**🧠 1. Oxeye Nedir?**

**Oxeye**, modern uygulamalardaki güvenlik açıklarını tespit etmek, önceliklendirmek ve geliştirici dostu çözümlerle düzeltmek amacıyla tasarlanmış bir **Application Security Testing (AST)** platformudur.

📌 Özellikle **microservices**, **cloud-native**, **CI/CD entegre** ortamlarda kullanılır.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🔍 Otomatik zafiyet tarama | Kaynak kodu ve runtime davranışı analiz eder |
| ⚙️ CI/CD entegrasyonu | GitHub, GitLab, Jenkins, Bitbucket ile uyumlu |
| ☁️ Cloud-native destek | Kubernetes, Docker, OpenShift, ECS, EKS ortamlarında çalışır |
| 🧠 Kod + Runtime analizi (hybrid) | Hem statik analiz (SAST) hem dinamik analiz (DAST) özelliklerini birleştirir |
| 🔐 Güvenlik Açığı Önceliklendirme | Gerçek çalışma ortamında etkisi olan açıklar filtrelenir |
| 🧩 Yazılımcı dostu | Geliştiricilere özel fix önerileri verir (Pull Request üzerinden) |

**🧰 3. Nasıl Çalışır?**

1. **Kod tabanı analiz edilir (SAST)**
2. **Uygulama çalışırken gözlemlenir (Runtime Sensor)**
3. **Zafiyetler eşleştirilir** (false positive azaltılır)
4. **CI/CD içinde raporlanır**
5. **Geliştiriciye özel çözüm yolları sunulur**

**⚙️ 4. Entegrasyonlar**

| **Entegrasyon Alanı** | **Desteklenen Platformlar** |
| --- | --- |
| ☁️ Cloud | AWS, Azure, GCP |
| 🔁 CI/CD | Jenkins, GitHub Actions, GitLab CI, Bitbucket |
| 🧱 Kod Repoları | Git, GitHub, GitLab, Bitbucket |
| 🔐 Güvenlik | Snyk, SonarQube, JFrog Xray |

📊 5. Örnek Güvenlik Açığı Raporu

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

📌 Oxeye, bu tür raporları CI/CD üzerinden geliştiriciye doğrudan PR (Pull Request) açarak iletebilir.

**📈 6. Avantajları**

✅ Uygulama güvenliği sadece build aşamasında değil, **çalışma zamanında da denetlenir**  
✅ Güvenlik ekibi ve yazılım ekibi arasında **köprü** olur  
✅ Gerçek zafiyetlere odaklanır → **false positive oranı düşüktür**

**🛡️ 7. Kullanım Alanları**

* DevSecOps pipeline’ları
* Bulut tabanlı uygulama güvenliği
* CI/CD güvenlik otomasyonu
* Runtime zafiyet görünürlüğü
* Zafiyet önceliklendirme ve güvenli kod geliştirme

**⚠️ 8. Etik ve Ticari Uyarı**

* Oxeye bir **ticari platformdur**
* Eğitim ve demo sürümü kullanımı için resmî web sitesinden başvuru yapılmalıdır:  
  🔗 https://www.oxeye.io

**🎯 9. Öğrenim Kazanımları**

* Modern web uygulamalarının nasıl test edildiğini anlama
* Kod + runtime analizinin farkını öğrenme
* DevSecOps ve CI/CD güvenliği hakkında bilgi kazanma
* Otomatik güvenlik testi platformlarının çalışma yapısını kavrama