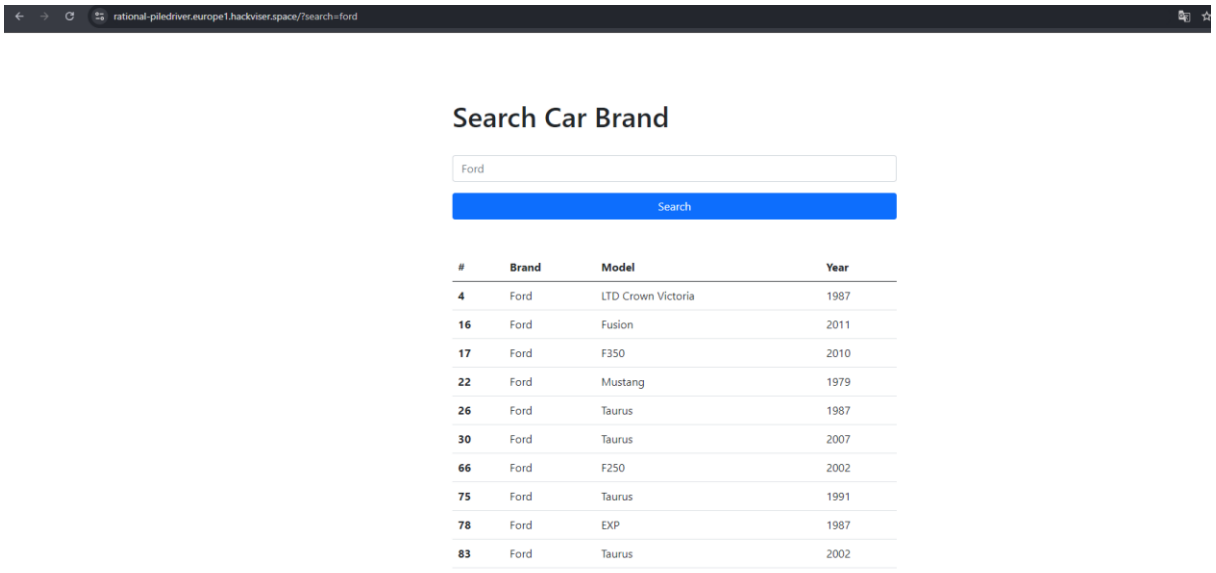
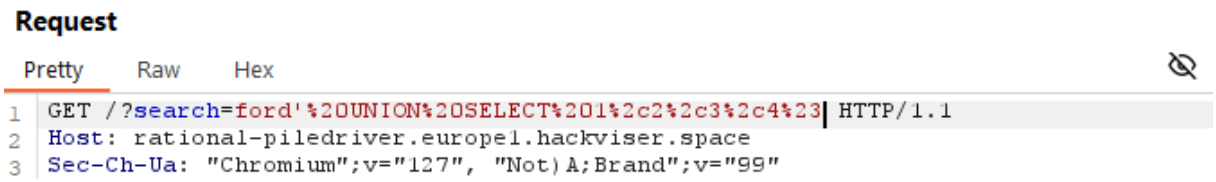
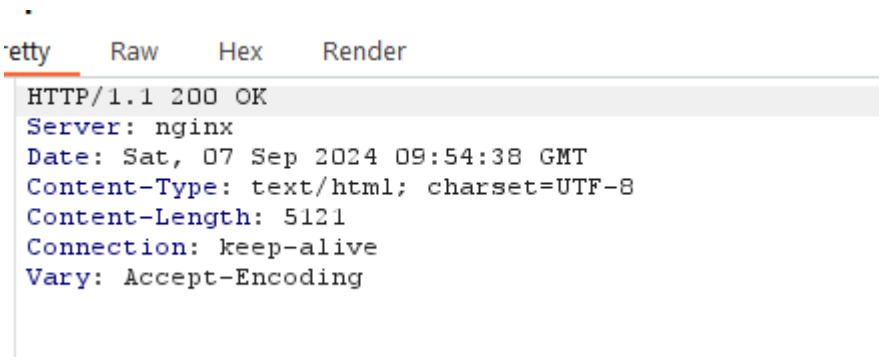
Union Based

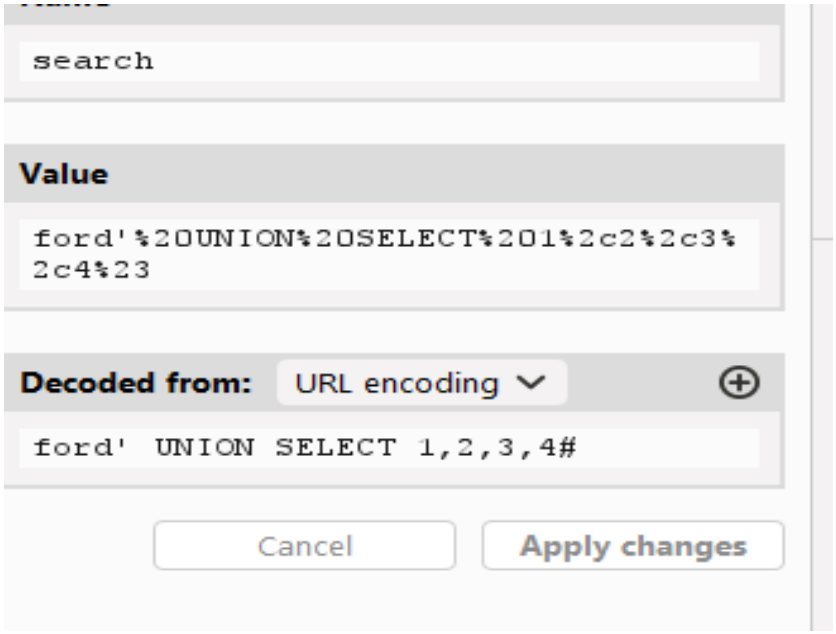
İkinci zafiyeti union based sql injection olarak seçtim. Zafiyet bir injection zafiyetiydi ve görevim kullanılan database ismini bulmaktı. İlk olarak siteye gidip biraz araştırma yapıyorum.



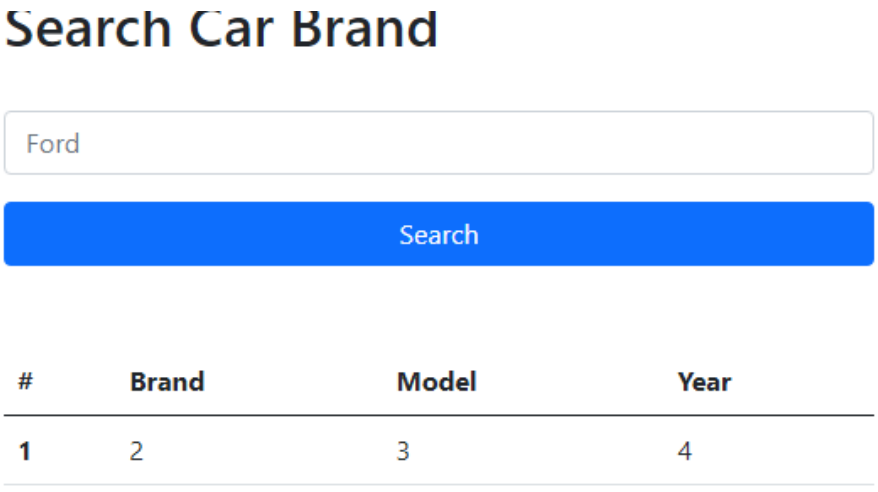
Resimde görüldüğü gibi arabaları filtreleyebileceğimiz bir site var burada. Burb ile araya girip biraz inceliyorum. Search bölümüne union based ile sırayla denemeler yapıyorum. 4. Denememde 200 döndüğünü gördüğümde sayıları arttırmayı bırakıyoruym.





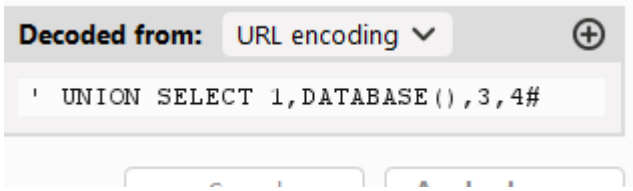


Ford yazısını da silince Render da eklenen verilerimizi görebiliyoruz.



Artık database ismini öğrenmeye geldi. İlk etapta sütunların sadece intager bir değer mi yoksa string de kabul edip etmediğini denemek için ‘a’, ‘b’ gibi karakterler denedim. Hepsiyle uyumluydu. Aklıma ilk gelen kodu **DB_NAME()** yazdım ama sonuç başarısız döndü. Biraz araştırmayla beraber farklı sql dillerinin farklı sorgularını öğrendim. **DATABASE()** ve **current_database()** olabileceğini öğrendim.

DATABASE() komutumu yerleştirerek çalıştırdım ve Database ismini alabildim.



#	Brand	Model	Year
1	ecliptica_cars	3	4