Kurumsal Web Güvenlik Checklist'i" Şablonu — Yazılım / Web Security (v1.0)

Asset Amaç: Bu checklist, kurumsal web sitelerinde "security by design" (tasarımdan itibaren güvenlik) yaklaşımını go-live (canlıya çıkış) öncesinde uygulanabilir kontrol noktalarına dönüştürür. OWASP Top 10 riskleri, kimlik doğrulama/rol yetkilendirmeleri, form/dosya yükleme güvenliği ve admin paneli sıkılaştırma (hardening) adımlarını tek bir entegre dokümanda toplar. Özellikle kullanıcı ve ödeme verisi barındıran büyük otel zincirleri ve kurumsal B2B projelerinde, canlı yayına geçiş öncesinde aşılması zorunlu bir güvenlik kapısı (security gate) işlevi görür.

Kim Kullanır?: Tech Lead, Front-End/Back-End Yazılım Geliştiriciler, DevOps Mühendisleri, QA (Kalite Güvence) Test Ekipleri, Siber Güvenlik Sorumluları ve Proje Yöneticileri.

Nasıl Kullanılır?

1. İlgili checklist bileşenlerini öncelikle canlı ortamın birebir kopyası olan Staging (test) ortamında çalıştırın, sızma ve açık tarama test bulgularını kayıt altına alın.
2. Tespit edilen zafiyetleri ve mimari riskleri "kök neden → çözüm" metodolojisiyle önceliklendirerek düzeltme planına dahil edin.
3. Dokümanda yer alan 14 günlük hızlandırılmış sprint planını uygulayarak hardening (sıkılaştırma) adımlarını tamamlayın ve go-live öncesi son kontrollerde açıkları tekrar doğrulayarak kapatın.

TEMPLATE — Kurumsal Web Güvenlik Checklist'i & Hardening Matrisi

A) Ölçüm & Önceliklendirme Checklist'i

Sistem bileşenlerinin yayına çıkış öncesi siber direnç durumunu doğrulayan ana kontrol listesi:

- **[ ] MFA + Rate Limit:** Yönetici panellerinde ve kritik kullanıcı giriş adımlarında Çok Faktörlü Kimlik Doğrulama (MFA) ile istek sınırlandırma (Rate Limiting) aktif mi?
- **[ ] RBAC Rol Matrisi:** Kullanıcıların sadece kendi yetki alanlarına erişmesini sağlayan Rol Tabanlı Erişim Kontrolü (RBAC) altyapısı kuruldu mu?
- **[ ] Input Validation / Output Escaping:** SQL Injection ve XSS zafiyetlerini önlemek adına tüm kullanıcı girdileri temizleniyor (validation) ve dışarı aktarılan veriler maskeleniyor (escaping) mu?
- **[ ] CSRF Koruması:** Form gönderimlerinde ve durum değiştiren tüm HTTP isteklerinde benzersiz CSRF (Cross-Site Request Forgery) token mekanizması devrede mi?
- **[ ] Upload Allowlist + Limit:** Dosya yükleme (upload) alanlarında sadece izin verilen uzantılar (allowlist) kabul ediliyor ve maksimum dosya boyutu sınırı uygulanıyor mu?
- **[ ] Admin Paneli Sıkılaştırma (VPN/IP):** Yönetim paneli girişleri halka açık internete kapalı mı; kurumsal VPN veya belirli IP adreslerine kısıtlandı mı?
- **[ ] Log / Alert Sistemleri:** Şüpheli giriş denemeleri, kaba kuvvet (brute force) saldırıları ve yetkisiz erişim adımları için anlık günlük kaydı ve alarm (alert) mekanizması var mı?

- **[ ] KVKK / PII Minimizasyonu:** Kullanıcı gizliliği yasaları uyarınca, veri tabanında ve log dosyalarında kişisel verilerin (PII) tutulma miktarı minimuma indirilip maskeleme yapıldı mı?

B) Problem → Kök Neden → Çözüm Tablosu

Checklist taramaları sonucunda en sık karşılaşılan kritik güvenlik açıklarının operasyonel çözüm matrisi:

Problem (image_a42e22.png)	**Kök Neden**	**Çözüm**	**Öncelik**
Admin brute force	Rate limit yok	Rate limit + MFA	Yüksek
XSS riski	Sanitize/escape yok	Output escape	Yüksek
Upload açıkları	Tür serbest	Allowlist + izolasyon	Yüksek
Yetki sızıntısı	RBAC yok	Rol matrisi + guard	Yüksek

C) 14 Günlük Güvenlik & Hardening Sprint Planı

Web sitesini siber tehditlere karşı tamamen izole etmek için kurgulanmış iki haftalık aksiyon takvimi:

- **Gün 1: Risk Yüzeyi Envanteri** → Sitedeki tüm auth, form ve admin giriş panellerinin haritasını çıkarın, envanter oluşturun.
- **Gün 2: MFA & Rate Limiting** → Brute force saldırılarını engellemek adına API uçlarına ve panellere istek kısıtı ve MFA entegre edin.
- **Gün 3: RBAC ve Yetki Kontrolleri** → Rol tabanlı yetki kontrol mimarisini test edin, dikey ve yatay yetki sızıntılarını engelleyin.
- **Gün 4: Input Validation Standardı** → Tüm form girdilerini backend seviyesinde doğrulama (validation) filtresinden geçirin.
- **Gün 5: CSRF Kontrolleri** → Durum değiştiren (POST/PUT/DELETE) tüm isteklere güvenli CSRF token doğrulamasını ekleyin.
- **Gün 6: Upload Hardening** → Dosya yükleme dizinlerinde script çalıştırılmasını (execution) engelleyin, allowlist kuralını uygulayın.
- **Gün 7: Admin Panel Erişim Kısıtları** → Admin paneli giriş URL'ini değiştirin, erişimi sadece şirket IP'si veya VPN ile kısıtlayın.
- **Gün 8: Log / Alert Kurgusu** → Başarısız giriş denemeleri ve anormallikleri Slack/E-posta kanallarına uyarı olarak gönderen log sistemini kurun.

- **Gün 9: PII Minimizasyon & Maskeleme** → Veri tabanında kayıtlı hassas müşteri bilgilerini, kredi kartı maskelerini ve log çıktılarını temizleyin.
- **Gün 10: Otel / B2B Kritik Akış Testleri** → Rezervasyon motoru, B2B sipariş formu ve ödeme adımları gibi kritik süreçleri siber testlere tabi tutun.
- **Gün 11: Staging Security Gate Dry-Run** → Canlıya çıkış öncesinde test sunucusunda tüm checklist maddelerini içeren kapsamlı bir simülasyon yapın.
- **Gün 12: Fix Deploy** → Yapılan testlerde ortaya çıkan son minör güvenlik açıklarını gideren yamaları (patch) test ortamına yükleyin.
- **Gün 13: Retest** → Kapatılan zafiyetlerin gerçekten düzeltilip düzeltilmediğini doğrulamak adına son kez doğrulama taraması gerçekleştirin.
- **Gün 14: Go-Live Checklist Final** → Güvenlik kapısı (security gate) onayını vererek projeyi tam kilitli ve korumalı şekilde canlıya alın.

D) Öncesi / Sonrası Güvenlik KPI Tablosu

Sıkılaştırma operasyonunun projenin güvenlik skoruna olan etkisini gösteren performans paneli:

KPI (image_a42b5d.png)	Önce	Sonra (30 gün)	Hedef
Kritik bulgu sayısı	TBD	TBD	↓
Form abuse oranı	TBD	TBD	↓
Yetkisiz erişim denemesi	TBD	TBD	↓
Incident sayısı	TBD	TBD	↓

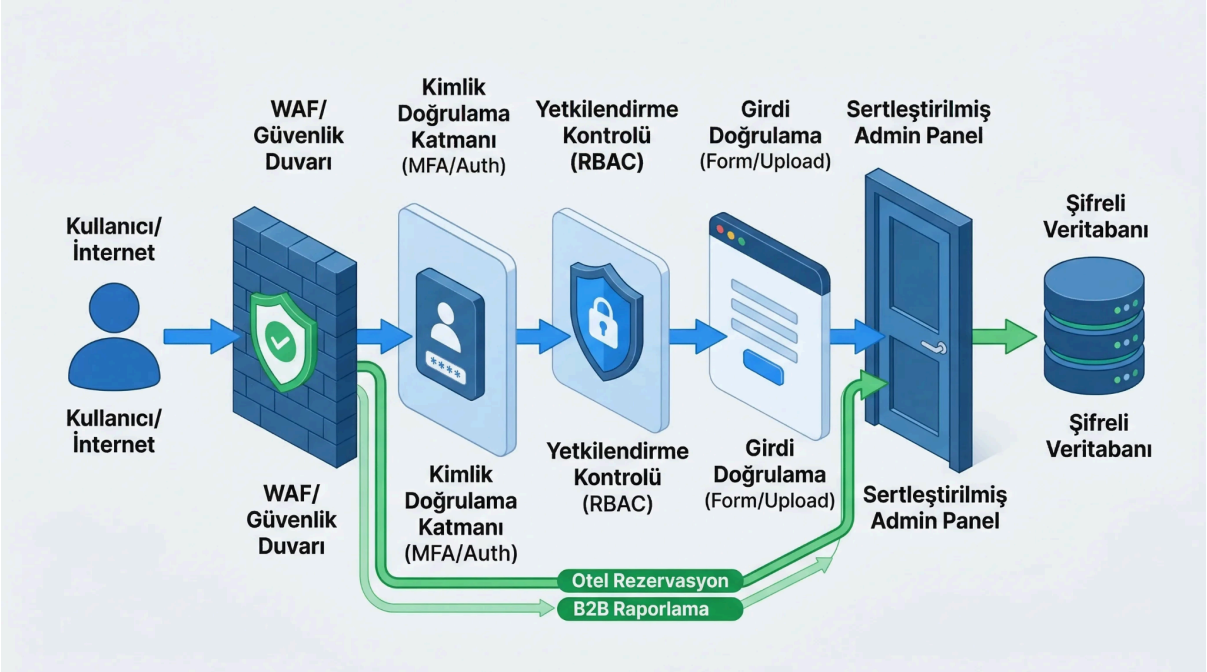
Teknik Kontrol Listesi (Checklist)

- [ ] **OWASP Uyumluluğu:** Sitedeki tüm dinamik sorgular ve kullanıcı giriş alanları en güncel OWASP Top 10 zafiyet standartlarına göre denetlendi.
- [ ] **Çift Katmanlı Koruma:** Yönetici ve bayi paneli (B2B) girişleri için rate limit ile birlikte MFA altyapısı teknik olarak kodlandı.
- [ ] **İzolasyon Güvencesi:** Yüklenen kullanıcı dosyalarının ana sunucudan bağımsız, script çalıştırma yetkisi olmayan izole bir bucket/sunucuda barındırılması sağlandı.
- [ ] **SLA ve Sprint Takibi:** 14 günlük güvenlik sprint takvimindeki tüm görevlerin tamamlandığı teknik ekiplerce teyit edildi.

Deliverables (Teslim Edilecek Çıktılar)

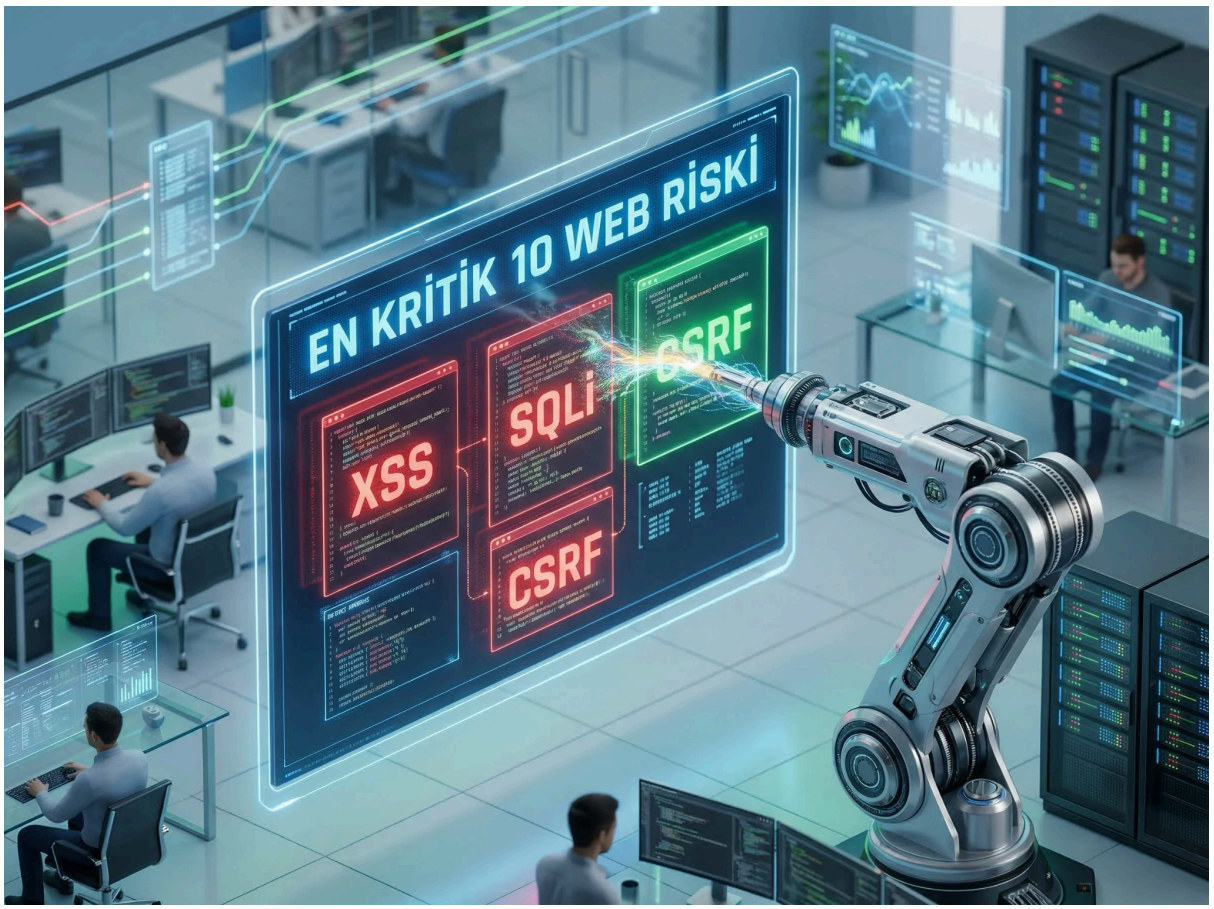
- Tüm Ekip Rollerini ve İzin Sınırlarını Belirleyen 1 Adet RBAC Yetki Matrisi

- Sunucu ve Yönetim Paneli Güvenliğini Sağlayan 1 Adet Admin Hardening Ayar Listesi
- Dosya Yükleme Açıklarını Sıfırlayan 1 Adet Kurumsal Upload Policy Dokümanı
- Canlıya Geçiş Onay Süreçlerinde Kullanılacak 1 Adet Go-Live Security Gate Checklist'i



[Layered Security Diagram] — 16:9 — katmanli-guvenlik-diyagrami.webp

Bir web uygulamasının siber saldırılara karşı savunma katmanlarını gösteren, 16:9 formatında çizilmiş teknik bir katmanlı güvenlik mimari diyagramı. Gece siyahı arka plan üzerinde, dıştan içe doğru iç içe geçmiş parlak halkalar şeklinde uzanan katmanlar scannable bir hiyerarşiyle sergileniyor. En dışta "WAF & Network Security (Rate Limit)" halkası neon mavi ışıldarken, sırasıyla içe doğru "Admin Hardening (VPN/IP)", "Application Gate (RBAC & CSRF Token)" ve en merkezde korunan çekirdek veri tabanını simgeleyen "Data Encryption & PII Masking" katmanı yer alıyor. Her katmanın birleşme noktasında küçük yeşil kilit ikonları bulunuyor.



[OWASP Control Card] — 1:1 — owasp-kontrol-kartu.webp

Yazılım geliştiricilerin monitör kenarlarına veya teknik wiki panellerine asarak hızlıca kontrol edebilecekleri, 1:1 kare formatında minimalist bir OWASP kontrol kartı tasarımı. Koyu antrasit zemin üzerinde, iki sütun halinde yer alan şemada sol tarafta popüler web açıkları (SQLi, XSS, Broken Auth) kırmızı uyarı şeritleriyle listelenirken; sağ tarafta bu açıklara karşı alınması gereken kod seviyesindeki önlemler (Sanitization, Output Escaping, MFA) temiz, beyaz fontlar ve onay kutucuklarıyla sunuluyor. Sağ alt köşede "Security Gate: Geçti" damgası mat yeşil bir mühür gibi parlayarak "clarity at a glance" felsefesini destekliyor.