2025 Yılında Gelişmiş Web Güvenliği: Alt Alan Adı Taraması, Uç Nokta Tespiti, Parametre Toplama, Zafiyet Taraması ve WAF Algılamaya Yönelik En Son 10 Teknik ve Trend

Yönetici Özeti

2025 yılı web güvenliği ortamı, saldırganların yapay zekayı (AI) yaygın bir şekilde benimsemesi ve API'ler, buluta özel dağıtımlar ve kapsamlı üçüncü taraf bağımlılıkları dahil olmak üzere dijital altyapıların artan karmaşıklığı nedeniyle yükselen bir tehdit ortamıyla karakterize edilmektedir. Bu bağlamda, proaktif, entegre ve yapay zeka destekli gelişmiş web güvenliği araçları artık isteğe bağlı değil, kurumsal dayanıklılık için kritik bir zorunluluk haline gelmiştir.

Bu rapor, 2025 yılında gelişmiş web güvenliğini tanımlayacak en etkili 10 teknik ve trendi belirlemektedir. Bu teknikler ve trendler, yapay zeka/makine öğrenimi destekli otomasyon, API öncelikli güvenlik, "shift-left" metodolojileri, gelişmiş saldırı yüzeyi yönetimi, proaktif tehdit istihbaratı, Sıfır Güven ilkeleri, yeni WAF atlatma tekniklerinin azaltılması, hibrit zafiyet tespiti, sağlam tedarik zinciri güvenliği ve sürekli tehdit maruziyeti yönetimi gibi alanları kapsamaktadır.

Kuruluşların, reaktif savunmadan sürekli, adaptif bir güvenlik duruşuna geçiş yapması gerekmektedir. Bu geçiş, derinlemesine keşif, akıllı zafiyet tespiti ve gelişen tehditlere, özellikle web uygulamalarını ve temel bileşenlerini hedef alanlara karşı dinamik savunma için yapay zekadan yararlanan entegre platformlara yatırım yapılmasını gerektirmektedir.

Giriş: 2025'te Gelişen Web Güvenliği Ortamı

Dijital dünya hızla gelişmekte ve beraberinde getirdiği zorluklar da aynı hızla artmaktadır. Kuruluşların saldırı yüzeyi, yanlış yapılandırılmış bulut ortamlarından gözden kaçan IoT cihazlarına ve karmaşık web uygulamalarına kadar her zamankinden daha hızlı genişlemektedir. Modern web uygulamaları artık monolitik yapılar değil, mikro hizmetlere, API'lere ve üçüncü taraf bileşenlere yoğun bir şekilde dayanmaktadır; bu da siber saldırılar için potansiyel giriş noktalarını önemli ölçüde genişletmektedir. Bu büyüme, kuruluşların tüm dijital varlıkları (bulut, şirket içi ve SaaS ortamları dahil) genelinde maruziyeti azaltmanın, risklerin birleşik görünürlüğünü ve bağlamsal anlayışını gerektirdiğini giderek daha fazla kabul etmesini yansıtmaktadır.

Siber güvenlik liderleri, güvenli, yapay zeka destekli iş dönüşümünü sağlamak için dokuz uygulama, teknik yetenek ve yapısal reformu önceliklendirmektedir. Bu, siber güvenlik risk sorumluluğunu resmileştirmeyi, siber yargıyı teşvik etmeyi, veri güvenliği yönetimi programlarını canlandırmayı ve kurumsal kimlik ve erişim yönetimi (IAM) stratejilerini makine kimliklerini içerecek şekilde genişletmeyi içermektedir. Önleme odaklı bir zihniyetten direnç odaklı bir yaklaşıma

("olursa değil, ne zaman olursa" zihniyeti) geçiş kritik öneme sahiptir. Bu, siber olayların işletme üzerindeki etkisini en aza indirmeyi ve uyarlanabilirliği artırmayı vurgulamakta, mutlak önleme yanılgılarından kaçınmayı hedeflemektedir. Bu durum, yalnızca tehditleri tespit etmekle kalmayıp aynı zamanda öngörebilen ve bunlara uyum sağlayabilen araçlara olan ihtiyacı ortaya koymaktadır.

Siber güvenlik teknolojisi optimizasyonu, satıcı konsolidasyonu yerine araç optimizasyonuna odaklanmaktadır; bu da kuruluşların doğru platform ve nokta çözümleri karışımını bulmalarına ve karmaşıklığı azaltma ile siber güvenlik hedeflerini karşılamak için araçları dağıtma esnekliği arasında bir denge oluşturmalarına olanak tanımaktadır. Bu gelişmeler, gelecekteki web güvenliği araçlarının "proaktif direnç" ilkesiyle tasarlanması gerektiğini göstermektedir. Bu, geleneksel reaktif taramaların ötesine geçerek sürekli izleme, tahminsel analiz ve hızlı yanıt yeteneklerini entegre etmeyi gerektirmektedir. Böyle bir yaklaşım, kuruluşların saldırı yüzeyindeki değişikliklerin hacmini ve hızını yönetmek için otomasyon ve zekadan yararlanarak gelişen tehditlerin önünde kalmasını sağlamaktadır.

Gelişmiş Web Güvenliği Araçlarının Temel Yetenekleri

Bu bölüm, gelişmiş bir web güvenliği aracının temel işlevlerini ve en son tekniklerin her bir yeteneği nasıl geliştirdiğini ayrıntılı olarak ele almaktadır.

Yeni Nesil Alt Alan Adı Numaralandırması ve Varlık Keşfi

Saldırı yüzeyini genişletmek ve bir hedefin altyapısının görünmeyen köşelerini ortaya çıkarmak için hem pasif hem de aktif gelişmiş alt alan adı numaralandırma teknikleri hayati öneme sahiptir. Pasif numaralandırma, hedefle doğrudan etkileşim kurmadan bilgi toplamayı içerir; bu, halka açık veritabanlarından ve üçüncü taraf kaynaklardan yararlanarak şüpheli trafik oluşturmadan geçmiş verileri toplamayı mümkün kılar. Bu, Censys ve Shodan gibi halka açık veritabanlarını ve Subfinder ve OWASP Amass gibi araçları kullanmayı içerir. OWASP tarafından geliştirilen Amass, açık kaynak istihbaratını (OSINT) aktif keşif teknikleriyle birleştirerek harici varlık keşfi yapar ve hedefin saldırı yüzeyinin doğru bir resmini oluşturmak için çeşitli kaynaklardan verileri ilişkilendirir. Google dorking (site:*.example.com gibi) de otomatik araçlar tarafından gözden kaçırılan aktif alt alan adlarını ortaya çıkarabilir.

Aktif numaralandırma ise hedefle doğrudan etkileşimi içerir ve halka açık olarak indekslenmemiş ancak aktif kullanımda olan alt alan adlarını ortaya çıkarmak için gereklidir. Ancak, bu yaklaşım, özellikle yüksek hacimli isteklerle, Web Uygulama Güvenlik Duvarları (WAF'lar) veya bot koruma mekanizmaları tarafından engellenme riski taşır. Teknikler arasında DNS kaba kuvvet saldırısı (Gobuster, Mksub gibi araçlar ve SecLists gibi kelime listeleriyle), Sanal Ana Bilgisayar (vhost) fuzzing (Gobuster, ffuf, wfuzz ile aynı sunucuyu paylaşan gizli hizmetleri ortaya çıkarmak için), Ters DNS aramaları (DnsX ile IP adreslerini alan adlarına çözümlemek için) ve tarama (Burp Suite ile HTTP

yanıtlarını ve DOM'u analiz ederek gizli API uç noktalarını veya dahili alt alan adlarını keşfetmek için) yer almaktadır. Toplanan alan adlarının gerçek web sunucuları olup olmadığını doğrulamak ve yanlış pozitifleri filtrelemek için httpx veya httprobe gibi araçlarla HTTP yoklaması yapılır.

Project Sleuth gibi araçların ortaya çıkışı, alt alan adı numaralandırması ve OSINT toplama dahil olmak üzere hata avcılığı ve keşif sürecini otomatikleştirmeyi amaçlamaktadır. Gelecekteki geliştirmeler, risk temelinde zafiyetleri önceliklendirmek için makine öğreniminin entegrasyonunu içerebilir. Yapay zeka ve makine öğrenimi (ML), saldırı yüzeyi yönetimi (ASM) için ayrılmaz hale gelmekte, kuruluşların tehditleri daha hızlı ve doğru bir şekilde belirlemesini sağlamaktadır. Yapay zeka destekli platformlar, insan analistlerin tespit etmesi neredeyse imkansız olacak zafiyetleri ortaya çıkararak büyük miktarda veriyi gerçek zamanlı olarak analiz etmektedir.

Gelişmiş bir aracın, sadece alt alan adlarını listelemekten öteye geçerek, yapay zeka destekli "akıllı keşif" yeteneklerini içermesi gerekmektedir. Bu, yapay zekanın mevcut teknikleri otomatikleştirmekten daha fazlasını yapabileceği anlamına gelmektedir; kalıpları analiz edebilir, potansiyel yeni alt alan adlarını tahmin edebilir ve tespitten kaçınmak için aktif numaralandırmayı akıllıca uyarlayabilir (örneğin, hız sınırlarını dinamik olarak ayarlayarak veya dönen proxy'ler kullanarak). Bu, bulut ortamları sürekli değiştiği ve sürekli keşif gerektirdiği için kritik öneme sahiptir. Bu durum, gelişmiş araçların alt alan adlarını akıllıca önceliklendireceği, gizli varlıkları (vhost kurulumlarının bir parçası olanlar dahil) belirleyeceği ve hedefin altyapısındaki gerçek zamanlı tehdit istihbaratına ve gözlemlenen değişikliklere dayanarak keşiflerini sürekli olarak uyarlayacağı anlamına gelmektedir.

Akıllı Uç Nokta ve Parametre Toplama

API'ler, modern uygulamaların önemli bir parçasıdır ve kritik saldırı yüzeyleri olarak kabul edilmektedir; güvenlikleri bu nedenle büyük önem taşımaktadır. API'ler, modern mobil ve web uygulamaları ile arka uç sunucuları arasında bir yazılım aracı görevi görür. API ekonomisi, kuruluşların verilere ve temel yeteneklere erişilebilirliği artırmak için API'leri kullanmasıyla yeniliği teşvik ederken, aynı zamanda önemli güvenlik riskleri de ortaya çıkarmaktadır. Hızlı dağıtım için güvenliğin göz ardı edilmesi, bir dizi zafiyeti ortaya çıkarır. RSA Konferansı 2025'te API güvenliği, yapay zeka sonrası en çok tartışılan ikinci konu olarak öne çıkmıştır; bu da API'lerin kritik saldırı yüzeyleri olarak artan anlayışını yansıtmaktadır. Akamai gibi firmalar, büyük dil modelleri için bir güvenlik duvarı etrafında API'ler için yeni korumalar başlatmıştır ve bu, OWASP'ın gelişen en iyi zafiyet listeleriyle uyumlu olarak büyük dil modellerinin artan benimsenmesi ve kritik koruma ihtiyacı etrafında müşteri tartışmalarının merkezinde yer almıştır. API'ler, REST, GraphQL, gRPC, WebSockets, Webhooks ve SOAP gibi çeşitli stillerde mevcuttur.

GraphQLer, GraphQL API'leri için bağlama duyarlı ilk güvenlik testi çerçeve-

sidir. Mevcut test araçlarının genellikle işlevsel doğruluğa odaklanıp sorgu bağımlılıklarından ve yürütme bağlamından kaynaklanan güvenlik risklerini gözden kaçırdığı durumlarda, yetkisiz veri erişimi, hizmet reddi (DoS) saldırıları ve enjeksiyonlar gibi önemli zafiyetleri ele alarak GraphQL güvenliğini artırmayı amaçlamaktadır. GraphQLer, mutasyonlar, sorgular ve nesneler arasındaki ilişkileri analiz etmek için bir bağımlılık grafiği oluşturarak kritik bağımlılıkları yakalar. Kimlik doğrulama ve yetkilendirme hatalarını, erişim kontrolü atlatmalarını ve kaynak kötüye kullanımlarını ortaya çıkarmak için ilgili sorgu ve mutasyonları akıllıca zincirler. Ayrıca, veri sızıntısı, ayrıcalık yükseltme ve tekrar saldırısı vektörlerini ortaya çıkarmak için dahili kaynak kullanımını izler. RESTful API'ler için **RESTTESTGEN** (İşlem Bağımlılık Grafiği oluşturur), **RESTLER** (aşamalı olarak test senaryoları oluşturur), **MOREST** (yürütme geri bildirimi ile RESTful hizmet Özellik Grafiği oluşturur) ve **MINER** (kritik girdi değerlerini tahmin etmek için sinir ağları kullanır) gibi çeşitli yöntemler, OpenAPI spesifikasyonlarını ayrıştırmaya ve test senaryoları oluşturmaya odaklanmaktadır. Ancak, bu genel kara kutu tekniklerinin çoğu, öncelikli olarak hataları (örneğin, 500 serisi HTTP durum kodları) belirlemeye odaklanmakta ve genel hataların ötesinde güvenlik zafiyetlerine özel olarak odaklanmamaktadır. **NAUTILUS** gibi yeni penetrasyon testi yöntemleri enjeksiyon zafiyetlerini ele alsa da, yetersiz kaynak yönetimi veya hız sınırlamasının eksikliği gibi diğer riskleri gözden kaçırabilir.

Gelişmiş bir aracın, sadece uç noktaları tespit etmek ve parametreleri toplamakla kalmayıp, "davranışsal API güvenlik testi"ne doğru ilerlemesi gerekmektedir. API'lerin karmaşıklığı (özellikle dinamik yürütme modeli ve bağımlılıkları olan GraphQL), zafiyetlerin tek uç nokta kusurlarından değil, birden çok API çağrısı arasındaki etkileşimden veya parametrelerin farklı işlemler arasında nasıl kullanıldığından kaynaklandığı anlamına gelmektedir. Bu durum, saldırı yüzeyini tek tek uç noktaların ötesine, bir uygulamanın API etkileşimlerinin mantıksal akışına genişletmektedir. Bu, ayrıntılı grafik analizi, durum takibi ve uygulama katmanı DDoS zafiyetleri için özel testler gerektirmektedir.

Gelişmiş Zafiyet Taraması ve Analizi

Yazılım testi ve doğrulama, modern yazılım sistemlerinin güvenilirliğini ve güvenliğini sağlamak için kritik öneme sahiptir. Geleneksel olarak, biçimsel doğrulama teknikleri (örneğin, model kontrolü, teorem ispatı) titiz çerçeveler sağlamıştır ancak karmaşık, gerçek dünya programlarına uygulandığında ölçeklenebilirlik zorluklarıyla karşılaşmaktadır. **Etkileşimli Uygulama Güvenlik Testi (IAST)**, yürütme sırasında güvenlik sorunlarını gözlemlemek için uygulamayı enstrümanlayarak hem statik hem de dinamik analizden elde edilen bilgileri harmanlar. **Fuzzing**, gizli zayıflıkları ortaya çıkarmak için beklenmedik veya yanlış biçimlendirilmiş girdilerden yararlanır. Geçen yıl 30.000'den fazla zafiyetin açıklandığı, önceki rakamlara göre %17'lik bir artış olduğu göz önüne alındığında, bu durum siber risklerdeki sürekli artışı yansıtmaktadır. Bu, daha verimli ve doğru tespit mekanizmalarına olan ihtiyacı

zorunlu kılmaktadır.

Son zamanlarda, **Büyük Dil Modelleri (LLM'ler)** tanıtılmış ve fuzzing'den değişmez üretimlere kadar yazılım testinin her alanında kullanılmaktadır. Bu modeller, güvensiz kodlama uygulamalarını anlama yeteneklerinden yararlanarak zafiyetleri tespit etmek için büyük kaynak kodu ve doğal dil korpusları üzerinde eğitilmiş sinir mimarileri kullanmaktadır. Yapay zeka, LLM tabanlı kalıp/kural/tohum üretimi gibi yollarla web uygulamaları için dinamik fuzzing'i geliştirebilir. LLM'ler ayrıca web sistemlerinde zafiyet tespiti için kullanılmakta ve SQL/XSS enjeksiyonu gibi çeşitli web zafiyetleri için kavram kanıtları (PoC'ler) üretebilmektedir. Yapay zeka savunmada (tehdit tespiti, Güvenlik Operasyon Merkezi (SOC) operasyonları) otomasyonu ilerletse de, savunma üzerindeki etkisi şu anda saldırıdan daha azdır. LLM'lerin gelecekteki yazılım geliştirmeye hakim olması beklenirken, birden fazla çalışma LLM'lerin incelenen tüm programlama dillerinde güvenlik zafiyetleri oluşturabileceğini ortaya koymaktadır.

Gelişmiş zafiyet tarama araçları, yapay zeka/makine öğrenimini yalnızca zafiyetleri tespit etmek için değil, aynı zamanda risk temelinde önceliklendirmek için de entegre etmelidir. **Project Sleuth**'un gelecekteki geliştirmelerinde zafiyetleri risk temelinde önceliklendirmek için ML'nin entegrasyonundan bahsedilmesi, bu alandaki kritik ihtiyacı vurgulamaktadır. Yapay zekanın savunma üzerindeki etkisinin (zafiyet triyajı ve düzeltme dahil) saldırıdan daha az olduğu göz önüne alındığında, bu durum yapay zekanın sadece hataları bulmakla kalmayıp, bunları istismar edilebilirlik ve iş etkisi temelinde akıllıca sıralaması gerektiğini göstermektedir. Özellikle açıklanan zafiyetlerin artan hacmi ve LLM'lerdeki yanlış pozitifler göz önüne alındığında, bu akıllı önceliklendirme hayati önem taşımaktadır. Bu, otonom zafiyet yönetimine doğru bir adım olup, düzeltme çabalarını etkili bir şekilde yönlendirmektedir.

WAF Sistemi Algılama ve Kaçınma Karşı Tedbirleri

Web Uygulama Güvenlik Duvarları (WAF'lar), gelen HTTP trafiğini inceleyerek kötü niyetli istekleri filtrelemek ve çeşitli web tabanlı tehditlere karşı savunma sağlamak için temel güvenlik geçitleri olarak tanıtılmıştır. Ancak, kritik rollerine rağmen, WAF'lar kaçınmaya karşı bağışık değildir. Geleneksel WAF kaçınma teknikleri genellikle saldırı yüklerini bozmaya dayanmaktadır, ancak WAF satıcıları bu bilinen atlatma tekniklerinin çoğuna karşı önlemler almıştır.

WAF'ları atlatmaya yönelik yeni, gerçek dünya yaklaşımı, WAF'lar ile web uygulama çerçeveleri arasındaki içerik ayrıştırma tutarsızlıklarını istismar etmektedir. Bu yöntem, saldırı yükünü sağlam tutar ancak yaygın olarak kullanılan `application/json`, `multipart/form-data` ve `application/xml` gibi içerik türlerini kullanarak başlıklar ve gövde segmentleri gibi belirli kötü niyetli olmayan bileşenleri mutasyona uğratır. Gelişmiş kara kutu fuzzing ile tanımlanan bu teknik, AWS, Azure, Cloud Armor, Cloudflare ve ModSecurity gibi 5 iyi bilinen WAF'ta 1207 atlatmayı doğrulamıştır. Atlatma sınıflarına örnek olarak,

sınır sınırlayıcı manipülasyonu, içerik türü parametre değişiklikleri, şema kapatma manipülasyonu ve alan sarıcı manipülasyonu verilebilir. **WAFFLED** aracı, bu tutarsızlığa dayalı atlatma vektörlerini bulmak için tasarlanmış ve uygulanmıştır.

Bu zafiyetleri azaltmak için **HTTP-Normalizer**, mevcut RFC standartlarına göre HTTP isteklerini titizlikle doğrulamak için tasarlanmış sağlam bir proxy aracı olarak tanıtılmıştır. Bu araç, tüm önerilen atlatmaların uygun teknikler uygulanarak önlenebilir olmasını sağlamakta, uyumlu istekleri normalleştirmekte veya uyumsuz olanları reddetmektedir.

WAF sistemlerini algılamak, 2025'te web güvenliğinde bir "RFC uyumluluk boşluğu" ve bunun istismarını ortaya koymaktadır. WAF'lar ve web uygulama çerçeveleri, RFC standartlarına farklı düzeylerde uyum nedeniyle HTTP isteklerini genellikle farklı yorumlamaktadır. Saldırganlar, kötü niyetli yükü gizlemeden WAF'ları atlatmak için bu "ayrıştırma tutarsızlığını" kullanmaktadır. Bu durum, sadece bir WAF'ı tespit etmenin yeterli olmadığını; gelişmiş bir aracın, WAF'ın bu sofistike, standart tabanlı atlatmalara karşı sağlamlığını da değerlendirmesi gerektiğini göstermektedir. HTTP-Normalizer'ın varlığı, katı RFC uyumluluğunun temel savunma olduğunu ima etmektedir. Bu, imza tabanlı WAF kaçınmasından yapısal ve protokol düzeyinde kaçınmaya doğru ince ama derin bir geçişi temsil etmektedir.

2025 Yılında Web Güvenliğinde En İyi 10 Teknik ve Trend

1. Web Güvenliğinde Yapay Zeka/Makine Öğrenimi Destekli Otomasyon

- **Açıklama**: Yapay zeka (AI), tehdit tespiti ve SOC operasyonlarında otomasyonu ilerletir, gerçek zamanlı anomali tespiti ve dinamik yanıtlar sağlar. Büyük Dil Modelleri (LLM'ler), zafiyet tespiti ve fuzzing için kavram kanıtları üretir.
- **Önem**: AI destekli kötü amaçlı yazılımlar statik savunmaları atlatabilir; bu nedenle adaptif, kendi kendine öğrenen savunma mekanizmaları kritik öneme sahiptir.
- **Potansiyel Etkiler ve Uygulama Alanları**: Zafiyet tarama doğruluğunu artırır, yanlış pozitifleri azaltır ve sıfır gün açıklıklarını tespit eder. Penetrasyon testi ve güvenlik araştırması için idealdir.
- **Kaynak**: SentinelOne: 10 Cyber Security Trends for 2025

2. Tasarım Gereği API Odaklı Güvenlik

- **Açıklama**: API güvenlik testi çerçeveleri, GraphQLer gibi bağlama duyarlı analizlerle API bağımlılıklarını ve iş mantığını test eder. REST ve GraphQL gibi API'lerdeki zafiyetleri tespit eder.
- **Önem**: API'ler, modern uygulamaların temelidir ve tedarik zinciri saldırıları için kritik bir hedef haline gelmiştir.

- **Potansiyel Etkiler ve Uygulama Alanları**: Veri sızıntılarını ve DDoS saldırılarını önler, üçüncü taraf entegrasyonlarını korur.
- **Kaynak**: RSA Conference 2025: A Barometer for Cybersecurity's Future

3. Shift-Left Güvenlik ve DevSecOps Entegrasyonu

- **Açıklama**: Güvenlik, yazılım geliştirme yaşam döngüsüne erken entegre edilir, geliştiricilere anında geri bildirim sağlar ve güvenli kodlama alışkanlıklarını güçlendirir.
- **Önem**: Zafiyetlerin erken tespiti, düzeltme maliyetlerini ve riskleri azaltır.
- **Potansiyel Etkiler ve Uygulama Alanları**: Geliştirme süreçlerini güvenli hale getirir, CI/CD işlem hatlarıyla entegrasyonu sağlar.
- **Kaynak**: Application Security Best Practices in 2025

4. Gelişmiş Harici Saldırı Yüzeyi Yönetimi (EASM)

- **Açıklama**: AI destekli platformlar, sürekli keşif ve gerçek zamanlı risk puanlaması ile kuruluşun dijital ayak izini izler.
- **Önem**: Bulut ortamlarının dinamik doğası, statik taramaları yetersiz kılar; sürekli izleme gereklidir.
- **Potansiyel Etkiler ve Uygulama Alanları**: Gölge BT ve üçüncü taraf risklerini ortaya çıkarır, buluta özel varlıkları yönetir.
- **Kaynak**: Top Attack Surface Management Trends for 2025

5. Proaktif Tehdit İstihbaratı Entegrasyonu

- **Açıklama**: Gerçek zamanlı tehdit istihbaratı, kuruluşun web saldırı yüzeyiyle ilişkilendirilerek eyleme geçirilebilir bilgiler sağlar.
- **Önem**: Sıfır gün saldırılarını ve tehlikeye atılmış verileri hızlıca tespit eder.
- **Potansiyel Etkiler ve Uygulama Alanları**: Proaktif savunma stratejileri oluşturur, karanlık web izlemeyi destekler.
- **Kaynak**: Best Security Threat Intelligence Products and Services

6. Web Uygulamaları için Sıfır Güven Mimarileri

- **Açıklama**: Her web isteği için sürekli doğrulama ve mikro segmentasyon, yanal hareket risklerini azaltır.
- **Önem**: Geleneksel ağ çevresi ortadan kalktıkça, her isteğin doğrulanması kritik hale gelir.
- **Potansiyel Etkiler ve Uygulama Alanları**: Ele geçirilmiş kimlik bilgilerinin etkisini azaltır, hassas veri erişimini korur.
- **Kaynak**: SentinelOne: 10 Cyber Security Trends for 2025

7. Ayrıştırma Tutarsızlıklarını İstismar Etme ve Azaltma (WAF Atlatma)

- **Açıklama**: WAF'lar ile web uygulama çerçeveleri arasındaki RFC uyumluluk boşluklarını hedef alan atlatma teknikleri tespit edilir ve önlenir.
- **Önem**: Yeni atlatma teknikleri, geleneksel WAF savunmalarını etkisiz kılabilir.
- **Potansiyel Etkiler ve Uygulama Alanları**: WAF'ların sağlamlığını artırır, XSS ve SQL enjeksiyonu gibi saldırılara karşı koruma sağlar.
- **Kaynak**: WAFFLED: Exploiting Parsing Discrepancies to Bypass Web Application Firewalls

8. Hibrit Zafiyet Tespiti Yaklaşımları

- **Açıklama**: Biçimsel doğrulama ve AI tabanlı analiz birleştirilerek zafiyet tespiti daha hızlı ve güvenilir hale getirilir.
- **Önem**: Geleneksel yöntemler ölçeklenebilirlikte zorlanırken, LLM'ler yanlış pozitifler üretebilir; hibrit yaklaşımlar bu boşluğu doldurur.
- **Potansiyel Etkiler ve Uygulama Alanları**: Daha kapsamlı ve verimli zafiyet taramaları sağlar.
- **Kaynak**: Vulnerability Detection: From Formal Verification to Large Language Models

9. Tedarik Zinciri Güvenliği ve SBOM Zorunlulukları

- **Açıklama**: Yazılım Malzeme Listesi (SBOM) ile üçüncü taraf bağımlılıklar izlenir ve zafiyetler otomatik olarak tespit edilir.
- **Önem**: Tedarik zinciri saldırıları, üçüncü taraf bileşenlerden kaynaklanan riskleri artırır.
- **Potansiyel Etkiler ve Uygulama Alanları**: Tüm yazılım yaşam döngüsünde güvenliği sağlar, uyumluluğu destekler.
- **Kaynak**: Application Security Best Practices in 2025

10. Sürekli Tehdit Maruziyeti Yönetimi (CTEM)

- **Açıklama**: Sürekli keşif, doğrulama ve önceliklendirme ile dinamik risk yönetimi sağlanır.
- **Önem**: Bulut ortamlarının sürekli değişimi, statik taramaları yetersiz kılar.
- **Potansiyel Etkiler ve Uygulama Alanları**: En kritik tehditlere odaklanarak savunmaları optimize eder.
- **Kaynak**: What Is Attack Surface Management in 2025?

Sonuçlar ve Öneriler

2025 yılı web güvenliği ortamı, artan karmaşıklık, yapay zekanın hem saldırganlar hem de savunucular tarafından benimsenmesi ve sürekli değişen dijital

varlıkların dinamik doğası ile tanımlanmaktadır. Bu ortamda, geleneksel, reaktif güvenlik yaklaşımları yetersiz kalmaktadır. Gelişmiş bir web güvenliği aracının, kuruluşların bu zorlukların üstesinden gelmesine yardımcı olmak için proaktif, entegre ve akıllı yetenekler sunması gerekmektedir.

Öneriler:

- **Entegre Platformlara Yatırım**: Kuruluşlar, AI/ML destekli otomasyon, API odaklı güvenlik, shift-left metodolojileri ve CTEM gibi teknikleri birleştiren platformlara yatırım yapmalıdır.
- **Geliştirici Odaklı Güvenlik**: Geliştirici iş akışlarına entegre araçlar, anında geri bildirim ve eğitim rehberliği ile güvenli kodlama alışkanlıklarını güçlendirmelidir.
- **Proaktif ve Adaptif Savunma**: Sürekli izleme, gerçek zamanlı tehdit istihbaratı ve Sıfır Güven ilkeleri, dinamik tehdit ortamında dayanıklılığı artırır.
- **Tedarik Zinciri Güvenliği**: SBOM oluşturma ve üçüncü taraf bağımlılıkların izlenmesi, tedarik zinciri risklerini azaltmak için zorunludur.

Bu yetenekleri benimseyerek ve güvenlik bilinci kültürünü teşvik ederek, kuruluşlar 2025'te siber tehditlere karşı dayanıklılıklarını önemli ölçüde artırabilirler.

Alıntılanan Çalışmalar

- Top Attack Surface Management Trends for 2025
- What Is Attack Surface Management in 2025?
- Top Cybersecurity Trends to Tackle Emerging Threats
- Subdomain enumeration: expand attack surfaces with active …
- Project Sleuth: A Comprehensive All-in-One Bug Bounty Automation …
- RSA Conference 2025: A Barometer for Cybersecurity's Future
- Vulnerability Testing of RESTful APIs Against Application Layer
- GraphQLer: Enhancing GraphQL Security with Context …
- Vulnerability Detection: From Formal Verification to Large Language Models
- 10 Cyber Security Trends For 2025
- Frontier AI's Impact on the Cybersecurity Landscape
- WAFFLED: Exploiting Parsing Discrepancies to Bypass Web Application Firewalls
- CyberSentinel: An Emergent Threat Detection System for AI Security
- Application Security Best Practices in 2025
- 18 DevSecOps Tools to Know in 2025
- Best Security Threat Intelligence Products and Services