WEB SİTESİ GÜVENLİK ÖN ANALİZİ VE ZAFİYET DENETİMİ RAPORU

Müşteri: [Örnek Şirket/Şahıs]

Denetim Tarihi: 14.01.2026

Denetim Kapsamı: example.com (Ana sayfa, iletişim formları, giriş panelleri)

Analiz Yöntemi: Manuel Kod Analizi, SQLi/XSS Testleri, Konfigürasyon Denetimi

---

1. YÖNETİCİ ÖZETİ (Executive Summary)

Bu rapor, hedef web uygulaması üzerinde gerçekleştirilen güvenlik ön analizi sonuçlarını içermektedir. Yapılan testler sonucunda sistemde **1 Kritik**, **2 Orta** ve **3 Düşük** seviyeli zafiyet tespit edilmiştir. Sistem genel güvenlik puanı 10 üzerinden **5.5** olarak belirlenmiştir.

Kritik Tavsiye: Veritabanı güvenliği ile ilgili tespit edilen açık, veri sızıntısı riski taşıdığı için 24 saat içerisinde müdahale gerektirmektedir.

---

2. TESPİT EDİLEN ZAFİYETLERİN DAĞILIMI

Seviye	Adet	Açıklama
Kritik	1	Acil müdahale gerektiren sistem dışı erişim riski.
Orta	2	Bilgi sızıntısı veya hizmet kesintisi riski.
Düşük	3	Güvenlik sıkılaştırma önerileri (Best Practices).

---

3. AYRINTILI BULGU ANALİZİ VE ÇÖZÜM REHBERİ

Bulgu #1: SQL Injection (Kritik Seviye)

- **Zayıf Nokta:** `/blog-detay.php?id=` sorgu parametresi.

- **Teknik Detay:** Kullanıcıdan alınan `id` değeri, veritabanı sorgusuna filtrelenmeden gönderilmektedir.
- **Risk:** Saldırgan, özel karakterler kullanarak veritabanındaki tüm tabloları (kullanıcılar, şifreler, siparişler) dökebilir.
- **Çözüm (Fix):** PDO veya MySQLi kütüphanelerinde "Prepared Statements" (Parametreli Sorgu) yapısı kullanılmalıdır.
    - *Hatalı:* `$db->query("SELECT * FROM posts WHERE id = " . $_GET['id']);`
    - *Doğru:* `$stmt = $db->prepare("SELECT * FROM posts WHERE id = ?"); $stmt->execute([$_GET['id']]);`

Bulgu #2: Güvensiz Form Gönderimi - CSRF (Orta Seviye)

- **Zayıf Nokta:** İletişim ve Kayıt formları.
- **Teknik Detay:** Form gönderimlerinde benzersiz bir "token" (belirteç) kullanılmamaktadır.
- **Risk:** Kullanıcıların haberi olmadan adlarına form doldurulabilir veya şifre değişikliği tetiklenebilir.
- **Çözüm (Fix):** Her form oturumuna özel, tahmin edilemez bir CSRF Token eklenmeli ve sunucu tarafında doğrulanmalıdır.

---

4. SONUÇ VE TAAHHÜTNAME

Bu rapor, sözleşme kapsamında belirtilen **"Web Zafiyet Testi Hizmet Sözleşmesi"** şartlarına uygun olarak hazırlanmıştır. Raporda yer alan bulgular denetim anındaki durumu yansıtır. Hizmet veren olarak, test sırasında elde edilen verilerin KVKK ve Gizlilik maddeleri uyarınca imha edildiğini taahhüt ederim.