**INVOICES WRİTE-UP**

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında IDOR zafiyetinin Invoices labının çözümünü anlatacağım.

**SENARYO:** Bu laboratuvar, uygulamadaki diğer müşterilerin faturalarına yetkisiz erişime izin veren bir Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

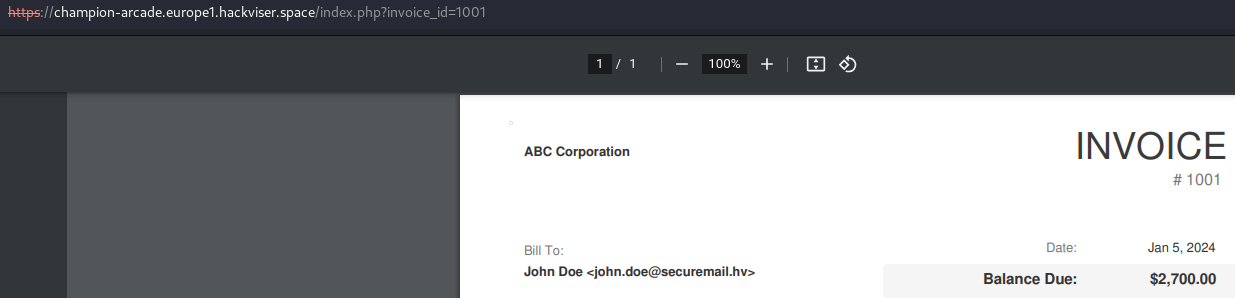
Laboratuvarı tamamlamak için URL'deki "invoice\_id" değerini değiştirerek diğer müşterilerin faturalarına erişin ve "Emilia Rawne" adlı müşterinin faturasını bulun.

Emilia Rawne adlı müşterinin e-posta adresi nedir?

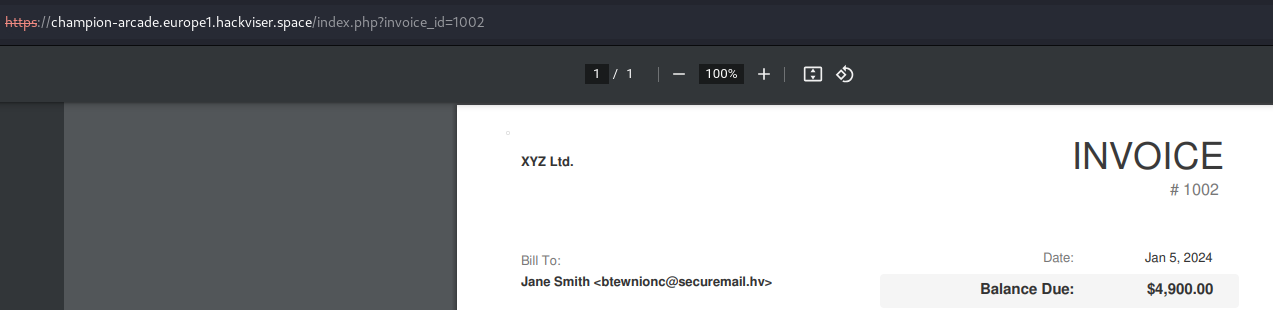
**ÇÖZÜM:**

*IDOR: Bu zafiyet URL üzerinde GET isteği ile gelen sayfaları manuel bir şekilde değiştirebildiğimiz güvenlik açığıdır.*

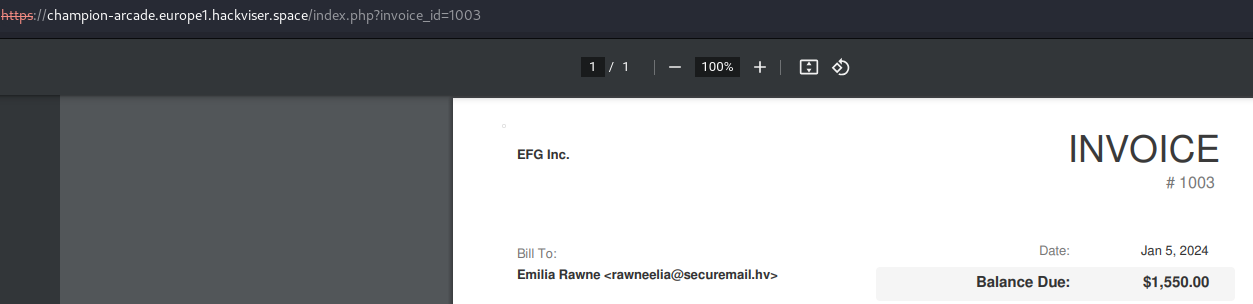
Siteye giriyoruz.



URL’de 1001 olan sayıyı değiştiriyoruz.



Başka bir kullanıcıya geçiş yaptı. Tekrardan değiştirelim.



Aradığımız kişiyi burada bulduk.

Cevap: **rawneelia@securemail.hv**