AI Latency Exploit — SWOT Analizi

1. Strengths (Güçlü Yönler)

Bu proje, yapay zekâ destekli faturalandırma sistemlerinde karar verme gecikmelerinin (latency) güvenlik zafiyetine dönüşebileceğini gösteren öncü bir çalışmadır. Literatürde çoğu çalışma veri doğrulama veya kimlik doğrulama süreçlerine odaklanırken, bu proje sistemin **zamanlama katmanındaki savunmasızlıkları** incelemektedir.
Yapay zekâ modülünün inferans süresinin gecikmesi, saldırganın geçerli OCPP mesajlarını milisaniye bazında planlayarak tespit mekanizmasını atlatabilmesine yol açmaktadır.
Bu yönüyle çalışma, hem **mantıksal hem de zaman temelli anomali tespiti** alanına katkı sağlar.

Ayrıca projenin güçlü yönlerinden biri, yalnızca teorik bir güvenlik açığını tanımlamakla kalmayıp, bunu **Python tabanlı bir simülasyon ortamı** ile doğrulamasıdır. asyncio yapısını kullanan bu simülasyon, hem saldırı hem de savunma senaryolarını aynı model üzerinden test etmeye imkân tanır. Bu sayede proje, yazılım mühendisliği açısından da **tekrarlanabilir, gözlemlenebilir ve ölçülebilir** bir deney ortamı sunar.

Son olarak, proje yalnızca OCPP protokolü özelinde değil, gecikmeye duyarlı tüm yapay zekâ tabanlı sistemler için (örneğin finansal karar sistemleri, IoT ağları, otonom araç kontrol yazılımları) **genel bir güvenlik farkındalığı** oluşturur. Bu yönüyle hem akademik hem de sektörel anlamda özgün, yenilikçi ve uygulanabilir bir örnektir.

2. Weaknesses (Zayıf Yönler)

Her ne kadar proje teknik olarak güçlü bir simülasyon modeli sunsa da, deney ortamı **gerçek dünyadaki değişkenleri** tam olarak temsil etmemektedir. Elektrikli araç şarj altyapılarında gecikmeler yalnızca yazılımdan değil; ağ yoğunluğu, donanım kapasitesi, güç elektroniği bileşenleri ve üçüncü taraf iletişim gecikmeleri gibi faktörlerden de etkilenir. Bu nedenle, projede tanımlanan zafiyetler gerçek sistemlerde farklı sonuçlar doğurabilir.

Diğer bir zayıf yön, kullanılan yapay zekâ modelinin **gerçek bir öğrenme algoritması** içermemesidir. Bu projede yapay zekâ yalnızca gecikmeyi (latency) taklit eden bir fonksiyonla temsil edilmiştir. Bu da projenin “AI” kısmını daha çok simülasyon

düzeyinde bırakır; gerçek zamanlı model davranışlarının (ör. TensorFlow veya PyTorch tabanlı) etkisi incelenmemiştir.

Ayrıca, sistemin saldırı ve savunma senaryoları tek bir cihaz üzerinden yürütülmüştür. Gerçek bir dağıtık mimaride (birden fazla şarj noktası veya sunucu) eşzamanlı işlem yükü çok daha karmaşık olabilir. Bu durum, önerilen savunma stratejilerinin ölçeklenebilirliğini sınırlayabilir.

Son olarak, saldırı senaryosunun etik sınırları tam olarak belirtilmemiştir. AI tabanlı güvenlik sistemlerine yönelik bu tür deneyler, dikkatli bir etik çerçeve içinde yapılmadığında yanlış anlaşılma riski taşır.

3. Opportunities (Fırsatlar)

Bu proje, yapay zekâ ve siber güvenliği birleştiren **yeni nesil güvenlik araştırmaları** arasında yer almaktadır. O yüzden birçok akademik, kurumsal ve endüstriyel fırsat barındırır. Öncelikle, bu çalışma **akademik yayın**, **bitirme projesi**, **TÜBİTAK 2209-A** veya **TEKNOFEST** gibi yarışmalarda özgün bir araştırma projesi olarak sunulabilir. Özellikle "AI güvenliği" veya "kritik altyapılarda zafiyet analizi" temalı etkinliklerde dikkat çekici bir örnek teşkil eder.

Ayrıca proje, yapay zekâ sistemlerinde "güvenilirlik ve zaman yönetimi" konularında çalışan araştırmacılar için **referans bir senaryo** oluşturabilir. Endüstri tarafında ise elektrikli araç üreticileri, enerji yönetim şirketleri veya siber güvenlik firmaları bu tür zafiyetleri analiz eden yaklaşımları kendi ürünlerinde değerlendirebilir.

Bir diğer fırsat da projenin **genişletilebilirliği**dir. Simülasyon ortamı geliştirildiğinde, farklı protokoller (örneğin MQTT, HTTP REST API) üzerinde aynı mantığın denenmesi mümkündür. Böylece bu çalışma yalnızca OCPP protokolüyle sınırlı kalmaz, IoT güvenliği veya akıllı şehir altyapıları gibi daha geniş alanlara da uygulanabilir.

4. Threats (Tehditler)

Projenin en belirgin tehditlerinden biri, **etik ve hukuki sınırların** hassas olmasıdır. "AI Latency Exploit" kavramı, kötü niyetli kişilerce yanlış anlaşılır veya kötüye kullanılırsa, gerçek sistemlerde zarar oluşturabilir. Bu nedenle çalışmanın açık kaynak olarak paylaşımı veya sunumu sırasında etik kuralların net biçimde belirtilmesi gereklidir.

Bunun yanı sıra, yapay zekâ sistemlerinin sürekli gelişmesi projenin **geçerlilik süresini** etkileyebilir. AI modülleri hızlandıkça (örneğin GPU destekli inferans motorlarıyla) bu zafiyetin etkisi azalabilir. Dolayısıyla proje, uzun vadede "geçici bir zafiyet" kategorisine düşme riski taşır.

Ayrıca, benzer araştırmaların artmasıyla rekabetin yükselmesi, projenin özgünlük değerini azaltabilir. Özellikle büyük güvenlik firmaları bu tür analizleri kendi sistemlerine entegre ettikçe, "AI latency exploit" kavramı yaygınlaşabilir. Bu durumda projenin yenilik etkisi azalır.

Son olarak, kamu veya özel sektör kurumlarının bu tür analizleri **riskli veya saldırı odaklı** görmesi, proje paylaşımını sınırlayabilir. Gerçek şarj altyapılarında test yapılması, regülasyonlar ve veri güvenliği yasaları gereği izin gerektirebilir. Bu durum, projenin saha testlerine taşınmasını zorlaştırabilir.