan gözlemlenebilir verilerden otomatik olarak üretilmiştir:

- **Subdomain Takeover:** Alt domainler Certificate Transparency loglarından (crt.sh, yedek olarak certSpotter) toplanır; her biri Cloudflare DoH ile DNS/CNAME çözümlemesinden geçirilir ve bilinen "dangling" (terk edilmiş bulut servisi) imza veritabanıyla karşılaştırılır.
- **API & Swagger Keşfi:** Yaygın API dokümantasyon yollarından oluşan sabit bir liste GET ile denenir; bulunan OpenAPI/Swagger şemaları ayrıştırılır ve hassas/kimlik-doğrulamasız uç noktalar işaretlenir (uç noktalar çağrılmaz).
- **CMS & Bilinen CVE:** HTTP başlıkları, `<meta generator>` ve HTML kalıpları üzerinden CMS ve sürüm parmak izi çıkarılır; generator gizlenmişse bilinen CMS yollarının VARLIĞI (yalnız GET/existence — giriş denemesi yok) ile doğrulanır. Tespit edilen sürüm, NVD (NIST Ulusal Zafiyet Veritabanı) sorgulanarak — sürümü açıkça kapsayan — bilinen CVE'lerle eşlenir; sürüm okunamazsa CVE eşlemesi yapılmaz (uydurma CVE yok).

> Tüm veriler dışarıdan, hedefe zarar vermeden toplanmıştır. Kimlik doğrulama gerektiren alanlar, iç ağ ve aktif sömürü bu paketin kapsamı dışındadır.

Subdomain Takeover Taraması

Genel risk seviyesi: Düşük — Sertifika şeffaflığı kayıtlarında alt domain görülmedi

Certificate Transparency (crt.sh / certSpotter) kayıtlarından **0** benzersiz alt domain envanterlendi; bunlardan **0** tanesinin CNAME kaydı çözümlenip devralma (subdomain takeover) açısından incelendi.

Çözümlenen CNAME kayıtlarında, terk edilmiş bir bulut kaynağına işaret eden **devralınabilir (dangling)** alt domain tespit edilmedi. Bu, dışarıdan görünen alt domain yüzeyinizin şu an için **dar ve kontrollü** göründüğünü gösterir.

> Kapsam: Yalnızca pasif kaynaklar (Certificate Transparency logları + gözlemlenebilir DNS). Alt domain brute-force / aktif tarama yapılmamıştır.

API & Swagger Keşfi

Genel risk seviyesi: Düşük — Herkese açık API/Swagger dokümantasyonu bulunamadı

Aşağıdaki **12** yaygın API dokümantasyon/keşif yolu GET ile denenmiştir. Hiçbir uç nokta çağrılmamış/istismar edilmemiştir (pasif keşif).

Denenen yollar (tam liste)

Yol	HTTP	Durum
/openapi.json	404	Bulunamadı
/swagger.json	404	Bulunamadı
/v2/api-docs	400	Bulunamadı
/v3/api-docs	400	Bulunamadı
/api-docs	404	Bulunamadı
/api/docs	400	Bulunamadı
/api/v1/docs	400	Bulunamadı
/swagger-ui.html	404	Bulunamadı
/swagger/index.html	400	Bulunamadı
/redoc	404	Bulunamadı
/.well-known/openapi.json	400	Bulunamadı
/graphql	404	Bulunamadı

Denenen yolların hiçbiri herkese açık bir API şeması/arayüzü döndürmedi. Herkese açık API dokümantasyonu bulunmaması, saldırganların API yüzeyinizi dışarıdan kolayca **haritalayamayacağı** anlamına gelir — bu, dış saldırı yüzeyi açısından olumlu bir işarettir.

> Kapsam: Yalnızca herkese açık dokümantasyon yolları GET ile denenmiştir; hiçbir uç nokta çağrılmamış/istismar edilmemiştir (pasif keşif).

CMS & Bilinen CVE Taraması

Genel risk seviyesi: Yüksek — Bilinen bir CMS parmak izi tespit edilmedi · sunucu/yazılım sürümünde 21 bilinen CVE

İncelenen parmak izi kaynakları

CMS/çatı ve sürüm tespiti için ana sayfa yanıtı üzerinde aşağıdaki **6 pasif sinyal kategorisine** bakıldı (Yönetici Özeti'ndeki “6+ pasif CMS/teknoloji sinyali” ifadesi tam olarak bu listeyi kasteder; “+” her kategorinin içindeki birden çok alt sinyali belirtir):

- HTTP yanıt başlıkları (`Server` , `X-Powered-By` , `X-Generator` , `X-Drupal-Cache` , `X-Magento-Cache-Debug`)
- `<meta name="generator">` etiketi

- HTML yol/kalıp izleri (`/wp-content/` , `/wp-includes/` , `Drupal.settings` , `/sites/all/` , `option=com_` , `/media/jui/` , `typo3conf` , `Magento_`)
- Yaygın sürüm dosyaları (WordPress `/readme.html` , Drupal `/CHANGELOG.txt`)
- Bilinen CMS yollarının VARLIĞI (`/wp-login.php` , `/wp-json/` , `/administrator/` , `/user/login` , `/typo3/` — yalnız var/yok kontrolü; giriş/parola denemesi YOK)
- Kütüphane/eklenti ipuçları (WooCommerce, jQuery sürümü)

Bu sinyallerin **hiçbiri** bilinen bir CMS/çatı ile eşleşmedi. Bu, özel geliştirilmiş bir uygulama veya CMS izlerini bilinçli olarak gizleyen bir kurulum olabileceğine işaret eder; her iki durum da dışarıdan otomatik CMS/CVE eşlemesini zorlaştırır.

Sunucu/Yazılım Banner Sürümü — Bilinen CVE (NVD)

Banner'dan çıkan sürüm(ler) NVD'ye bağlandı (istismar/doğrulama YOK — yalnız "bu sürüm için bilinen CVE var mı" göstergesi):

Yazılım/Sürüm	NVD sonucu	Örnek CVE
Apache httpd 2.4.25	sorgulanamadı (temiz DEĞİL)	—
PHP 7.1.26	⚠ **21 bilinen CVE**	CVE-2017-8923

> **Not:** Aşağıdaki CVE listesi, tespit edilen sürümle NVD (NIST Ulusal Zafiyet Veritabanı) üzerinden **otomatik eşlenen** bilinen zafiyetlerdir; sürümünüz için sömürülebilir oldukları **doğrulanmamıştır** ve bir kısmı eklenti/tema kaynaklı olabilir. Kesin durum için güncelleme + hedefli doğrulama önerilir.

> Kapsam: Pasif parmak izi + NVD üzerinden bilinen-CVE eşlemesi. Hiçbir CVE **istismar edilmemiş/doğrulanmamıştır**.

USOM/SGB Bildirim Eşlemesi

Bu bölüm, T.C. Siber Güvenlik Başkanlığı'nın (USOM/SGB) **KAMUYA AÇIK** olarak yayımladığı güvenlik bildirimleriyle, yukarıdaki Keşif parmak-izini (CMS/sunucu-banner) dışarıdan gözlemlenebilir düzeyde eşleştirir. Yeni bir tarama yapılmaz; mevcut keşif sinyali ikinci bir katalogla karşılaştırılır.

> **Bağımsız eşleme — resmî statü değildir:** Bu, bağımsız bir eşleme hizmetidir; SGB/USOM ile **resmî bir bağı, onayı veya yetkilendirmesi YOKTUR**. "SGB onaylı", "resmî/ulusal tarama" veya "zorunlu kontrol" DEĞİLDİR; resmî denetim/sertifikasyon yerine geçmez. Yalnız kamuya açık bildirimlerle eşleme yapar.

Kapsam (dürüstlük): Katalogda **129** gerçek bildirim var; bunların **yalnız 16 tanesi dışarıdan gözlemlenebilir** ürüne (ör. Apache/nginx/PHP sunucu banner'ı, WordPress/Joomla/Drupal CMS) aittir ve eşlenebilir. Bir ürünün sürümü dışarıdan görülemiyorsa (ör. bir güvenlik cihazı/uç-nokta ürünü) eşleme YAPILMAZ — bu bölüm katalogun tamamının değil, yalnız dış-yüzeyden görülebilen alt kümenin durumunu gösterir. Sürüm banner'dan gizlenebildiği ve backport yamalar sürüm dizesini değiştirmediği için **"kesin etkileniyorsunuz" ASLA denmez** — çıktı yalnız bir GÖSTERGEDİR.

Katalog son güncelleme: 2026-09-01 (kamuya açık USOM/SGB akışından otomatik senkron).

*Kalan **113** bildirim, sürümü dış yüzeyden görülemeyen ürünlere (ör. güvenlik cihazı, uç-nokta/istemci yazılımı, iç sistem) ait olduğu için bu bölümde listelenmez — bu ürünler dışarıdan eşlenemediğinden haklarında bir sonuç üretilemez.*

Taranan dış-gözlemlenebilir bildirimler (tam liste)

Yukarıdaki **16** sayısı soyut değildir; hedefin dış yüzeyiyle karşılaştırılan bildirimlerin tamamı aşağıdadır:

TR No	Eşleme imzası (ürün/teknoloji)	Bildirim başlığı	Kaynak
TR-24-1843	Apache httpd	Apache Çoklu Ürün Güvenlik Bildirimi	bildirim

TR No	Eşleme imzası (ürün/teknoloji)	Bildirim başlığı	Kaynak
TR-23-0072	Apache httpd	Apache Zafiyeti	bildirim
TR-25-0035	WordPress	WordPress Eklenti Güvenlik Bildirimi	bildirim
TR-25-0127	WordPress	WordPress Eklenti Güvenlik Bildirimi	bildirim
TR-25-0130	WordPress	WordPress Eklenti Güvenlik Bildirimi	bildirim
TR-26-0894	WordPress	TR-26-0894 (WordPress Eklenti Güvenlik Bildirimi)	bildirim
TR-26-0865	Apache httpd	TR-26-0865 (Apache Çoklu Ürün Güvenlik Bildirimi)	bildirim
TR-26-0884	WordPress	TR-26-0884 (WordPress Eklenti Güvenlik Bildirimi)	bildirim
TR-26-0861	WordPress	TR-26-0861 (WordPress Eklenti Güvenlik Bildirimi)	bildirim
TR-26-0890	Apache httpd	TR-26-0890 (Apache Çoklu Ürün Güvenlik Bildirimi)	bildirim
TR-26-0914	Drupal	TR-26-0914 (Drupal Güvenlik Bildirimi)	bildirim
TR-26-0900	WordPress	TR-26-0900 (WordPress Eklenti Güvenlik Bildirimi)	bildirim
TR-26-0927	Apache httpd	TR-26-0927 (Apache APISIX Güvenlik Bildirimi)	bildirim
TR-26-0926	WordPress	TR-26-0926 (WordPress Eklenti Güvenlik Bildirimi)	bildirim
TR-26-0946	WordPress	TR-26-0946 (WordPress Eklenti Güvenlik Bildirimi)	bildirim
TR-26-0958	WordPress	TR-26-0958 (WordPress Eklenti Güvenlik Bildirimi)	bildirim

Üç-durum (dürüstlük): ✓ *Sinyal yok* = bu bildirimin imzası hedefte görülmedi · ⚠ *Sinyal var — sürüm doğrulanamadı* = ürün/teknoloji görüldü ama etkilenen sürümde olup olmadığı dışarıdan doğrulanamıyor · ⚠ *Etkilenen aralıkta olabilir* = yalnız güvenilir sürüm sinyali etkilenen aralığa düşerse.

Aşağıdaki kamuya açık bildirimlerin imzası dış-yüzeyde **gözlemlendi** (istismar/doğrulama YOK — yalnız gösterge):

TR No	Ürün / Teknoloji	Durum	CVE	Kaynak
TR-24-1843	Apache Çoklu Ürün Güvenlik Bildirimi	**⚠ Sinyal var — sürüm doğrulanamadı (görülen sürüm 2.4.25)**	—	bildirim
TR-23-0072	Apache Zafiyeti	**⚠ Sinyal var — sürüm doğrulanamadı (görülen sürüm 2.4.25)**	—	bildirim
TR-26-0865	TR-26-0865 (Apache Çoklu Ürün Güvenlik Bildirimi)	**⚠ Sinyal var — sürüm doğrulanamadı (görülen sürüm 2.4.25)**	CVE-2026-34884, CVE-2026-73632, CVE-2026-73631	bildirim
TR-26-0890	TR-26-0890 (Apache Çoklu Ürün Güvenlik Bildirimi)	**⚠ Sinyal var — sürüm doğrulanamadı (görülen sürüm 2.4.25)**	CVE-2026-63016, CVE-2026-63015, CVE-2026-47359	bildirim
TR-26-0927	TR-26-0927 (Apache APISIX Güvenlik Bildirimi)	**⚠ Sinyal var — sürüm doğrulanamadı (görülen sürüm 2.4.25)**	CVE-2026-75005, CVE-2026-63041, CVE-2026-74848	bildirim

Önerilen resmî çözüm (özet): İlgili ürünü, kaynak bildirimde belirtilen güncel/yamalı sürüme yükseltin ve sürüm/teknoloji

ifşasını azaltın. Kesin durum için bağlı bildirimi inceleyin ve sürümünüzü içeriden doğrulayın.

POZİTİF GÜVENCE — DENENEN KEŞİF YÖNTEMLERİ

Keşif çoğu sağlıklı hedefte temiz çıkar; bu bölüm "bir şey bulunamadı" sonucunu da ŞEFFAF kılar — GERÇEKTEN ne denendiğini gösterir. Aşağıda geçen **2 sayfa**, ana sayfanız ile site haritası ve robots.txt'ten türetilen sayfalardır (kendi sitenizin dışında hiçbir sayfa çekilmemiştir):

Keşif Alanı	Sonuç
Subdomain-Takeover Taraması	**✓ 0 alt domain kaydı denendi (siteye bağlı alt adresler — isim isim liste: "Subdomain Takeover Taraması" bölümü); devralma göstergesi bulunamadı (başkasının ele geçirebileceği boşta kayıt yok)**
API & Swagger Keşfi	**✓ 12 yol denendi (12 sabit + 0 site-haritası adayı, 2 sayfadan — denenen yolların TAM listesi: "API & Swagger Keşfi" bölümü); herkese açık API şeması bulunamadı (dışarıdan okunabilen API dokümanı yok)**
CMS / Framework CVE Eşleşmesi	**✓ 6 pasif sinyal kategorisi incelendi (başlıklar, meta generator, HTML izleri, sürüm dosyaları, bilinen CMS yolları, kütüphane ipuçları — tam liste: "CMS & Bilinen CVE Taraması" bölümü); bilinen bir CMS/çatı parmak izi tespit edilmedi**
Sunucu/Yazılım Banner → Bilinen CVE	**⚠ Banner sürümünde 21 bilinen CVE (PHP 7.1.26 — CVE numaraları: "Sunucu/Yazılım Banner Sürümü" bölümü)**
Site haritası + robots.txt yol keşfi	**✓ Site haritası + robots.txt Disallow'dan türetilen 0 yol denendi (yalnız var/yok kontrolü — aday yolların listesi: "API & Swagger Keşfi" bölümü); hassas/idari uç bulunamadı**
USOM/SGB Bildirim Eşlemesi	**⚠ 5 kamuya açık bildirim imzası gözlemlendi (sürüm doğrulanamadı — gösterge; hangi bildirimler: "USOM/SGB Bildirim Eşlemesi" bölümündeki eşleşme tablosu)**

Üç-durum ayrımı (dürüstlük): ✓ *Gösterge bulunamadı* = yöntem çalıştı, temiz · ⚠ *Gösterge var* = yukarıda ayrıntılı · ⚠ *İncelenemedi* = veri toplanamadı (güvenli anlamına GELMEZ).

Bu paket NE değerlendirir, NE değerlendirmez

DEĞERLENDİRİR (pasif keşif — yalnız GET, dış kaynak): alt domain envanteri + devralma (dangling CNAME), herkese açık API/Swagger/OpenAPI dokümanı, CMS/çatı ve sunucu/yazılım banner (Apache/nginx/PHP) parmak izi + bilinen CVE eşleşmesi (NVD), site haritası + robots.txt Disallow'dan türeyen API/idari-görünümlü yolların VARLIK tespiti, USOM/SGB kamuya açık bildirim kataloğuyla dış-yüzey eşlemesi (yalnız dış-gözlemlenebilir alt küme — bağımsız, resmî onay değildir) — yukarıda tanımlanan 2 sayfa üzerinden (ana sayfa + site haritası/robots.txt türevleri).

DEĞERLENDİRMEZ: aktif enjeksiyon/IDOR/XSS doğrulaması ve keşfedilen uçlara yetki testi (**Aktif Doğrulama / Tam Pentest** kapsamı), HTTP güvenlik başlığı/CORS/çerez/CSP detayı (**Basit Tarama / Dış Yüzey** kapsamı), KVKK/PCI/ISO çerçeve-eşleme (**Uyum** kapsamı). USOM/SGB eşlemesi bir **resmî onay/sertifika DEĞİLDİR**, canlı istismar yapmaz ve dışarıdan görülemeyen ürünlerin (ör. güvenlik cihazı/uç-nokta ürünü) sürümünü doğrulamaz. Bir alanda "gösterge bulunamadı" ifadesi **güvenli olduğunuzu KANITLAMAZ** — yalnız denenen pasif yöntemlerle bir gösterge çıkmadığını gösterir.

İYİ PRATİKLER / ÖNERİLEN SONRAKİ ADIMLAR

Bu tarama sonucundan bağımsız olarak, saldırı yüzeyinizi dar tutmak için önerilen kalıcı uygulamalar:

- **Kullanılmayan CNAME kayıtlarını düzenli olarak temizleyin** — terk edilmiş bulut kaynaklarına işaret eden kayıtlar subdomain takeover riski taşır; bulut kaynağını silmeden önce DNS kaydını kaldırın.

- **API dokümantasyonunuz (Swagger/OpenAPI) varsa** yalnızca kimlik doğrulamalı erişime açık tutun; üretimde herkese açık yayınlamayın.
- **CMS, eklenti ve tema sürümlerinizi** otomatik güncelleme veya düzenli takiple güncel tutun; bilinen CVE'lere karşı yamalı kalın.
- **Certificate Transparency (CT) log izleme** araçları (crt.sh, certSpotter vb.) ile yeni/beklenmeyen alt domain sertifikalarını erken fark edin.
- **Sürüm/teknoloji ifşasını azaltın** — `Server`, `X-Powered-By`, `<meta generator>` gibi başlık/etiketlerle gereksiz sürüm bilgisi sızdırmayın.
- **Alt domain envanterinizi belgeleyin** — hangi alt domainin hangi servise/ekibe ait olduğunu bilmek, boşta kalan kayıtları hızlıca fark etmenizi sağlar.

Metodoloji

Aşama	Açıklama
Keşif	Hedefin dış yüzeyi, sayfaları ve (SPA ise) JS bundle'ından gerçek uç/parametreler çıkarılır.
Otomatik tespit	Keşfedilen yüzeyde deterministik, güvenli (read-only) göstergeler aranır.
Manuel-deterministik doğrulama	Bulgular kod-tabanlı kurallarla doğrulanır; "kanıtla, istismar etme".
Yetki & oturum	Kimlik-doğrulamalı pakette çerez/oturum/yetki ve login-sonrası yüzey incelenir.
Yapılandırma	Başlık, TLS, e-posta/DNS ve ifşa yapılandırmaları gözlemlenir.

Risk Derecelendirme Kriterleri

Şiddet	Tanım
Kritik	Doğrudan/kolay istismar edilebilen, ciddi veri/erişim etkisi olan gösterge.
Yüksek	Öne çıkan, öncelikli giderilmesi gereken güçlü gösterge.
Orta	Dikkat gerektiren, bağlama göre doğrulanması önerilen gösterge.
Düşük	Sertleştirme/olgunluk fırsatı; düşük öncelikli.

Şiddet yalnız bant etiketidir (sayısal CVSS skoru kullanılmaz); tüm bulgular "gösterge, doğrulama gerekir" çerçevesindedir.

---

4. AI Çözüm Önerileri

Bu bölüm, keşif taramanızda tespit edilen tüm eksiklikler için alan alan düzeltme önerileri içerir.

Subdomain Takeover — proaktif izleme rehberi

Şu an devralınabilir alt domain tespit edilmedi. Bu durumu **sürekli** korumak için, yeni/beklenmeyen alt domain sertifikalarını erken yakalayacak bir Certificate Transparency (CT) izleme sistemi kurun:

1) certSpotter ile ücretsiz e-posta/webhook uyarısı

`sslmate.com/certspotter` üzerinde alan adınızı (ör. `nomorelink.com`, alt domainler dahil) izlemeye ekleyin; yeni sertifika yayınlandığında e-posta/webhook uyarısı alırsınız (yeni bir alt domain sertifikası, sizin oluşturmadığınız bir kayıt olabilir).

2) crt.sh'i periyodik sorgulayan basit bir cron (kendi sunucunuzda)

Her gün alt domain listesini çekip bir öncekiyle karşılaştıran, yeni giren alt domainde uyarı veren örnek betik:

```
#!/usr/bin/env bash
# /etc/cron.daily/ct-watch  (chmod +x)
DOMAIN="ornek.com"
STATE="/var/lib/ct-watch/$DOMAIN.txt"
```

```
mkdir -p "$(dirname "$STATE")"; touch "$STATE"
curl -s "https://crt.sh/?q=%25.$DOMAIN&output=json" \
  | jq -r ".[].name_value" | tr "[:upper:]" "[:lower:]" | sed "s/^\*\.//" \
  | sort -u > /tmp/ct-now.txt
NEW=$(comm -13 "$STATE" /tmp/ct-now.txt)
if [ -n "$NEW" ]; then
  echo "$NEW" | mail -s "[CT] Yeni alt domain: $DOMAIN" siz@ornek.com
  cp /tmp/ct-now.txt "$STATE"
fi
```

3) Alt domain envanteri tutun — hangi alt domainin hangi servise/ekibe ait olduğunu belgeleyin; boşta kalan (kullanılmayan) CNAME kayıtlarını, bulut kaynağını silmeden önce DNS'ten kaldırın (kaldırma sırası önemlidir).

API & Swagger Keşfi — proaktif sertleştirme rehberi

Herkese açık API dokümantasyonu bulunamadı. Bunu kalıcı kılmak için, Swagger/OpenAPI/ReDoc gibi şema uçlarını üretimde kimlik doğrulama veya IP kısıtı arkasına alın. Platformunuza uygun örneği uygulayın:

Nginx — `/swagger*`, `/api-docs*`, `/openapi.json` için IP allowlist + Basic-Auth

```
location ~* ^/(swagger|api-docs|v2/api-docs|v3/api-docs|openapi\.json|redoc) {
    allow 203.0.113.0/24;   # ofis/VPN IP bloğunuz
    deny all;               # geri kalan herkese kapalı
    auth_basic "Restricted";
    auth_basic_user_file /etc/nginx/.htpasswd;  # htpasswd ile oluşturun
    # ... mevcut proxy_pass/try_files yönergeleriniz ...
}
```

Apache (.htaccess)

```
<LocationMatch "^/(swagger|api-docs|openapi\.json|redoc)">
    AuthType Basic
    AuthName "Restricted"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
    Require ip 203.0.113.0/24
</LocationMatch>
```

Caddy

```
@apidocs path /swagger* /api-docs* /openapi.json /redoc*
basic_auth @apidocs {
    admin $2a$14$...   # caddy hash-password ile üretin
}
```

Ek öneriler: OpenAPI şemanıza global `security` tanımı ekleyin; GraphQL kullanıyorsanız üretimde introspection'ı kapatın (`introspection: false`).

CMS & Bilinen CVE — proaktif güncel kalma rehberi

Bilinen bir CMS tespit edilmedi (özel/gizlenmiş uygulama olabilir). Güncel kalmayı ve bilinen-zafiyet takibini otomatikleştirin:

1) WordPress kullanıyorsanız — otomatik minor + güvenlik güncellemesi

`wp-config.php` içine:

```
define( 'WP_AUTO_UPDATE_CORE', 'minor' );  // güvenlik/minor sürümleri otomatik
```

Eklenti/tema otomatik güncellemesi için (WP-CLI):

```
wp plugin auto-updates enable --all
wp theme auto-updates enable --all
```

2) CI/CD'ye ücretsiz bağımlılık taraması (SCA) ekleyin

- **Dependabot** (GitHub, ücretsiz): depoya `.github/dependabot.yml` ekleyin:

```
version: 2
updates:
  - package-ecosystem: "composer"   # WordPress/PHP için; npm/pip/… da desteklenir
    directory: "/"
    schedule: { interval: "weekly" }
```

- **npm audit** (Node projeleri): CI adımınıza `npm audit --audit-level=high` ekleyin; yüksek/kritik açık varsa derleme kırılsın.

3) Sürüm ifşasını azaltın — `<meta generator>`, `X-Powered-By`, `/readme.html`, `/CHANGELOG.txt` gibi sürüm sızdıran noktaları kaldırın/kapatın; böylece otomatik CVE eşlemesi saldırganlar için zorlaşır.

5. Ek — Sözlük

XSS	Cross-Site Scripting — sayfaya kötü amaçlı betik enjekte edilebilmesi.
IDOR	Yetkisiz Nesne Erişimi — kimlik parametresiyle başka kaydın erişilebilmesi.
TLS	Taşıma katmanı şifrelemesi (HTTPS'in temeli).
HSTS	Tarayıcıyı yalnız HTTPS kullanmaya zorlayan güvenlik başlığı.
CSP	İçerik Güvenlik Politikası — XSS/enjeksiyon azaltma başlığı.
CORS	Kaynaklar-arası paylaşım politikası; gevşek yapılandırma risklidir.
KVKK	Kişisel Verilerin Korunması Kanunu (Türkiye).