2025 Yılında Web Uygulama Güvenliğindeki En Son ve En Etkili 10 Teknik ve Trend Raporu

Yönetici Özeti

Bu rapor, 2025 yılı için web uygulama güvenliği alanındaki en etkili on tekniği ve trendi kapsamlı bir şekilde incelemektedir. Modern web uygulamalarının artan karmaşıklığı, yapay zeka destekli tehditlerin yükselişi ve düzenleyici baskıların artması, kuruluşların güvenlik stratejilerini yeniden değerlendirmesini zorunlu kılmaktadır. Raporda ele alınan trendler, yapay zeka destekli tehdit tespitinden gelişmiş yazılım tedarik zinciri güvenliğine, API güvenliğine odaklanmadan Sıfır Güven mimarisinin yaygınlaşmasına, DevSecOps entegrasyonundan konteyner güvenliğine, kullanıcı ve varlık davranış analizinden yapay zekaya özgü güvenliğe, kapsamlı saldırı yüzeyi yönetiminden insan dışı kimliklerin güvenliğine kadar geniş bir yelpazeyi kapsamaktadır. Bu eğilimler, web uygulamalarını korumak için proaktif, yapay zeka odaklı ve entegre güvenlik yaklaşımlarının vazgeçilmez olduğunu ortaya koymaktadır.

Giriş: 2025 Yılında Web Uygulama Güvenliğinin Gelişen Manzarası

2025 yılına gelindiğinde, dijital ortam, kötü niyetli aktörler için birincil hedef haline gelen giderek karmaşıklaşan web uygulamalarıyla karakterize edilmektedir. Bu uygulamalar artık tek parça yapılar olmaktan çıkmış, üçüncü taraf ve açık kaynak kütüphaneleri, konteynerler, mikro hizmetler ve hızla artan sayıda API ile iç içe geçerek saldırı yüzeylerini önemli ölçüde büyütmüş ve daha karmaşık hale getirmiştir.[1] Uygulamalarda ve uygulama geliştirmede yapay zekanın patlaması, mevcut eğilimleri daha da kötüleştirmekte ve yeni endişeler yaratmaktadır; işletmelerin %33'ü halihazırda üretim uygulamalarında üretken yapay zeka kullanmaktadır.[1] Bu durum, güvenlik ekipleri için daha önce hiç olmadığı kadar karmaşık bir ortam yaratmaktadır.

Finansal riskler de çarpıcı bir şekilde artmaktadır. IBM'in 2024 Veri İhlali Maliyeti Raporu'na göre, bir veri ihlalinin ortalama maliyeti 2023'teki 4,35 milyon dolardan 2024'te 4,88 milyon dolara yükselmiştir.[4] Bu yükselen maliyet, işletmeler üzerinde web uygulamalarını etkili bir şekilde güvence altına alma konusunda muazzam bir baskı oluşturmaktadır. Saldırganlar giderek daha sofistike hale gelmekte, yapay zekayı kullanarak son derece hedefli oltalama e-postaları hazırlamakta ve hatta kişisel kimlikleri klonlamaktadır; bu da geleneksel güvenlik önlemlerinin etkinliğini azaltmaktadır.[5] Bu durum, tehditleri ortaya çıkmadan önce tahmin edebilen ve azaltabilen gelişmiş, proaktif ve entegre güvenlik stratejilerine geçişi zorunlu kılmaktadır.[3] Uygulama mimarilerinin artan karmaşıklığı, her bir yeni bileşenin veya mimari tarzın (mikro hizmetler veya sunucusuz gibi) kendi güvenlik açıklarını ve

entegrasyon zorluklarını beraberinde getirmesiyle, genel saldırı yüzeyini ve güvenliği sağlamanın zorluğunu katlayarak artırmaktadır. Bu, geleneksel, çevre odaklı güvenlik modellerinin yetersiz kaldığı anlamına gelmektedir; güvenlik araçları, son derece dağıtılmış, birbirine bağlı ve dinamik ortamları anlayacak ve güvence altına alacak şekilde gelişmelidir.

2025 Yılında Web Uygulama Güvenliğindeki En Son ve En Etkili 10 Teknik ve Trend

Bu bölüm, 2025 yılında web uygulama güvenliğinde en kritik olması beklenen teknikleri ve trendleri detaylandırmakta, bunların doğası, işleyişi, önemi, potansiyel etkileri ve ilgili kaynakları hakkında derinlemesine bilgi sunmaktadır.

Tablo 1: 2025 Yılında Web Uygulama Güvenliğindeki En İyi 10 Trende Genel Bakış

Trend Başlığı	Kısa Açıklama	Temel Uygulama Alanı	Birincil Kaynak
1. Yapay Zeka Destekli Tehdit Tespiti ve Otomatik Yanıt	Yapay zeka ve makine öğrenimi ile gerçek zamanlı veri analizi, anomali tespiti ve otomatik tehdit yanıtı.	Tüm web uygulamaları, API'ler, konteynerler, güvenlik operasyonları.	Forrester, Savvycom Software, Qwiet.ai, SentinelOne
2. Gelişmiş Yazılım Tedarik Zinciri Güvenliği	Üçüncü taraf bileşenler ve açık kaynak kodlarından kaynaklanan güvenlik açıklarına karşı tüm yazılım yaşam döngüsünün güvence altına alınması.	Yazılım geliştirme, CI/CD, konteynerleştirilmiş uygulamalar.	Forrester, Savvycom Software, Qwiet.ai, AccuKnox
3. Birincil Saldırı Yüzeyi Olarak API Güvenliği	Modern web uygulamalarının bel kemiği olan API'lerin kimlik doğrulama, yetkilendirme, giriş doğrulama ve gerçek zamanlı izleme ile korunması.	Mikro hizmet mimarileri, mobil uygulamalar, üçüncü taraf entegrasyonları.	Savvycom Software, API7.ai, SecureMyOrg, Qwiet.ai
4. Yaygın Sıfır Güven	"Asla güvenme, her	Ağ güvenliği,	Qwiet.ai,

Mimarisi Benimsenmesi	zaman doğrula" ilkesiyle her kullanıcı, cihaz ve uygulamanın varsayılan olarak güvenilmez kabul edilmesi.	uygulama katmanı, bulut ve SaaS ortamları.	SecureMyOrg, Cyber Defense Magazine, AccuKnox
5. Sürekli Güvenlik için DevSecOps Entegrasyonu	Güvenlik uygulamalarının yazılım geliştirme yaşam döngüsünün her aşamasına entegre edilmesi.	Yazılım geliştirme, CI/CD, otomasyon, bulut yerel uygulamalar.	Savvycom Software, Qwiet.ai, AccuKnox, Wisp.blog
6. Gelişmiş Konteyner Güvenliği ve Çalışma Zamanı Koruması	Konteynerleştirilmiş ortamların güvenlik açıklarına, sır yönetimine ve çalışma zamanı tehditlerine karşı korunması.	Bulut yerel altyapılar, mikro hizmetler, Kubernetes.	AccuKnox, Wisp.blog, Savvycom
7. Kullanıcı ve Varlık Davranış Analizi (UEBA)	Makine öğrenimi kullanarak kullanıcı ve varlık davranışlarını izleme ve anormallikleri tespit etme.	İç tehdit tespiti, hesap ele geçirme, APT tespiti.	Teramind, Okta
8. Yapay Zekaya Özgü Güvenlik (örn. LLM Güvenliği)	Yapay zeka ve Büyük Dil Modeli (LLM) sistemlerinin kendilerine özgü güvenlik açıklarına karşı korunması.	Yapay zeka destekli web uygulamaları, sohbet robotları, karar destek sistemleri.	Forrester, HiddenLayer, OWASP Top 10 for LLM
9. Kapsamlı Saldırı Yüzeyi Yönetimi (ASM)	Kuruluşun tüm dijital ayak izi üzerinde gerçek zamanlı görünürlük ve kontrol sağlanması.	Bulut yerel mimariler, mikro hizmetler, sunucusuz teknolojiler, gölge BT.	Qwiet.ai, Forrester
10. İnsan Dışı Kimlikler (NHI)	API anahtarları, tokenlar, hizmet	Otomasyon, CI/CD, bulut dağıtımları,	OWASP Non-Human Identities Top 10

Güvenliğine Odaklanma	hesapları gibi insan dışı varlıkların kimliklerinin güvence altına alınması.	mikro hizmetler arası iletişim.	

---

1. Yapay Zeka Destekli Tehdit Tespiti ve Otomatik Yanıt

Nedir ve Nasıl Çalışır: Yapay zeka (YZ) ve Makine Öğrenimi (ML), siber güvenliği dönüştürmekte, araçların büyük miktardaki veriyi gerçek zamanlı olarak analiz etmesini, kullanıcı davranışındaki, trafik modellerindeki ve uygulama kullanımındaki anormallikleri tespit etmesini sağlamaktadır.[3] Geleneksel imza tabanlı yöntemlerin aksine, YZ sistemleri, yerleşik taban çizgilerinden sapmaları tespit ederek sıfır gün veya gizli saldırılar da dahil olmak üzere ortaya çıkan tehditleri tahmin etmeyi ve belirlemeyi öğrenir.[6] Bu, günlük verilerini analiz etme ve ağ etkinliğini izleme gibi tekrarlayan ve zaman alıcı görevleri otomatikleştirerek güvenlik ekiplerinin daha değerli görevlere odaklanmasına olanak tanır.[3]

2025 İçin Neden Önemli: Siber saldırılar giderek daha sofistike hale geldikçe ve YZ destekli saldırılar insan analistlerin takip edebileceği hızdan daha hızlı değiştikçe, YZ destekli savunmalar hızlı tespit ve yanıt için vazgeçilmez hale gelmektedir.[4] Bu sistemler, olayları tespit etme (MTTD) ve yanıtlama (MTTR) ortalama süresini önemli ölçüde düşürerek ihlallerin etkisini azaltır.[6] Ayrıca, YZ, geleneksel olarak önemli manuel çaba gerektiren süreçleri kolaylaştırarak yönetişim, risk ve uyumluluk (GRC) süreçlerinde de kritik bir rol oynamaktadır.[3] YZ sistemleri, kalıplardan ve olaylardan öğrenerek olası saldırıları tahmin etme ve daha hızlı yanıt verme yeteneği, kuruluşların reaktif güvenlikten proaktif bir duruşa geçişini sağlayan temel mekanizmadır. Bu, araçların yalnızca bilinen güvenlik açıklarını bulmanın ötesine geçerek, yeni saldırı vektörlerini veya sıfır gün açıklarını gösteren davranışsal anormallikleri belirlemesi gerektiği anlamına gelir.

Potansiyel Etkileri ve Uygulama Alanları: YZ, karmaşık saldırı modellerini belirleyerek güvenlik açığı taramasını geliştirecek, web uygulama trafiğini şüpheli etkinlikler için gerçek zamanlı olarak izleyecek ve kötü niyetli IP'leri engelleme veya şüpheli trafiği kısıtlama gibi olay yanıtı eylemlerini otomatikleştirecektir.[9] API'leri [9] ve konteynerleştirilmiş ortamları anomali tespiti için güvence altına almada kritik olacaktır.[7] Siber güvenlik yetenek açığının devam etmesiyle birlikte, YZ'nin güvenlik araçlarına entegrasyonu, insan yeteneklerini artırarak ve rutin görevleri otomatikleştirerek bu açığı kapatmaya yardımcı olacaktır.[3] Bu, YZ destekli otomasyonu içeren güvenlik araçlarının, yetenek kıtlığı çeken kuruluşlar için önemli bir pazar

farklılaştırıcısı olabileceğini göstermektedir.

Ana Kaynak/Referans: Forrester'ın "Uygulama Güvenliğinin Durumu, 2025" [1], Savvycom Software'ın "Web Uygulama Güvenliği Kapsamlı Rehberi 2025" [4], Qwiet.ai'nin "Siber Güvenliği Şekillendiren En İyi 10 Uygulama Güvenliği Trendi 2025" [3], SentinelOne'ın "2025 İçin YZ Siber Güvenlik Şirketleri".[6]

---

2. Gelişmiş Yazılım Tedarik Zinciri Güvenliği

Nedir ve Nasıl Çalışır: Bu trend, özellikle üçüncü taraf kütüphaneler, açık kaynak bileşenleri ve satıcı kodu aracılığıyla ortaya çıkan güvenlik açıklarına karşı tüm yazılım geliştirme ve dağıtım hattını güvence altına almaya odaklanmaktadır.[1] Kapsamlı kod denetimleri, bağımlılıkların sürekli izlenmesi ve bileşenlerdeki güvenlik açıklarını izlemek ve belirlemek için Yazılım Bileşimi Analizi (SCA) ve Yazılım Malzeme Listeleri (SBOM'ler) gibi araçların kullanılmasını içerir.[3]

2025 İçin Neden Önemli: Yazılım tedarik zinciri, saldırganların kötü niyetli kodları büyük ölçekte enjekte etmek için bu zayıf halkayı hedef almasıyla küresel bir endişe kaynağıdır.[1] SolarWinds ve Log4j gibi yüksek profilli olaylar, bu tür saldırıların yıkıcı etkisini vurgulamıştır.[3] Hükümet düzenleyicileri daha fazla şeffaflık talep etmektedir; AB'nin Aralık 2024'te yürürlüğe giren Siber Dayanıklılık Yasası, AB'de satılan dijital ürünler için SBOM'ler gerektirmekte ve ABD federal kurumları da bunları talep edebilmektedir.[1] Bu, uyumluluğun artık ikincil bir husus değil, sağlam tedarik zinciri güvenlik önlemlerinin uygulanması için doğrudan, müzakere edilemez bir itici güç olduğu anlamına gelmektedir.

Potansiyel Etkileri ve Uygulama Alanları: Kuruluşlar, üçüncü taraf kütüphaneleri izlemek ve güvenlik açıklarını belirlemek için SCA araçlarının kullanımını yoğunlaştıracak, satıcı kodlarının düzenli denetimlerini yapacak ve tedarik zinciri riskleri için sürekli izleme uygulayacaktır.[4] Bağımlılıklara görünürlük kazanmak ve iyileştirmeyi önceliklendirmek için YZ destekli SBOM'lerin oluşturulması ve kullanılması standart bir uygulama haline gelecektir.[3] Konteyner güvenliği ile tedarik zinciri güvenliği arasında güçlü bir bağlantı bulunmaktadır; konteynerler, görüntülerin ve bağımlılıkların katmanlarından inşa edildiği için, tedarik zinciri saldırılarına doğal olarak açıktır.[12] Bu, konteynerleri güvence altına almanın, temel tedarik zincirini güvence altına almayı gerektirdiğini göstermektedir.

Ana Kaynak/Referans: Forrester'ın "Uygulama Güvenliğinin Durumu, 2025" [1], Savvycom Software'ın "Web Uygulama Güvenliği Kapsamlı Rehberi 2025" [4], Qwiet.ai'nin "Siber Güvenliği Şekillendiren En İyi 10 Uygulama Güvenliği Trendi 2025" [3],

AccuKnox'un "Konteyner Güvenliği".[12]

---

3. Birincil Saldırı Yüzeyi Olarak API Güvenliği

Nedir ve Nasıl Çalışır: Bu trend, modern web uygulamalarının ve mikro hizmet mimarilerinin bel kemiği olan Uygulama Programlama Arayüzlerini (API'ler) güvence altına almak için özel stratejilere ve araçlara odaklanmaktadır.[3] OAuth 2.0 ve JWT gibi sağlam kimlik doğrulama, RBAC/ABAC gibi ince taneli yetkilendirme, sıkı giriş doğrulama ve sanitizasyon, hız sınırlama ve anormal davranışlar için sürekli izleme gibi uygulamaları içerir.[10] Yapay zeka ve makine öğrenimi, gerçek zamanlı tehditleri tespit etmek için API ağ geçitlerine ve güvenlik araçlarına giderek daha fazla entegre edilmektedir.[9]

2025 İçin Neden Önemli: API trafiği, geleneksel web trafiğini geride bırakarak API'leri siber saldırılar için en sık giriş noktası haline getirmiştir.[10] API'ler hassas verileri ve işlevselliği açığa çıkarır ve Kırık Nesne Düzeyi Yetkilendirme (BOLA), Kırık Fonksiyon Düzeyi Yetkilendirme (BFLA) ve çeşitli enjeksiyon saldırıları gibi yaygın güvenlik açıkları sıklıkla istismar edilmektedir.[4] 2025'teki T-Mobile ihlali, saldırganların savunmasız API uç noktalarını kullanarak müşteri hesap bilgilerine eriştiği bir örnek olarak bu riskleri acı bir şekilde hatırlatmaktadır.[4] Mikro hizmetlerin hızlı geliştirilmesi ve benimsenmesi, API yayılmasına yol açarak yönetilmeyen ve genellikle bilinmeyen bir saldırı yüzeyi oluşturmaktadır.[10]

Potansiyel Etkileri ve Uygulama Alanları: Kuruluşlar, keşif, test, izleme ve tehdit tespitini birleştiren birleşik API yönetim platformlarını giderek daha fazla benimseyecektir.[10] "API'ler için Sıfır Güven" modeli, sürekli doğrulama ve en az ayrıcalıklı erişim uygulayarak yaygınlaşacaktır.[10] API güvenliği, OpenAPI gibi araçlar kullanılarak şema doğrulama ve sözleşme testi için DevOps boru hatlarına "Kod Olarak" gömülecektir.[10] Klasik enjeksiyon saldırıları hala bir tehdit olsa da, API'ye özgü mantık kusurları (BOLA, BFLA gibi) birincil endişe kaynağı haline gelmektedir. Bu, web uygulamaları için tehdit ortamında niteliksel bir değişimi temsil etmektedir.

Ana Kaynak/Referans: Savvycom Software'ın "Web Uygulama Güvenliği Kapsamlı Rehberi 2025" [4], API7.ai'nin "2025'teki En İyi 8 API Yönetimi Trendi" [9], SecureMyOrg'un "2025'te API Güvenliğinin Durumu" [10], Qwiet.ai'nin "Siber Güvenliği Şekillendiren En İyi 10 Uygulama Güvenliği Trendi 2025".[3]

---

4. Yaygın Sıfır Güven Mimarisi Benimsenmesi

Nedir ve Nasıl Çalışır: "Asla güvenme, her zaman doğrula" ilkesiyle çalışan Sıfır Güven modeli, konumlarından bağımsız olarak her kullanıcıyı, cihazı ve uygulamayı varsayılan olarak güvenilmez kabul eder.[3] Her erişim noktasında sürekli doğrulama gerektiren sıkı erişim kontrolleri uygular. Uygulama katmanında bu, API'leri, hizmetleri ve verileri belirli görevler için yalnızca gerekli olanla sınırlı erişimle güvence altına almayı ve bir ihlal durumunda yanal hareketi önlemek için mikro segmentasyon kullanmayı içerir.[3]

2025 İçin Neden Önemli: Sıfır Güven, kuruluşların gelişen siber tehditleri ve genellikle şirket içi, bulut ve hibrit altyapıları harmanlayan modern BT ortamlarının artan karmaşıklığını ele alma ihtiyacını fark etmesiyle önemli bir ivme kazanmıştır.[3] Yetkisiz erişim olasılığını önemli ölçüde azaltır ve saldırganlar için birden fazla engel oluşturarak iç tehditleri azaltır ve ihlalleri kontrol altında tutar.[3] Uygulamalar daha dağıtık hale geldikçe (mikro hizmetler, bulut yerel, sunucusuz), geleneksel ağ çevresi ortadan kalkmaktadır. Sıfır Güven, kimlik ve erişime her etkileşim noktasında odaklanarak bu son derece dağıtılmış ortamları güvence altına almak için gerekli felsefi ve mimari çerçeveyi sağlar.

Potansiyel Etkileri ve Uygulama Alanları: Sıfır Güven ilkeleri, bulut ve SaaS ortamları da dahil olmak üzere tüm BT ortamlarında kapsamlı bir şekilde genişletilecek, kullanıcı kimliklerinin ve erişim ayrıcalıklarının sürekli izlenmesi ve doğrulanması sağlanacaktır.[5] API ağ geçitleri, kullanıcı kimliğinin sürekli doğrulanmasını, en az ayrıcalıklı erişim kontrollerini ve tüm aşamalarda şifrelemeyi uygulayacaktır.[10] Sıfır Güven benimseyen kuruluşların bile bulut ve SaaS ortamlarında "gizli izinler"e sahip olabileceği ve bunun saldırganlar için büyük bir fırsat olabileceği belirtilmektedir.[5] Bu, Sıfır Güven'in tek seferlik bir uygulama değil, sürekli izleme ve doğrulama gerektiren "devam eden bir yolculuk" olduğunu vurgulamaktadır.

Ana Kaynak/Referans: Qwiet.ai'nin "Siber Güvenliği Şekillendiren En İyi 10 Uygulama Güvenliği Trendi 2025" [3], SecureMyOrg'un "2025'te API Güvenliğinin Durumu" [10], Cyber Defense Magazine'in "2025 Siber Güvenlik Tahminleri" [5], AccuKnox'un "Konteyner Güvenliği".[12]

---

5. Sürekli Güvenlik için DevSecOps Entegrasyonu

Nedir ve Nasıl Çalışır: DevSecOps, güvenlik uygulamalarını yazılım geliştirme yaşam döngüsünün (SDLC) ilk kodlama ve tasarımdan dağıtım ve operasyonlara kadar her aşamasına entegre eder.[3] Bu "sola kaydırma" yaklaşımı, güvenliğin sonradan eklenen bir düşünce olmaktan çok, en başından itibaren "geliştirme sürecine dahil edilmesini" sağlar.[3] Kod taraması (SAST), dinamik analiz (DAST) ve güvenlik açığı kontrolleri gibi

güvenlik kontrollerinin doğrudan CI/CD boru hatlarına otomatik olarak dahil edilmesini içerir.[3]

2025 İçin Neden Önemli: Güvenliği erken ve sürekli olarak yerleştirmek, insan hatasını azaltır, güvenli uygulamaların teslimini hızlandırır ve güvenlik açıklarını düzeltme maliyetini önemli ölçüde düşürür.[3] Bir kusuru geliştirme aşamasında düzeltmek, dağıtımdan sonra ele almaktan çok daha kolay ve ucuzdur.[12] Ayrıca, geliştirme, operasyon ve güvenlik ekipleri arasında daha güçlü işbirliğini ve ortak sorumluluğu teşvik eder.[3] DevSecOps, sadece araç entegrasyonundan daha fazlasıdır; kuruluş kültürü ve geliştirme süreçlerinde temel bir değişimdir, ortak sorumluluğu ve erken katılımı teşvik eder.

Potansiyel Etkileri ve Uygulama Alanları: Kuruluşlar, CI/CD boru hatlarında otomatik güvenlik testlerine, tehdit modellemeye ve otomatik politika uygulamasına öncelik verecektir.[3] DevSecOps, konteynerleştirilmiş iş yükleri için süreçleri kolaylaştıracak, geliştirilmiş izleme, uyarı ve test çerçeveleri sunacaktır.[13] Güvenlik açıklarının SDLC'de ne kadar ileri giderse, düzeltme maliyetinin de o kadar arttığı göz önüne alındığında, "sola kaydırma" güvenlik yaklaşımının güçlü bir ekonomik gerekçesi bulunmaktadır.

Ana Kaynak/Referans: Savvycom Software'ın "Web Uygulama Güvenliği Kapsamlı Rehberi 2025" [4], Qwiet.ai'nin "Siber Güvenliği Şekillendiren En İyi 10 Uygulama Güvenliği Trendi 2025" [3], AccuKnox'un "Konteyner Güvenliği" [12], Wisp.blog'un "2025'te Sunucusuz Nereye Gidiyor" [13], Savvycom'un "2025'te 8 Konteyner İzleme Trendi".[7]

---

6. Gelişmiş Konteyner Güvenliği ve Çalışma Zamanı Koruması

Nedir ve Nasıl Çalışır: Bu trend, bulut yerel altyapının bel kemiği haline gelen konteynerleştirilmiş ortamları güvence altına almaya odaklanmaktadır.[12] Konteyner görüntülerinin güvenlik açığı taramasını, sağlam sır yönetimini, tehditleri tespit etmek ve engellemek için gerçek zamanlı çalışma zamanı korumasını ve otomatik politika uygulamasını kapsar.[12] Uygulamalar arasında boru hattı boyunca sürekli tarama, erişimi ve ayrıcalıkları en aza indirme (en az ayrıcalık), şüpheli davranışlar için canlı konteyner etkinliğini izleme (örneğin, olağandışı dosya erişimi, ağ bağlantıları) ve mikro segmentasyon kullanarak iş yüklerini izole etme yer alır.[12]

2025 İçin Neden Önemli: Konteyner dağıtımlarının büyük ölçeği ve dinamik doğası genellikle minimum görünürlüğe yol açarken, saldırganlar bu ortamlardaki yanlış yapılandırılmış API'leri, açıkta kalan panoları veya sızdırılmış sırları kullanmak için gelişmektedir.[12] Tehlikeye atılmış temel görüntüler aracılığıyla tedarik zinciri saldırıları da önemli bir endişe kaynağıdır.[12] Düzenleyici baskı da artmakta, standartlar açık

konteyner düzeyinde güvenlik beklemektedir.[12] Bir konteynerin tehlikeye girmesi durumunda "patlama yarıçapını" azaltmak için iş yüklerinin izolasyonu kritik bir savunma stratejisidir; bu, yalnızca önleyici tedbirlerden ziyade dayanıklılık ve sınırlamaya doğru bir kaymayı temsil eder.

Potansiyel Etkileri ve Uygulama Alanları: Gelişmiş konteyner güvenlik çözümleri, çalışma zamanı izlemesi için YZ destekli anomali tespitinden yararlanacak [7], daha iyi sır yönetimi, gelişmiş erişim kontrolleri ve iyileştirilmiş denetim yetenekleri sunacaktır.[13] KubeArmor gibi araçlar, çekirdek düzeyinde güvenlik politikalarını uygulayacak ve Sıfır Güven segmentasyonu konteynerleri otomatik olarak izole edecektir.[12] Konteyner güvenliği, Sıfır Güven ve tedarik zinciri güvenliği gibi daha geniş güvenlik felsefeleri ve tehditleriyle derinden iç içe geçmiş durumda olup, tek başına bir alan değildir.[12]

Ana Kaynak/Referans: AccuKnox'un "Konteyner Güvenliği" [12], Wisp.blog'un "2025'te Sunucusuz Nereye Gidiyor" [13], Savvycom'un "2025'te 8 Konteyner İzleme Trendi".[7]

---

7. Kullanıcı ve Varlık Davranış Analizi (UEBA)

Nedir ve Nasıl Çalışır: Kullanıcı ve Varlık Davranış Analizi (UEBA), hem insan kullanıcıların hem de insan dışı varlıkların (cihazlar ve uygulamalar gibi) ağ etkinliğini sürekli olarak izlemek ve analiz etmek için makine öğrenimini kullanır.[8] "Normal" davranışın bir temelini oluşturur ve ardından bu modellerden potansiyel güvenlik tehditlerini gösterebilecek ince sapmaları veya anormallikleri belirler.[8] UEBA sistemleri, yanlış pozitifleri azaltmak ve önemli tehditleri önceliklendirmek için zaman içinde birden fazla davranışsal sinyali ilişkilendirebilir.[8]

2025 İçin Neden Önemli: UEBA, iç tehditler, ele geçirilmiş hesaplar, kaba kuvvet saldırıları ve Gelişmiş Kalıcı Tehditler (APT'ler) gibi geleneksel imza tabanlı güvenlik araçlarının gözden kaçırabileceği sofistike ve genellikle ince tehditleri tespit etmek için kritik öneme sahiptir.[8] Olağandışı erişim modellerini, oturum açma sürelerini, veri sızdırmayı veya ağlar içindeki yanal hareketi belirleyebilir, gerçek zamanlı uyarılar sağlayabilir ve otomatik risk yanıtlarını etkinleştirebilir.[8] UEBA, bir saldırganın ilk erişimi sağladıktan *sonraki* eylemlerini tespit etmede üstündür, bu da onu güvenlik açığı tespitini önlemeye odaklanan araçları tamamlayan kritik bir güvenlik katmanı yapar.

Potansiyel Etkileri ve Uygulama Alanları: UEBA, olağandışı oturum açma modellerini işaretleyerek web uygulamalarına yönelik kimlik bilgisi doldurma ve hesap ele geçirme girişimlerinin tespitini geliştirecektir.[14] API erişimi veya veri sızdırma ile ilgili anormal davranışları belirleyebilir, ihlaller için erken uyarılar sağlayabilir.[14] Güvenlikte yaygın bir sorun olan uyarı yorgunluğunu gidermek için UEBA, birden fazla davranışsal sinyali

zaman içinde ilişkilendirerek yanlış pozitifleri azaltır ve önemli tehditleri önceliklendirmek için bağlamsal risk puanlaması uygular.[8] Bu, güvenlik uyarılarını daha eyleme geçirilebilir hale getirir.

Ana Kaynak/Referans: Teramind'in "Kullanıcı ve Varlık Davranış Analizi (UEBA) Rehberi 2025" [14], Okta'nın "UEBA (kullanıcı ve varlık davranış analizi) Nedir?".[8]

---

8. Yapay Zekaya Özgü Güvenlik (örn. LLM Güvenliği)

Nedir ve Nasıl Çalışır: Bu trend, web uygulamalarına giderek daha fazla entegre edilen Yapay Zeka (YZ) ve Büyük Dil Modeli (LLM) sistemlerinin kendilerini güvence altına almaya odaklanmaktadır.[1] Prompt enjeksiyonu (doğrudan, dolaylı, çok modlu), hassas bilgi ifşası, veri zehirlenmesi, yanlış çıktı işleme, aşırı ajans ve sistem prompt sızıntısı gibi YZ'ye özgü güvenlik açıklarını ele alır.[1] Ayrıca, YZ güvenlik açıklarını proaktif olarak belirlemek için düşmanca makine öğrenimi (ML) testlerini de içerir.[15]

2025 İçin Neden Önemli: YZ modelleri, halihazırda üretim uygulamalarında üretken YZ kullanan işletmelerin %33'ü ile saldırı yüzeyine yeni, karmaşık bir boyut katmaktadır.[1] Saldırganlar, YZ sistemlerini istismar etmek ve manipüle etmek için gelişmiş teknikler geliştirmekte, YZ özellikli uç noktaları hedef alan "YZ Destekli Siber Saldırılar" (AIPC) ile saldırıları yoğunlaştırmaktadır.[11] Derin sahte teknolojileri nedeniyle dijital içeriğe olan güvenin aşınması da önemli bir endişe kaynağıdır.[15] Bu, YZ'nin sadece bir savunma aracı olmaktan çıkıp, kendisinin de bir saldırı yüzeyi haline geldiği anlamına gelmektedir.

Potansiyel Etkileri ve Uygulama Alanları: YZ sistemlerine özel olarak uyarlanmış resmi olay yanıtı yönergeleri geliştirilecektir.[15] Kuruluşlar, YZ için güvenli geliştirme uygulamalarına, model sağlamlığına, hassas veri kümeleri için veri güvenliğine ve YZ etkileşimlerinin sürekli izlenmesine odaklanacaktır.[15] LLM'ler için OWASP Top 10 [1] kritik bir rehber görevi görecektir. Kuruluşların etik YZ çerçevelerine bağlı kalarak "YZ güvenliği yaptığını" düşünebileceği, ancak temel güvenlik açıklarının ele alınmadığı önemli bir kör nokta bulunmaktadır.[15]

Ana Kaynak/Referans: Forrester'ın "Uygulama Güvenliğinin Durumu, 2025" [1], HiddenLayer'ın "YZ Güvenliği 2025 Tahminleri ve Önerileri" [15], LLM Uygulamaları için OWASP Top 10.[1]

---

9. Kapsamlı Saldırı Yüzeyi Yönetimi (ASM)

Nedir ve Nasıl Çalışır: Kapsamlı Saldırı Yüzeyi Yönetimi, bir kuruluşun bulut yerel

mimarileri, mikro hizmetler, sunucusuz teknolojiler ve üçüncü taraf entegrasyonları dahil olmak üzere bilinen, bilinmeyen ve sahte varlıklar genelinde tüm dijital ayak izi üzerinde gerçek zamanlı görünürlük ve kontrol sağlamayı içerir.[3] Geleneksel güvenlik açığı taramasının ötesine geçerek, açıkta kalan varlıkları belirlemeyi, yanlış yapılandırmaları tespit etmeyi ve "gölge BT"yi ortaya çıkarmak da dahil olmak üzere tüm karmaşık sistemdeki güvenlik açıklarını önceliklendirmeyi hedefler.[3]

2025 İçin Neden Önemli: Uygulamalar daha dağıtık ve birbirine bağlı hale geldikçe, saldırı yüzeyi katlanarak genişlemekte, manuel yönetimi imkansız hale getirmekte ve "bilinmeyen bilinmeyenler" olasılığını artırmaktadır.[1] Saldırganlar, yanlış yapılandırmaları ve açıkta kalan varlıkları aktif olarak taramaktadır. ASM, bu karmaşıklığı yönetmek ve saldırılar için potansiyel giriş noktalarını proaktif olarak belirlemek için gerekli bütünsel görünümü sağlar. Güvenlik açığı taramasından, tüm varlıkları keşfetmeye ve bunların birbirine bağlılığını ve maruz kalma durumunu anlamaya doğru bir geçiş söz konusudur; bilinmeyen bir varlıktaki bir güvenlik açığı hala kritik bir risktir.

Potansiyel Etkileri ve Uygulama Alanları: ASM çözümleri, otomatik varlık keşfi, sürekli izleme ve bağlama ve potansiyel etkiye dayalı risklerin akıllı önceliklendirilmesi için YZ destekli yeteneklerden giderek daha fazla yararlanacaktır.[3] Bu, bir kuruluşun gerçek risk duruşunu anlama yeteneğini geliştirecektir. Sıfır Güven (doğrulamak için her "varlığı" bilmeyi gerektiren) ve DevSecOps (tüm boru hattını güvence altına almayı gerektiren) gibi diğer güvenlik yaklaşımlarının etkin bir şekilde uygulanması, saldırı yüzeyinin kapsamlı bir şekilde anlaşılmasına bağlıdır.[3]

Ana Kaynak/Referans: Qwiet.ai'nin "Siber Güvenliği Şekillendiren En İyi 10 Uygulama Güvenliği Trendi 2025" [3], Forrester'ın "Uygulama Güvenliğinin Durumu, 2025".[1]

---

10. İnsan Dışı Kimlikler (NHI) Güvenliğine Odaklanma

Nedir ve Nasıl Çalışır: Bu yeni trend, API anahtarları, tokenler, şifreleme anahtarları, sertifikalar, hizmet hesapları ve makine kimlikleri gibi insan dışı varlıkların kimliklerini güvence altına almaya odaklanmaktadır.[1] Yanlış işten çıkarma (izlenmeyen, kullanımdan kaldırılmış hizmetler), sır sızıntısı (sabit kodlu veya düz metin depolama), güvenli olmayan kimlik doğrulama, aşırı ayrıcalıklı NHI'ler, ortam izolasyonu başarısızlıkları (geliştirme/üretim ortamlarında NHI'lerin yeniden kullanılması), uygulamalar arasında NHI yeniden kullanımı ve otomatik görevler için NHI'lerin insan tarafından kötüye kullanılması gibi NHI'lere özgü riskleri ele alır.[1]

2025 İçin Neden Önemli: İnsan dışı kimlikler, modern, dağıtılmış uygulamalarda, özellikle mikro hizmetlerde ve CI/CD boru hatlarında yaygındır.[1] Bir NHI'nin tehlikeye

girmesi, genellikle insan gözetimi veya geleneksel denetim izleri olmaksızın hassas sistemlere ve verilere kalıcı ve potansiyel olarak ayrıcalıklı erişim sağlayabilir.[1] Bu OWASP İnsan Dışı Kimlikler (NHI) için Top 10, 2025 için yeni olup, kritik, genellikle ihmal edilen bir saldırı vektörünü vurgulamaktadır.[1] Yüksek düzeyde otomatikleştirilmiş, bulut yerel ortamlarda, insan dışı kimlikler kritik operasyonları gerçekleştiren "yeni kullanıcılar"dır. Bu "kullanıcılar"ın tehlikeye girmesi, insan hesabının tehlikeye girmesi kadar ciddi, hatta daha ciddi sonuçlar doğurabilir.

Potansiyel Etkileri ve Uygulama Alanları: Kuruluşlar, sağlam sır yönetimi çözümlerine öncelik verecek, NHI'ler için uygun işten çıkarma prosedürleri uygulayacak, güvenli kimlik doğrulama mekanizmalarını uygulayacak, NHI'lere en az ayrıcalık ilkesini uygulayacak, sıkı ortam izolasyonu sağlayacak ve NHI yeniden kullanımından kaçınacaktır.[1] OWASP Top 10'da "Güvenli Olmayan Bulut Dağıtım Yapılandırmaları" ve "Sır Sızıntısı"nın (genellikle API anahtarlarını içeren) en önemli NHI riskleri olarak listelenmesi, bulut yerel mimarilerin ve mikro hizmetlerin yaygın olarak benimsenmesinin NHI'lerle ilgili saldırı yüzeyini doğrudan artırdığını göstermektedir.[1]

Ana Kaynak/Referans: OWASP İnsan Dışı Kimlikler Top 10 - 2025.[1]

WebAnalyzerTool İçin Stratejik Çıkarımlar

2025 yılı için belirlenen trendler, WebAnalyzerTool için önemli fırsatlar ve zorluklar sunmaktadır. Web uygulama güvenliğinde öncü konumunu sürdürmek için aracın geliştirme yol haritası bu değişimlerle stratejik olarak uyumlu olmalıdır:

- **Tespit İçin Gelişmiş YZ/ML Entegrasyonu:**
  - **Çıkarım:** İmza tabanlı tespitin ötesine geçmek için gelişmiş YZ/ML modelleri geliştirilmelidir. Web trafiğinde, kullanıcı davranışında (potansiyel olarak UEBA benzeri içgörülerle) ve uygulama kullanım modellerindeki anormalliklerin tespitine odaklanılmalıdır. Bu, WebAnalyzerTool'un sıfır gün açıklarını ve sofistike, YZ tarafından oluşturulan saldırıları belirlemesini sağlayacaktır.[3]
  - **Eylem:** Davranış analizi için derin öğrenme araştırılmalı ve uygulanmalı, güvenlik açığı keşfi için tahmine dayalı analitik ve yeni saldırı vektörü tespiti için potansiyel olarak YZ destekli fuzzing kullanılmalıdır.
- **Kapsamlı API Güvenlik Modülü:**
  - **Çıkarım:** API'ler birincil saldırı yüzeyi olduğundan [10], WebAnalyzerTool, BOLA, BFLA ve GraphQL sorgu analizi de dahil olmak üzere karmaşık enjeksiyon saldırıları gibi API'ye özgü güvenlik açıkları için özel tarama sunmalıdır.
  - **Eylem:** Mevcut API taraması, mantık tabanlı yetkilendirme kusurları, hız sınırlama atlamaları ve aşırı veri ifşasını içerecek şekilde genişletilmelidir.

Kullanıcıların tüm API saldırı yüzeylerini belirlemelerine yardımcı olmak için API keşif özellikleri düşünülmelidir.[10]

- **Entegre Yazılım Tedarik Zinciri Analizi:**
  - **Çıkarım:** Artan düzenleyici baskı ve saldırı karmaşıklığı göz önüne alındığında [1], WebAnalyzerTool, web uygulamalarında kullanılan üçüncü taraf ve açık kaynak bileşenlerindeki güvenlik açıklarını belirlemek için Yazılım Bileşimi Analizi (SCA) içermelidir.
  - **Eylem:** SBOM'leri oluşturma ve doğrulama ve yeni keşfedilen güvenlik açıkları için bağımlılıkları sürekli izleme özellikleri uygulanmalıdır.
- **Derin Konteyner ve Bulut Yerel Güvenlik İçgörüleri:**
  - **Çıkarım:** Konteynerler yaygınlaştıkça [12], WebAnalyzerTool, konteyner görüntüleri için ayrıntılı güvenlik analizi, çalışma zamanı koruma önerileri ve Kubernetes yapılandırmalarına ilişkin bilgiler sağlamalıdır.
  - **Eylem:** Sırlar [12], yanlış yapılandırmalar [12] ve en az ayrıcalık ilkelerine uyum için konteyner görüntülerini taramak üzere modüller geliştirilmelidir. Mikro segmentasyon ve çalışma zamanı politika uygulaması hakkında rehberlik sunulmalıdır.
- **DevSecOps İş Akışları için Destek:**
  - **Çıkarım:** "Sola kaydırma" güvenliğini kolaylaştırmak için [3], WebAnalyzerTool, CI/CD boru hatlarına sorunsuz bir şekilde entegre olmalı ve geliştiricilere hızlı geri bildirim sağlamalıdır.
  - **Eylem:** Popüler CI/CD araçları için eklentiler sunulmalı, geliştirici dostu güvenlik açığı raporları sağlanmalı ve geliştirme ve dağıtım sırasında otomatik güvenlik politikası uygulaması desteklenmelidir.[12]
- **İnsan Dışı Kimlikler (NHI) Güvenliğini Ele Alma:**
  - **Çıkarım:** NHI'nin en önemli OWASP endişesi olarak ortaya çıkması [1], WebAnalyzerTool'un API anahtarları, tokenlar ve hizmet hesaplarıyla ilgili güvenli olmayan uygulamaları belirlemesine ve işaretlemesine yardımcı olması gerektiği anlamına gelir.
  - **Eylem:** Web uygulama kod tabanlarında ve yapılandırmalarında sabit kodlu kimlik bilgilerini, güvenli olmayan sır yönetimi uygulamalarını ve aşırı ayrıcalıklı NHI erişimini taramak için uygulamalar geliştirilmelidir.
- **Yapay Zekaya Özgü Web Uygulama Güvenliği Potansiyeli:**
  - **Çıkarım:** WebAnalyzerTool, YZ/LLM'leri entegre eden web uygulamalarını güvence altına almayı hedefliyorsa, prompt enjeksiyonu, veri zehirlenmesi ve diğer YZ'ye özgü güvenlik açıklarını tespit etmek için yeni yeteneklere ihtiyaç duyacaktır.[15]
  - **Eylem:** YZ modeli güvenlik testi araştırmaları keşfedilmeli ve potansiyel olarak LLM destekli web uygulamaları için özel bir modül geliştirilmelidir.

- **Kapsamlı Saldırı Yüzeyi Yönetimine Katkı:**
  - **Çıkarım:** WebAnalyzerTool, saldırı yüzeyinin web uygulama katmanına ilişkin ayrıntılı bilgiler sağlayarak bir kuruluşun genel ASM stratejisine [3] katkıda bulunabilir.
  - **Eylem:** Web'e dönük varlıklar, alt alan adları ve web uygulaması bağlamındaki gölge BT için keşif yetenekleri geliştirilmelidir.

Sonuç: Web Güvenliğinin Geleceğinde Yol Almak

2025 yılında web uygulama güvenliği ortamı, artan karmaşıklık, sofistike yapay zeka destekli tehditler ve şeffaflık ve proaktif savunma için artan düzenleyici zorunluluklarla tanımlanacaktır. Mikro hizmetlerin, API'lerin ve konteynerleştirilmiş ortamların yükselişi, saldırı yüzeyini temelden genişleterek geleneksel güvenlik yaklaşımlarını yetersiz hale getirmiştir.

Bu gelecekte etkili bir şekilde yol almak için kuruluşlar, yapay zeka destekli tehdit tespiti, sağlam tedarik zinciri güvenliği, API güvenliğine birincil odaklanma, Sıfır Güven ilkelerinin yaygın olarak benimsenmesi ve DevSecOps aracılığıyla güvenliğin geliştirme iş akışlarına derinlemesine entegrasyonu ile karakterize edilen bütünsel ve uyarlanabilir bir güvenlik duruşu benimsemelidir. Ayrıca, yapay zekaya özgü güvenlik ve genellikle göz ardı edilen insan dışı kimlikler gibi yeni alanlar özel dikkat gerektirecektir.

WebAnalyzerTool için ileriye giden yol, özellikle daha akıllı, daha proaktif güvenlik açığı tespiti için yapay zekadan yararlanmak, kapsamını modern web uygulama bileşenlerinin (API'ler, konteynerler, YZ modelleri) tüm genişliğini kapsayacak şekilde genişletmek ve otomatik geliştirme ve operasyonel boru hatlarına sorunsuz bir şekilde entegre olmak gibi sürekli yenilikleri içermektedir. Bu trendleri benimseyerek, WebAnalyzerTool, sürekli gelişen bir tehdit ortamında kuruluşların dayanıklı dijital deneyimler oluşturmasını ve dağıtmasını sağlayarak yeni nesil web uygulamalarını güvence altına almak için vazgeçilmez bir araç olarak konumunu sağlamlaştırabilir.

Works cited

1. The State Of Application Security, 2025: Yes, AI Just Made It Harder ..., accessed June 5, 2025, https://www.forrester.com/blogs/application-security-2025-yes-ai-just-made-it-harder-to-do-this-right/
2. The State Of Application Security, 2025 - Forrester, accessed June 5, 2025, https://www.forrester.com/report/the-state-of-application-security-2025/RES182779
3. The Top 10 AppSec Trends Shaping Cybersecurity in 2025 - Qwiet AI, accessed June 5, 2025,

https://qwiet.ai/appsec-resources/the-top-10-appsec-trends-shaping-cybersecurity-in-2025/
4. Web App Security: 2025 Complete Guide | Savvycom Software, accessed June 5, 2025, https://savvycomsoftware.com/blog/web-app-security-complete-guide-2025/
5. 2025 Cyber Security Predictions: Navigating the Ever-Evolving Threat Landscape, accessed June 5, 2025, https://www.cyberdefensemagazine.com/2025-cyber-security-predictions-navigating-the-ever-evolving-threat-landscape/
6. 8 AI Cybersecurity Companies For 2025 - SentinelOne, accessed June 5, 2025, https://www.sentinelone.com/cybersecurity-101/data-and-ai/ai-cybersecurity-companies/
7. 8 Container monitoring trends in 2025 - DEV Community, accessed June 5, 2025, https://dev.to/swetha_suresh_18c9975c236/8-container-monitoring-trends-in-2025-3mkj
8. What is UEBA (user and entity behavior analytics)? | Okta, accessed June 5, 2025, https://www.okta.com/identity-101/ueba/
9. api7.ai, accessed June 5, 2025, https://api7.ai/blog/2025-top-8-api-management-trends#:~:text=Security%20Enhancements&text=By%202025%2C%20AI%20will%20be,addresses%20or%20throttling%20suspicious%20traffic.
10. The State of API Security in 2025: Emerging Threats and Best ..., accessed June 5, 2025, https://securemyorg.com/2025/04/05/the-state-of-api-security-in-2025/
11. 2025 Cybersecurity Predictions - ConnectWise, accessed June 5, 2025, https://www.connectwise.com/blog/2025-cybersecurity-predictions
12. Container Security And How To Secure Containers In 2025, accessed June 5, 2025, https://accuknox.com/blog/container-security
13. Where is Serverless Going in 2025? - Wisp CMS, accessed June 5, 2025, https://www.wisp.blog/blog/where-is-serverless-going-in-2025
14. The 2025 Guide to User & Entity Behavior Analytics (UEBA), accessed June 5, 2025, https://www.teramind.co/blog/user-and-entity-behavior-analytics-guide/
15. AI Security: 2025 Predictions & Recommendations - HiddenLayer, accessed June 5, 2025, https://hiddenlayer.com/innovation-hub/ai-security-2025-predictions-recommendations/
16. OWASP Top 10 2025 for LLM Applications: What's new? Risks, and Mitigation Techniques, accessed June 5, 2025, https://www.confident-ai.com/blog/owasp-top-10-2025-for-llm-applications-risks-and-mitigation-techniques
17. OWASP Top 10 LLM, Updated 2025: Examples & Mitigation Strategies - Oligo Security, accessed June 5, 2025, https://www.oligo.security/academy/owasp-top-10-llm-updated-2025-examples-and-mitigation-strategies
18. OWASP Top 10 Non-Human Identities Risks - 2025, accessed June 5, 2025, https://owasp.org/www-project-non-human-identities-top-10/2025/top-10-2025

/