Insecure Direct Object References (IDOR)/Invoices

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **Insecure Direct Object References (IDOR)/Invoices** labının çözümünü anlatacağım.

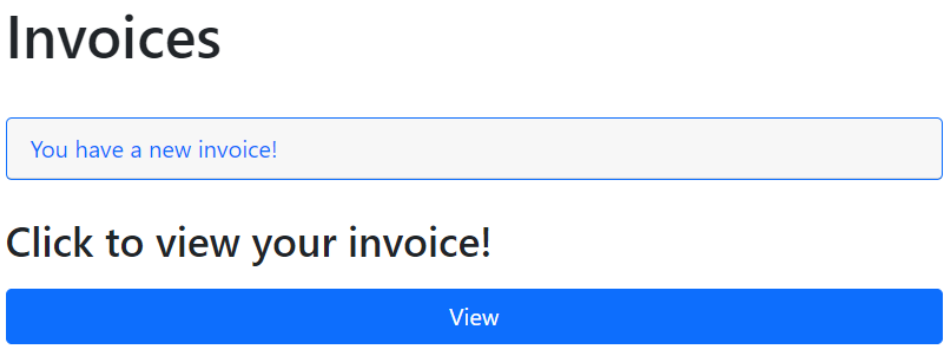
İnsecure Direct Object References (IDOR) açığı, bir web uygulamasının nesnelere doğrudan erişim için yeterli yetkilendirme kontrollerini uygulamamasından kaynaklanır. Bu güvenlik açığı sayesinde saldırgan, doğrudan bir nesneye (dosya, kayıt, kullanıcı profili gibi) erişim sağlayarak yetkisiz işlemler gerçekleştirebilir. Saldırgan, URL veya form girdileri üzerinden doğrudan bu nesnelerin kimlik bilgilerini (ID, numara vb.) değiştirerek başka bir kullanıcının verilerine izinsiz erişebilir.

IDOR açığı, kullanıcıların doğrudan bir kaynağın kimlik numarasına (örneğin URL'deki kullanıcı kimliği veya dosya ID'si) erişim sağladığı her yerde bulunabilir. Profil sayfaları, fatura görüntüleme ekranları, dosya indirme linkleri gibi bölümler IDOR açığı için potansiyel hedeflerdir.

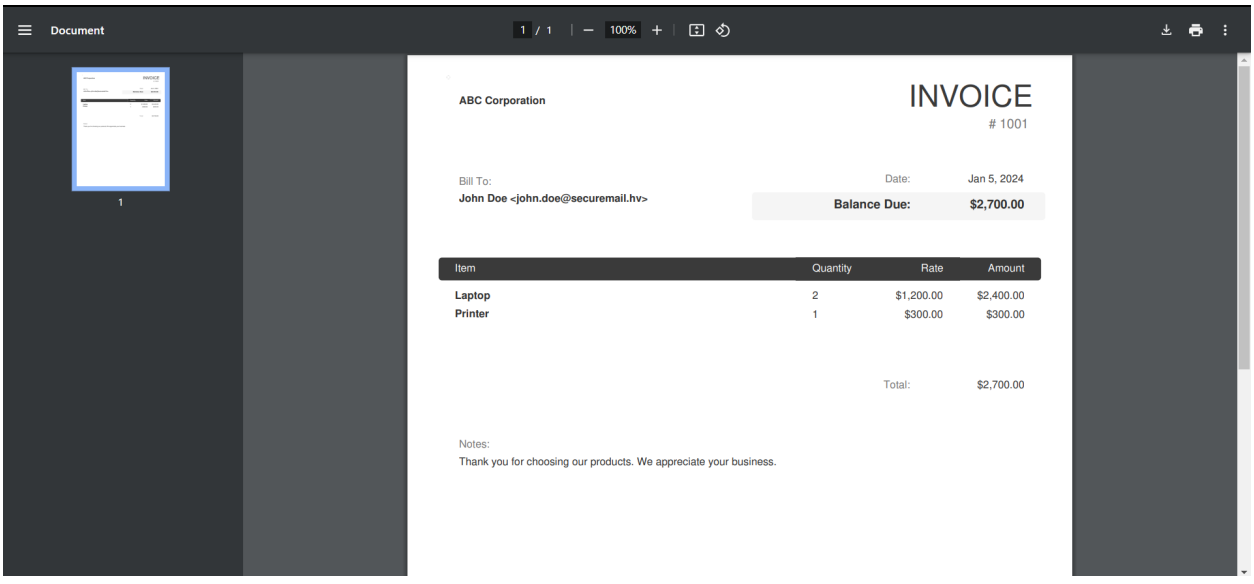
Açığın çözümü, her nesneye erişim için güçlü yetkilendirme kontrollerinin uygulanması ve kullanıcı kimliklerinin doğrulanmasıdır.

Sırada ise makinenin çözümü var.

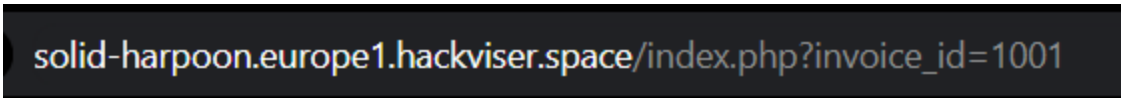
Siteye ilk girdiğimizde bizi aşağıdaki gibi bir ekran karşılıyor



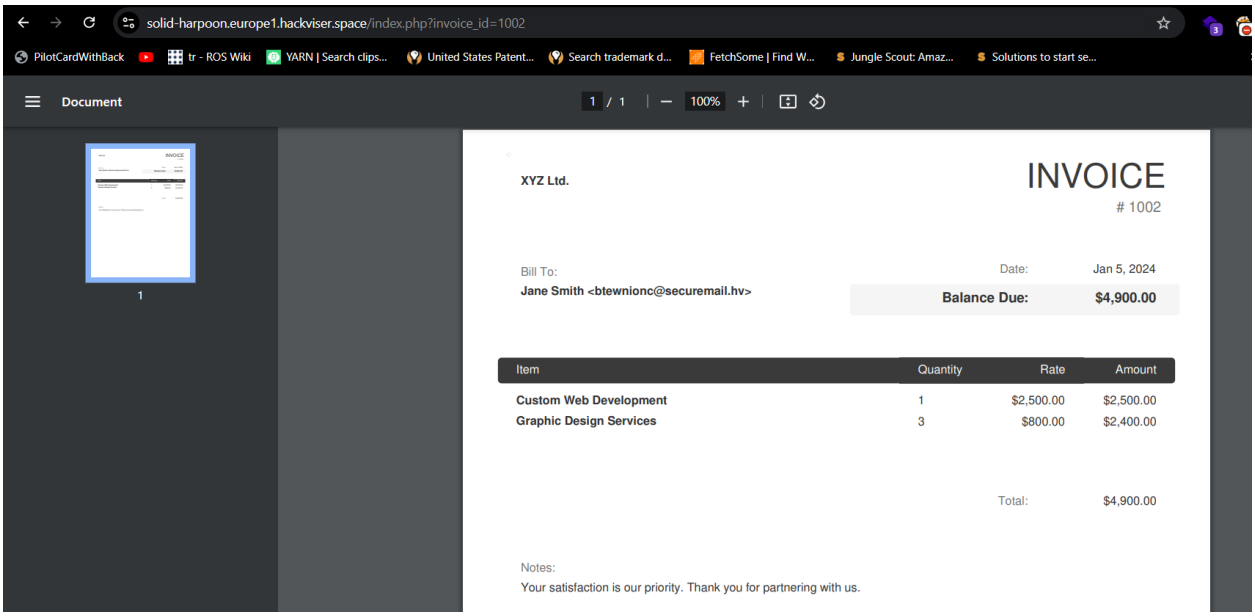
"View" butonuna tıkladığımız zaman da aşağıdaki gibi fatura kısmı bizi karşılıyor



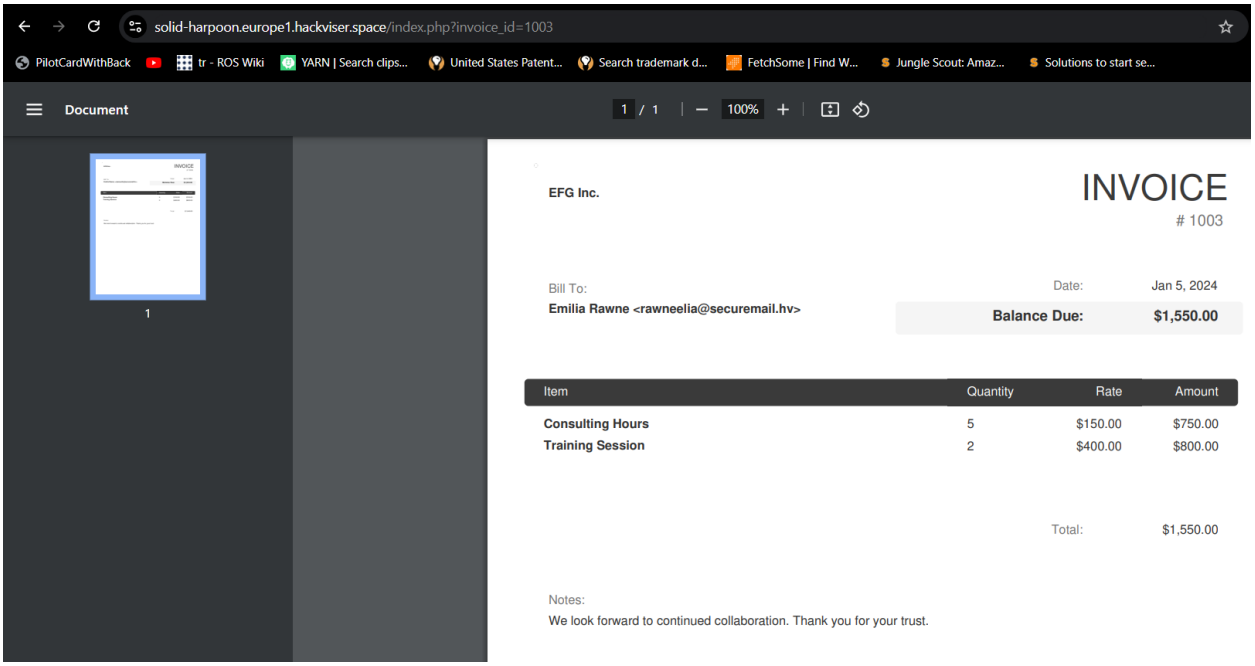
url kısmındaki id değeri kafamda bir soru işareti oluşturuyor. Bu id değerini değiştirirsem ne olacağına bakmak istiyorum.



1002 değerinde “Jane Smith” kullanıcısının bilgilerini görüyorum ve burada IDOR zafiyeti olduğundan emin oluyorum.



Değerleri sırayla artırıyorum.



1003 değerine geldiğim zaman bizden istenen Emilia Rawne kullanıcısının mail hesabı önüme düşüyor ve soruyu başarılı bir şekilde tamamlıyorum.

Peki, bu açığı kullanarak neler yapabileceğimize bakalım. IDOR açığını kullanarak başka bir kullanıcının hesap bilgilerine erişebilir, başkalarına ait hassas verilere ulaşabilir, yetkisiz veri değiştirme işlemleri yapabilir veya başka kullanıcıların özel bilgilerini görebilirim. Ayrıca, kullanıcıların dosyalarına izinsiz erişebilir, onların adına işlem yapabilir ya da yetkileri olmayan kaynaklara erişerek uygulamanın işleyişini bozabilirim... Liste uzar gider.

Şimdi de bu açığı nasıl kapatabileceğimize bakalım:

1. **Her nesneye erişim yetkilendirilmelidir**. Kullanıcı, bir nesneye (örneğin, bir kullanıcı profili ya da dosya) erişmeye çalıştığında, bu kullanıcının gerçekten bu nesneye erişim hakkı olup olmadığı doğrulanmalıdır.
2. **Nesnelerin kimlik bilgilerini kullanıcıya göstermemek** ya da **kimlik bilgilerini tahmin edilemez hale getirmek** (örneğin UUID kullanarak), IDOR riskini azaltabilir. Bu sayede, kullanıcı ID'lerini veya dosya numaralarını değiştirerek başka nesnelere ulaşma olasılığı azaltılmış olur.
3. **Her kullanıcıya sadece kendi verileri üzerinde işlem yapma yetkisi verilmelidir**. Kullanıcılar, başkalarına ait verilere erişememeli veya bu veriler üzerinde değişiklik yapamamalıdır.

Bunlar çözümlerden sadece birkaçı. IDOR gibi zafiyetlerin önüne geçmek için güvenli kod geliştirme tekniklerine ve sıkı yetkilendirme kontrollerine odaklanarak bu riskleri büyük oranda azaltabiliriz.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar!