CyberTestify

Otomatik Güvenlik Tarama Raporu

HEDEF	PAKET	TARİH
ornek-site.com	SSL/TLS Yapılandırma Denetimi	15 Ocak 2026

GENEL DEĞERLENDİRME Orta Risk

Bu taramada kısa vadede giderilmesi önerilen önemli güvenlik bulguları tespit edildi.

Bulgular

ornek-site.com SSL/TLS Konfigürasyon Denetim Raporu

Yönetici Özeti

ornek-site.com alanı için gerçekleştirilen pasif ve aktif SSL/TLS konfigürasyon denetimi, sunucunun modern güvenlik standartlarına uygun şekilde yapılandırıldığını göstermektedir. Sertifika geçerli, TLS protokol desteği güncel, şifreleme algoritmaları güçlü ve HSTS başlığı konfigürasyonu mükemmeldir. Tespit edilen bulgular orta ve düşük seviyede olup, önerilen iyileştirmeler uygulanması halinde sistem daha da sağlamlaştırılacaktır. Immediate action gerektiren kritik veya yüksek seviyeli bir sorun bulunmamaktadır.

1. Sertifika Analizi

Geçerlilik Durumu

- **Durum**: ✅ Geçerli
- **Geçerlilik Başlangıcı**: 9 Haziran 2026 12:53:56 GMT
- **Geçerlilik Sonu**: 7 Eylül 2026 13:53:11 GMT
- **Kalan Süre**: 66 gün (denetim tarihi: 2 Ağustos 2026)

Sertifika Bilgileri

- **Sahibi (CN)**: paylasimli-sertifika.net
- **İçeren Kurum (Issuer)**: Google Trust Services (WR3)
- **Anahtar Tipi**: RSA 2048-bit
- **İmza Algoritması**: SHA256withRSAEncryption
- **Sertifika Tipi**: X.509 v3 (End-Entity)

Sertifika Zinciri

Sertifika zinciri dört seviyede ve tamamen geçerlidir:

1. **Yaprak Sertifikası**: ornek-site.com (Google Trust Services tarafından imzalanmış)
2. **Ara CA**: Google Trust Services WR3 (GTS Root R1 tarafından imzalanmış, geçerli: Dec 13 2023 – Feb 20 2029)
3. **Ara CA**: Google Trust Services LLC GTS Root R1 (GlobalSign Root CA tarafından imzalanmış, geçerli: Jun 19 2020 – Jan 28 2028)
4. **Kök CA**: GlobalSign Root CA (self-signed, tüm işletim sistemleri tarafından güvenilir)

Doğrulama Sonucu: OK (Verify return code: 0)

Hostname Eşleştirmesi

- **Common Name (CN)**: paylasimli-sertifika.net (hedef ile uyumsuz)
- **Subject Alternative Names (SANs)**:
  - paylasimli-sertifika.net
  - www.paylasimli-sertifika.net
  - **ornek-site.com** ✓
  - www.ornek-site.com

Eşleştirme Sonucu: ✓ BAŞARILI (SAN alanında ornek-site.com bulunmaktadır; modern TLS uygulamaları SAN'ı kullanarak doğrulama yapmaktadır)

---

2. TLS Protokol Desteği

Desteklenen Protokoller

Protokol	Destek	Durum
TLS 1.3	✓ Evet	Güncel, önerilen
TLS 1.2	✓ Evet	Güvenli, uyumlu
TLS 1.1	✗ Hayır	Başarıyla reddedildi
TLS 1.0	✗ Hayır	Başarıyla reddedildi
SSL 3.0	✗ Hayır	Devre dışı

Protokol Test Sonuçları

TLS 1.3 (Birincil)

- **Anlaşılan Protokol**: TLSv1.3
- **Cipher Suite**: TLS_AES_128_GCM_SHA256
- **Anahtar Değişimi**: X25519MLKEM768 (kuantum-sonrası hibrit)
- **İleri Gizlilik**: Etkin
- **Sıkıştırma**: Devre dışı
- **Handshake Sonucu**: ✓ Başarılı (Verify return code: 0)

TLS 1.2 (Yedek)

- **Anlaşılan Protokol**: TLSv1.2
- **Cipher Suite**: ECDHE-RSA-CHACHA20-POLY1305
- **Anahtar Değişimi**: ECDHE (Elliptic Curve Diffie-Hellman)
- **İleri Gizlilik**: Etkin
- **Kimlik Doğrulama**: AEAD
- **Handshake Sonucu**: ✓ Başarılı (Verify return code: 0)

TLS 1.1 Handshake Testi

- **Bağlantı**: TCP bağlantısı kuruldu
- **Handshake**: ✗ Başarısız
- **Hata Mesajı**: "no protocols available"
- **Güvenlik Değerlendirmesi**: ✓ OLUMLU (BEAST saldırılarına açık olduğundan reddi doğru)

TLS 1.0 Handshake Testi

- **Bağlantı**: TCP bağlantısı kuruldu
- **Handshake**: ✕ Başarısız
- **Hata Mesajı**: "no protocols available"
- **Güvenlik Değerlendirmesi**: ✓ OLUMLU (BEAST, POODLE, Heartbleed'e açık olduğundan reddi endüstri best practice'dir)

SSL 3.0 Protokolü

- **Test Durumu**: Yapılamadı (Modern OpenSSL kütüphaneleri POODLE CVE-2014-3566 nedeniyle SSL 3.0 desteğini kaldırmıştır)
- **Güvenlik Değerlendirmesi**: ✓ OLUMLU (Sunucu kesinlikle SSL 3.0'ı desteklemez)

---

3. Şifreleme Algoritmaları

Kullanılan Cipher Suite'ler

TLS 1.3'te Anlaşılan:

- **TLS_AES_128_GCM_SHA256**
  - Şifreleme: AES-128 GCM (128-bit kimlikaştırmalı şifreleme)
  - Hash: SHA-256
  - AEAD Modu: Evet (Galois Counter Mode)
  - Güvenlik Seviyesi: ✓ Güçlü

TLS 1.2'de Anlaşılan:

- **ECDHE-RSA-CHACHA20-POLY1305**
  - Anahtar Değişimi: ECDHE (Elliptic Curve Diffie-Hellman)
  - Kimlik Doğrulama: RSA
  - Şifreleme: ChaCha20 (modern akış şifrelemesi)
  - Kimlik Doğrulama Etiketi: Poly1305
  - Güvenlik Seviyesi: ✓ Güçlü

Zayıf Cipher Suite'ler Kontrolü

- ✕ NULL cipherler: Tespit edilmedi ✓
- ✕ Export-grade cipherler: Tespit edilmedi ✓
- ✕ RC4: Tespit edilmedi ✓
- ✕ DES, 3DES: Tespit edilmedi ✓
- ✕ CBC modu (TLS 1.3'te): Kullanılmıyor ✓
- ✕ MD5 hash: Kullanılmıyor ✓

Sonuç: Tüm aktif cipher suite'ler modern, güçlü ve kimlikaştırmalı şifrelemedir.

---

4. Güvenlik Başlıkları

HSTS (HTTP Strict-Transport-Security)

- **Durum**: ✓ Mevcut
- **Max-Age**: 31556926 saniye (1 yıl)
- **Includesubdomains**: Evet
- **Preload**: Evet
- **Değerlendirme**: ✓ Mükemmel konfigürasyon

Diğer Güvenlik Başlıkları

- **X-Frame-Options**: ✕ Mevcut değil
- **X-Content-Type-Options**: ✕ Mevcut değil
- **Content-Security-Policy**: ✕ Mevcut değil

---

5. HTTP → HTTPS Yönlendirmesi

- **Durum**: ✓ Mevcut
- **Yönlendirme Kodu**: 301 (Permanent Redirect)
- **Değerlendirme**: ✓ Doğru konfigürasyon

---

6. Bulguların Sınıflandırması

⚠ CRİTİCAL (Kritik)

Tespit edilmemiştir.

● HIGH (Yüksek)

Tespit edilmemiştir.

◍ MEDIUM (Orta)

Bulgu 1: Eksik X-Frame-Options Başlığı

- **Açıklama**: X-Frame-Options başlığı HTTP yanıtında bulunmamaktadır. Bu başlık, clickjacking saldırılarını önlemek için kullanılır.
- **Etki**: Sayfanız başka bir web sitesinin iframe'i içinde yüklenmesi suretiyle kullanıcılar yanıltılabilir.
- **Şiddet**: Orta
- **Önem**: Acil olmayan ancak önerilir

Bulgu 2: Eksik X-Content-Type-Options Başlığı

- **Açıklama**: X-Content-Type-Options başlığı HTTP yanıtında bulunmamaktadır. Bu başlık, MIME type sniffing saldırılarını önlemek için kullanılır.
- **Etki**: Tarayıcı, sunucunun belirttiği Content-Type'ı görmezden gelerek dosya türünü tahmin edebilir ve XSS saldırılarına açık hale gelebilir.
- **Şiddet**: Orta
- **Önem**: Acil olmayan ancak önerilir

Bulgu 3: Eksik Content-Security-Policy Başlığı

- **Açıklama**: Content-Security-Policy (CSP) başlığı HTTP yanıtında bulunmamaktadır. CSP, XSS ve injection saldırılarını azaltmak için kullanılır.
- **Etki**: Sayfaya enjekte edilen kötü amaçlı JavaScript kodları çalışabilir.
- **Şiddet**: Orta
- **Önem**: Acil olmayan ancak önerilir

◍ LOW (Düşük)

Bulgu 4: RSA Anahtar Boyutu 2048-bit

- **Açıklama**: Sertifika 2048-bit RSA anahtarı kullanmaktadır. NIST minimum eşiği karşılamakla birlikte, en iyi uygulama 4096-bit'tir.
- **Etki**: Minimal; 2048-bit RSA 2030'ların ortasına kadar güvenli kabul edilmektedir.
- **Şiddet**: Düşük

- **Not**: Sertifika sağlayıcısı (Google Trust Services) tarafından desteklenmektedir.
- **Önem**: Uzun vadeli (sertifika yenileme sırasında değerlendirin)

---

7. Genel Değerlendirme

Güvenlik Durumu: ✓ İYİ

ornek-site.com'un SSL/TLS konfigürasyonu aşağıdaki açılardan güvenlidir:

1. **Sertifika**: Geçerli, uygun şekilde imzalanmış, zinciri tam ve doğru, SAN doğrulaması başarılı
2. **Protokoller**: Modern (TLS 1.3 + 1.2), eski protokoller (TLS 1.1, 1.0, SSL 3.0) reddedilmiş
3. **Şifreleme**: Güçlü AEAD cipher suite'ler (AES-128-GCM, ChaCha20-Poly1305), zayıf algoritmalar yok
4. **İleri Gizlilik**: Etkin (ECDHE, X25519)
5. **HSTS**: Doğru şekilde yapılandırılmış (max-age=1 yıl, includesubdomains, preload)
6. **HTTP Yönlendirmesi**: 301 ile HTTPS'e yönlendirme var
7. **Kuantum-Sonrası Hazırlık**: X25519MLKEM768 hibrit anahtar değişimi

Iyileştirme Alanları

1. Eksik güvenlik başlıkları (X-Frame-Options, X-Content-Type-Options, CSP) eklenmeli
2. RSA anahtar boyutu ileride 4096-bit'e yükseltilmesi önerilir
3. Sertifika son kullanma tarihi (7 Eylül 2026) yakındır; yenileme planı yapılmalı

---

8. Sonuç

ornek-site.com, SSL/TLS açısından **güvenli ve modern** bir konfigürasyona sahiptir. Tespit edilen bulgular orta-düşük seviyede olup, önerilen düzeltmeler uygulanması halinde sistem daha da sağlamlaştırılacaktır. Sunucu, endüstri best practice'lerine büyük ölçüde uyumlu olup, immediate action gerektiren kritik bir sorun bulunmamaktadır.

Genel Güvenlik Notu: Sertifika zinciri doğrulanmış, TLS handshake başarılı, moderne protokoller kullanılmakta ve güçlü şifrelemeler tercih edilmektedir. Sistem production ortamında güvenli olarak kabul edilebilir.

Yasal Uyari ve Kapsam

- **Yapay zeka uretimi:** Bu rapor yapay zeka tabanli otomatik bir ajan tarafindan uretilmistir; olgusal ifadeler bagimsiz dogrulanmadan kullanilmamalidir.
- **Kapsam:** Tarama YALNIZCA sahipligi dogrulanmis hedefle ve **pasif** yontemlerle sinirlidir; ic ag, kimlik dogrulamali test ve sizma testi KAPSAM DISIDIR.
- **Resmi degildir:** Bu rapor resmi uyumluluk denetimi/sertifikasyon (ASV/QSA vb.) yerine gecmez.
- **Sorumluluk:** Bulgularin dogrulanmasi ve giderilmesi musterinin sorumlulugundadir.