OWASP

Open Worldwide Application Security Project (OWASP), yazılım güvenliğini iyileştirmeye adanmış kar amacı gütmeyen bir vakıftır. OWASP, herkesin ilgili çevrimiçi sohbetlere, projelere ve daha fazlasına katılabileceği ve katkıda bulunabileceği bir sistemde geliştirilmiştir. OWASP, çevrimiçi araçlar ve videolardan forumlara ve etkinliklere kadar her şeyin ücretsiz ve kolayca erişilebilir olmasını sağlamak için çalışır ve bu hizmetleri web sitesi üzerinden sunar.

En Önemli 10 Web Uygulaması Güvenlik Zaafiyeti

1. **Broken Access Control (A01:2021):** Daha önce listede 5. sırada yer alan bozuk erişim kontrolü, bir saldırganın kullanıcı hesaplarına erişim sağlamasına olanak tanıyan bir zaafiyettir ve 2021 yılında 1. sıraya yükselmiştir. Bu bağlamda, saldırgan sistemde bir kullanıcı veya bir yönetici olarak işlev görebilir.

   Çözüm: Seeker® gibi etkileşimli bir uygulama güvenlik testi (IAST) çözümü, siteler arası istek sahteciliğini veya hassas verilerinizin güvensiz bir şekilde saklanmasını zahmetsizce tespit etmenize yardımcı olabilir. Ayrıca, JSON Web Token'ların (JWT) işlenmesinde kullanılan hatalı veya eksik mantığı da belirler. Penetrasyon testi, IAST faaliyetlerine manuel bir destek sağlayarak, istenmeyen erişim kontrollerini tespit etmeye yardımcı olabilir.

2. **Cryptographic Failures (A02:2021):** Önceden 3. sırada yer alan ve daha önce hassas veri ifşası olarak bilinen bu madde, bir belirti yerine kök neden olarak doğru bir şekilde tanımlamak amacıyla kriptografik hatalar olarak yeniden adlandırıldı. Kriptografik hatalar, önemli saklanan veya iletilen verilerin (örneğin sosyal güvenlik numarası gibi) tehlikeye girmesi durumunda ortaya çıkar.

   Çözüm: Seeker'ın denetleyicileri, hem yetersiz şifreleme gücünü hem de zayıf veya sabitlenmiş kriptografik anahtarları tarayabilir ve ardından bozuk veya riskli kriptografik algoritmaları tespit edebilir. Black Duck® kriptografi modülü, açık kaynak yazılımda (OSS) kullanılan kriptografik yöntemleri ortaya çıkarır, böylece bunlar güç açısından daha fazla değerlendirilebilir. Hem Coverity® statik uygulama güvenlik testi (SAST) hem de Black Duck yazılım bileşimi analizi (SCA), kod ve bileşen seviyelerinde "belirli bir an" anlık görüntüsü sağlayabilen denetleyicilere sahiptir. Ancak, hassas verilerin diğer dahili ve harici yazılım bileşenleriyle yapılan entegre testler sırasında sızdırılmadığından emin olmak için IAST ile destek sağlamak, sürekli izleme ve doğrulama açısından kritik öneme sahiptir.

3. **Injection (A03:2021)**
   Injection, 1. sıradan 3. sıraya düşmüştür ve siteler arası betik çalıştırma (cross-site scripting) artık bu kategorinin bir parçası olarak kabul edilir. Temel olarak, bir saldırganın geçersiz verileri bir web uygulamasına göndermesiyle kod enjeksiyonu gerçekleşir ve bu, uygulamanın tasarlandığı şekilde çalışmaması için yapılır.

   Çözüm: Sürekli entegrasyon/sürekli teslimat (CI/CD) hattınıza SAST ve IAST araçlarını dahil etmek, Injection hatalarını hem statik kod seviyesinde hem de uygulama çalışma zamanı testi sırasında dinamik olarak tespit etmenize yardımcı olur. Seeker gibi modern uygulama güvenlik testi (AST) araçları, yazılım uygulamasını çeşitli test aşamalarında güvence altına almaya yardımcı olabilir ve SQL enjeksiyonlarının yanı sıra çeşitli Injection saldırılarını da kontrol edebilir. Örneğin, NoSQL Injectionları, komut Incjectionları, LDAP Injectionları, şablon Injectionları ve günlük Injectionlarını tespit edebilir. Seeker, Log4Shell güvenlik açıklarını tespit etmek için özel olarak tasarlanmış yeni bir denetleyici sunan ilk araçtır. Log4J'nin nasıl yapılandırıldığını belirler, nasıl davrandığını test eder ve bu bulguları patentli Aktif Doğrulama motoruyla doğrular (veya geçersiz kılar).

4. **Insecure Design (A04:2021)**
   Güvensiz tasarım, 2021 için yeni bir kategori olup, tasarım hatalarıyla ilgili zafiyetlere odaklanır. Organizasyonlar "sola kaydırma" (shift left) stratejisini sürdürdükçe, tehdit modelleme, güvenli tasarım desenleri ve prensipleri ile referans mimariler yeterli olmamaktadır.

   Çözüm: Seeker IAST, yüksek derecede karmaşık web, bulut ve mikro hizmet tabanlı uygulamalarda güvenlik açıklarını tespit eder ve tüm giriş ve çıkış API'lerini, hizmetlerini ve işlev çağrılarını ortaya çıkarır. Veri akışını ve ilgili uç noktaları görsel olarak sunarak, uygulama tasarımındaki zayıflıkları belirgin hale getirir ve penetrasyon testi ile tehdit modelleme çabalarına yardımcı olur.

5. **Security Misconfiguration (A05:2021)**
   Önceki external entities kategorisi artık bu zaafiyet kategorisinin bir parçası olup, 6. sıradan yükselmiştir. Güvenlik yapılandırma hataları, bir yapılandırma hatası veya eksikliğinden kaynaklanan tasarım veya yapılandırma zayıflıklarıdır.

   Çözüm: Coverity SAST gibi çözümler, hata mesajları aracılığıyla erişilebilir bilgi ifşasını tespit eden bir denetleyici içerir. Seeker IAST gibi dinamik araçlar ise, uygulama çalışma zamanı testleri sırasında bilgi ifşasını ve uygunsuz HTTP başlık yapılandırmalarını tespit edebilir.

6. **Vulnerable and Outdated Components (A06:2021)**
   Bu kategori, 9. sıradan yükselmiştir ve yalnızca bilinen değil, potansiyel güvenlik zaafiyetleri de taşıyan bileşenlerle ilgilidir. Bilinen güvenlik açıklarına sahip bileşenler, örneğin CVE'ler, tanımlanmalı ve yamanmalıdır; eski veya kötü amaçlı bileşenler ise uygulanabilirlikleri ve oluşturabilecekleri zaafiyetler açısından değerlendirilmelidir.

   Çözüm: Black Duck gibi yazılım bileşimi analiz (SCA) araçları, statik analiz ve IAST ile birlikte kullanılarak bir uygulamadaki eski ve güvensiz bileşenlerin tanımlanmasını ve tespit edilmesini sağlar. IAST ve SCA, zayıf veya eski bileşenlerin gerçekten nasıl kullanıldığını anlamada iyi bir uyum sağlar. Seeker IAST ve Black Duck SCA birlikte çalışarak, sadece zayıf bir bileşeni tanımlamakla kalmaz, aynı zamanda bu bileşenin test edilen uygulama tarafından şu anda yüklenip yüklenmediği gibi ayrıntıları da ortaya çıkarır. Ayrıca, geliştirici etkinliği, katkıda bulunanların itibarı ve sürüm geçmişi gibi metrikler, eski veya kötü amaçlı bir bileşenin potansiyel zaafiyetleri hakkında kullanıcıya bilgi verebilir.

7. **Identification and Authentication Failures (A07:2021)**
   Daha önce bozuk kimlik doğrulama olarak bilinen bu madde, 2. sıradan aşağıya düşmüştür ve artık kimlik doğrulama hatalarıyla ilgili CWL'leri de içermektedir. Özellikle, kimlik doğrulama ve oturum yönetimiyle ilgili işlevler yanlış bir şekilde uygulandığında, saldırganların şifreleri, anahtar kelimeleri ve oturumları tehlikeye atmasına olanak tanır, bu da kullanıcı kimliklerinin çalınmasına ve daha fazlasına yol açabilir.

   Çözüm: Çok faktörlü kimlik doğrulama, tehlikeye atılmış hesap zaafiyetini azaltmaya yardımcı olabilir ve otomatik statik analiz, bu tür zayıflıkları bulmada oldukça faydalıdır. Özellikle özelleştirilmiş kimlik doğrulama sistemlerini değerlendirirken manuel statik analiz de güç katabilir. Coverity SAST, özellikle bozuk kimlik doğrulama güvenlik açıklarını tanımlayan bir denetleyici içerir. Seeker IAST ise sabitlenmiş şifreler ve kimlik bilgilerini, ayrıca uygunsuz kimlik doğrulama veya kimlik doğrulamada kritik adımların eksikliğini tespit edebilir.

8. **Software and Data Integrity Failures (A08:2021)**

Bu, 2021 için yeni bir kategori olup, yazılım güncellemeleri, kritik veriler ve bütünlüğü doğrulanmadan kullanılan CI/CD hatlarına odaklanır. Ayrıca, bu maddeye dahil edilen güvensiz deserialization, bir saldırganın sistemde uzaktan kod çalıştırmasına olanak tanıyan bir deserialization hatasıdır.

Çözüm: Uygulama güvenliği araçları, deserialization hatalarını tespit etmeye yardımcı olur ve penetrasyon testi bu sorunu doğrulayabilir. Seeker IAST ayrıca güvensiz deserialization kontrolü yapabilir ve güvensiz yönlendirmeler veya token erişim algoritmalarında yapılan herhangi bir müdahaleyi tespit etmeye yardımcı olabilir.

9. **Security Logging and Monitoring Failures (A09:2021)**

Daha önce yetersiz günlüğe kayıt ve izleme olarak bilinen bu madde, 10. sıradan yükselmiş ve daha fazla türdeki hataları içerecek şekilde genişletilmiştir. Günlüğe kayıt ve izleme, bir web sitesinde sıklıkla yapılması gereken faaliyetlerdir ve bunu yapmamak, bir siteyi daha ciddi tehlikelere karşı savunmasız bırakır.

Çözüm: Penetrasyon testi gerçekleştirdikten sonra, geliştiriciler test günlüklerini inceleyerek olası eksiklikleri ve güvenlik açıklarını belirleyebilir. Coverity SAST ve Seeker IAST, kaydedilmemiş güvenlik istisnalarını tespit etmeye yardımcı olabilir.

10. **Server-Side Request Forgery (A10:2021)**

2021 yılında yeni eklenen bir kategori olan sunucu tarafı istek sahteciliği (SSRF), bir web uygulaması kullanıcının sağladığı URL'yi doğrulamadan uzaktaki bir kaynağı aldığında meydana gelebilir. Bu, bir saldırganın uygulamanın beklenmedik bir hedefe özel olarak hazırlanmış bir istek göndermesini sağlar; bu, sistem bir güvenlik duvarı, VPN veya ek ağ erişim kontrol listesi ile korunmuş olsa bile geçerlidir. SSRF saldırılarının şiddeti ve sıklığı, bulut hizmetleri ve mimarilerin artan karmaşıklığı nedeniyle artmaktadır.

Çözüm: Seeker, ek tarama ve sınıflandırma yapmadan SSRF'yi izleyebilen, takip edebilen ve tespit edebilen modern AST araçlarından biridir. Gelişmiş enstrümantasyon ve ajan tabanlı teknolojisi sayesinde, Seeker potansiyel SSRF açıklarını da tespit edebilir.

Hüseyin Tazegül