2025 Küresel Uygulama Güvenliği Durumu: OWASP İlk 10 Analizi

1. Yönetici Özeti: 2025 Yılında Riskin Mimarisi

OWASP İlk 10: 2025 sürümünün yayınlanması, uygulama güvenliği tarihinde kritik bir dönüm noktasını temsil etmektedir. Sektör, izole kodlama hatalarına odaklanan bir dönemden; sistemik, mimari ve tedarik zinciri bağımlılıklarıyla mücadele eden bir döneme geçiş yapmıştır. 2021 yılında "tasarımın" önemi vurgulanırken, 2025 standardı modern uygulamaların sadece yazılmadığını, aynı zamanda düşmanca bir ekosistem içinde **birleştirildiğini** ve **işletildiğini** kabul etmektedir. **Yazılım Tedarik Zinciri Hataları (A03)** maddesinin üst düzey bir risk olarak ortaya çıkması ve **İstisnai Durumların Yanlış Yönetilmesi (A10)** maddesinin listeye girmesi, güvenliğin artık "girdi temizliğinden" (input sanitization) ziyade **dayanıklılık (resilience)** ve **köken (provenance)** üzerine kurulması gerektiğini göstermektedir.[1]

Bu rapor, **Shai-Hulud solucanı** ve **tj-actions** ihlali gibi son dönemde yaşanan yıkıcı olaylardan elde edilen verileri sentezleyerek, risklerin operasyonel krizlere nasıl dönüştüğünü incelemektedir. Analizler, **Kırık Erişim Kontrolü (A01)** gibi geleneksel tehditlerin liderliğini koruduğunu, ancak tedarik zinciri saldırılarının hızının modern altyapı için en büyük varoluşsal tehdidi oluşturduğunu ortaya koymaktadır.[3]

---

2. Standardın Evrimi: Metodoloji ve Paradigma Değişimleri

OWASP Top 10, basit bir farkındalık belgesi olmaktan çıkıp küresel bir uyumluluk standardına dönüşmüştür. 2025 listesi, "semptomlardan" ziyade "kök nedenlere" odaklanan veri odaklı bir yaklaşımın ürünüdür. Örneğin, 2021 listesindeki "Hassas Veri İfşası" (bir semptom), yerini verinin ifşa olmasına *neden olan* **Kriptografik Hatalar** veya **Güvenlik Yanlış Yapılandırması** gibi kök nedenlere bırakmıştır.[1]

2021 ve 2025 Karşılaştırmalı Risk Tablosu

Sıra	OWASP İlk 10: 2021	OWASP İlk 10: 2025	Trend Analizi
A01	Kırık Erişim Kontrolü	**Kırık Erişim Kontrolü**	**Durgun:** Mikro hizmetlerin karmaşıklığı ve API

			kullanımı nedeniyle 1 numaralı risk. SSRF buraya dahil edildi.[5]
A02	Kriptografik Hatalar	**Güvenlik Yanlış Yapılandırması**	**Yükselişte:** Bulut altyapısı ve yapılandırma karmaşıklığı riski 2. sıraya taşıdı.[2]
A03	Enjeksiyon	**Yazılım Tedarik Zinciri Hataları**	**Yeni/Kritik:** Eski "Savunmasız Bileşenler" maddesi genişletilerek CI/CD ve dağıtım risklerini kapsadı.[6]
A04	Güvensiz Tasarım	**Kriptografik Hatalar**	**Düşüşte:** Sıralamada düştü ancak veri koruma regülasyonları nedeniyle etkisi hala kritik.
A05	Güvenlik Yanlış Yapılandırması	**Enjeksiyon**	**Düşüşte:** Modern framework'ler bu riski azaltsa da eski kodlarda hala yaygın.
A06	Savunmasız Bileşenler	**Güvensiz Tasarım**	**Düşüşte:** Tehdit modellemenin önemini vurgulamaya devam ediyor.
A07	Kimlik Doğrulama Hataları	**Kimlik Doğrulama Hataları**	**Durgun:** Kimlik yönetimi saldırı yüzeyinin merkezi olmaya devam

			ediyor.
A08	Bütünlük Hataları	**Yazılım veya Veri Bütünlüğü Hataları**	**Durgun:** Güncellemelerin ve verinin doğrulanmasına odaklanıyor.
A09	Günlükleme Hataları	**Güvenlik Günlüğü ve Uyarı Hataları**	**Durgun:** "Uyarı" (Alerting) eklemesi, tepki vermenin önemini vurguluyor.[5]
A10	SSRF	**İstisnai Durumların Yanlış Yönetilmesi**	**Yeni:** Sistemin hata anındaki davranışına ve güvenli başarısızlığa (fail-safe) odaklanıyor.[7]

---

3. 2025 İlk 10 Riskin Derinlemesine Analizi

A01:2025 – Kırık Erişim Kontrolü (Broken Access Control)

Kırık Erişim Kontrolü, web güvenliğinin en kritik maddesi olmaya devam etmektedir. Özellikle mikro hizmet mimarilerinde yetkilendirme mantığının karmaşıklaşması bu riski beslemektedir.

- **SSRF Birleşmesi:** 2021'de A10 olan Sunucu Taraflı İstek Sahteciliği (SSRF), artık bir erişim kontrolü hatası olarak kabul edilip A01 ile birleştirilmiştir.
- **Vaka Analizi: Kia Web Portalı (Haziran 2024):** Araştırmacılar, Kia bayi portalındaki bir zafiyet sayesinde sadece plaka numarası kullanarak araçların kontrolünü (kapıları açma, motoru çalıştırma) ele geçirebilmiştir. Bu, sistemin kullanıcının kimliğini doğruladığı (Authentication) ancak o araca erişim yetkisi olup olmadığını kontrol etmediği (Authorization) klasik bir A01 hatasıdır.[8]

A02:2025 – Güvenlik Yanlış Yapılandırması (Security Misconfiguration)

5. sıradan 2. sıraya yükselen bu madde, bulut tabanlı (cloud-native) altyapıların yükselişini yansıtır. Artık altyapı koddur (IaC) ve bir geliştiricinin yapacağı basit bir izin hatası (örneğin S3 bucket'ı halka açmak) tüm sistemi tehlikeye atabilir.[2]

A03:2025 – Yazılım Tedarik Zinciri Hataları (Software Supply Chain Failures)

Listenin en önemli yeni başlığıdır. Saldırganlar artık güçlendirilmiş kurumsal ağları hedeflemek yerine, bu kurumların kullandığı açık kaynak kütüphaneleri ve derleme araçlarını hedef almaktadır.

- **Vaka Analizi: Shai-Hulud Solucanı (2025):** npm ekosistemini hedef alan bu solucan, geliştirici hesaplarını ele geçirerek popüler paketlere zararlı kod enjekte etmiş ve kendini "solucan" gibi yayarak binlerce projeyi etkilemiştir.[3]
- **Vaka Analizi: tj-actions (Mart 2025):** Popüler GitHub Action tj-actions/changed-files, saldırganlar tarafından ele geçirilmiş ve bu eylemi kullanan CI/CD hatlarından (pipeline) gizli anahtarların (secrets) sızdırılmasına neden olmuştur. Bu olay, üçüncü taraf derleme araçlarına duyulan "zımni güvenin" tehlikesini kanıtlamıştır.[13]

A04:2025 – Kriptografik Hatalar (Cryptographic Failures)

Hassas veri ifşasının temel nedenidir. Zayıf şifreleme algoritmaları, kod içine gömülen şifreleme anahtarları (hardcoded keys) ve güvensiz veri iletimi (TLS eksikliği) bu kategoride değerlendirilir.

A05:2025 – Enjeksiyon (Injection)

Sıralamada gerilese de (modern framework'lerin koruması sayesinde), hala yıkıcı etkileri vardır. Özellikle **MOVEit Transfer** zafiyeti (CVE-2023-34362), SQL Enjeksiyonunun (SQLi) 2024 ve 2025'te bile milyonlarca verinin çalınmasına neden olabileceğini göstermiştir.[15]

A06:2025 – Güvensiz Tasarım (Insecure Design)

Bu kategori, kodlama hatalarından ziyade mimari ve mantıksal hatalara odaklanır. Güvenliğin yazılım geliştirme yaşam döngüsünün en başına (Shift-Left) taşınmasını ve Tehdit Modelleme (Threat Modeling) yapılmasını zorunlu kılar.

A07:2025 – Kimlik Doğrulama Hataları (Authentication Failures)

Kimlik hırsızlığı, "credential stuffing" saldırıları ve zayıf şifre politikaları bu maddenin temelini oluşturur. MFA (Çok Faktörlü Kimlik Doğrulama) eksikliği en büyük zafiyetlerden biridir.

A08:2025 – Yazılım veya Veri Bütünlüğü Hataları

Yazılım güncellemelerinin, CI/CD hatlarının ve verinin bütünlüğünün doğrulanmamasını kapsar. Güvensiz tersine serileştirme (Insecure Deserialization) de bu kapsamdadır.

A09:2025 – Güvenlik Günlüğü ve Uyarı Hataları

2025 güncellemesiyle başlığa "Uyarı" (Alerting) eklenmiştir. Sadece log tutmak yetmez; saldırı

anında sistemin anormallikleri tespit edip güvenlik ekiplerini uyarması (SIEM entegrasyonu) gerekir.[5]

A10:2025 – İstisnai Durumların Yanlış Yönetilmesi (Mishandling of Exceptional Conditions)

Listenin **yeni ve kritik** maddesidir. Sistem bir hata ile karşılaştığında (veritabanı çökmesi, zaman aşımı vb.) ne yapar?

- **Açık Başarısızlık (Fail Open):** Bir güvenlik kontrolü hata verirse sistem erişime izin mi veriyor? Güvenlik her zaman "Kapalı Başarısız" (Fail Closed) olmalıdır.
- **Bilgi Sızıntısı:** Kullanıcıya gösterilen hata mesajları (Stack Trace), sistemin iç yapısını ifşa etmemelidir. Bu, saldırganlara yol haritası sunar (CWE-209, CWE-754).[7]

---

4. Sonuç ve Stratejik Öneriler

OWASP İlk 10: 2025, güvenliğin bir kod parçasından ibaret olmadığını, tüm ekosistemin bir parçası olduğunu vurgular. Organizasyonlar için öncelikli adımlar şunlardır:

1. **Tedarik Zinciri Güvenliği:** SBOM (Yazılım Malzeme Listesi) kullanımı standartlaştırılmalı ve bağımlılıklar sabitlenmelidir (pinning).
2. **Yapılandırma Otomasyonu:** Altyapı değişiklikleri manuel yapılmamalı, kod olarak yönetilmeli ve otomatik taranmalıdır.
3. **Hata Yönetimi Testleri:** Uygulamaların sadece çalıştığı durumlar değil, çöktüğü durumlar da test edilmeli; sistemin "güvenli bir şekilde başarısız olduğu" (fail-safe) doğrulanmalıdır.
4. **Sıfır Güven (Zero Trust):** Erişim kontrolleri her katmanda sürekli doğrulanmalı, varsayılan olarak güvenilmemelidir.

Alıntılanan çalışmalar

1. OWASP Top 10 2025: Key Changes & What They Mean | Orca ..., erişim tarihi Aralık 15, 2025, https://orca.security/resources/blog/owasp-top-10-2025-key-changes/
2. OWASP Top 10 2025 Updates: Supply Chain, Secrets, And Misconfigurations Take Center Stage, erişim tarihi Aralık 15, 2025, https://securityboulevard.com/2025/11/owasp-top-10-2025-updates-supply-chain-secrets-and-misconfigurations-take-center-stage/
3. Widespread Supply Chain Compromise Impacting npm Ecosystem - CISA, erişim tarihi Aralık 15, 2025, https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem
4. Supply Chain Compromise of Third-Party tj-actions/changed-files (CVE-2025-30066) and reviewdog/action-setup@v1 (CVE-2025-30154) | CISA, erişim tarihi Aralık 15, 2025, https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-t

hird-party-tj-actionschanged-files-cve-2025-30066-and-reviewdogaction
5. The New 2025 OWASP Top 10 List: What Changed, and What You Need to Know - Fastly, erişim tarihi Aralık 15, 2025, https://www.fastly.com/blog/new-2025-owasp-top-10-list-what-changed-what-you-need-to-know
6. A03 Software Supply Chain Failures - OWASP Top 10:2025, erişim tarihi Aralık 15, 2025, https://owasp.org/Top10/2025/A03_2025-Software_Supply_Chain_Failures/
7. A10 Mishandling of Exceptional Conditions - OWASP Top 10:2025, erişim tarihi Aralık 15, 2025, https://owasp.org/Top10/2025/A10_2025-Mishandling_of_Exceptional_Conditions/
8. Millions of Kia Cars Were Vulnerable to Remote Hacking ..., erişim tarihi Aralık 15, 2025, https://www.securityweek.com/millions-of-kia-cars-were-vulnerable-to-remote-hacking-researchers/
9. Kia's Web Portal Vulnerability: A Wake-Up Call for API Security, erişim tarihi Aralık 15, 2025, https://www.securityjourney.com/post/kias-web-portal-vulnerability-a-wake-up-call-for-api-security
10. Broken Access Control: The 40% Surge in 2025's Most Exploited Vulnerability - Medium, erişim tarihi Aralık 15, 2025, https://medium.com/@instatunnel/broken-access-control-the-40-surge-in-2025s-most-exploited-vulnerability-fc57e7fb943d
11. "Shai-Hulud" Worm Compromises npm Ecosystem in Supply Chain ..., erişim tarihi Aralık 15, 2025, https://unit42.paloaltonetworks.com/npm-supply-chain-attack/
12. Defending against supply chain attacks like Chalk/Debug and the Shai-Hulud worm - AWS, erişim tarihi Aralık 15, 2025, https://aws.amazon.com/blogs/security/defending-against-supply-chain-attacks-like-chalk-debug-and-the-shai-hulud-worm/
13. GitHub Action tj-actions/changed-files supply chain attack | Wiz Blog, erişim tarihi Aralık 15, 2025, https://www.wiz.io/blog/github-action-tj-actions-changed-files-supply-chain-attack-cve-2025-30066
14. tj-actions changed-files through 45.0.7 allows remote attackers to discover secrets by reading actions logs. · CVE-2025-30066 - GitHub, erişim tarihi Aralık 15, 2025, https://github.com/advisories/ghsa-mrrh-fwg8-r2c3
15. MOVEit transfer data breaches Deep Dive - ORX, erişim tarihi Aralık 15, 2025, https://orx.org/resource/moveit-transfer-data-breaches
16. CVE-2023-34362 Detail - NVD, erişim tarihi Aralık 15, 2025, https://nvd.nist.gov/vuln/detail/cve-2023-34362
17. OWASP Top 10 2025: A10—Mishandling of Exceptional Conditions - Authgear, erişim tarihi Aralık 15, 2025, https://www.authgear.com/post/owasp-2025-mishandling-of-exceptional-conditions
18. CWE 209: Information Exposure Through an Error Message | Java - Veracode, erişim tarihi Aralık 15, 2025, https://www.veracode.com/security/java/cwe-209/