Hackviser Insecure Direct Object References (IDOR)

Invoices

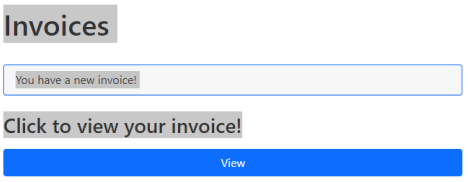
Başlangıçta bize lab hakkında bilgi vermiş

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.

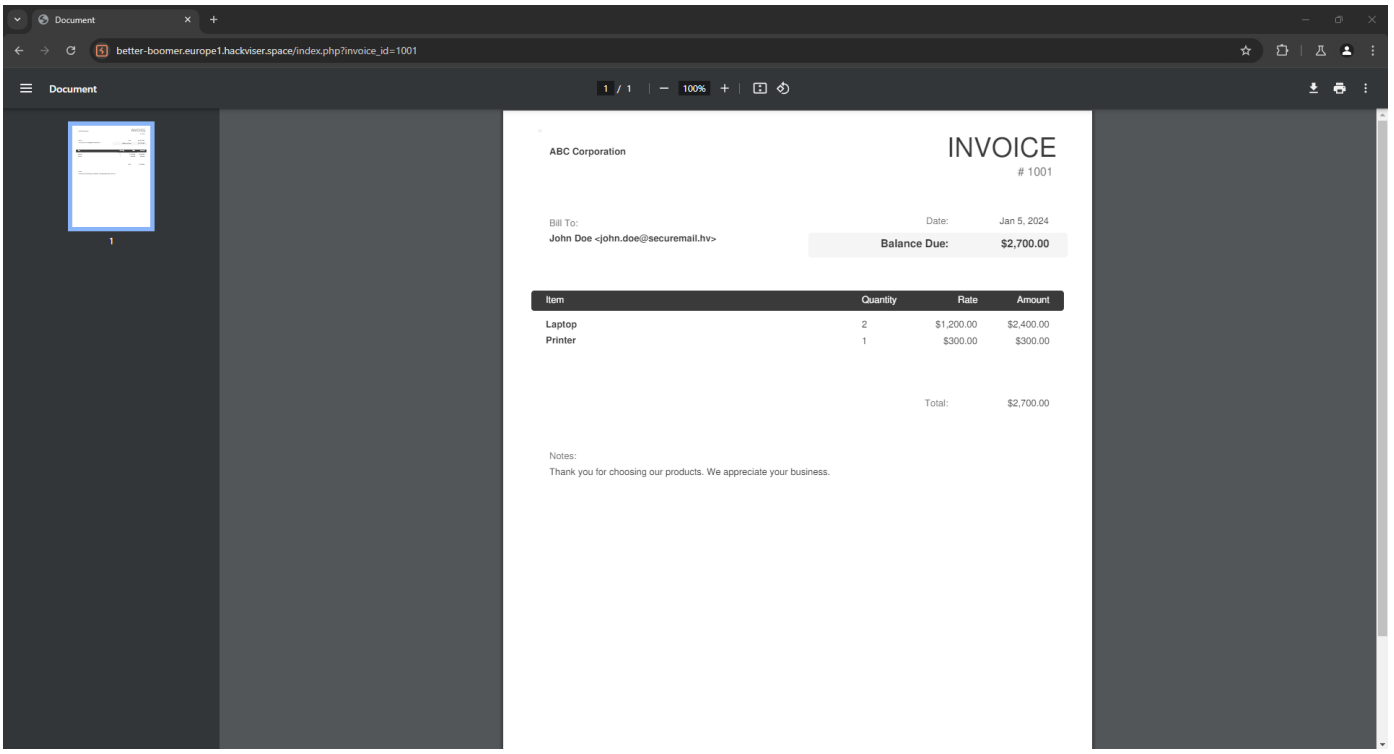
Emilia Rawne adlı müşterinin e-posta adresi nedir?

Öncelikle web sitesine gidelim

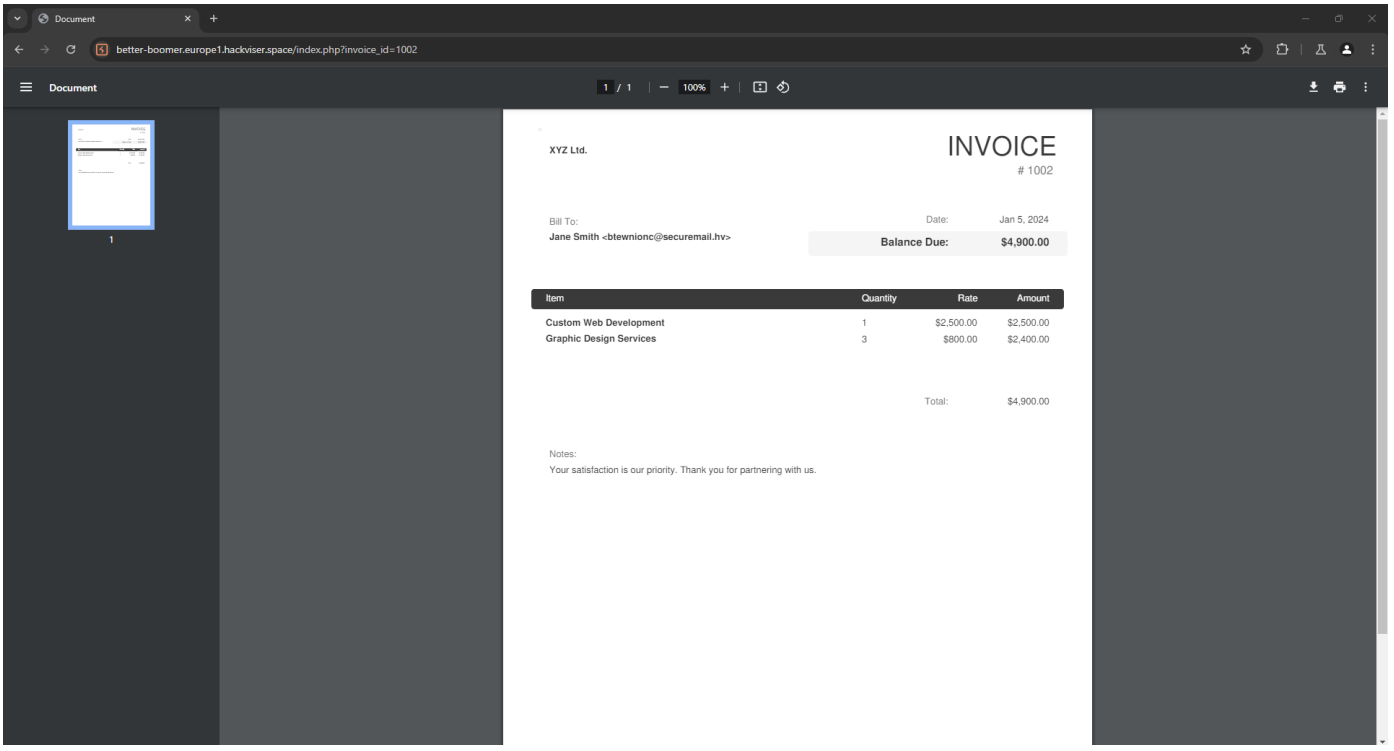


Faturalar
Yeni bir faturanız var!
Faturanızı görüntülemek için tıklayın!

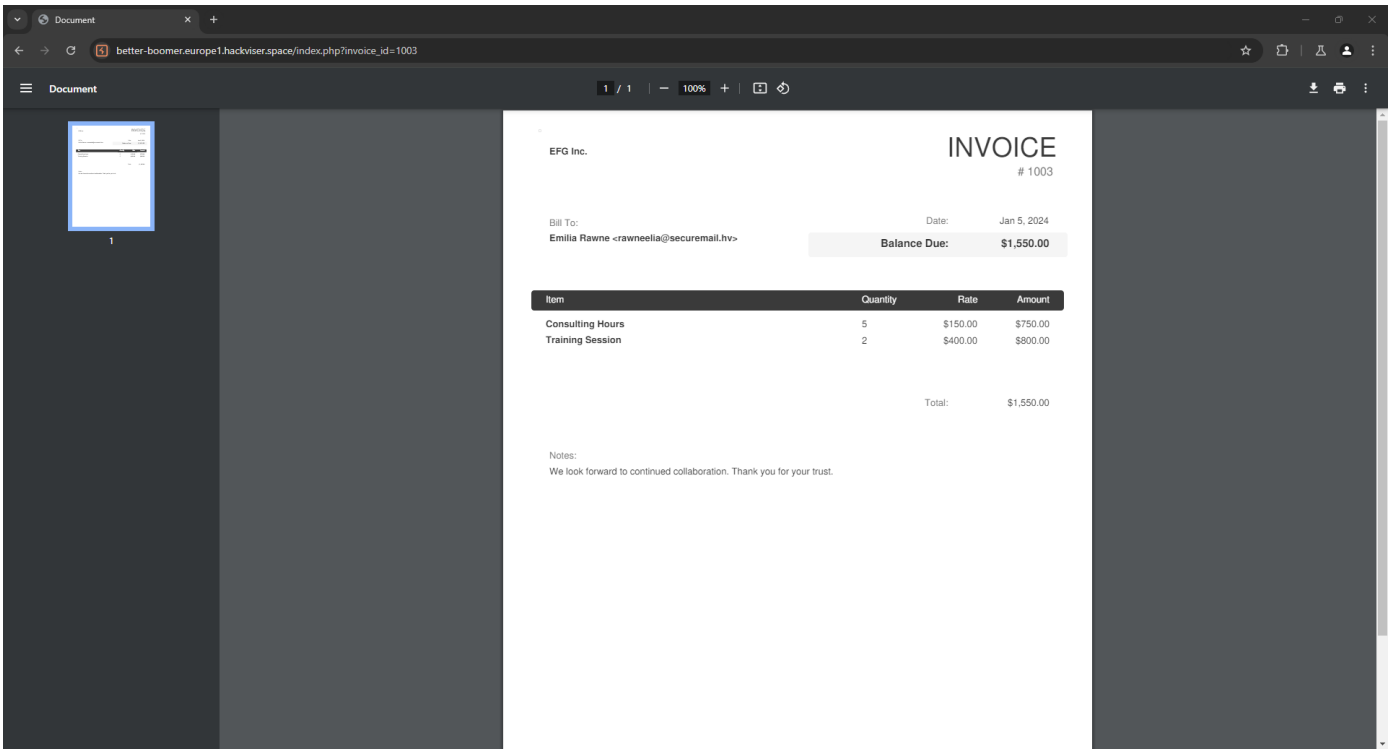
Görüntüleyelim



Görüntülediğimizde urlde invoice kısmı ilgimi çekiyor ve arttırmayı deniyorum



1002 yaptığımda Jane Smith adında bir kişinin e posta bilgilerine erişiyorum



1003 yaptığımda ise Emilia Rawne adlı müşterinin e-posta adresine ulaşmayı başarıyorum

---

Ticket Sales

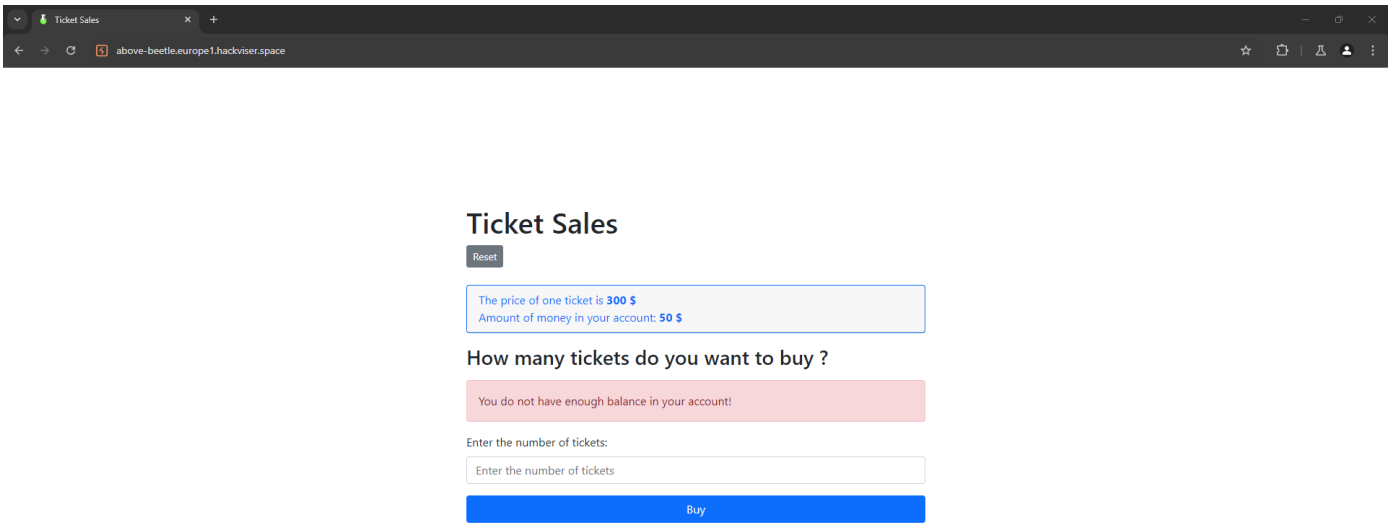
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, bir ürünün daha düşük bir fiyata satın alınabilmesine neden olan bir Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

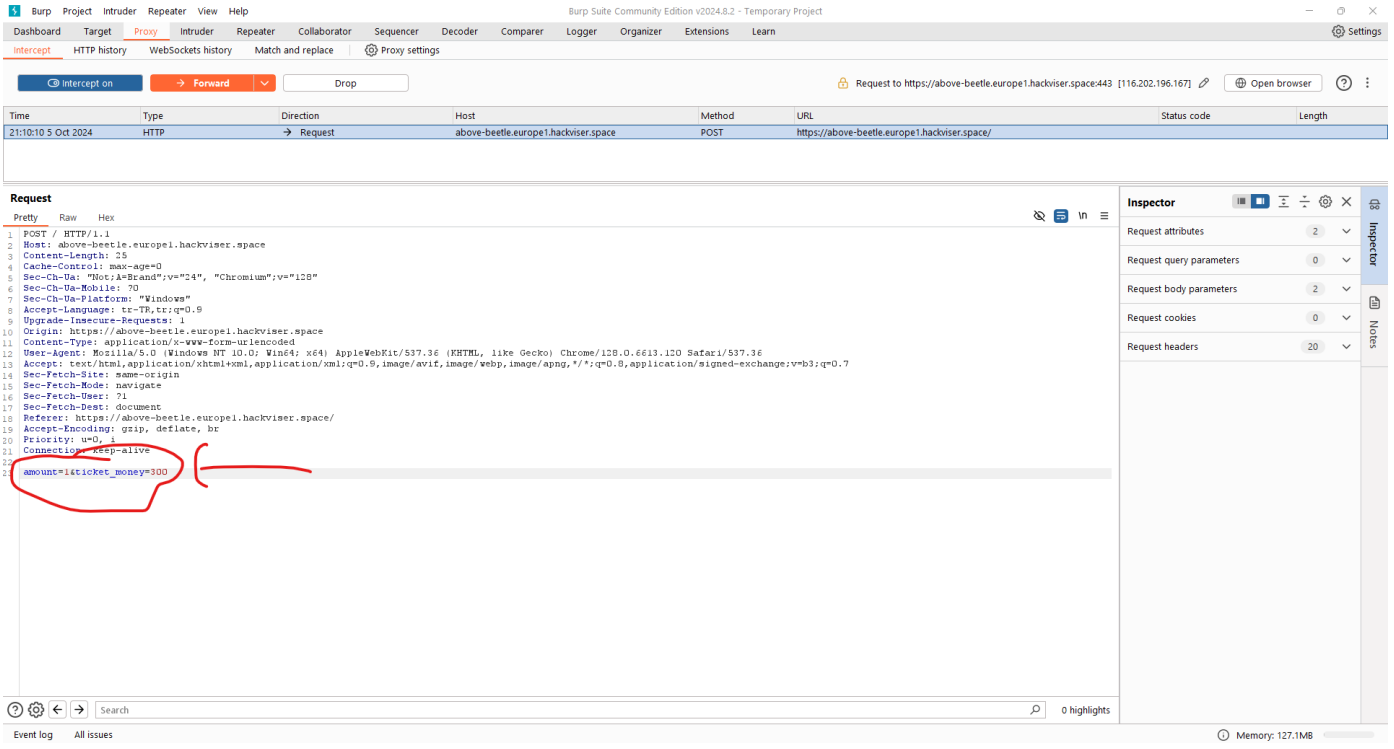
Başlangıç bakiyeniz bilet satın almak için yeterli değildir. Laboratuvarı tamamlamak için bilet satın alımı esnasında sunucuya gönderilen fiyatı manipüle ederek bilet satın alın.

Bilet satın alındıktan sonra görünen sipariş numarası nedir?

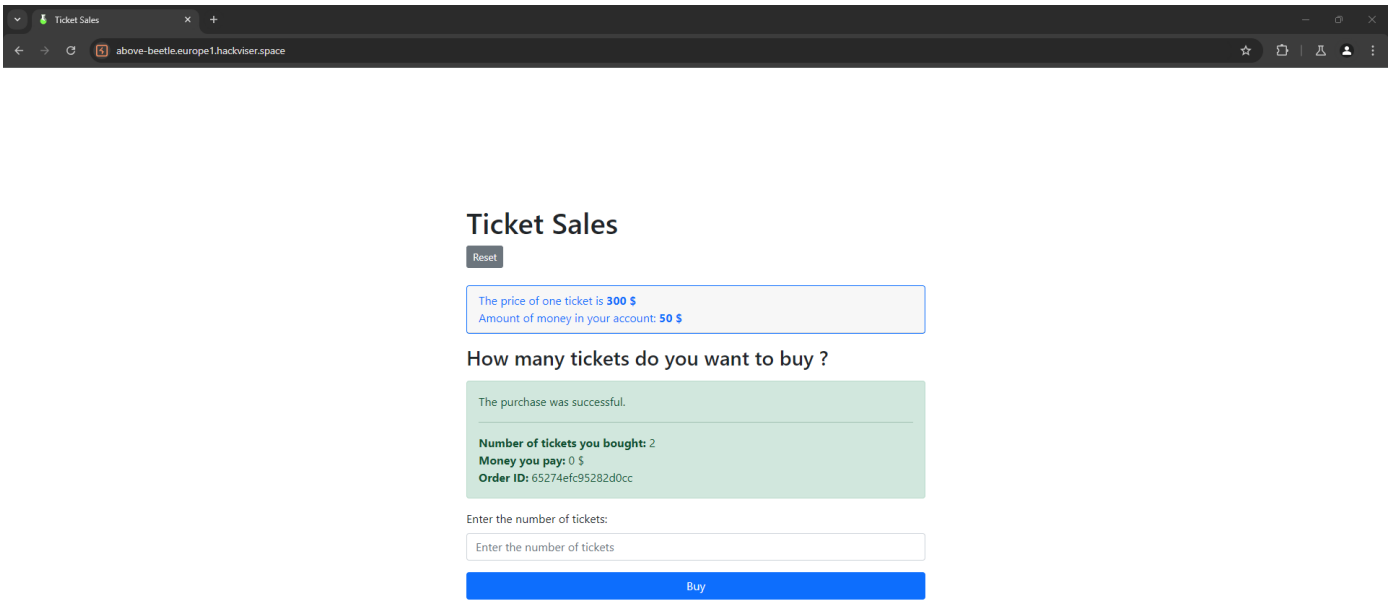
Öncelikle web sitesine gidelim



50 dolar bakiyemiz var bilet almak için 300 dolara ihtiyacımız varmış. Satın al dedikten sonra burp ile araya girerek IDOR zafiyetini uygulamaya çalışabiliriz



Burp ile araya girdiğimizde bilet adetini ve fiyatını görebiliyoruz. Fiyatı 0 Bilet sayısınıda 2 yapmayı deneyebiliriz.



Ve evet sipariş numarasını görüntülemeyi başardık.

Change Password

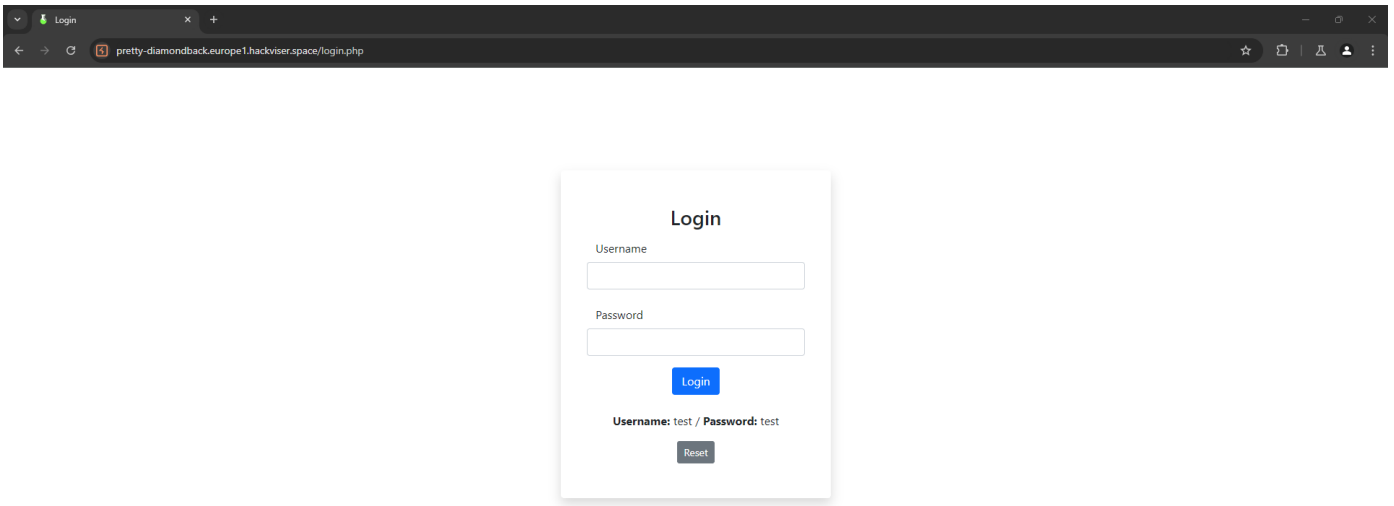
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, diğer kullanıcıların parolasını yetkisiz bir şekilde değiştirmeye yol açan Güvensiz Doğrudan Nesne Referansları (IDOR) güvenlik açığı içerir.

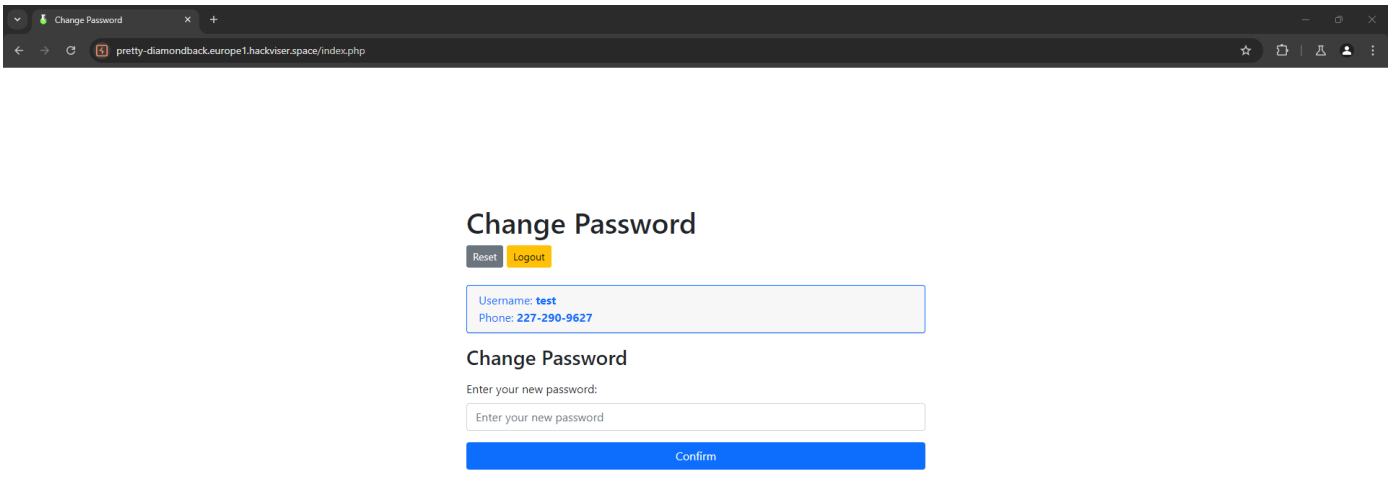
Laboratuvarı tamamlamak için "admin" kullanıcısının parolasını, parola değiştirme uç noktasındaki IDOR zafiyetini istismar ederek değiştirin ve hesabına giriş yapın.

"admin" isimli kullanıcının telefon numarası nedir? (Cevap Formatı: 000-000-0000)

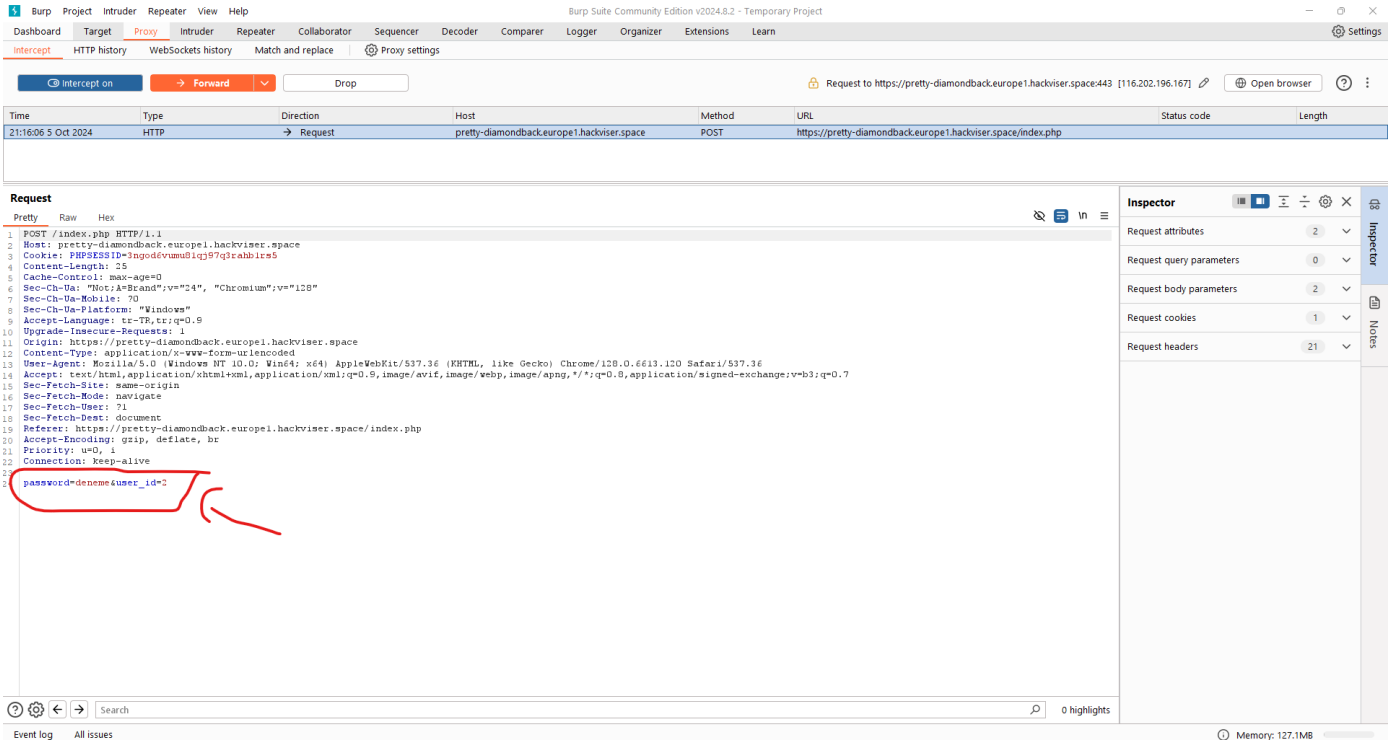
Öncelikle web sitesini ziyaret edelim



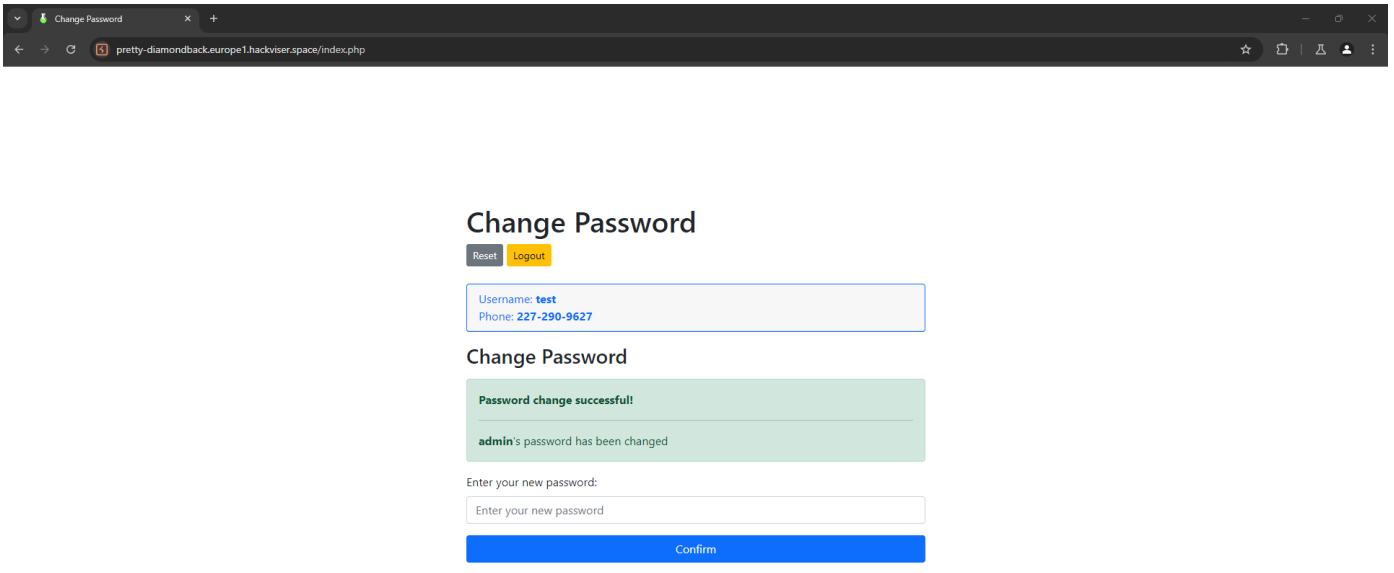
test / test yazarak giriş yapalım



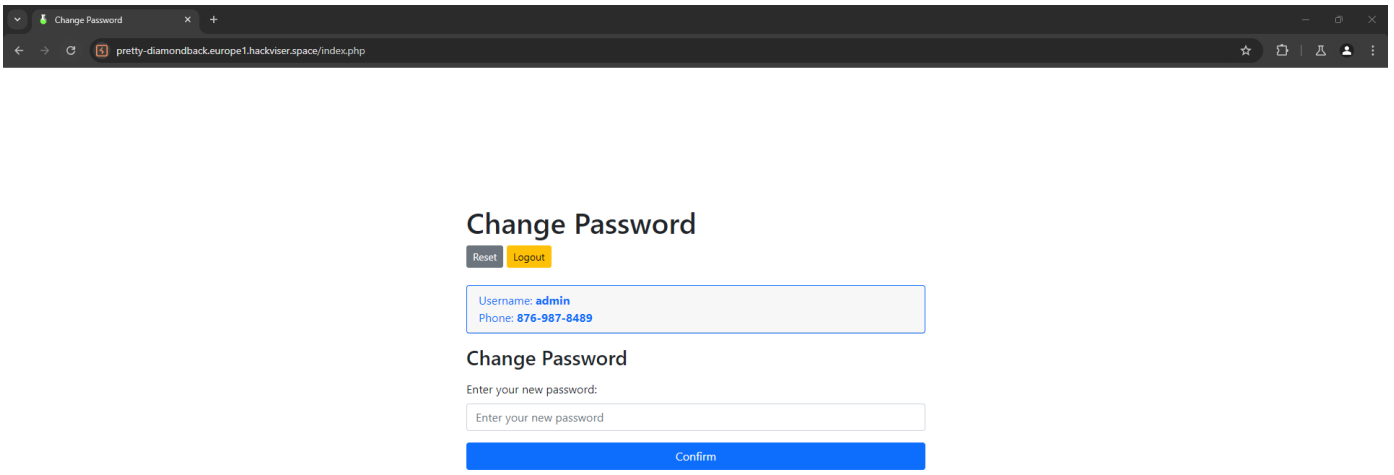
Bi parola değiştirme ekranımız var. Şifremizi değiştirelim değiştirirkende burp ile araya girelim



Evet değiştirmek istediğimiz şifreyi ve user_id yi görüyoruz user id miz 2 olarak verilmiş genellikle user id si 1 olan kullanıcı admindir site kurulduğu gibi açılan ilk hesap onun olduğu için ondan dolayı şimdi şifreyi deneme yapıp user id yide 1 olarak vereceğim ve admin hesabına admin / deneme olarak giriş yapmayı deneyeceğim



Evet adminin parolasının değiştiğini görüyoruz. Şimdi gidip giriş yapalım



Ve evet adminin hesabına giriş yaparak telefon numarasını görüntülemeyi başardık.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş