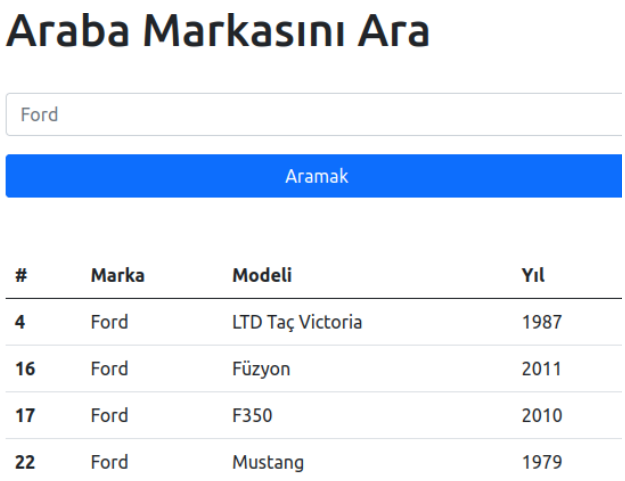
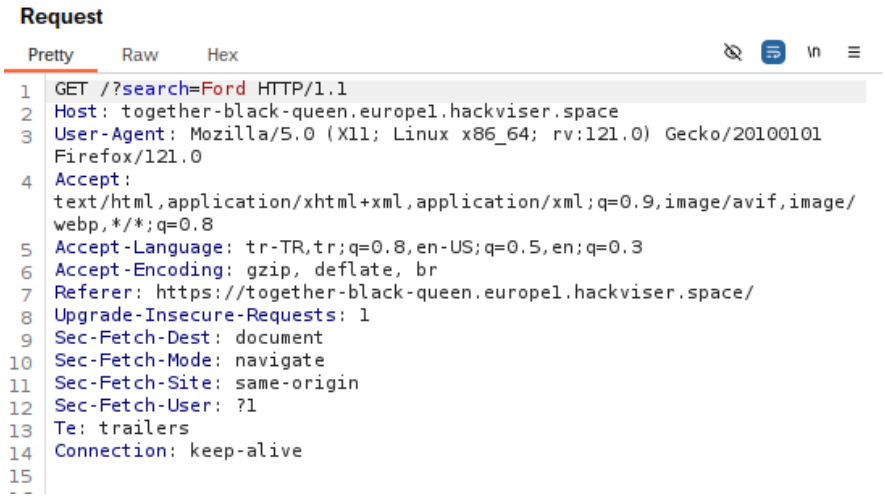
SQL INJECTİON

2.1 Union-Based SQL;

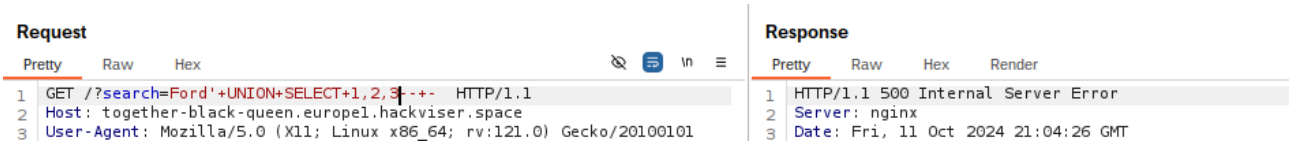
Bu SQL zafiyeti türümüz UNION tabanlı bir zafiyet, yazdığımız sorgu sonucunu ekrana bastırabiliyoruz ve asıl önemlisi sorgu birleştiriyoruz mesala, database adını ekrana yazdırabiliriz. Tam olarak bizden istenen de bu, web sayfasına bir göz atalım.



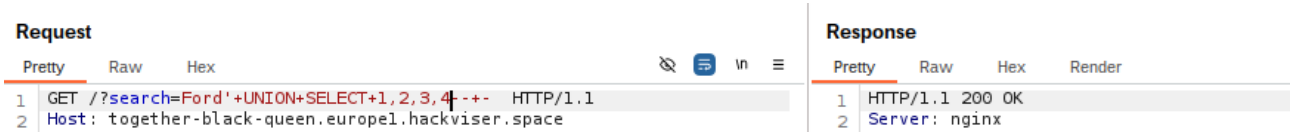
Galiba bir Galerici'e ait olan bir web sayfası.Araba markaları arıyabiliyoruz % ile filtreleme kullanılmış. Bu şekilde veritabanından verileri getiriyor.
Burada biraz deneme yanılma yapıp veritabanı ismini tespit edeceğimiz için, ben Burp Suite kullanmayı tercih ediyorum.
İntercept'imi açık search= değişkenine yani arama alanına bir araba markası aratıyorum Ford. Ve isteği yakalıyorum. Ve Repeater alanına atıyorum.



Burada Ford bizim verdiğimiz string değeri. Denemeleri burada gerçekleştiricem sağ sekmede giden isteklerin cevaplarını görebileceğimiz bir alan var.



Burada ki sorgu mantığımız ise UNION İle arkada dönen sorguyla bizim yazdığımız sorguyu, birleştiriyoruz.
Ve databasenin 3 adet columu var dedim. Ancak 500 Inernal Server hatası aldık, demek ki 3 tane değil bunu 1 den başlayıp sayıyı 1+ arttıra arttıra sonuca ulaşmaya çalışılır. Bakalım biz kaçıncıda 200 durum kodu alıcaz.Ve sonda ki – yorum satırına almak demek, bu veritabanı sql dilinden dolayı değişiklik gösterebiliyor. -- 2 TANE tek çizgiden sonra bir adet – tek çizgi var bu da güvenlik duvarından kaçmak içindir.



Evet 4 adet column varmış veritabanı'nın şimdi ise veritabanı'nın ismini öğrenmekte. Ama istersek sizlere response de ne gözüküyor onu göstermek isterim.

Araba ilanın isimlerinin yazdığı kısımda bizim columlar sayı ismiyle belirlendi.
Aslında yaptığımız yöntem bir nevi yanlış, biz çünkü int değer ile bulmaya çalıştık, NULL ifadesiyle araştırmak daha doğru, çünkü colmn adı stringmi int mi bilmiyoruz veya 2 si bir arada mı?
Şimdi veritabanı adını öğrenelim ek olarak versiyon bilgisi de öğrenelim.
Bunları öğrenmek için sayıların yerine
veritabanı adı için : database()
versiyon için : version() | Cevabımızı öğrenelim ;
Versiyon bilgimiz : 8.0.35
CEVAP: ecliptica_cars

```
    <td>
      2002
    </td>
  </tr>
  <tr>
    <th scope="row">
      1
    </th>
    <td>
      ecliptica_cars
    </td>
    <td>
      8.0.35
    </td>
    <td>
      4
    </td>
  </tr>
```

CEVAP:
Versiyon

ecliptica_cars
bilgimiz’de 8.0.35