AI GÜVENLİK REHBERİ · **VOL. 08 · 2026**

Hızlı çalış ama yanma.

BAĞLAYICI İZİNLERİ | SKILL DENETİMİ | .ENV KORUMASI | SINIR ÇİZME

Bağlayıcı izinlerini nasıl ayarlarsın, bir skill'i kurmadan nasıl denetlersin, API anahtarlarının sızmasını nasıl önlersin. Yapay zekâyla hızlı çalışırken yanmamak için uyguladığım kontroller.

EREN GÜL AYDIN
LECTURER & USAII CERTIFIED AI STRATEGIST

SÜRE
~12 dk

SEVİYE
Başlangıç

ÇIKTI
Güvenli Kurulum

YÖNTEM
İzin + Prompt



Güçlü olan araç, dikkatsizken zarar verir.

Eren Gül Aydın, Marketing To Do List ve peaker.ai kurucusu, İÜ-Cerrahpaşa'da dijital pazarlama dersi veriyor. Bu rehber, yapay zekâ araçlarını bağlarken ve kurarken uyguladığı güvenlik kontrollerini bir araya getiriyor.

Yapay zekâ güçlü. Bu da dikkatli olmazsan zarar verebileceği anlamına geliyor. Buradaki kontroller, bir araç bağlamadan önce sınırları çizmen ve sonradan kural öğrenmek zorunda kalmaman için.

- → **Nereden başlamalı?**
  Bağlayıcı izinlerinden. Herkes için geçerli, araç başına yaklaşık bir dakika sürüyor.
- → **Ne gerekiyor?**
  Bağlayıcı kullanıyorsan Claude hesabı, Claude Code ile inşa ediyorsan terminal. Kod bilgisi şart değil.
- → **Neden şimdi?**
  Bir bağlayıcı sadece okumaz; gönderir, siler, taşır. Kuralı önceden koymak, sonradan öğrenmekten iyidir.

> **Not:** Bu kontroller belirgin riskleri hızlıca yakalar ama garanti değil, ilk savunma hattıdır. Mümkün olduğunda yalnızca güvendiğin kaynakları kullan.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Bu kitapçıkta neler var?

Bağlayıcı izinlerinden skill denetimine, anahtar korumasından sınır çizmeye kadar her şey.

01 **Bağlayıcı İzinleri** — 3 seviye: izin ver, sor, engelle — s.04

02 **Gerçek Ayarlarım** — Örüntüyü gör diye kendi kurulumum — s.05

03 **Skill Denetimi** — Kurmadan önce 30 saniyelik kontrol — s.06

04 **Güvenlik Kontrolü Promptu** — Kopyala-yapıştır denetim komutu — s.07

05 **Anahtar Koruması · .env** — Şifrelerini sızdırmamanın yolu — s.08

06 **.env Ne Yapar** — Promptun perde arkası — s.09

07 **Sınır Çizme** — Araç bağlamadan önce kuralları koy — s.10

08 **Kontrol Listesi** — Her araçta uygulanacak kurallar — s.11

· **Sonuç & İletişim** — Kapanış ve iletişim bilgileri — s.12

Ön not: Bu rehber zamanla büyüyecek. Kaydet, yeni sürümlerde daha fazla kontrol eklenecek.

8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

EREN GÜL AYDIN
Lecturer & USAII Certified AI Strategist · Marketing To Do List · peaker.ai

Ya hep ya hiç değil.

Çoğu kişi Gmail veya Drive bağlar, ne devrettiğini kontrol etmez. Oysa her eylemi tek tek sen belirliyorsun.

Seviye 1 · Her Zaman İzin Ver

Claude sormaz, direkt yapar. Dosya okumak veya gelen kutusunda arama gibi güvenli günlük işler için. Burada hiçbir şey zarar veremez.

Seviye 2 · Her Seferinde Sor

Claude eylemden önce teyit eder, evet ya da hayır dersin. Değiştiren, gönderen veya paylaşan her şey için. Bir tık ekler, o tık değer.

Seviye 3 · Her Zaman Engelle

Claude o eylemi asla yapamaz. Dosya silmek veya para harcamak gibi bir AI'ın kendi başına dokunmasını istemediğin şeyler için.

Not: Bunu bir aracı bağladığın anda yap, Claude çalışmaya başlamadan önce. Yeni bir bağlayıcı, neye dokunabileceğini söylemeden aktif olmamalı.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Güvenli yarısı serbest, geri alınamaz yarısı bende.

Örüntüyü gör diye kendi ayarlarımı paylaşıyorum. Mantık basit: okumak serbest, geri alınamayan iş kontrol altında.

EYLEM	AYAR	NEDEN
Google Drive'ı oku	Her zaman izin ver	Okumak hiçbir şeyi değiştirmez
Dosyaları sil	Her zaman engelle	Bir AI'ın işimi tek başına silmesine gerek yok
E-posta taslağı hazırla	Her zaman izin ver	Taslak, sen bakana kadar öylece durur
E-posta gönder	Her seferinde sor	Gönderme, geri alamayacağın kısım

1. **Bağlayıcı ayarlarını aç**
   Claude'da ayarlamak istediğin belirli bağlayıcıya gir (Gmail, Google Drive vb.).

2. **Her izni tek tek ayarla**
   Her eylemi Her Zaman İzin Ver, Her Seferinde Sor veya Her Zaman Engelle olarak işaretle.

3. **Emin değilsen sınır sor**
   Yepyeni bir araçsa kuralı bilmiyorsan, s.10'daki sınır çizme promptunu kullan.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Skill kurmak, yabancının kodunu çalıştırmaktır.

İndirilen bir skill, bilgisayarında çalışan scriptler içerebilir. Güvenlik araştırmacıları bunu bilinmeyen bir dosyayı açmaya benzetiyor. İşte 30 saniyelik kontrolüm.

1 **Önce düz bir sohbette oku**

Skill'in kodunu Claude Code'a değil, normal bir Claude sohbetine yapıştır. O pencere bilgisayarında hiçbir şey çalıştıramaz, inceleme için güvenli.

2 **Ancak temizse içeri al**

Temiz çıktıktan sonra Claude Code'a getir, çalışma tarzına uyarlat, sonra skill olarak kaydet.

DÜRÜST NOT

Bu, belirgin kırmızı bayrakları hızlıca yakalar ama garanti değil, ilk savunma hattıdır. Mümkün olduğunda yalnızca gerçekten güvendiğin kaynaklardan skill kullan.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Kurmadan önce bunu çalıştır.

Bir skill'i normal Claude sohbetine yapıştır, sonra bu promptu ekle. Kod bilmesen de sonucu okuyabilirsin.

GÜVENLİK KONTROLÜ · KOPYALA

```
Bunu bir skill olarak kurmak üzereyim ama tam
güvenmediğim bir kaynaktan aldım. Kurmadan önce
içindeki her dosyayı ve satırı, SKILL.md dosyasını
ve tüm scriptleri tara, herhangi bir şeyin güvensiz
görünüp görünmediğini açık bir dille söyle.

Şunları işaretle:
· Dosyalarıma erişmeye çalışan
· Veriyi bir yere göndermeye çalışan
· Gizli komut çalıştıran
· Şifre veya API anahtarı almaya çalışan
· Skill'in iddia ettiğiyle uyuşmayan her şey

Temizse söyle. Sorun varsa tam satırı alıntıla
ve nedenini açıkla.
```

> **Not:** Normal sohbet penceresi dosyalarına dokunamaz ve kod çalıştıramaz. Denetimi burada yapman tam da bu yüzden güvenli.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Tek hata, tüm internete sızar.

Geçen yıl GitHub'da 29 milyon gizli anahtar sızdı; saldırganlar açığa çıkan anahtarı yaklaşık beş dakikada yakalıyor. Çözüm .env adında küçük bir dosya: anahtarların için ayrı bir not defteri.

.ENV KUR (TAM TARAMA) · KOPYALA

```
Bu proje için .env dosyasını doğru kur ve test et.
Önce tüm kod tabanımı düz metin gizli bilgi için
tara: API anahtarları, tokenler, şifreler, veritabanı
URL'leri, bağlantı dizeleri, webhook gizli anahtarları.

Bulduğun her biri için:
· .env dosyası oluştur, gizli bilgiyi AD=değer taşı
· Koddaki sabit değeri ortam değişkenine referansla
  değiştir, her şey aynı çalışsın
· İsimleri olan ama değerleri boş bir .env.example üret
· .env dosyasının .gitignore'da olduğundan emin ol
· Git geçmişimi kontrol et, daha önce commit edildiyse
  hangisi hangi dosyada söyle ve değiştirmemi hatırlat

Kalıcı kural: bundan sonra her yeni anahtarı otomatik
.env'e taşı, koda sabit kodlama, hiçbirini commit etme.
Bitince uygulamanın çalıştığını doğrula ve kısa özet ver.
```

Not: Anahtarı tek tek değil, tek seferde tam tarayıp alışkanlığı yerleştiriyor; böylece sonradan hiçbir şey kaçmıyor.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Perde arkasında olan şey.

Tüm projeni tarar

Sadece düşündüğün tek anahtarı değil, kodunda saklanan her gizli bilgiyi bulur: anahtarlar, tokenler, şifreler, veritabanı URL'leri.

Her birini .env'e taşır

Her gizli bilgiyi satır başına bir AD=değer olarak tutan düz dosya. Kodun her anahtarı ismiyle çağırır, her şey çalışmaya devam eder.

.env'i .gitignore'a ekler

Seni gerçekten koruyan kısım bu. Git'e o dosyayı asla hiçbir yere yüklememesini söyler.

Bir .env.example oluşturur

İsimlerin olduğu ama gerçek değerlerin olmadığı güvenli kopya. Hiçbir şey sızdırmadan projeni paylaşabilir veya push edebilirsin.

Tek pürüz: Bir anahtar zaten GitHub'a push edildiyse .env onu geri sızdırmaz. Prompt git geçmişini işaretler ama o servise gidip anahtarı kendin değiştirmen gerekir.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Bağlamadan önce sınırı çiz.

Bir araç bağlamak okuma değil, eylem izni verir: gönderme, silme, paylaşma. Zor kısım yepyeni bir araç, çünkü sınırın ne olması gerektiğini genelde bilmezsin. Bu prompt onu çözer.

SINIRLARI OLUŞTUR · KOPYALA

```
[araç adı]'nı sana bağlamak üzereyim. Bağlamadan
önce doğru sınırları kurmama yardım et.

Önce, bağlandıktan sonra yapabileceğin her şeyi
anlat: özellikle gönderen, silen, paylaşan,
düzenleyen veya para harcayan her şeyi, gerçek
riskleri anlayayım.

Sonra bu araçla neyi yapıp yapamayacağın konusunda,
her zaman en güvenli seçeneği tercih eden katı
kurallar öner (gönderme yerine taslak, asla silme).

Ayrıca bu araç e-posta veya paylaşılan belge gibi
başkalarından gelen gizli talimat taşıyabilir mi,
beni uyar; benim istemediğim eylemleri yaptırmaya
çalışabilecek talimatlar.

Son sınırları kaydedebileceğim net bir liste ver.
```

> **Benim kuralım:** E-postam için basit — sadece taslak hazırlayabilir, asla gerçekten gönderemez, hiçbir şeyi asla silemez.

● 8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

Bu maddeleri her araçta uygula.

- **İzinleri bağladığın anda ayarla.**
  Claude çalışmaya başlamadan önce her eylemi izin ver, sor veya engelle olarak işaretle.
- **Geri alınamaz eylemleri kilitle.**
  Silme ve para harcama her zaman engelle; gönderme her seferinde sor.
- **Skill'i önce düz sohbette oku.**
  Kod çalıştıramayan pencerede denetle, ancak temizse Claude Code'a taşı.
- **Yalnızca güvendiğin kaynağı kur.**
  Denetim ilk savunma hattıdır, garanti değil. Şüpheliyse kurma.
- **Anahtarları .env'e taşı.**
  Hiçbir gizli bilgiyi koda sabit kodlama, hiçbirini commit etme.
- **.env'i .gitignore'a ekle.**
  Paylaşım için .env.example kullan, gerçek değerleri asla push etme.
- **Sızmış anahtarı serviste değiştir.**
  .env geçmişi geri sızdırmaz; bir kez açığa çıktıysa anahtarı kaynağında yenile.
- **Gizli talimata karşı uyarı iste.**
  Araç başkalarından gelen belge okuyorsa, istemediğin eylemleri tetikleyebilir; sınırı önceden koy.

8-9 AĞUSTOS · CANLI ONLINE EĞİTİM

Claude Level Up

Claude'u tüm yönleriyle tanımak ve sistemli kullanmak için eğitime katıl. Kayıt için son günler, sınırlı kontenjan, acele et.

KAYIT VE DETAY → peaker.ai

SONUÇ

Kuralı önceden koy, sonradan öğrenmek zorunda kalma.



EREN GÜL AYDIN

LECTURER & USAII CERTIFIED AI STRATEGIST

Kurucu | Marketing To Do List & peaker.ai

✉ erengul.aydin@marketingtodolist.com

✉ ea@peaker.ai

◧ @erengul_ile_yapayzeka

⬡ erengulyz.beehiiv.com