İşine göre *5 güvenlik katmanı*

Yayına almadan önce: sızan anahtar, bot, müşteri verisi, tuzak anahtar ve kayıt. Her katmanın kurulum adımı, ücretsiz sınırı ve sektörüne göre hangisinin önce geldiği.

Önce genel kısım, *sonra* kendi sayfan.

01 Önce 'tek bakışta' tablosuna ve kendi sektör sayfana bak: hangi katman önce, orada yazıyor.

02 Sonra o katmanın kurulum sayfasına geç. Komutları kopyalayıp kendi bilgisayarında ya da sunucunda çalıştır.

03 Her hafta tek katman kur. Beşini aynı gün kurmaya çalışma.

04 Yapay zekâya kod yazdırıyorsan 'sorman gereken sorular' sayfasını her yayından önce kullan.

05 Komut satırı sana yabancıysa bu sayfaları geliştiricine ver; neyi istediğini bilmek yarı iş.

SEKTÖRLER

Butik mağaza / e-ticaret s. 14
Diş kliniği s. 15
Psikolog / psikolojik danışman s. 16
Avukat s. 17
Mali müşavir s. 18
Emlak ofisi s. 19
Butik otel s. 20
Kafe-restoran s. 21
Kurs / eğitmen s. 22
Spor salonu s. 23
Düğün organizasyonu s. 24
Fotoğrafçı s. 25

Herkes için *ortak* kısım

BU REHBER KİMİN İÇİN

Siteni, randevu ya da sipariş uygulamanı yapay zekâyla (Lovable, Cursor, Claude gibi) kurduysan ya da biri senin için kurduysa bu sayfalar senin için. Karuseldeki 5 katmanın her biri için kurulum adımı, ücretsiz sınır ve kontrol yolu var. Shopify, Wix, ikas gibi hazır bir platform kullanıyorsan katmanların bir kısmı platformun işi; sektör sayfanda hangisinin sana kaldığı yazıyor.

5 KATMAN, TEK BAKIŞTA (ÜCRETSİZ SINIRLAR 10 EKİM 2026)

KATMAN	HAZIR SERVIS · ÜCRETSIZ KISIM	AÇIK KAYNAK
1 · Sızan anahtar	GitGuardian Starter: 25 geliştiriciye kadar, kart istemez	TruffleHog (AGPL-3.0)
2 · Bot saldırısı	Cloudflare Free: DDoS koruması, Bot Fight Mode, 1 hız kuralı, 5 özel kural	CrowdSec (MIT)
3 · Müşteri verisi	Supabase Free: Postgres RLS, 2 aktif proje, 500 MB	PocketBase (MIT)
4 · Tuzak anahtar	Canarytokens: tamamen ücretsiz	canarytokens-docker (kendi sunucunda)
5 · Kayıt (log)	Better Stack: 10 izleyici, ayda 3 GB log, 3 gün saklama	SigNoz (kendi sunucunda)

SEKTÖRE GÖRE HANGİ KATMAN ÖNCE

Hassas veri tutan işler (diş kliniği, psikolog, avukat, mali müşavir, fotoğrafçı, kurs) Katman 3 ile başlar. Form ve sipariş alanlar (kafe-restoran, emlak, düğün organizasyonu) Katman 2 ile. Ödeme ya da dış sistem anahtarı bağlayanlar (e-ticaret, butik otel, spor salonu) Katman 1 ile. Ayrıntısı kendi sayfanda.

> Bu 5 katman temel koruma; profesyonel bir güvenlik denetiminin yerini tutmaz. Komutlar ve sınırlar 10 Ekim 2026'da resmî sayfalardan kontrol edildi. Ücretsiz planlar değişebilir, kurmadan önce sağlayıcının fiyat sayfasına bir kez bak.

Katman 1 · *Sızan anahtar*

ÖNCE ŞUNU BİL

.env, uygulamanın API anahtarlarını ve şifrelerini tuttuğu dosya. Yapay zekâ araçları bu dosyayı bazen koda gömer ya da GitHub'a gönderir. İlk iş: .env dosyasının adı .gitignore içinde mi, bak. Sonra deponun geçmişini tara; silinmiş bir anahtar eski commit'te hâlâ duruyor olabilir.

TRUFFLEHOG: KENDİ BİLGİSAYARINDA TARA

```
# macOS
brew install trufflehog
# Linux / macOS kurulum betiği
curl -sSfL
https://raw.githubusercontent.com/trufflesecurity/trufflehog/main/scripts/install.sh
| sh -s -- -b /usr/local/bin
# Windows: Docker Desktop açıkken, proje klasöründe (PowerShell)
docker run --rm -it -v "${PWD}:/pwd" trufflesecurity/trufflehog:latest filesystem
/pwd

# Deponun bütün geçmişini tara (proje klasöründe)
trufflehog git file://. --results=verified,unknown
# Git olmayan bir klasörü tara
trufflehog filesystem ./proje
```

> Bir anahtar bulunduysa dosyadan silmek yetmez, git geçmişinde kalır. Sıra şöyle: sağlayıcının panelinde (OpenAI, Stripe, iyzico...) o anahtarı iptal et, yenisini üret, yenisini yalnız .env'e ya da barındırma panelinin gizli değişkenlerine yaz. 'verified' sonuç, anahtarın hâlâ çalıştığı anlamına gelir; önce onları kapat.

Katman 1 · *Sürekli izleme*

GİTGUARDİAN: DEPOYU CANLI İZLET

- gitguardian.com'da ücretsiz Starter hesabı aç (kart istemez).
- Settings > Integrations > Sources > GitHub > Install. Depolarını seç; uygulama yalnız okuma izni alır.
- Sızıntı olunca e-posta gelir. Starter'da gerçek zamanlı tarama sınırsız; geçmiş taramada 500 bulguya, ayda 10 bin API çağrısına kadar.
- Bilgisayarına ggshield kur: brew install ggshield ya da pipx install ggshield; Windows'ta choco install ggshield.
- ggshield auth login ile bağlan, ggshield install --mode global ile her commit'ten önce otomatik taramayı aç. Elle tarama: ggshield secret scan repo .

GİTHUB'DA HER GÖNDERİMDE TRUFFLEHOG (.GİTHUB/WORKFLOWS/SİZİNTİ.YML)

```
on:
  push:
    branches: [main]
  pull_request:
jobs:
  tara:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
        with:
          fetch-depth: 0
      - uses: trufflesecurity/trufflehog@main
        with:
          extra_args: --results=verified,unknown
```

Katman 2 · *Bot saldırısı*

CLOUDFLARE ÜCRETSİZ PLAN: ADIM ADIM

- dash.cloudflare.com'da hesap aç. Domains > Onboard a domain, alan adını yaz, Free planı seç.
- DNS kayıtlarını kontrol et. Alan adını aldığın firmada DNSSEC açıksa kapat, nameserver'ları Cloudflare'in verdikleriyle değiştir. Aktif olması 24 saati bulabilir; sonra DNSSEC'i Cloudflare'den yeniden aç.
- Bot Fight Mode: Security Settings > 'Bot traffic' filtresi > Bot fight mode'u aç.
- Hız kuralı: Security rules > Create rule > Rate limiting rules. Ücretsizde 1 kural var; yalnız IP'ye göre sayar, 10 saniyelik pencere ve 10 saniyelik engel, koşul olarak yalnız adres yolu (ör. /api/siparis). En çok saldırı alan formunu seç.
- Ücretsizde ayrıca 5 özel güvenlik kuralı var: ör. yönetici paneli yolunu yalnız Türkiye'den gelen trafiğe aç.

> Bot Fight Mode istisna tanımaz; mobil uygulama ya da API trafiğini yanlışlıkla engelleyebilir. Açtıktan sonra formunu ve uygulamanı telefondan bir kez dene. Panel menüleri yeni Cloudflare arayüzüne göre yazıldı; eski arayüzde adlar farklı olabilir.

Katman 2 · Kendi sunucunda *CrowdSec*

NE ZAMAN GEREKİR

CrowdSec, kendi sunucunu (VPS) yönetiyorsan işe yarar: sunucudaki kayıtları okur, saldırı deseni gördüğü IP'yi engeller ve topluluğun zararlı IP listesini kullanır. Siten Vercel, Netlify ya da hazır bir platformdaysa sunucuya erişimin yoktur; o durumda Cloudflare yeter.

UBUNTU / DEBİAN SUNUCUDA KURULUM

```
curl -s https://install.crowdsec.net | sudo sh
sudo apt update && sudo apt install crowdsec
# Engelleyici (bouncer): güvenlik duvarı ya da nginx
sudo apt install crowdsec-firewall-bouncer-iptables
sudo apt install crowdsec-nginx-bouncer
# Nginx senaryolarını ekle
sudo cscli collections install crowdsecurity/nginx
# Ne engellendi, ne çalışıyor?
sudo cscli decisions list
sudo cscli metrics
# Ücretsiz Console'a bağla (anahtar: app.crowdsec.net > Engines)
sudo cscli console enroll [anahtarın]
```

BİLMEN GEREKENLER

- Ücretsiz topluluk listesi: sinyal paylaşan ücretsiz kullanıcıya 3 bin IP'lik liste verilir.
- Windows sunucuda MSI ya da choco install crowdsec, engelleyici olarak crowdsec-windows-firewall-bouncer.
- İki engelleyiciden birini seç: nginx kullanıyorsan nginx bouncer yeter.

Katman 3 · Müşteri verisi (*RLS*)

RLS NE, SUPABASE'DE DURUM NE

RLS (Row Level Security), her satırı kimin görebileceğini veritabanının kendisinde belirleyen kural. Supabase 7 Ocak 2026'da açıkladı: panelden açılan tablolarda RLS artık varsayılan açık. Ama yapay zekâ aracının SQL ya da migration ile açtığı tablolarda kontrol şart. Panelde Advisors > Security bölümü RLS'si kapalı tabloyu 'rls_disabled_in_public' hatasıyla gösterir.

SQL EDİTOR'DA ÇALIŞTIR

```
-- 1) RLS'si kapalı tabloları bul
select tablename from pg_tables
where schemaname = 'public' and rowsecurity = false;

-- 2) Bir tabloda RLS'yi aç
alter table public.siparisler enable row level security;

-- 3) Herkes yalnız kendi satırını görsün
create policy "kendi siparisini gorur"
on public.siparisler for select
to authenticated
using ( (select auth.uid()) = user_id );
```

> RLS açık ama politika yoksa tablo kimseye veri döndürmez; uygulama 'boş' görünürse sebep bu. service_role anahtarı RLS'yi atlar, asla tarayıcıya giden koda koyma. 30 Ekim 2026'dan itibaren mevcut projelerde de yeni tablolar API'ye kendiliğinden açılmıyor; açmak için önce yetki (grant), sonra RLS.

Katman 3 · *PocketBase* ve sınırlar

POCKETBASE: KENDİ SUNUCUNDA, YETKİSİ HAZIR

- pocketbase.io'dan işletim sistemine uygun dosyayı indir, aç, ./pocketbase serve çalıştır.
- Yönetim paneli: http://127.0.0.1:8090/_/ — ilk süper kullanıcıyı burada oluştur.
- Her koleksiyonun API Rules sekmesi var. Yeni koleksiyonda kurallar kilitli gelir (yalnız süper kullanıcı). Kuralı boş bırakmak herkese açar; dikkat.
- Kendi kaydını görme kuralı örneği: user = @request.auth.id (koleksiyondaki 'user' alanı giriş yapan kişiye eşitse).
- Sürüm v0.40.5 (10 Ekim 2026). 1.0'a kadar güncellemelerde geriye uyumluluk garantisi yok; güncellemeden önce yedek al.

SUPABASE ÜCRETSİZ PLAN (10 EKİM 2026)

KALEM	SINIR
Aktif proje	2
Veritabanı	Proje başına 500 MB
Aylık aktif kullanıcı	50.000
Dosya depolama	1 GB
Hareketsizlik	1 hafta işlem olmazsa proje duraklatılır

Katman 4 · *Tuzak anahtar*

CANARYTOKENS'TA AWS ANAHTARI TUZAĞI

- canarytokens.org/generate adresine gir, listeden AWS Keys'i seç.
- 'Bunu nereye koydum' notunu yaz: ör. 'randevu sitesi .env, sunucu'. Uyarı gelince hangi tuzak olduğunu bununla anlarsın.
- Uyarının gideceği e-posta adresini ya da webhook adresini gir.
- Çıkan iki anahtarı (access key ve secret) sahte bir credentials dosyasına ya da .env'e gerçekmiş gibi koy.
- Biri o anahtarla bir şey denediği an e-posta ya da webhook bildirimi gelir. Tuzak anahtar hiçbir yere erişim vermez.

BAŞKA TUZAKLAR

Aynı sayfada MS Word ve MS Excel belgesi (açılınca haber verir), MySQL döküm dosyası, QR kod, web bug ve DNS tuzağı da var; hepsi ücretsiz. Ör. 'musteri-listesi.xlsx' adında bir Excel tuzağını gerçek dosyaların yanına koyabilirsin. Kendi sunucunda çalıştırmak istersen: github.com/thinkst/canarytokens-docker.

> Bildirim e-posta ve webhook ile geliyor. Slack ve Discord için resmî bir seçenek yok; telefon SMS'i de ücretsiz serviste yok. Tuzağı herkese açık bir depoya koyma: GitHub'ı tarayan botlar sürekli tetikleyebilir, gerçek alarmı kaçırırsın.

Katman 5 · *Kayıt* ve izleme

BETTER STACK: HAZIR SERVİS

- betterstack.com'da ücretsiz hesap aç. İlk iş Uptime'da sitenin ve en önemli formunun adresine izleyici ekle.
- Ücretsiz planda 10 izleyici ve 1 durum sayfası var; kontrol 3 dakikada bir yapılır. Uyarı e-posta ve Slack ile gelir; telefon ve SMS ücretli planlarda.
- Logs (eski adı Logtail): ayda 3 GB kayıt, 3 gün saklama. Uygulamanı bağlamak için Better Stack dokümanında kullandığın dile (Node, Python...) uygun adımı izle.
- Ayda 100 bine kadar hata kaydı (exception) da ücretsiz kısımda.

SİGNOZ: KENDİ SUNUCUNDA (EN AZ 4 GB RAM, DOCKER)

```
# Güncel kurulum aracı: Foundry
curl -fsSL https://signoz.io/foundry.sh | bash
# casting.yaml dosyasını yaz (kind: Installation,
# flavor: compose, mode: docker); tam örnek:
# signoz.io/docs/install/docker
foundryctl cast -f casting.yaml
# Arayüz: http://localhost:8080
```

> Eski 'git clone + docker compose' kurulumu SigNoz'da artık önerilmiyor. Windows'ta Docker Desktop yerine WSL2 içinde Docker Engine gerekiyor. Hangisini seçersen seç: kayıtlara şifre, kart numarası, hasta ya da müvekkil adı yazdırma.

Yapay zekâya kod yazdırırken *sor*

YAYINA ALMADAN ÖNCE YAPIŞTIR

```
Bu kodu yayına almadan önce kontrol et. Her soruya
evet/hayır ve ilgili dosya adıyla cevap ver:
1. .env dışında bir API anahtarı ya da şifre var mı?
2. .env dosyası .gitignore içinde mi?
3. Tarayıcıya giden kodda gizli anahtar var mı?
4. Her tabloda RLS açık mı, politikası ne?
5. Adresteki numarayı değiştiren başkasının verisini görür mü?
6. Form ve API uçlarında hız sınırı var mı?
7. Kullanıcı girdisi sunucuda doğrulanıyor mu?
8. Hata mesajı iç detay (sorgu, dosya yolu) gösteriyor mu?
9. Kayıtlara şifre ya da kişisel veri yazılıyor mu?
10. Paketlerde bilinen açık var mı? (npm audit)
Her sorun için düzeltme öner, kendi başına değiştirme.
```

CEVABI NASIL OKURSUN

- 'Evet, güvenli' cevabı yeterli değil. 5. soruyu kendin tarayıcıda dene: giriş yap, adresteki numarayı bir artır.
- 'Bilmiyorum' ya da belirsiz cevap gelen her madde, bir geliştiriciye bakılacak madde.
- Düzeltmeleri tek tek uygulat, her birinden sonra uygulamayı dene.

Sıradaki seri: kısa *kontrol listesi*

KARUSELİN SONUNDA ANDIĞIMIZ 4 KONU

KONU	NE DEMEK	BU HAFTA YAP
Girdi doğrulama	Formdan gelen her veriyi sunucuda kontrol etmek	İzin verilen biçimi tanımla (telefon yalnız rakam, e-posta biçimi). Tarayıcıdaki kontrol tek başına yetmez.
Bağımlılık güvenliği	Kullandığın hazır paketlerdeki bilinen açıklar	npm audit çalıştır. GitHub'da Dependabot uyarılarını aç; tüm planlarda ücretsiz.
Gizli anahtar yenileme	Anahtarları belli aralıkla ve ayrılıklardan sonra değiştirmek	Ödeme ve yapay zekâ anahtarlarının yenileme tarihini takvime yaz. Ekipten biri ayrılınca o gün yenile.
İki adımlı doğrulama ve oturum	Girişi şifreden fazlasına bağlamak, oturumu zamanında kapatmak	Yönetici hesaplarında iki adımlı doğrulama zorunlu olsun. Girişten sonra oturum kimliği yenilensin, boşta kalan oturum kapansın.

KAYNAKLAR (10 EKİM 2026)

- OWASP Cheat Sheet Series: Input Validation, Secrets Management, Multifactor Authentication, Session Management.
- docs.npmjs.com: npm audit · docs.github.com: Dependabot.

- Oturum çerezlerinde Secure, HttpOnly ve SameSite ayarlarını yapay zekâya ayrıca sor.

01 Butik mağaza / e-ticaret

Mağazada en pahalı açık ödeme tarafında: sızan bir ödeme anahtarı, bot dolu bir kupon formu ya da başkasının sipariş adresini gösteren bir sayfa.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Sızan anahtar	Ödeme sağlayıcının (iyzico, PayTR gibi) gizli anahtarı koda yazıldıysa, sızdığı gün başkası senin adına işlem denemeye başlayabilir.
2	Bot saldırısı	Kupon, sepet ve üye ol formları botların ilk hedefi. Sahte sipariş ve deneme-yanılma burada olur.
3	Veri yetkisi	Sipariş ve adres tablosu yalnız siparişin sahibine açık olmalı.

BU HAFTA

- Uygulamanı kendin ya da yapay zekâyla yazdırdıysan deponu TruffleHog ile tara (genel bölüm, Katman 1).
- Ödeme panelinde test anahtarıyla canlı anahtarı ayır; canlı anahtar yalnız sunucuda dursun.
- Cloudflare'de ödeme ya da kupon adresine tek hız sınırı kuralını yaz.
- Supabase kullanıyorsan RLS kontrol sorgusunu çalıştır; sipariş tablosu listede çıkmamalı.

> Shopify, ikas, Ticimax gibi hazır altyapı kullanıyorsan 1–3. katmanların büyük kısmı platformun işi. Sana kalan: panel hesabında iki adımlı doğrulama, eklenti ve entegrasyon anahtarlarını kimseyle paylaşmamak, ayrılan çalışanın erişimini aynı gün kapatmak.

02 Diş kliniği

Klinikte korunacak asıl şey hasta bilgisi. KVKK'da sağlık verisi özel nitelikli kişisel veri; sızarsa sorumluluğu ağır. Sıra ona göre kuruldu.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Veri yetkisi	Online randevu tablosunu yalnız klinik görsün. Adresteki numarayı değiştiren biri başka hastanın kaydını açamamalı.
2	Tuzak anahtar	Randevu sisteminin klasörüne sahte bir anahtar koy; biri sistemi kurcalarsa ilk anda haber al.
3	Kayıt (log)	Kim ne zaman hangi kayda baktı, görebilmen gerekir.

BU HAFTA

- Online randevu formunda yalnız ad, telefon ve uygun saat iste. Şikâyet ya da tedavi alanı açma.
- Randevu tablosunda RLS açık mı, genel bölümdeki sorguyla kontrol et.
- Kayıtlara (log) hasta adı ya da telefon yazdırma; kayıt numarası yeter.

> Tedavi notu, röntgen, anamnez gibi sağlık verisini yapay zekâyla hızlıca kurulmuş bir deneme uygulamasına ya da bulut tabanlı bir yapay zekâ aracına koyma. Bu katmanlar temel koruma; hasta verisi işliyorsan KVKK uyumu için bir uzmana da danış.

03 Psikolog / psikolojik danışman

Seans içeriği sızarsa geri dönüşü yok. Bu yüzden yapay zekâyla kurulan bir randevu sitesinde bile ilk iş, hassas bilginin o sisteme hiç girmemesi.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Veri yetkisi	Danışan listesi ve randevular yalnız sana açık olmalı. Başka danışanın kaydı tek tıkla açılmamalı.
2	Sızan anahtar	Randevu ve ödeme bağlantılarının anahtarları koda yazıldıysa önce onları temizle.
3	Tuzak anahtar	Sahte bir 'danisan-listesi' belgesi koy; açılırsa haberin olsun.

BU HAFTA

- Randevu formunda yalnız ad, iletişim ve uygun saat iste. 'Neden geliyorsunuz' alanını kaldır.
- Seans notlarını bu sistemde değil, bilgisayarında şifreli bir klasörde tut.
- Canarytokens'tan bir Word tuzağı oluştur, not klasörünün yanına koy (genel bölüm, Katman 4).

> Seans notlarını ve danışan sağlık bilgisini bulut tabanlı yapay zekâ araçlarına yükleme; gerekiyorsa adı ve tanınmayı sağlayan her şeyi silerek anonimleştir. KVKK ve meslek etiği burada güvenlik ayarından önce gelir.

04 Avukat

Müvekkil dosyası hem KVKK hem meslek sırrı kapsamında. Yapay zekâyla kurulan bir belge paylaşım portalı varsa, açığın bedeli sadece teknik değil.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Veri yetkisi	Müvekkil portalında her müvekkil yalnız kendi dosyasını görmeli. Belge bağlantıları tahmin edilemez olmalı.
2	Tuzak anahtar	Belge klasörüne sahte bir Word dosyası koy; açıldığı an e-posta gelsin.
3	Sızan anahtar	E-imza, UYAP ya da bulut depolama erişim bilgileri hiçbir kod dosyasında durmamalı.

BU HAFTA

- Portaldaki belge adreslerini dene: numarayı bir artırınca başka dosya açılıyor mu?
- Herkese açık paylaşım linklerini kapat; süreli ve kişiye özel link kullan.
- Canarytokens'tan MS Word tuzağı oluştur, ana dosya klasörüne 'muvekkil-listesi' adıyla koy.

> Müvekkil bilgisini ve dava belgelerini bulut tabanlı yapay zekâ araçlarına yükleme. Bu sayfa teknik bir başlangıç; KVKK ve sır saklama yükümlülüğün için bir bilişim hukuku uzmanıyla birlikte değerlendir.

05 Mali müşavir

Büroda en tehlikeli dosya, mükelleflerin şifrelerinin durduğu yer. Yapay zekâyla hazırlanmış bir mükellef portalı ya da takip tablosu varsa sıra şöyle.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Sızan anahtar	Şifreler ve API anahtarları kodda, tabloda ya da e-postada düz yazıyla durmamalı.
2	Veri yetkisi	Mükellef portalında herkes yalnız kendi belgesini görmeli.
3	Tuzak anahtar	Sahte bir 'sifreler' Excel dosyası koy; açan olursa haberin olsun.

BU HAFTA

- Ortak klasörde 'şifre' geçen dosyaları ara; düz metin şifreleri bir şifre yöneticisine taşı.
- Kendi geliştirdiğin bir araç varsa deposunu TruffleHog ile tara.
- Canarytokens'tan Excel tuzağı oluştur, gerçek dosyaların yanına koy.
- Beyanname takvimi yoğunken site çökerse fark etmek için Better Stack'te ücretsiz bir uptime izleyicisi aç.

> e-Beyanname, GİB ve SGK şifrelerini hiçbir yapay zekâ aracına, sohbete ya da paylaşılan tabloya yazma. Mükellef verisi KVKK kapsamında.

06 Emlak ofisi

Ofiste değerli olan şey müşteri telefon listesi ve portföy. İletişim formu da botların sevdiği bir yer: spam, sahte talep, toplu numara denemesi.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Bot saldırısı	İlan sayfasındaki iletişim formu ilk hedef. Spam talepler gerçek müşteriyi gölgeler.
2	Veri yetkisi	Müşteri listesi ve fiyat notları yalnız ofise açık olmalı.
3	Kayıt (log)	Form çalışmayı bıraktığında ilk sen öğren, müşteri değil.

BU HAFTA

- Cloudflare ücretsiz planında Bot Fight Mode'u aç, iletişim formu adresine hız kuralı yaz.
- Müşteri tablosunda RLS kontrol sorgusunu çalıştır.
- Better Stack'te sitenin ve formun çalıştığını kontrol eden ücretsiz izleyici aç.

> Portal ilanlarına (sahibinden, Emlakjet gibi) giden bağlantı anahtarların varsa onları da kod dosyasından çıkar. Ev sahibinin ve alıcının bilgisi KVKK kapsamında; listeyi kimseyle e-tabloda paylaşma.

07 Butik otel

Otelde site gece çöker, rezervasyon formu gece spam yer. Bir de kanal yöneticisi ve ödeme bağlantılarının anahtarları var; sızarsa iş büyür.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Sızan anahtar	Kanal yöneticisi (OTA bağlantısı) ve ödeme anahtarları koda yazıldıysa önce onları temizle.
2	Bot saldırısı	Rezervasyon ve iletişim formuna gelen sahte talepler gerçek misafiri gölgeler.
3	Kayıt (log)	Site gece 3'te düşerse sabah değil, o an haberin olsun.

BU HAFTA

- Rezervasyon sitesini yapay zekâyla kurduysan deposunu TruffleHog ile tara.
- Cloudflare'de rezervasyon formu adresine hız kuralı yaz.
- Better Stack'te ana sayfa ve rezervasyon sayfası için iki ücretsiz izleyici aç, uyarıyı telefonundaki e-postaya bağla.

> Misafirin kimlik ve kart bilgisini kendi kurduğun formla toplama; ödeme sağlayıcının kendi güvenli sayfasını kullan. Kimlik bilgisi KVKK kapsamında.

08 Kafe-restoran

Online sipariş ya da QR menü sayfası en yoğun saatte çökerse siparişi kaçırırsın. Sahte sipariş de mutfağı boşuna yorar.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Bot saldırısı	Sipariş formuna art arda gelen sahte siparişler mutfağı ve kuryeyi boşa yorar.
2	Kayıt (log)	Öğle yoğunluğunda menü açılmıyorsa ilk sen bil.
3	Sızan anahtar	Sipariş sistemini ödeme ya da yemek platformu entegrasyonuna bağladıysan anahtarları koddan çıkar.

BU HAFTA

- Cloudflare'de Bot Fight Mode'u aç; sipariş adresine tek hız kuralı yaz.
- Better Stack'te QR menü adresi için ücretsiz izleyici aç.
- Sipariş formunda telefon doğrulaması ya da en az sipariş tutarı gibi basit bir fren koy.

> QR menü sadece bir PDF ya da hazır bir menü servisiyse bu katmanların çoğu sana düşmez. Sipariş ve ödeme alan bir uygulaman varsa hepsi geçerli.

09 Kurs / eğitmen

Üye girişli ders platformunda iki risk var: parasını ödemeyen birinin derse girmesi ve giriş sayfasına deneme-yanılma saldırısı.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Veri yetkisi	Ders ve video kaydı yalnız satın alan öğrenciye açılmalı; kuralı kodda değil veritabanında kur.
2	Bot saldırısı	Giriş sayfasına art arda şifre denemesi gelir; hız kuralı keser.
3	Kayıt (log)	Kim hangi derse ne zaman girdi, görebilmelisin.

BU HAFTA

- Satın almadan bir ders adresini açmayı dene. Açılıyorsa RLS politikası eksik.
- Supabase Storage'da video klasörü (bucket) herkese açık mı, kontrol et.
- Cloudflare'de giriş adresine hız kuralı yaz.

> Öğrenci listesi ve not bilgileri kişisel veri. 18 yaş altı öğrencin varsa veli bilgisini ayrıca koru ve gereğinden fazla bilgi isteme.

10 Spor salonu

Salonda üyelik, ödeme ve bazen ölçüm bilgisi aynı sistemde durur. Ölçüm ve sağlık beyanı hassas veri sayılır.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Veri yetkisi	Her üye yalnız kendi üyelik, ödeme ve ölçüm kaydını görmeli.
2	Sızan anahtar	Ödeme ve turnike/kapı sistemi anahtarları kodda durmamalı.
3	Bot saldırısı	Deneme dersi ve üye ol formu spam toplar.

BU HAFTA

- Üye panelinde adresteki numarayı değiştirip başka üyenin kaydı açılıyor mu dene.
- Deponu TruffleHog ile tara; ödeme anahtarını sunucu tarafına taşı.
- Cloudflare'de deneme dersi formuna hız kuralı yaz.

> Sağlık beyanı, kilo ve vücut ölçüsü gibi bilgileri gerekmedikçe uygulamada tutma. Tutacaksan yalnız üyenin ve eğitmenin görebileceği şekilde kur.

11 Düğün organizasyonu

Teklif formu en çok spam alan sayfa. Çiftlerin telefonu, tarihi ve bütçesi de rakibin görmek isteyeceği bilgiler.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Bot saldırısı	Teklif formuna gelen sahte talepler gerçek çifti listede aşağı iter.
2	Veri yetkisi	Çift bilgileri ve tedarikçi fiyat listesi yalnız ekibe açık olmalı.
3	Kayıt (log)	Form bozulduğunda aylarca talep kaçırmamak için.

BU HAFTA

- Cloudflare'de Bot Fight Mode'u aç, teklif formuna hız kuralı yaz.
- Teklif tablosunda RLS kontrol sorgusunu çalıştır.
- Better Stack'te teklif sayfası için ücretsiz izleyici aç.

> Tedarikçilerle çift bilgisini paylaşırken tüm listeyi değil, yalnız o işin bilgisini gönder.

12 Fotoğrafçı

Şifreli müşteri galerisi, adresi tahmin edilebiliyorsa şifresiz galeridir. /galeri/12'yi /galeri/13 yapan, başka çiftin fotoğraflarını görmemeli.

HANGİ KATMAN ÖNCE

SIRA	KATMAN	BU IŞTE NEDEN
1	Veri yetkisi	Galeri adresleri tahmin edilemez olmalı; dosyalar herkese açık klasörde durmamalı.
2	Bot saldırısı	Galeri şifresine deneme-yanılma ve toplu indirme botları gelir.
3	Tuzak anahtar	Sahte bir galeri bağlantısı koy; açılırsa birinin kurcaladığını anlarsın.

BU HAFTA

- Bir galeri adresindeki numarayı değiştirmeyi dene.
- Supabase Storage kullanıyorsan galeri klasörünü (bucket) özel yap, süreli imzalı bağlantı kullan.
- Cloudflare'de galeri giriş adresine hız kuralı yaz.

> Hazır galeri servisi (Pixieset gibi) kullanıyorsan bu katmanlar platformda; sana kalan güçlü şifre, iki adımlı doğrulama ve süreli paylaşım. Çocuk fotoğraflarını herkese açık galeride hiç tutma.

Takıldığın yer *olursa* yaz.

Bu 5 katman kapıyı kilitler, ama evi denetlemez. Hangi katmandan başlayacağına karar veremediysen ya da bir komutta takıldıysan DijiKoçum'a yaz, birlikte bakalım.

Bu rehberi Instagram'da yoruma **KALKAN** yazdığın için gönderdik. Sektörün listede yoksa DM'den yaz, en yakın sayfayı birlikte uyarlayalım.

Ücretsiz dijital *kontrol*

Sitene, Google ve yapay zekâ görünürlüğüne birlikte bakalım.

dijikocum.com/digital-checkup