IDOR

4.0 Insecure Direct Object References (IDOR)

Nedir; IDOR zafiyeti, kullanıcıların yetkisiz bir şekilde sistemdeki nesnelere (örneğin, dosyalar, kullanıcı hesapları) doğrudan erişim sağlamasına olanak tanıyan bir güvenlik açığıdır.

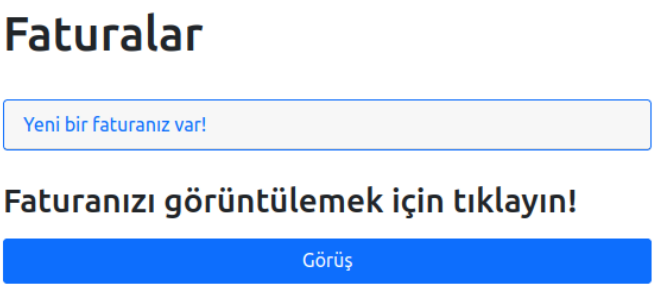
Nasıl Önlenir;Bu zafiyeti önlemek için, kullanıcıların erişim izinleri kontrol edilmeli ve nesne kimlikleri gizli tutulmalı; her bir erişim isteği için yetkilendirme ve doğrulama mekanizmaları uygulanmalıdır.

Sorunun bizden istediği ;

Emilia Rawne adlı müşterinin e-posta adresi nedir?

ÇÖZÜM

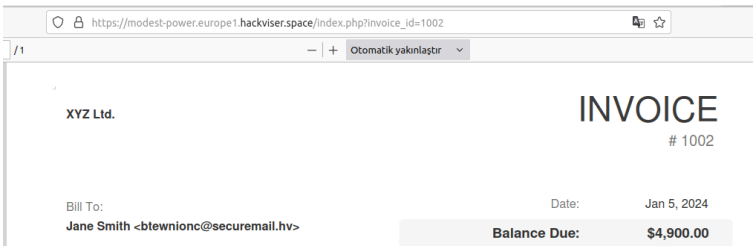
Ana sayfa bu şekilde ;



Görüş/View diyelim

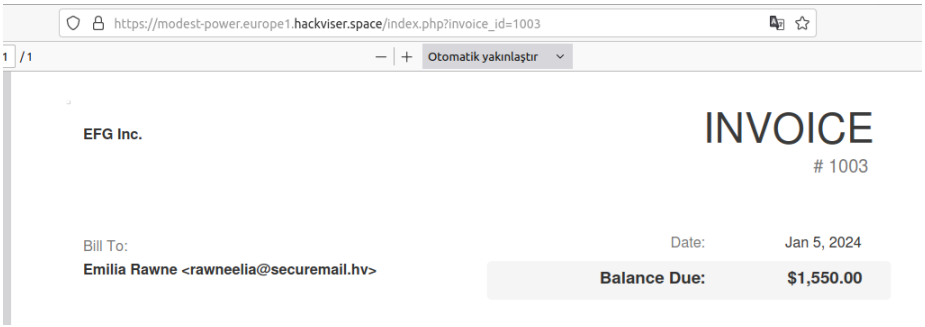
Bu bizim faturamızın url'i ve id'si

Bunu 1002 yapınca



başkasının faturası geliyor, ama istenilen kullanıcıya ulaşamadık henüz 1 daha attıralaım id değerini

Ve işte mail adresini bulduk.



Soru : Emilia Rawne adlı müşterinin e-posta adresi nedir?
Cevap : rawneelia@securemail.hv